Achieving Path Diversity over the Internet using MDS Codes

Shervan Fashandi, Shahab Oveis Gharan and Amir K. Khandani

Electrical and Computer Engineering Department
University of Waterloo, Waterloo, ON, Canada
Email:{sfashand,shahab, khandani}@cst.uwaterloo.ca

Technical Report UW-E&CE#2007-38

Dec 19, 2007

Achieving Path Diversity over the Internet using MDS Codes

Shervan Fashandi, Shahab Oveis Gharan and Amir K. Khandani
ECE Dept., University of Waterloo, Waterloo, ON, Canada, N2L3G1
email: {sfashand,shahab,khandani}@cst.uwaterloo.ca

Abstract

Path diversity works by setting up multiple parallel connections between the end points using the topological path redundancy of the network. In this paper, *Forward Error Correction* (FEC) is applied across multiple independent paths to enhance the end-to-end reliability. Internet paths are modeled as erasure Gilbert-Elliot channels [1], [2]. First, it is shown that over any erasure channel, *Maximum Distance Separable* (MDS) codes achieve the minimum probability of irrecoverable loss among all block codes of the same size. Then, based on the adopted model for Internet paths, we prove that the probability of irrecoverable loss for MDS codes decays exponentially for the asymptotically large number of paths. Moreover, it is shown that in the optimal rate allocation, each path is assigned a positive rate *iff* its quality is above a certain threshold. The quality of a path is defined as the percentage of the time it spends in the bad state. In other words, including a redundant path improves the reliability *iff* this condition is satisfied. Finally, using dynamic programming, a heuristic suboptimal algorithm with polynomial runtime is proposed for rate allocation over the available paths. This algorithm converges to the asymptotically optimal rate allocation when the number of paths is large. The simulation results show that the proposed algorithm approximates the optimal rate allocation very closely for the practical number of paths, and provides significant performance improvement compared to the alternative schemes of rate allocation.[1]

I. Introduction

In recent years, *path diversity* over the Internet has received significant attention. It has been shown that path diversity has the ability to simultaneously improve the end-to-end rate and reliability [3]–[5]. In a dense network like the Internet, it is usually possible to find multiple disjoint paths between any pair of nodes [6]. In this paper, *Forward Error Correction* (FEC) is applied across multiple disjoint paths. Knowing that packet loss and delay patterns are independent over such paths, we expect path diversity to enhance the performance of FEC.

References [7] and [8] have proposed both centralized and distributed algorithms to find multiple independent paths over a large connected graph. Although the distributed algorithms do not require the end nodes to know the entire topology of the network, they impose some modifications on the intermediate nodes. Indeed, modification of the routing protocol and the signaling between the nodes is extremely costly over the traditional IP networks. To avoid such an expense, overlay networks are introduced [9]. The basic idea of overlay networks is to equip very few nodes (smart nodes) with the desired new functionalities while the rest remain unchanged. The smart nodes form a virtual network connected through virtual or logical links on top of the actual network. Thus, the overlay networks can be used to set up disjoint paths between the end nodes. Reference [10]

[1]Financial support provided by Nortel and the corresponding matching funds by the Natural Sciences and Engineering Research Council of Canada (NSERC), and Ontario Centres of Excellence (OCE) are gratefully acknowledged.

addresses the problem of overlay network design based on a game theoretical approach. Also, reference [6] has experimentally studied the number of available disjoint paths in the Internet using overlay networks.

Recently, path diversity is utilized in many applications (see [2], [11], [12]). Reference [12] combines multiple description coding and path diversity to improve quality of service (QoS) in video streaming. Packet scheduling over multiple paths is addressed in [13] to optimize the rate-distortion function of a video stream. In [3], multipath routing of TCP packets is applied to control the congestion with minimum signaling overhead.

Moreover, references [5] and [4] study the problem of rate allocation over multiple paths. Assuming each path follows the leaky bucket model, reference [5] shows that a water-filling based scheme provides the minimum end-to-end delay. On the other hand, reference [4] considers a scenario of multiple senders and a single receiver, assuming all the senders share the same source of data. The connection between each sender and the receiver is assumed to follow the Gilbert-Elliot model. They propose a receiver-driven protocol for packet partitioning and rate allocation. The packet partitioning algorithm ensures no sender sends the same packet, while the rate allocation algorithm minimizes the probability of irrecoverable loss in the FEC scheme [4]. They only address the path allocation problem for the case of two paths. A brute-force search algorithm is proposed in [4] to solve the problem. Generalization of this algorithm over multiple paths results in an exponential complexity in terms of the number of paths. Moreover, it should be noted that the scenario of [4] is equivalent, without any loss of generality, to the case in which multiple independent paths connect a pair of end-nodes as they assume the senders share the same data.

Maximum Distance Separable (MDS) codes have been shown to be optimum in the sense that they achieve the maximum possible minimum distance (d_{min}) among all the block codes of the same size [14]. Indeed, any $[n, k]$ MDS code with block length n and k symbols of informatoin can be successfully recovered from any subset of its entries of length k or more. This property makes MDS codes favorable FEC schemes over the erasure channels like the Internet [15]–[17]. However, the simple and practical encoding-decoding algorithms for such codes have quadratic time complexity in terms of the code size [18]. Theoretically, more efficient ($O\left(n \log^2(n)\right)$) MDS codes can be constructed based on evaluating and interpolating polynomials over specially chosen finite fields using Discrete Fourier Transform [19], but these methods are not competitive in practice with the simpler quadratic methods except for extremely large block sizes. Recently, a family of almost-MDS codes with low encoding-decoding time complexity (linear in term of the code length) is proposed and shown to be practical over the erasure channels like the Internet [20], [21]. In these codes, any subset of symbols of size $k(1+\epsilon)$ is sufficient to recover the original k symbols with high probability [21].

MDS codes also require alphabets of a large size. Indeed, all the known MDS codes have alphabet sizes growing at least linearly with the block length n. There is a conjecture stating that all the $[n, k]$ MDS codes over the Galois field $\mathbb{F}(q)$ with $1 < k < n-1$ have the property that $n \leq q+1$ with two exceptions [14]. However, this is not an issue in the practical networking applications since the alphabet size is $q = 2^r$ where r is the packet size, i.e. the block size is much smaller than the alphabet size. Algebraic computation over Galois fields ($\mathbb{F}(q)$) of such cardinalities is now practically possible with the increasing processing power of electronic circuits. For instance, the novel practical network coding schemes proposed and applied for content distribution over large networks require the same degree of computational complexity [22]–[24].

In this work, we utilize path diversity to improve the performance of FEC. The details of path setup process is not discussed here. It is just assumed that L independent paths are set up by a smart overlay network or any other means [9], [10]. Probability of irrecoverable loss (P_E) is defined as the measure of FEC performance. First, it is shown that MDS block codes have the minimum probability of error over our *Internet Channel* model, and over any other erasure channel with or without memory. Applying MDS codes in FEC, our analysis shows an exponential decay of P_E with respect to the number of paths. Of course,

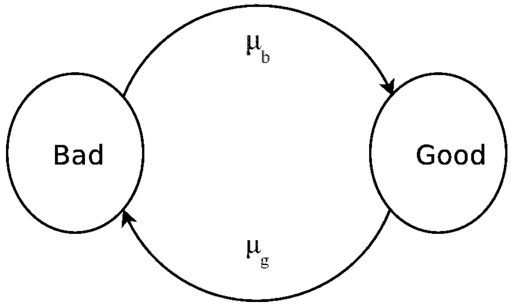


Fig. 1. Continuous-time two-state Markov model of an Internet channel

in many practical cases, the number of *independent* or *disjoint* paths between the end nodes is limitted. However, in our asymptotic analysis, we have assumed that it is possible to find L independent paths between the end points even when L is large. Moreover, the optimal rate allocation problem is solved in the asymptotic case where the number of paths is large. It is seen that in the optimal rate allocation, each path is assigned a positive rate *iff* its quality is above a certain threshold. Modeling each path with a two-state continuous time markov process called Gilbert-Elliot channel [1], [2], the quality of a path is defined as the percentage of the time it spends in the bad state. Furthermore, using dynamic programming, a heuristic suboptimal algorithm is proposed for rate allocation over the available paths. Unlike the brute-force search, this algorithm has a polynomial complexity, in terms of the number of paths. It is shown that the result of this algorithm converges to the asymptotically optimal solution for large number of paths. Finally, the simulation results verify the near-optimal performance of the proposed algorithm for practical number of paths.

The rest of this paper is organized as follows. Section II describes the system model. Probability distribution of the bad burst duration is discussed in section III. Performance of FEC in three cases of a single path, multiple identical paths, and non-identical paths are analyzed in section IV. Section V studies the rate allocation problem, and proposes a suboptimal rate allocation algorithm. Finally, section VI concludes the paper.

II. System Modeling and Formulation

A. Internet Channel Model

From an end to end protocol's perspective, performance of the lower layers in the protocol stack can be modeled as a random *channel* called an *Internet channel*. Since each packet usually includes an internal error detection coding (for instance a CRC), the Internet channel is satisfactorily modeled as an erasure channel. Although there is no well defined capacity limit for the Internet channel, a maximum TCP-friendly rate is introduced in [25]. Delay of an Internet channel is strongly correlated with the packet loss pattern, and affects the QoS considerably [26], [27].

In this work, the model assumed for the Internet channel is a two-state Markov model called Gilbert-Elliot cell, depicted in Fig. 1. The channel spends an exponentially distributed random amount of time with the mean $\frac{1}{\mu_g}$ in the *Good* state. Then, it alternates to the *Bad* state and stays in that state for another random duration exponentially distributed with the mean $\frac{1}{\mu_b}$. It is assumed that the channel state does not change during the transmission of one packet [2]. Hence, if a packet is transmitted from the source at anytime during the good state, it will be received correctly. Otherwise, if it is transmitted during the bad state, it will eventually be lost before reaching the destination. Therefore, the average probability of error is equal to the steady state probability of being in the bad state $\pi_b = \frac{\mu_g}{\mu_g+\mu_b}$. To have a reasonably low probability of error, μ_g must be much smaller than μ_b. This model is widely used for theoretical analysis where delay is not a significant factor [1]. Despite its simplicity, this

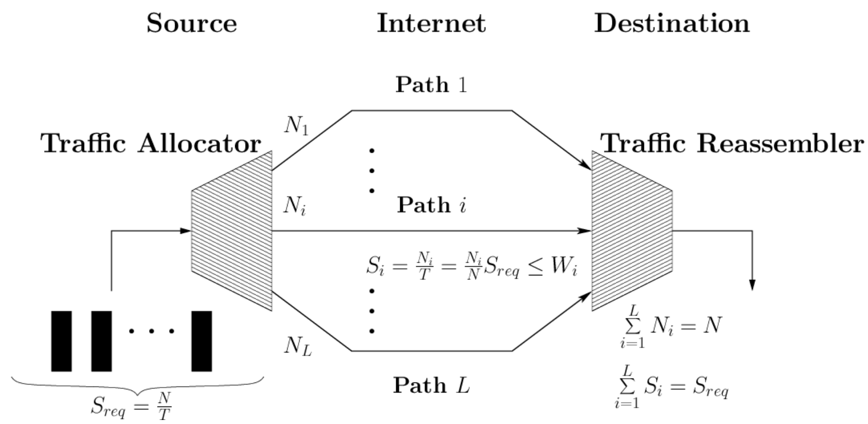


Fig. 2. Rate allocation problem: a block of N packets is being sent from the source to the destination through L independent paths over the Internet during the time Interval T with the required rate $S_{req} = \dfrac{N}{T}$. The block is distributed over the paths according to the vector $\mathbf{N} = (N_1, \ldots, N_L)$ which corresponds to the rate allocation vector $\mathbf{S}$

model captures the bursty error characteristic of Internet channels satisfactorily. More comprehensive models like the hidden Markov model are introduced in [27]. Although analytically cumbersome, such models express the correlation of loss and delay more accurately.

B. Typical FEC Model

A concatenated coding is used for packet transmission. The coding inside each packet can be a simple CRC which enables the receiver to detect an error inside each packet. Then, the receiver can consider the Internet channel as an erasure channel. Other than the coding inside each packet, a *Forward Error Correction* (FEC) scheme is applied between packets. Every K packets are encoded to a *Block* of N packets where $N > K$ to create some redundancy. The ratio of $\alpha = \frac{N-K}{N}$ defines the FEC overhead. A *Maximum Distance Separable* (MDS) (N, K) code, such as Reed-Solomon code, can reconstruct the original K data packets on the receiver side if K or more of the N packets are received correctly [14]. According to the following theorem, a MDS code is the optimum block code we can design over any erasure channel. Although FEC imposes some bandwidth overhead, it might be the only option when feedback and retransmission are not feasible or fast enough to provide the desirable QoS.

Theorem I. An erasure channel is defined as the one which maps every input symbol to either itself or to an erasure symbol ξ. Consider an arbitrary erasure channel (memoryless or with memory) with the input vector $\mathbf{x} \in \mathcal{X}^N$, $|\mathcal{X}| = q$, the output vector $\mathbf{y} \in (\mathcal{X} \cup \{\xi\})^N$, and the transition probability $p(\mathbf{y}|\mathbf{x})$ satisfying:

1) $p(y_j \notin \{x_j, \xi\} | x_j) = 0, \ \forall \ j.$
2) Defining the erasure identifier vector $\mathbf{e}$ where

$$e_j = \begin{cases} 1 & y_j = \xi \\ 0 & \text{otherwise} \end{cases}$$

   $p(\mathbf{e}|\mathbf{x})$ is independent of $\mathbf{x}$.

A block code (N, K) with equiprobable codewords over this channel has the minimum probability of error using the optimum (maximum likelihood) decoder among all block codes of the same size *iff* that code is *Maximum Distance Separable* (MDS). The proof can be found in the appendix A.

C. Rate Allocation Problem

The network is modeled as follows. L independent paths, $1, 2, \ldots, L$, connect the source to the destination, as indicated in Fig. 2. Information bits are transmitted as packets each of constant length r. Furthermore, there is a constraint on the maximum rate for each path meaning that the i'th can provide the maximum rate of W_i packets per second. This constraint can be considered as an upperbound imposed by the physical characteristics of the path. As an example, [25] introduces the concept of the *maximum TCP-friendly bandwidth* for the maximum capacity of a network path. W_i's are assumed to be known at the transmitter side. For a specific application and FEC scheme, we require the rate S_{req} from source to the destination. Obviously, we should have $S_{req} \leq \sum_{i=1}^{L} W_i$ to have a feasible solution. The information bits are assumed to be coded in blocks of length N packets. Hence, it takes $T = \frac{N}{S_{req}}$ to transmit a block of packets. According to the FEC model, we can send N_i packets through the path i as long as $\sum_{i=1}^{L} N_i = N$ and $\frac{N_i}{T} \leq W_i$. Then, the rate assigned to path i can be expressed as $S_i = \frac{N_i}{T} = \frac{N_i}{N} S_{req}$. Obviously, we have $\sum_{i=1}^{L} S_i = S_{req}$. The objective of the rate allocation problem is to find the optimal rate allocation vector or the vector $\mathbf{N} = (N_1, \cdots, N_L)$ which minimizes the probability of irrecoverable loss (P_E).

The above formulation of rate allocation problem is valid for any value of N and L. However, in section IV where the performance of path diversity for large number of paths is studied and also in Theorem III where the optimality of the proposed suboptimal algorithm is proved for the asymptotic case, we assume that N grows linearly in terms of the number of paths, i.e. $N = n_0 L$. At the same time, it is assumed that the delay imposed by FEC, T, stays fixed with respect to L. This model results in a linearly increasing rate as the number of paths grows. We will later show that utilizaing multiple paths, it is possible to simultaneously achieve an exponential decay in P_E and a linear growth in rate while the delay stays constant.

In this work, an irrecoverable loss is defined as the event where more than $N - K$ packets are lost in a block of N packets. P_E denotes the probability of this event. It should be noted that this probability is different from the decoding error probability of a maximum likelihood decoder performed on an MDS (N, K) code, denoted by $\mathbb{P}\{\mathcal{E}\}$. Theoretically, an optimum maximum likelihood decoder of a MDS code may still decode the original codeword correctly with a positive but very small probability if it receives less than K symbols (packets). More precisely, such a decoder is able to correctly decode a MDS code over $\mathbb{F}_q$ with the probability of $\frac{1}{q^i}$ after receiving $K - i$ correct symbols (see the proof of Theorem I in the appendix for more details). Of course, for Galois fields with large cardinality, this probability is usually negligible. The relationship between P_E and $\mathbb{P}\{\mathcal{E}\}$ can be summarized as follows

$$\begin{aligned} \mathbb{P}\{\mathcal{E}\} &= P_E - \sum_{i=1}^{K} \frac{\mathbb{P}\{K - i \text{ Packets received correctly}\}}{q^i} \qquad (1) \\ &\geq P_E - \frac{1}{q} \sum_{i=1}^{K} \mathbb{P}\{K - i \text{ Packets received correctly}\} \\ &= P_E \left(1 - \frac{1}{q}\right). \end{aligned}$$

Hence, $\mathbb{P}\{\mathcal{E}\}$ is bounded as

$$P_E \left(1 - \frac{1}{q}\right) \leq \mathbb{P}\{\mathcal{E}\} \leq P_E. \qquad (2)$$

The reason P_E is used as the measure of system performance is that while many practical low-complexity decoders of MDS codebooks work perfectly if the number of correctly received symbols is at least K, their probability of correct decoding is much less than that of maximum likelihood decoders when the number of correctly received symbols is less than K. Thus, in the rest of this paper, P_E is used as a close approximation of decoding error.

III. Probability Distribution of Bad Bursts

The continuous random variable B_i is defined as the duration of time that the path i spends in the bad state in a block duration, T. We denote the values of B_i with parameter t to emphasize that they are expressed in the time unit. In this section, we focus on one path, for example path 1. Therefore, the index i can be temporarily dropped in analyzing the probability distribution function (pdf) of B_i.

We define the events g and b, respectively as the channel being in the good or bad states at the start of a block. Then, the distribution of B can be written as

$$f_B(t) = f_{B|b}(t)\pi_b + f_{B|g}\pi_g. \tag{3}$$

To proceed further, two assumptions are made. First, it is assumed that $\pi_g \gg \pi_b$ or equivalently $\frac{1}{\mu_g} \gg \frac{1}{\mu_b}$. This condition is valid for a channel with a reasonable quality. Besides, the block time T is assumed to be much shorter than the average good state duration $\frac{1}{\mu_g}$, i.e. $1 \gg \mu_g T$, such that T can contain only zero or one intervals of bad burst (see [1], [2], [4] for justification). More precisely, the probability of having at least two bad bursts is negligible compared to the probability of having exactly one bad burst. However, it should be noted that all the results of this paper except subsection IV-A stay valid regardless of these two assumptions. Of course, in that case, the exact probability distribution function of B_i should be applied instead of the approximated one here (refer to Remark I in subsection IV-B).

Hence, the pdf of B conditioned on the event b can be approximated as

$$f_{B|b}(t) \approx \mu_b e^{-\mu_b t} + \delta(t-T)e^{-\mu_b T} \tag{4}$$

where $\delta(u)$ is the Dirac delta function. (4) follows from the memoryless nature of the exponential distribution, the assumption that T contains at most one bad burst, and the fact that any bad burst longer than T has to be truncated at $B = T$.

To approximate $f_{B|g}(t)$, we have

$$f_{B|g}(t) = \mathbb{P}\{B = 0|g\}\delta(t) - \frac{\partial}{\partial t}\mathbb{P}\{B > t|g\} \tag{5}$$

where

$$\mathbb{P}\{B = 0|g\} = e^{-\mu_g T} \approx 1 - \mu_g T \tag{6}$$

and

$$\mathbb{P}\{B > t|g\} \overset{(a)}{\approx} (1 - e^{-\mu_g (T-t)})e^{-\mu_b t} \approx \mu_g (T-t)e^{-\mu_b t} \tag{7}$$

where (a) is resulted from the fact that $\{B > t|g\}$ is equivalent to the initial good burst being shorter than $T - t$ and the following bad burst larger than t. Now, combining (6), (7), (5), and (4), $f_B(t)$ can be computed.

A. The Expected Value of B

Throughout this paper, $\mathbb{E}\{\}$ stands for the expected value operator. $\mathbb{E}\{B\}$ can be computed as

$$\mathbb{E}\{B\} = \mathbb{E}\{B|g\}\pi_g + \mathbb{E}\{B|b\}\pi_b \tag{8}$$

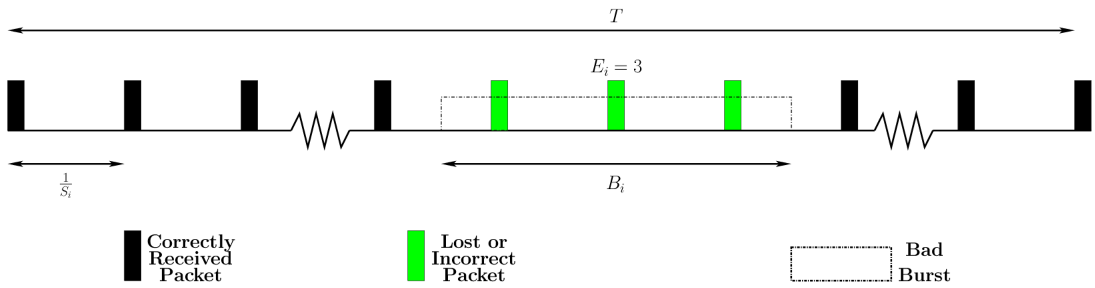


Fig. 3. A bad burst of duration B_i happens in a block of length T. $E_i = 3$ packets are corrupted or lost during the interval B_i. Packets are transmitted every $\frac{1}{S_i}$ seconds, where S_i is the rate of path i in pkt/sec.

where

$$\begin{aligned}
\mathbb{E}\{B|b\} &= \int_0^T t f_{B|b}(t)dt = \frac{1}{\mu_b}(1 - e^{-\mu_b T}) \\
\mathbb{E}\{B|g\} &= \int_0^T t f_{B|b}(t)dt \\
&= \frac{\mu_g(\mu_b T + 3)}{\mu_b^2} - \frac{\mu_g T e^{-\mu_b T}(\mu_b T + 3)}{\mu_b} - \frac{\mu_g e^{-\mu_b T}(\mu_b T + 3)}{\mu_b^2} - \mu_g T^2 e^{-\mu_b T} \qquad (9)
\end{aligned}$$

In the special case where the block transmission time being much larger than the average bad burst length ($T >> \frac{1}{\mu_b}$), $\mathbb{E}\{B\}$ can be simplified as follows

$$\begin{aligned}
\mathbb{E}\{B|b\} &\approx \frac{1}{\mu_b} \\
\mathbb{E}\{B|g\} &\approx \frac{\mu_g T}{\mu_b} \\
\Rightarrow \mathbb{E}\{B\} &\approx \frac{\pi_b}{\mu_b} + \frac{\pi_g \mu_g T}{\mu_b} \overset{(a)}{\approx} \pi_b T \qquad (10)
\end{aligned}$$

where (a) follows from the fact that $\mu_g << \mu_b$. This result can be intuitively justified as follows. As T grows large, due to the ergodicity of the process, the average fraction of time the channel spends in the bad state is almost equal to the steady state probability of being in that state.

B. Discrete to Continuous Approximation

To detect an irrecoverable loss, we are interested in the probability of k_i packets being lost out of the N_i packets transmitted through the path i. Let us denote the number of erroneous or lost packets with the random variable E_i. Any two subsequent packets in a block are $\frac{1}{S_i}$ seconds apart in time, where S_i is the transmission rate over the path i. We observe that the probability $\mathbb{P}\{E_i \geq k_i\}$ can be approximated with the continuous counterpart $\mathbb{P}\{B_i \geq \frac{k_i}{S_i}\}$ when the inter-packet interval is much shorter than the typical bad burst ($\frac{1}{S_i} \ll \frac{1}{\mu_b}$ or equivalently $\mu_b \ll S_i$). The necessity of this condition can be intuitively justified as follows. In case this condition does not hold, any two consecutive packets have to be transmitted on two independent states of the channel. Thus, there would be no gain achieved by applying diversity over multiple independent paths since each path is already being used on the moments where its states are independent. Fig. 3 shows an example of this approximation in detail. The continuous approximation simplifies the mathematical analysis of section IV.

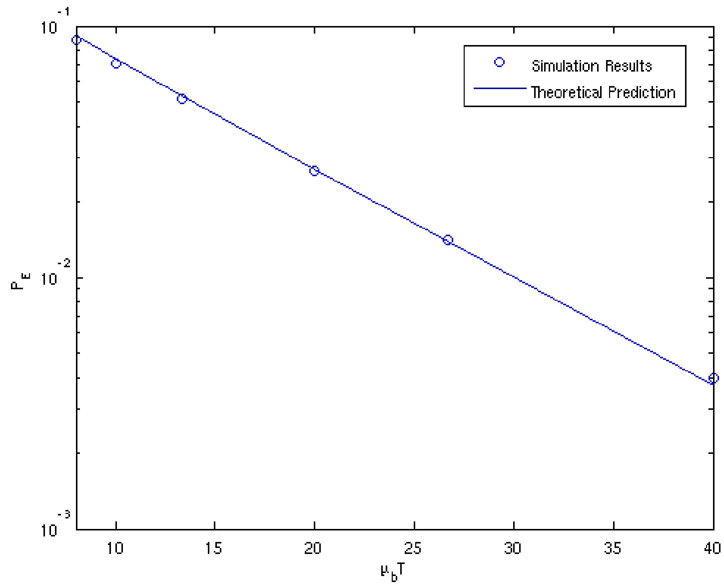


Fig. 4. Probability of irrecoverable loss versus $\mu_b T$ for one path with fixed μ_g, T and α.

IV. Performance Analysis of FEC on Multiple Paths

Assume that a rate allocation algorithm assigns N_i packets to the path i. When the N_i packets of the FEC block are sent over path i, the loss count can be approximated as $\frac{B_i}{T}N_i$. Hence, The total ratio of lost packets is equal to

$$\sum_{i=1}^{L}\frac{B_iN_i}{TN}=\sum_{i=1}^{L}\frac{B_i\rho_i}{T}$$

where $\rho_i=\frac{S_i}{S_{req}}$, $0\le\rho_i\le 1$, denotes the portion of the bandwidth assigned to the path i. $x_i=\frac{B_i}{T}$ is defined as the portion of time the path i has been in the bad state ($0\le x_i\le 1$). Hence, the probability of irrecoverable loss is equal to

$$P_E=\mathbb{P}\left\{\sum_{i=1}^{L}\rho_i x_i>\alpha\right\} \tag{11}$$

where $\alpha=\frac{N-K}{N}$. In order to find the optimum rate allocation, P_E has to be minimized with respect to the allocation vector (ρ_i's), subject to the following constraints

$$0\le\rho_i\le\min\left\{1,\frac{W_i}{S_{req}}\right\},\quad \textstyle\sum_{i=1}^{L}\rho_i=1 \tag{12}$$

where W_i is the bandwidth constraint on path i defined in subsection II-C. Note that the pdf of x_i's are given and proportional to that of B_i's.

A. Performance of FEC on a Single Path

Probability of irrecoverable loss for one path is equal to

$$P_E=\mathbb{P}\{B>\alpha T\}=\mathbb{P}\{B>\alpha T|b\}\pi_b+\mathbb{P}\{B>\alpha T|g\}\pi_g$$

where $\mathbb{P}\{B>\alpha T|b\}$ and $\mathbb{P}\{B>\alpha T|g\}$ can be computed as

$$\begin{aligned}\mathbb{P}\{B>\alpha T|b\}&=\textstyle\int_{\alpha T}^{T}f_{B|b}(t)dt&&=e^{-\mu_b\alpha T},\\ \mathbb{P}\{B>\alpha T|g\}&=\textstyle\int_{\alpha T}^{T}f_{B|g}(t)dt&&=\mu_g(1-\alpha)Te^{-\mu_b\alpha T}\end{aligned}$$

As a result

$$P_E = \pi_b e^{-\mu_b \alpha T}(1+\mu_b(1-\alpha)T) \approx \left[\frac{1}{\mu_b} + (1-\alpha)\,T\right]\mu_g e^{-\mu_b \alpha T}. \tag{13}$$

As we observe, for large values of $\mu_b T$, P_E decays exponentially with $\mu_b T$. Fig. 4 shows the results of simulating a typical scenario of streaming data between two end-points with the rate $S_{req} = 1000\frac{pkt}{sec}$, the block length $N = 200$, and the number of information packets $K = 180$. These values result in block transmission time of $T = 200ms$. The ratio of block transmission time to the average good burst of the Internet channel stays fixed at $\mu_g T = \frac{1}{5}$. However, the ratio of T to the average bad burst, $\mu_b T$, varies from 8 to 40, in accordance with the values in [2], [4]. The slope of the best linear fit (in semilog scale) to the simulation points is 0.097 which is in accordance with the value of 0.100, resulted from the theoretical approximation (13).

B. Identical Paths

When the paths are identical, due to the symmetry of the problem, the uniform rate allocation ($\rho_i = \frac{1}{L}$) is obviously the optimum solution. Of course, the solution is feasible only when for all paths, we have $\frac{1}{L} \leq \frac{W_i}{S_{req}}$. Then, the probability of irrecoverable loss can be simplified as

$$P_E = \mathbb{P}\left\{\frac{1}{L}\sum_{i=1}^{L} x_i > \alpha\right\}. \tag{14}$$

Let us define $Q(x)$ as the probability distribution function of x. Since x is defined as $x = \frac{B}{T}$, clearly we have $Q(x) = T f_B(xT)$. We observe that in (14), the random variable x_i's are bounded and independent. Hence, the following well-known upperbound in large deviation theory [28] can be applied

$$P_E \leq e^{-u(\alpha)L}$$
$$u(\alpha) = \begin{cases} 0 & \text{for } \alpha \leq \mathbb{E}\{x\} \\ \lambda\alpha - \log(\mathbb{E}\{e^{\lambda x}\}) & \text{otherwise} \end{cases} \tag{15}$$

where the $\log$ function is computed in Neperian base, and λ is the solution of the following non-linear equation, which will be shown to be unique by Lemma I.

$$\alpha = \frac{\mathbb{E}\{xe^{\lambda x}\}}{\mathbb{E}\{e^{\lambda x}\}}. \tag{16}$$

Since λ is unique, we can define $l(\alpha) = \lambda$. Even though an upperbound, inequality (15) is shown to be exponentially tight for large values of L [28]. More precisely

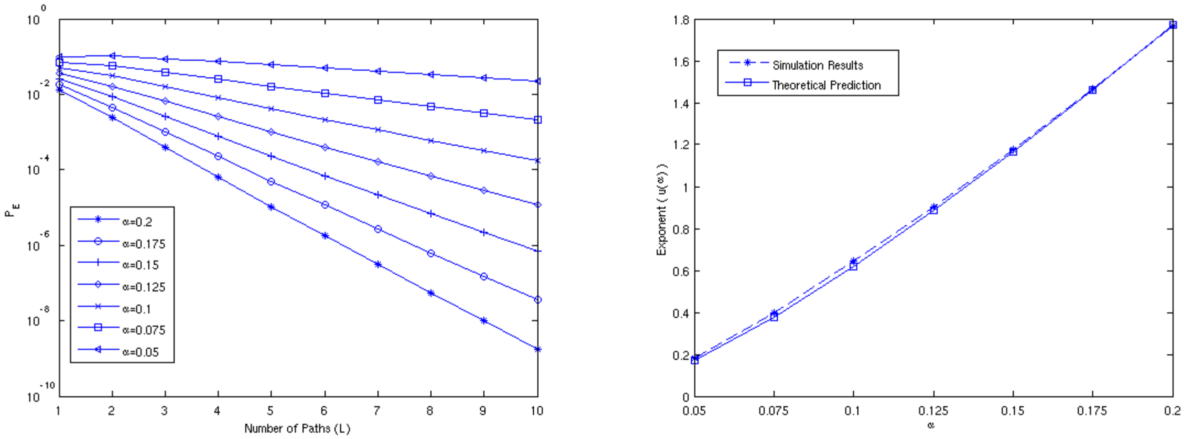
$$P_E \doteq e^{-u(\alpha)L} \tag{17}$$

where the notation $\doteq$ means $\lim_{L->\infty} -\frac{\log P_E}{L} = u(\alpha)$. Now, we state two useful lemmas whose proofs can be found in the appendices B and C.

Lemma I. $u(\alpha)$ and $l(\alpha)$ have the following properties:

1) $\frac{\partial}{\partial\alpha} l(\alpha) > 0$
2) $l(\alpha = 0) = -\infty$
3) $l(\alpha = \mathbb{E}\{x\}) = 0$
4) $l(\alpha = 1) = +\infty$
5) $\frac{\partial}{\partial\alpha} u(\alpha) = l(\alpha) > 0$ for $\alpha > \{x\}$

Lemma II. Defining $y = \frac{1}{L}\sum_{i=1}^{L} x_i$, where x_i's are i.i.d. random variables as already defined, the probability density function of y has the property of $f_y(\alpha) \doteq e^{-u(\alpha)L}$, for all $\alpha > \mathbb{E}\{x\}$.



(a) (b)

Fig. 5. (a) P_E vs. L for different values of α. (b) The Exponent (slope) of plot (a) for different values of α: experimental versus theoretical values.

Fig. 5 compares the theoretical and simulation results. The connection has the fixed block transmission time of $T = 200ms$. The block length is proportional to the number of paths as $N = 20L$. The ratio of block transmission time to the average good burst is fixed at $\mu_g T = \frac{1}{5}$. The Internet channel has the error probability of $\pi_b = 0.015$. Coding overhead is changed from $\alpha = 0.05$ to $\alpha = 0.2$. The probability of irrecoverable loss is plotted versus the number of paths, L, in semilogarithmic scale in Fig. 5(a) for every fixed value of α. We observe that as L increases, $\log P_E$ decays linearly which is expectable from equation (15). Also, Fig. 5(b) compares the slope of each plot in Fig. 5(a) with $u(\alpha)$. Fig. 5 shows a good agreement between the theory and the simulation results, and also verifies the fact that the stronger the FEC code is (larger α), the more gain we achieve from path diversity (larger exponent).

Remark I. Equation (17) is a direct result of the discrete to continuous approximation in subsection III-B. Therefore, it remains valid even if the other approximations in section III do not hold. For example, if the block time contains more than one bad burst, equations (4) and (7) are no longer valid. However, the result (17) is still true as long as the discrete to continuous approximation is used. Of course, in this case, the exact distributions of B and x should be used to compute $u(\alpha)$ and λ instead of the simplified versions.

Remark II. A special case is when the block code uses all the bandwidth resources of the paths. In this case, we have $N = LWT$, where W is the maximum bandwidth of each path, and T is the block time duration. Assuming $\alpha > \mathbb{E}\{x\}$ is a constant independent of L, we observe that the information packet rate is equal to $\frac{K}{T} = (1-\alpha)WL$, and the error probability is $P_E \doteq e^{-u(\alpha)L}$. This shows using MDS codes over multiple independent paths provides an exponential decay in the irrecoverable loss probability and a linearly growing end-to-end rate in terms of the number of paths, simultaneously.

Remark III. The result of (15) can be applied to analyze the error exponent of an MDS code over a memoryless erasure channel as follows. Consider the case where the block length is equal to the number of paths ($N = L$). Then, transmitting over L independent paths is equivalent to sending a block of L symbols over a memoryless erasure channel depicted in Fig. 6. The arguments of this section can be used with minor modifications. In this case, the discrete to continuous approximation of subsection III-B is not valid anymore. However, similar results are easy to obtain by an alternative approach. Let x_i denote

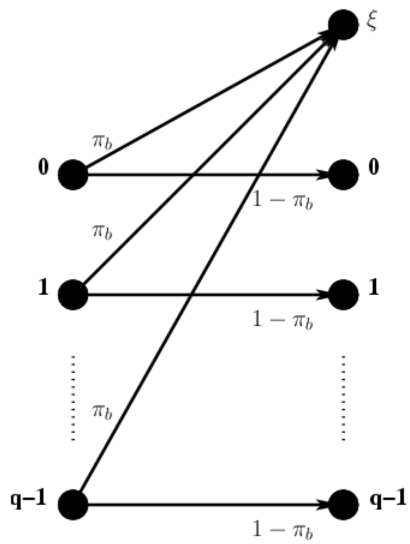


Fig. 6. Erasure memoryless channel model with the probability of erasure π_b, and the erasure symbol ξ.

the random variable indicating successful transmission over the i'th path, i.e.

$$x_i = \begin{cases} 0 & \text{if path } i \text{ in good state} \\ 1 & \text{if path } i \text{ in bad state.} \end{cases} \tag{18}$$

The number of lost packets in a block would be $\sum_{i=1}^{L} x_i$, and the probability of irrecoverable loss can be written as

$$P_E = \mathbb{P}\left\{ \frac{1}{L} \sum_{i=1}^{L} x_i > \alpha \right\} \tag{19}$$

which is very similar to (14), except that x_i's are discrete random variables here. Based on the reference [28], and the same arguments of (15) and (16), we have

$$\mathbf{P}\{\mathcal{E}\} \overset{(a)}{\doteq} P_E \doteq e^{-u(\alpha)L} \tag{20}$$

where $\mathbf{P}\{\mathcal{E}\}$ is the maximum-likelihood decoder probability of error, and (a) follows from inequality (2). $u(\alpha)$ is defined as

$$u(\alpha) = \begin{cases} 0 & \text{for } \alpha \le \pi_b \\ \alpha \log\left(\dfrac{\alpha(1-\pi_b)}{\pi_b(1-\alpha)}\right) - \log\left(\dfrac{1-\pi_b}{1-\alpha}\right) & \text{for } \pi_b < \alpha \le 1. \end{cases} \tag{21}$$

MDS coding error exponent, $u()$, can be expressed in terms of the information transmission rate, R, instead of α as well. When a q-arry (N, K) MDS code with the overhead $\alpha = \dfrac{N-K}{N}$ is used, the rate per symbol is equal to

$$R = \frac{K}{N} \log q = (1-\alpha) \log q$$

where K should be an integer, and we should have $q \ge N$ for a feasible MDS code. Thus, the finest resolution of rates achievable by a single MDS codebook would be $R = \dfrac{i}{q} \log q$ for $i = 1, 2, \ldots, q$. Of course, it is also possible to achieve the rates in the intervals $\dfrac{i}{q} \log q < R < \dfrac{i+1}{q} \log q$ by time sharing between two MDS codebooks of sizes (q, i) and $(q, i+1)$ respectively. However, in such cases, the smaller error exponent belonging to the codebook of the size $(q, i+1)$ dominates.

Therefore, $u(R)$ will have the stepwise shape of the form

$$u(R) = \begin{cases} 0 & \text{for } 1-\pi_b \le \frac{1}{q}\left\lceil \frac{qR}{\log q} \right\rceil \\ -\frac{1}{q}\left\lceil \frac{qR}{\log q} \right\rceil \log\left(\frac{(1-\pi_b)\left(1-\frac{1}{q}\left\lceil \frac{qR}{\log q} \right\rceil\right)}{\pi_b \frac{1}{q}\left\lceil \frac{qR}{\log q} \right\rceil} \right) - \log\left(\frac{\pi_b}{1-\frac{1}{q}\left\lceil \frac{qR}{\log q} \right\rceil} \right) & \text{for } 0 < \frac{1}{q}\left\lceil \frac{qR}{\log q} \right\rceil \le 1-\pi_b. \end{cases} \tag{22}$$

It is interesting to compare the above exponent with the random coding error exponent as described in [29]. This exponent, $E_r(R)$, can be written as

$$E_r(R) = \max_{0\le\rho\le 1} \left\{ -\rho R + \max_{\mathbf{Q}} E_0(\rho, \mathbf{Q}) \right\} \tag{23}$$

where $\mathbf{Q}$ is the input distribution, and $E_0(\rho, \mathbf{Q})$ equals

$$E_0(\rho, \mathbf{Q}) = -\log\left(\sum_{j=0}^{q} \left[\sum_{k=0}^{q-1} Q(k) P(j|k)^{\frac{1}{1+\rho}} \right]^{1+\rho} \right). \tag{24}$$

Due to the symmetry of the channel transition probabilities, the uniform distribution maximizes (23) over all possible input distributions. Therefore, $E_0(\rho, \mathbf{Q})$ can be simplified as

$$E_0(\rho, \mathbf{Q}) = -\log\left(\frac{1-\pi_b}{q^\rho} + \pi_b \right). \tag{25}$$

Solving the maximization (23), gives us $E_r(R)$ as

$$E_r(R) = \begin{cases} -\log\left(\frac{1-\pi_b+\pi_b q}{q} \right) - R & \text{for } 0 \le \frac{R}{\log q} \le \frac{1-\pi_b}{1-\pi_b+\pi_b q} \\ -\frac{R}{\log q} \log\left(\frac{(1-\pi_b)\left(1-\frac{R}{\log q}\right)}{\pi_b \frac{R}{\log q}} \right) - \log\left(\frac{\pi_b}{1-\frac{R}{\log q}} \right) & \text{for } \frac{1-\pi_b}{1-\pi_b+\pi_b q} \le \frac{R}{\log q} \le 1-\pi_b. \end{cases} \tag{26}$$

Comparing (22) and (26), we observe that the MDS code and the random code perform exponentially the same for the rate range $\frac{1-\pi_b}{1-\pi_b+\pi_b q} \le \frac{R}{\log q} \le 1-\pi_b$. However, for the interval $0 < \frac{R}{\log q} \le \frac{1-\pi_b}{1-\pi_b+\pi_b q}$ where the error exponent of the random code decays linearly with R, MDS coding achieves a larger error exponent. It is worth noting that this interval is negligible for large alphabet sizes. Moreover, the stepwise graph of $u(R)$ meets its envelope as the steps are very small for large values of q.

Fig. 7 depicts the error exponents of random coding and MDS coding for an alphabet size of $q = 128$ over an erasure channel with $\pi_b = 0.015$. As observed, $E_r(R)$ can be approximated by its envelope very closely even for a relatively low alphabet size ($q = 128$).

C. Non-Identical Paths

Now, let us assume there are J types of paths between the source and the destination, consisting of L_j identical paths from type j ($\sum_{j=1}^{J} L_j = L$). Without loss of generality, we can assume that the paths are ordered according to their associated type, i.e. the paths from $1 + \sum_{k=1}^{j-1} L_k$ to $\sum_{k=1}^{j} L_k$ are of type j. We denote $\gamma_j = \frac{L_j}{L}$. According to the i.i.d. assumption, it is obvious that ρ_i has to be the same for all paths from the same type. η_j and y_j are defined as

$$\begin{aligned} \eta_j &= \sum_{\sum_{k=1}^{j-1} L_k < i \le \sum_{k=1}^{j} L_k} \rho_i \\ y_j &= \frac{\eta_j}{L\gamma_j} \sum_{\sum_{k=1}^{j-1} L_k < i \le \sum_{k=1}^{j} L_k} x_i. \end{aligned} \tag{27}$$

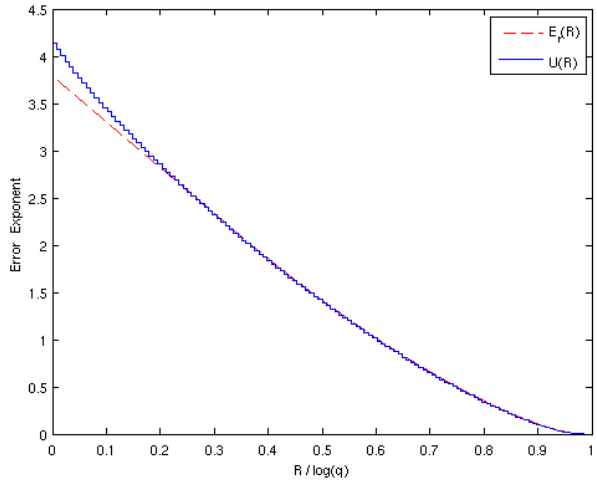


Fig. 7. Error exponents of random coding ($E_r(R)$) and MDS coding ($u(R)$).

Following Lemma II, we observe that $f_{y_j}(\beta_j) \doteq e^{-\gamma_j u_j(\frac{\beta_j}{\eta_j})L}$. We define the sets $\mathcal{S}_I$, $\mathcal{S}_O$ and $\mathcal{S}_T$ as

$$\begin{aligned}\mathcal{S}_I &= \left\{(\beta_1, \beta_2, \cdots, \beta_J)\,|0 \le \beta_j \le 1,\ \sum_{j=1}^{J} \beta_j > \alpha\right\}\\ \mathcal{S}_O &= \left\{(\beta_1, \beta_2, \cdots, \beta_J)\,|0 \le \beta_j \le 1,\ \sum_{j=1}^{J} \beta_j = \alpha\right\}\\ \mathcal{S}_T &= \left\{(\beta_1, \beta_2, \cdots, \beta_J)\,|\eta_j \mathbb{E}\{x_j\} \le \beta_j, \sum_{j=1}^{J} \beta_j = \alpha\right\},\end{aligned}$$

respectively. Hence, P_E can be written as

$$\begin{aligned}P_E &= \mathbb{P}\left\{\sum_{j=1}^{J} y_j > \alpha\right\}\\ &= \oint_{\mathcal{S}_I} \prod_{j=1}^{J} f_{y_j}(\beta_j) d\beta_j\\ &\doteq \oint_{\mathcal{S}_I} e^{-L\sum_{j=1}^{J}\gamma_j u_j(\frac{\beta_j}{\eta_j})} d\beta_j\\ &\overset{(a)}{\doteq} e^{-L \min_{\beta\in\mathcal{S}_I\cup\mathcal{S}_O} \sum_{j=1}^{J}\gamma_j u_j\left(\frac{\beta_j}{\eta_j}\right)}\\ &\overset{(b)}{\doteq} e^{-L \min_{\beta\in\mathcal{S}_O} \sum_{j=1}^{J}\gamma_j u_j\left(\frac{\beta_j}{\eta_j}\right)}\\ &\overset{(c)}{\doteq} e^{-L \min_{\beta\in\mathcal{S}_T} \sum_{j=1}^{J}\gamma_j u_j\left(\frac{\beta_j}{\eta_j}\right)}\\ &\overset{(d)}{\doteq} e^{-L \sum_{j=1}^{J}\gamma_j u_j\left(\frac{\beta_j^\star}{\eta_j}\right)}\end{aligned} \tag{28}$$

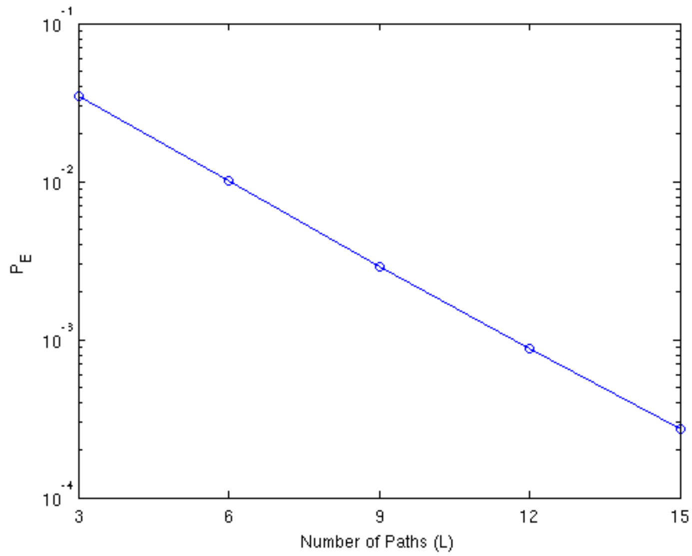


Fig. 8. P_E versus L for the combination of two path types, one third from type I and the rest from type II.

where (a) follows from Lemma III, (b) is resulted from the fact $u_j(\alpha)$ is a strictly increasing function of α, for $\alpha > \mathbb{E}\{x_j\}$, and (c) follows from the property that $u_j(\alpha) = 0, \forall \alpha \leq \mathbb{E}\{x_j\}$. Finally, applying Lemma IV results in (d) where $\beta^\star$ is defined in the Lemma.

Lemma III. For any continuous positive function $h(\mathbf{x})$ over a convex set $\mathcal{S}$, and defining $H(L)$ as

$$H(L) = \oint_{\mathcal{S}} e^{-h(\mathbf{x})L} d\mathbf{x}$$

we have

$$\lim_{L \to \infty} -\frac{\log(H(L))}{L} = \inf_{\mathcal{S}} h(\mathbf{x}) = \min_{cl(\mathcal{S})} h(\mathbf{x})$$

where $cl(\mathcal{S})$ denotes the closure of $\mathcal{S}$ (refer to [30] for the definition of the closure operator).

Lemma IV. There exists a unique vector $\beta^\star$ with the elements $\beta_j^\star = \eta_j l_j^{-1}\left(\frac{\nu \eta_j}{\gamma_j}\right)$ which minimizes the convex function $\sum_{j=1}^{J} \gamma_j u_j(\frac{\beta_j}{\eta_j})$ over the convex set $\mathcal{S}_T$, where ν satisfies the following condition

$$\sum_{j=1}^{J} \eta_j l_j^{-1}\left(\frac{\nu \eta_j}{\gamma_j}\right) = \alpha. \tag{29}$$

$l^{-1}()$ denotes the inverse of the function $l()$ defined in subsection IV-B. The proofs of Lemmas III and IV can be found in the appendices D and E.

Equation (28) is valid for any fixed value of η. To achieve the most rapid decay of P_E, the exponent must be maximized over η.

$$\lim_{L -> \infty} -\frac{\log P_E}{L} = \max_{0 \leq \eta_j \leq 1} \sum_{j=1}^{J} \gamma_j u_j\left(\frac{\beta_j^\star}{\eta_j}\right) \tag{30}$$

where $\beta^\star$ is defined for any value of the vector η in Lemma IV. Theorem II solves the maximization problem of (30) and identifies the asymptotically optimum rate allocation (for large number of paths).

Theorem II. Consider a point-to-point connection over the Internet with L independent paths from the source to the destination, each modeled as a Gilbert-Elliot cell, with no bandwidth constraint. The paths are from J different types, L_j paths from the type j. Assume a block FEC of the size (N, K) is sent during an interval time T. Let N_j denote the number of packets in a block of size N assigned to the paths of type j, such that $\sum_{j=1}^{J} N_j = N$. The rate allocation vector η is defined as $\eta_j = \frac{N_j}{N}$. For fixed values of $\gamma_j = \frac{L_j}{L},\ n_0 = \frac{N}{L},\ k_0 = \frac{K}{L},\ T$ and asymptotically large number of paths (L), the optimum rate allocation vector $\eta^\star$ can be found by solving the following optimization problem

$$\max_{\eta} g(\eta),$$
$$\text{s.t. } \sum_{j=1}^{J} \eta_j = 1,\ 0 \leq \eta_j \leq 1$$

where $g(\eta) = \sum_{j=1}^{J} \gamma_j u_j \left(\frac{\beta_j^\star}{\eta_j}\right)$, and $\beta^\star$ is an implicit function of η defined in Lemma IV. The functions $u_j()$ and $l_j()$ are defined in subsections IV-B and IV-C. Solving the above optimization problem gives the unique solution $\eta^\star$ as

$$\eta_j^\star = \begin{cases} 0 & \text{if } \alpha \leq \mathbb{E}\{x_j\} \\ \dfrac{\gamma_j l_j(\alpha)}{\sum\limits_{i=1,\ \alpha \leq \mathbb{E}\{x_i\}}^{J} \gamma_i l_i(\alpha)} & \text{otherwise} \end{cases} \tag{31}$$

if there is at least one $1 \leq j \leq J$ for which $\alpha > \mathbb{E}\{x_j\}$. The maximum value of the objective function is $g(\eta^\star) = \sum_{j=1}^{J} \gamma_j u_j(\alpha)$ which is indeed the exponent of P_E versus L. The proof of the theorem can be found in F.

Remark IV. Theorem II can be interpreted as follows. For large values of L, adding a new type of path contributes to the path diversity *iff* the path satisfies the quality constraint $\alpha > \mathbb{E}\{x\}$, where x is the percentage of time that the path spends in the bad state in the time interval $[0, T]$. Only in this case, adding the new type of path exponentially improves the performance of the system in terms of the probability of irrecoverable loss.

Remark V. Observing the exponent coefficient corresponding to the optimum allocation vector $\eta^\star$, we can see that the typical error event occurs when the ratio of lost packets on all types of paths is the same as the total fraction of lost packets , α. However, this is not the case for any arbitrary rate allocation vector η.

Fig. 8 shows P_E of the optimum rate allocation versus L for a system consisting of two types of path. The optimal rate allocation is found by exhaustive search among all possible allocation vectors. The block transmission time is fixed at $T = 200ms$. The block length is proportional to the number of paths as $N = 20L$. The ratio of block transmission time to the average good burst is equal to $\mu_g T = \frac{1}{5}$ for both types of paths. $\gamma_1 = \frac{1}{3}$ of the paths benefit from shorter bad bursts and lower error probability of $\pi_{b,1} = 0.015$, and the rest suffer from longer congestion bursts resulting higher error probability of $\pi_{b,2} = 0.025$. The coding overhead is fixed at $\alpha = 0.1$. The figure depicts a linear behavior in semi-logarithmic scale with the exponent of 0.403, which is comparable to 0.389 resulted from (31).

In the scenario of Fig. 8, let us denote $\eta_1^\star$ as the value of of the first element of η in equation (31). Obviously, $\eta_1^\star$ does not depend on L. Moreover, η_1^{opt} is defined as the normalized aggregated weight of type I paths in the optimal rate allocation. Fig. 9 compares η_1^{opt} with $\eta_1^\star$ for different number of paths. It is observed that η_1^{opt} converges rapidly to $\eta_1^\star$ as L grows. Fig. 8 also verifies that the allocation vector candidate $\eta^\star$ proposed by Theorem II indeed meets the optimal allocation vector for large values of L.

V. Suboptimal Rate Allocation

In order to compute the complexity of the rate allocation problem, we go back to the original discrete formulation in subsection II-C. According to the model of subsection IV-C, we assume the available paths are from J types, L_j paths from

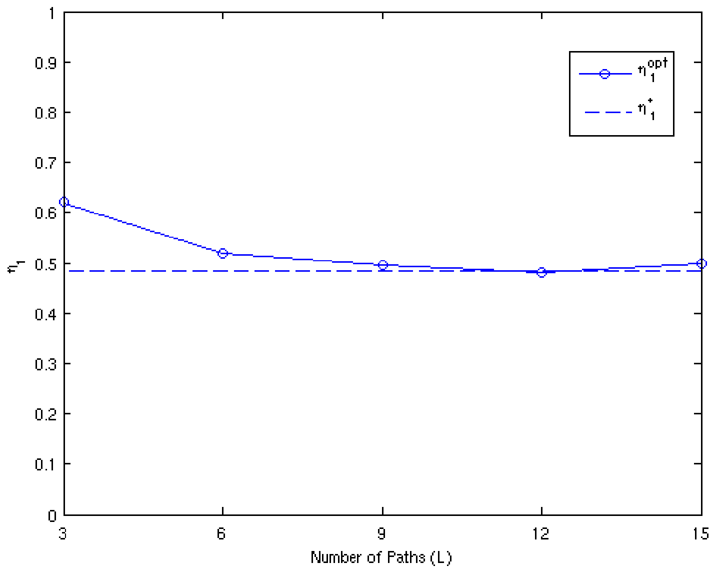


Fig. 9. The normalized aggregated weight of type I paths in the optimal rate allocation (η_1^{opt}), compared with the value of η_1 which maximizes the exponent of equation (30) ($\eta_1^{\star}$).

type j, such that $\sum_{j=1}^{J} L_j = L$. Obviously, all the paths from the same type should take equal rate. Therefore, the rate allocation problem is turned into finding the vector $\mathbf{N} = (N_1, \ldots, N_J)$ such that $\sum_{j=1}^{J} N_j = N$, and $0 \leq N_j \leq L_j W_j T$ for all j. N_j denotes the number of packets to the paths of type j all together. Let us temporarily assume all paths have enough bandwidth such that N_j can vary from 0 to N for all j. There are $\binom{N+J-1}{J-1}$ L-dimensional non-negative vectors of the form $(N_1, \ldots, N_J)$ which satisfy the equation $\sum_{j=1}^{J} N_j = N$ each representing a distinct rate allocation to the different available types. Hence, the number of candidates is exponential in terms of J.

First, we prove the problem of rate allocation is NP in the sense that P_E can be computed in polynomial time for any candidate vector $\mathbf{N} = (N_1, \ldots, N_J)$. Let us define $P_e^{\mathbf{N}}(k, j)$ as the probability of having more than k errors over the paths of types 1 to j for a specific allocation vector $\mathbf{N}$. We also define $Q_j(n, k)$ as the probability of having exactly k errors out of the n packets sent over the paths of type j. $Q_j(n, k)$ can be computed and stored for all path types and values of n and k with polynomial complexity as explained in appendices G and H. Then, the following recursive formula holds for $P_e^{\mathbf{N}}(k, j)$

$$\begin{aligned} P_e^{\mathbf{N}}(k,j) &= \begin{cases} \sum_{i=0}^{N_j} Q_j(N_j,i) P_e^{\mathbf{N}}(k-i,j-1) & \text{if } k \geq 0 \\ 1 & \text{if } k < 0 \end{cases} \\ P_e^{\mathbf{N}}(k,1) &= \sum_{i=k+1}^{N_1} Q_1(N_1,i). \end{aligned} \tag{32}$$

Using dynamic programming, it is obvious that the above formula computes $P_e^{\mathbf{N}}(K, J)$ with the complexity of $O(K^2 J)$. Following appendix H, we note that for each j, $Q_j(N_j, k)$ for $0 \leq k \leq K$ is computed offline with the complexity of $O(K^2 N_j)$. Hence, the total complexity of computing $P_e^{\mathbf{N}}(K, J)$ adds up to $O(K^2 J) + \sum_{j=1}^{J} O(K^2 N_j) = O\left(K^2 (J + N)\right)$.

Now, we propose a suboptimal polynomial time algorithm to estimate the best path allocation vector, $\mathbf{N}^{opt}$. Let us define $P_e^{opt}(n, k, j)$ as the probability of having more than k errors for a block of length n over the paths of types 1 to j minimized over all possible rate allocations ($\mathbf{N} = \mathbf{N}^{opt}$). First, we find a lowerbound $\hat{P}_e(n, k, j)$ for $P_e^{opt}(n, k, j)$ from the following recursive formula

$$
\begin{aligned}
\hat{P}_e(n,k,j) &= \begin{cases} \min\limits_{0\le n_j\le \min\{n,\lfloor L_jW_jT\rfloor\}} \sum\limits_{i=0}^{n_j} Q_j(n_j,i)\hat{P}_e(n-n_j,k-i,j-1) & \text{if } k>0 \\ \\ 1 & \text{if } k\le 0 \end{cases} \\
\hat{P}_e(n,k,1) &= \sum_{i=k+1}^{n} Q_1(n,i).
\end{aligned} \tag{33}
$$

According to the recursive definition above, it is easy to verify that $\hat{P}_e(N,K,J)$ can be computed with the complexity of $O(N^2K^2J)$ using dynamic programming. The following lemma guarantees that $\hat{P}_e(n,k,j)$ is in fact a lowerbound for $P_e^{opt}(n,k,j)$.

Lemma V. $P_e^{opt}(n,k,j) \ge \hat{P}_e(n,k,j)$. The proof has come in the appendix I.

The following algorithm recursively finds a suboptimum allocation vector $\hat{\mathbf{N}}$ based on the lowerbound of Lemma V.

(1): *Initialize* $j \leftarrow J,\ n \leftarrow N,\ k \leftarrow K$.

(2): *Set*

$$
\begin{aligned}
\hat{N}_j &= \operatorname*{argmin}_{0\le n_j\le \min\{n,\lfloor L_jW_jT\rfloor\}} \sum_{i=0}^{n_j} Q_j(n_j,i)\hat{P}_e(n-n_j,k-i,j-1) \\
K_j &= \operatorname*{argmax}_{0\le i\le \hat{N}_j} \hat{P}_e(n-\hat{N}_j,k-i,j-1)Q_j(\hat{N}_j,i)
\end{aligned}
$$

(3): *Update* $n \leftarrow n-\hat{N}_j,\ k \leftarrow k-K_j,\ j \leftarrow j-1$.

(4): *If* $j>1$ *and* $k\ge 0$, *goto (2).*

(5): *For* $m=1$ *to* j, *set* $\hat{N}_m \leftarrow \lfloor \frac{n}{j} \rfloor$.

(6): $\hat{N}_j \leftarrow \hat{N}_j + Rem(n,j)$ *where* $Rem(a,b)$ *denotes the remainder of dividing* a *by* b.

Intuitively saying, the above algorithm tries to recursively find the typical error event (K_j's) which has the maximum contribution to the error probability, and assigns the rate allocations ($\hat{N}_j$'s) such that the estimated typical error probability ($\hat{P}_e$) is minimized. Indeed, Lemma V shows that the estimate used in the algorithm ($\hat{P}_e$) is a lower-bound for the minimum achievable error probability (P_e^{opt}). Comparing (33) and the step (2) of our algorithm, we observe that the values of $\hat{N}_j$ and K_j can be found in $O(1)$ during the computation of $\hat{P}_e(N,K,J)$. Hence, complexity of the proposed algorithm is the same as that of computing $\hat{P}_e(N,K,J)$, $O(N^2K^2J)$. The following theorem guarantees that the output of the above algorithm converges to the asymptotically optimal rate allocation introduced in Theorem II of section IV-C, and accordingly, it performs optimally for large number of paths.

Theorem III. Consider a point-to-point connection over the Internet with L independent paths from the source to the destination, each modeled as a Gilbert-Elliot cell with no bandwidth constraint. The paths are from J different types, L_j paths from the type j. Assume a block FEC of the size (N,K) is sent during an interval time T. For fixed values of $\gamma_j = \frac{L_j}{L},\ n_0 = \frac{N}{L},\ k_0 = \frac{K}{L},\ T$ and asymptotically large number of paths (L) we have

1) $\hat{P}_e(N,K,J) \doteq e^{-L\sum\limits_{j=1}^{J}\gamma_j u_j(\alpha)}$

2) $$\frac{\hat{N}_j}{N} = \begin{cases} o(1) & \text{if } \alpha \leq \mathbb{E}\{x_j\} \\ \\ \dfrac{\gamma_j l_j(\alpha)}{\displaystyle\sum_{i=1,\ \alpha\leq\mathbb{E}\{x_i\}}^{J} \gamma_i l_i(\alpha)} + o(1) & \text{otherwise} \end{cases}$$

3) $\frac{K_j}{\hat{N}_j} = \alpha + o(1)$ for $\alpha > \mathbb{E}\{x_j\}$.

where $\alpha = \dfrac{k_0}{n_0}$, and $u_j()$ and $l_j()$ are defined in subsections IV-B and IV-C. $\hat{P}_e(N, K, J)$ is the lowerbound for $P_e^{opt}(n, k, j)$ defined in equation (33). $\hat{N}_j$ is the total number of packets assigned to the paths of type j by the suboptimal rate allocation algorithm. K_j is also defined in step (2) of the algorithm. The notation $f(L) = o(g(L))$ means $\lim_{L\to\infty} \frac{f(L)}{g(L)} = 0$. The proof can be found in the appendix J.

The proposed algorithm is compared with four other allocation schemes over $L = 6$ paths in Fig. 10. The optimal method uses exhaustive search over all possible allocations. '*Best Path Allocation*' assigns everything to the best path only, ignoring the rest. '*Equal Distribution*' scheme distributes the packets among all paths equally. Finally, the '*Asymptotically Optimal*' allocation assigns the rates based on the equation (31). The block length and the number of information packets are assumed to be $N = 100$ and $K = 90$, respectively. The overall rate is $S_{req} = 1000pkt/sec$ which results in $T = 100ms$. the ratio of block transmission time to the average good duration is the same for all paths as $\mu_g T = \dfrac{1}{10}$. However, quality of the paths are different as they have different average bad burst durations. Packet error probability of the paths are listed as $[0.0175 \pm \frac{\Delta}{2}, 0.0175 \pm \frac{3\Delta}{2}, 0.0175 \pm \frac{5\Delta}{2}]$, such that the median is fixed at 0.0175. Δ is also defined as a measure of deviation from this median. $\Delta = 0$ represents the case where all paths are identical. The larger Δ is, the more variety we have among the paths and the more diversity gain might be achieved using a judicious rate allocation.

As seen in a wide range, our suboptimal algorithm tracks the optimal algorithm so closely that the corresponding curves are not easily distinguishable. However, the '*Asymptotically Optimal*' rate allocation results in lower performance since there is only one path from each type which makes the asymptotic analysis assumptions invalid. When $\Delta = 0$, '*Equal Distribution*' scheme obviously coincides the optimal allocation. This scheme eventually diverges from the optimal algorithm as Δ grows. However, it still outperforms the best path allocation method as long as Δ is not too large. For very large values of Δ, the best path dominates all the other ones, and we can ignore the rest of the paths. Hence, the best path allocation eventually converges to the optimal scheme when Δ increases.

VI. Conclusion

In this work, we study the performance of forward error correction over a block of packets sent through multiple independent paths. First, it is shown that *Maximum Distance Separable* (MDS) block codes are optimum over our *Internet Channel* model, and any other erasure channel with or without memory, in the sense that their probability of error is minimum among all block codes of the same size. Then, the probability of irrecoverable loss, P_E, is analyzed for the cases of a single path, multiple identical, and non-identical paths based on the discrete to continuous relaxation. When there are L identical paths, P_E is upperbounded using large deviation theory. This bound is shown to be exponentially tight in terms of L. The asymptotic analysis shows that the exponential decay of P_E with L is still valid in the case of non-identical paths. Furthermore, the optimal rate allocation problem is solved in the asymptotic case where L is very large. It is seen that in the optimal rate allocation, each path is assigned a positive rate *iff* its quality is above a certain threshold. The quality of a path is defined as

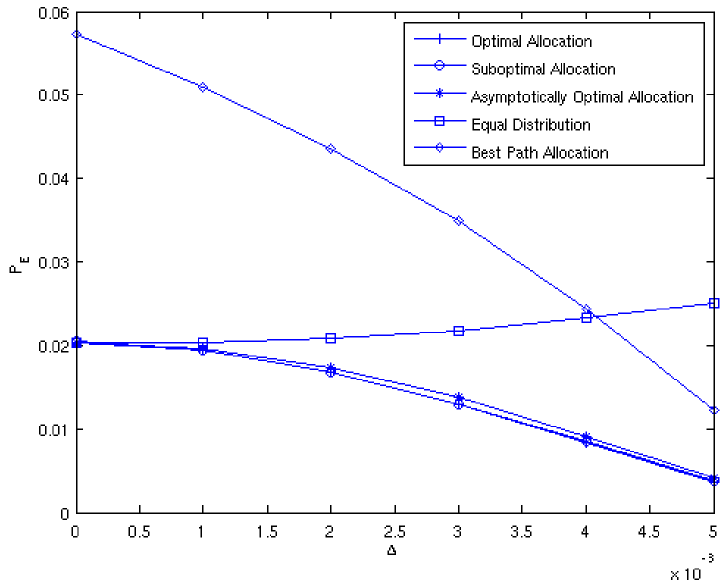


Fig. 10. Optimal and suboptimal rate allocations are compared with equal distribution and best path allocation schemes for different values of Δ

the percentage of the time it spends in the bad state. In other words, including a redundant path improves the reliability *iff* this condition is satisfied. Finally, we focus on the problem of optimum path rate allocation when L is not necessarily large. A heuristic suboptimal algorithm is proposed which estimates the optimal allocation in polynomial time. For large values of L, the result of this algorithm converges to the optimal solution of the asymptotic analysis. Moreover, the simulation results verify the validity of our theoretical analyses in multiple practical scenarios, and also show that the proposed suboptimal algorithm approximates the optimal allocation very closely.

APPENDIX A
PROOF OF THEOREM I

Consider a (N, K, d) codebook $\mathcal{C}$ with the q-ary codewords of length N, number of codes q^K, and minimum distance d. The distance between two codewords is defined as the number of different symbols in the same positions. A codeword $\mathbf{x} \in \mathcal{C}$ is transmitted and a vector $\mathbf{y} \in (\mathcal{X} \cup \{\xi\})^N$ is received. The number of erased symbols is equal to the Hamming weight of $\mathbf{e}$ denoted by $w(\mathbf{e})$. Decoding error event, $\mathcal{E}$, happens when the decoder decides on a codeword different from $\mathbf{x}$. Let us assume that the probability of having a specific erasure pattern $\mathbf{e}$ is $\mathbb{P}\{\mathbf{e}\}$ which is obviously independent of the transmitted codeword, and depends only on the channel. We assume a specific erasure vector $\mathbf{e}$ of weight m happens. The decoder decodes the transmitted codeword based on the $N - m$ correctly received symbols. We partition the codebook set, $\mathcal{C}$, into q^{N-m} bins, each bin representing a specific received vector satisfying the erasure pattern $\mathbf{e}$. The number of codewords in the i'th bin is denoted by $b_{\mathbf{e}}(i)$ for $i = 1$ to q^{N-m}. Knowing the erasure vector $\mathbf{e}$ and the received vector $\mathbf{y}$, the decoder selects the bin i corresponding to $\mathbf{y}$. The set of possible transmitted codewords is equal to the set of codewords in bin i. In fact, all the codewords in bin i are equiprobable to be transmitted. If $b_{\mathbf{e}}(i) = 1$, the transmitted codeword $\mathbf{x}$ can be decoded with no ambiguity. Otherwise, the optimum decoder randomly decides on one of the $b_{\mathbf{e}}(i) > 1$ codewords in the bin. Thus, the probability of error is $1 - \dfrac{1}{b_{\mathbf{e}}(i)}$ when bin i is selected. Bin i is selected if one of the codewords it contains is transmitted.

Hence, probability of selecting bin i is equal to $\frac{b_{\mathbf{e}}(i)}{q^K}$. Based on the above arguments, we have

$$\begin{aligned}
\mathbb{P}\{\mathcal{E}\} &\overset{(a)}{=} \sum_{m=d}^{N} \sum_{\mathbf{e}:w(\mathbf{e})=m} \mathbb{P}\{\mathbf{e}\}\mathbb{P}\{\mathcal{E}|\mathbf{e}\} \\
&= \sum_{m=d}^{N} \sum_{\mathbf{e}:w(\mathbf{e})=m} \mathbb{P}\{\mathbf{e}\} \sum_{i=1,\ b_{\mathbf{e}}(i)>0}^{q^{N-m}} \left(1-\frac{1}{b_{\mathbf{e}}(i)}\right)\frac{b_{\mathbf{e}}(i)}{q^K} \\
&\overset{(b)}{=} \sum_{m=d}^{N} \sum_{\mathbf{e}:w(\mathbf{e})=m} \mathbb{P}\{\mathbf{e}\} \left(1-\frac{b_{\mathbf{e}}^{+}}{q^K}\right) \\
&\geq \sum_{m=d}^{N} \sum_{\mathbf{e}:w(\mathbf{e})=m} \mathbb{P}\{\mathbf{e}\} \left(1-\frac{q^{N-m}}{q^K}\right) \qquad (34)
\end{aligned}$$

where $b_{\mathbf{e}}^{+}$ indicates the number of bins containing one or more codewords. (a) follows from the fact that the transmitted codeword can be uniquely decoded if the number of erasures in the channel is less than the minimum distance of the codebook and (b) follows from the fact that $\sum_{i=1}^{q^{N-m}} b_{\mathbf{e}}(i) = q^K$.

According to (34), $\mathbb{P}\{\mathcal{E}\}$ is minimized for a codebook $\mathcal{C}$ *iff* two conditions are satisfied. First, the minimum distance of $\mathcal{C}$ should achieve the maximum possible value, i.e. we should have $d = N-K+1$. Secondly, we should have $b_{\mathbf{e}}^{+} = q^{N-m}$ for all possible erasure vectors $\mathbf{e}$ with any weight $d \leq m \leq N$. Any MDS code satisfies the first condition by definition. Moreover, it is easy to show that $b_{\mathbf{e}}(i) = q^{K-N+m}$ for any MDS code. We first prove this statement for the case of $m = N-K$. Consider the bins of a MDS code for any arbitrary erasure pattern $\mathbf{e}, w(\mathbf{e}) = N-K$. From the fact that $d = N-K+1$ and $\sum_{i=1}^{q^K} b_{\mathbf{e}}(i) = q^K$, it is concluded that each bin contains exactly one codeword. Therefore, there exists only one codeword which matches any K correctly received symbols. Now, consider any general erasure pattern $\mathbf{e}, w(\mathbf{e}) = m > N-K$. For the i'th bin, concatenating any $K-N+m$ arbitrary symbols to the $N-m$ correctly received symbols gives us a distinct codeword of the MDS codebook. Having q^{K-N+m} possibilities to expand the received $N-m$ symbols to K symbols, we have $b_{\mathbf{e}}(i) = q^{K-N+m}$. This completes the proof.

APPENDIX B
PROOF OF LEMMA I

1) We define the function $v(\lambda)$ as

$$v(\lambda) = \frac{\mathbb{E}\{xe^{\lambda x}\}}{\mathbb{E}\{e^{\lambda x}\}}. \qquad (35)$$

Then, the first derivation of $v(\lambda)$ will be

$$\frac{\partial}{\partial\lambda}v(\lambda) = \frac{\mathbb{E}\{x^2e^{\lambda x}\}\mathbb{E}\{e^{\lambda x}\} - [\mathbb{E}\{xe^{\lambda x}\}]^2}{[\mathbb{E}\{e^{\lambda x}\}]^2}. \qquad (36)$$

According to Cauchy-Schwarz inequality, the following statement is always true for any two functions of $f()$ and $g()$

$$[\int_x f(x)g(x)dx]^2 < [\int_x f^2(x)dx][\int_x g^2(x)dx] \qquad (37)$$

unless $f(x) = Kg(x)$ for a constant K and all values of x. If we choose $f(x) = \sqrt{x^2Q(x)e^{x\lambda}}$ and $g(x) = \sqrt{Q(x)e^{x\lambda}}$, they can not be proportional to each other for all values of x. Therefore, the enumerator of equation (36) has to be strictly positive for all λ. Since the function $v(\lambda)$ is strictly increasing, it has an inverse $v^{-1}(\alpha)$ which is also strictly increasing. Moreover, the non-linear equation $v(\lambda) = \alpha$ has a unique solution of the form $\lambda = v^{-1}(\alpha) = l(\alpha)$.

2) To show that $l(\alpha = 0) = -\infty$, we prove the equivalent statement of the form $\lim_{\lambda \to -\infty} v(\lambda) = 0$. Since x is a random variable in the range of $[0, 1]$ with the probability density function $Q(x)$, for any $0 < \epsilon < 1$ we can write

$$\begin{aligned}
\lim_{\lambda \to -\infty} v(\lambda) &= \lim_{\lambda \to -\infty} \frac{\int_0^\epsilon xQ(x)e^{x\lambda}dx + \int_\epsilon^1 xQ(x)e^{x\lambda}dx}{\int_0^1 Q(x)e^{x\lambda}dx} \\
&\leq \lim_{\lambda \to -\infty} \frac{\int_0^\epsilon xQ(x)e^{x\lambda}dx}{\int_0^\epsilon Q(x)e^{x\lambda}dx} + \frac{\int_\epsilon^1 xQ(x)dx}{\int_0^\epsilon Q(x)e^{(x-\epsilon)\lambda}dx} \\
&\stackrel{(a)}{=} \lim_{\lambda \to -\infty} \frac{\int_0^\epsilon xQ(x)e^{x\lambda}dx}{\int_0^\epsilon Q(x)e^{x\lambda}dx} \\
&\stackrel{(b)}{=} \lim_{\lambda \to -\infty} \frac{x_1 Q(x_1)e^{\lambda x_1}}{Q(x_2)e^{\lambda x_2}}
\end{aligned} \tag{38}$$

for some $x_1, x_2 \in [0, \epsilon]$. (a) follows from the fact that for $x \in [0, \epsilon]$, $(x - \epsilon)\lambda \to +\infty$ when $\lambda \to -\infty$, and (b) is a result of mean value theorem for integration. This theorem states that for every continuous function $f(x)$ in the interval $[a, b]$, we have

$$\exists\ x_0 \in [a, b] \quad s.t. \quad \int_a^b f(x)dx = f(x_0)[b - a]. \tag{39}$$

Equation (38) is valid for any arbitrary $0 < \epsilon < 1$. If we choose $\epsilon \to 0$, x_1 and x_2 are both squeezed in the interval $[0, \epsilon]$. Thus, we have

$$\lim_{\lambda \to -\infty} v(\lambda) \leq \lim_{\lambda \to -\infty} \lim_{\epsilon \to 0} \frac{x_1 Q(x_1)e^{\lambda x_1}}{Q(x_2)e^{\lambda x_2}} = \lim_{\epsilon \to 0} x_1 = 0 \tag{40}$$

Based on the distribution of x, $v(\lambda)$ is obviously non-negative for any λ. Hence, the inequality in (40) can be replaced by equality.

3) By observing that $v(\lambda = 0) = \mathbb{E}\{x\}$, it is obvious that $l(\alpha = \mathbb{E}\{x\}) = 0$.

4) To show that $l(\alpha = 1) = +\infty$, we prove the equivalent statement of the form $\lim_{\lambda \to +\infty} v(\lambda) = 1$. For any $0 < \epsilon < 1$ and $x \in [1 - \epsilon, 1]$, $(x - 1 + \epsilon)\lambda \to +\infty$ when $\lambda \to +\infty$. Then, defining $\zeta = 1 - \epsilon$, we have

$$\lim_{\lambda \to +\infty} \frac{\int_0^\zeta xQ(x)e^{x\lambda}dx}{\int_0^1 Q(x)e^{x\lambda}dx} \leq \lim_{\lambda \to +\infty} \frac{\int_0^\zeta xQ(x)dx}{\int_\zeta^1 Q(x)e^{(x-\zeta)\lambda}dx} = 0. \tag{41}$$

Since the fraction in (41) is obviously non-negative for any λ, this inequality can be replaced by an equality. Similarly, we have

$$\lim_{\lambda \to +\infty} \frac{\int_0^\zeta Q(x)e^{x\lambda}dx}{\int_\zeta^1 xQ(x)e^{x\lambda}dx} \leq \lim_{\lambda \to +\infty} \frac{\int_0^\zeta Q(x)dx}{\int_\zeta^1 xQ(x)e^{(x-\zeta)\lambda}dx} = 0. \tag{42}$$

which can also be replaced by equality. Now, the limit of $v(\lambda)$ is written as

$$\begin{aligned}
\lim_{\lambda \to +\infty} v(\lambda) &= \lim_{\lambda \to +\infty} \frac{\int_0^\zeta xQ(x)e^{x\lambda}dx + \int_\zeta^1 xQ(x)e^{x\lambda}dx}{\int_0^1 Q(x)e^{x\lambda}dx} \\
&\stackrel{(a)}{=} \left(\lim_{\lambda \to +\infty} \frac{\int_0^\zeta Q(x)e^{x\lambda}dx + \int_\zeta^1 Q(x)e^{x\lambda}dx}{\int_\zeta^1 xQ(x)e^{x\lambda}dx} \right)^{-1} \\
&\stackrel{(b)}{=} \left(\lim_{\lambda \to +\infty} \frac{\int_\zeta^1 Q(x)e^{x\lambda}dx}{\int_\zeta^1 xQ(x)e^{x\lambda}dx} \right)^{-1} \\
&\stackrel{(c)}{=} \left(\lim_{\lambda \to +\infty} \frac{Q(x_1)e^{x_1\lambda}}{x_2 Q(x_2)e^{x_2\lambda}} \right)^{-1}
\end{aligned} \tag{43}$$

for some $x_1, x_2 \in [1 - \epsilon, 1]$. (a) and (b) follow from equations (41) and (42) respectively, and (c) is a result of mean value theorem for integration. If we choose $\epsilon \to 0$, x_1 and x_2 are both squeezed in the interval $[1 - \epsilon, 1]$. Then, equation (43) turns into

$$\lim_{\lambda\to+\infty} v(\lambda) \leq \lim_{\lambda\to+\infty}\lim_{\epsilon\to 0}\frac{Q(x_1)e^{x_1\lambda}}{x_2 Q(x_2)e^{x_2\lambda}} = \lim_{\epsilon\to 0}\frac{1}{x_2} = 1.$$

5) According to equations (15) and (16), derivation of $u(\alpha)$ gives us

$$\frac{\partial u(\alpha)}{\partial\alpha} = l(\alpha) + \alpha\frac{\partial l(\alpha)}{\partial\alpha} - \frac{\mathbb{E}\{xe^{\lambda x}\}}{\mathbb{E}\{e^{\lambda x}\}}\frac{\partial l(\alpha)}{\partial\alpha} = l(\alpha).$$

APPENDIX C
PROOF OF LEMMA II

Based on the definition of probability density function, we have

$$\begin{aligned}
\lim_{L\to\infty} -\frac{1}{L}\log\left(f_y(\alpha)\right) &= \lim_{L\to\infty} -\frac{1}{L}\log\left(\lim_{\delta\to\ 0}\frac{\mathbb{P}\{y>\alpha\}-\mathbb{P}\{y>\alpha+\delta\}}{\delta}\right)\\
&\geq \lim_{\delta\to\ 0}\lim_{L\to\infty}\frac{1}{L}\left[-\log\left(\mathbb{P}\{y>\alpha\}\right)+\log\delta\right]\\
&\overset{(a)}{=} u(\alpha)
\end{aligned} \tag{44}$$

where (a) follows from equation (17). The exponent of $f_y(\alpha)$ can be upper-bounded as

$$\begin{aligned}
\lim_{L\to\infty} -\frac{1}{L}\log\left(f_y(\alpha)\right) &= \lim_{\delta\to\ 0}\lim_{L\to\infty}\frac{-\log\left(\mathbb{P}\{y>\alpha\}-\mathbb{P}\{y>\alpha+\delta\}\right)+\log\delta}{L}\\
&\overset{(a)}{\leq} \lim_{\delta\to\ 0}\lim_{L\to\infty}\frac{-\log\left(e^{-L(u(\alpha)+\epsilon)}-e^{-L(u(\alpha+\delta)-\epsilon)}\right)+\log\delta}{L}\\
&= \lim_{\delta\to\ 0}\lim_{L\to\infty} u(\alpha)+\epsilon-\frac{\log\left(1-e^{-L\chi}\right)}{L}\\
&\overset{(b)}{=} u(\alpha)+\epsilon
\end{aligned} \tag{45}$$

where $\chi = u(\alpha+\delta)-u(\alpha)-2\epsilon$. Since $u(\alpha)$ is a strictly increasing function (Lemma I), we can make χ positive by choosing ϵ small enough. (a) follows from the definition of limit if L is sufficiently large, and (b) is a result of χ being positive. Making ϵ arbitrarily small, results (44) and (45) prove the lemma.

APPENDIX D
PROOF OF LEMMA III

According to the definition of infimum, we have

$$\begin{aligned}
\lim_{L\to\infty} -\frac{\log(H(L))}{L} &\geq \lim_{L\to\infty} -\frac{1}{L}\log\left(e^{-L\inf\limits_{\mathcal{S}} h(\mathbf{x})}\oint_{\mathcal{S}} d\mathbf{x}\right)\\
&\overset{(a)}{=} \inf_{\mathcal{S}} h(\mathbf{x}).
\end{aligned} \tag{46}$$

where (a) follows from the fact that $\mathcal{S}$ is a bounded region. Since $h(\mathbf{x})$ is a continuous function, it has a minimum in the bounded closed set $cl(\mathcal{S})$ which is denoted by $\mathbf{x}^\star$. Due to the continuity of $h(\mathbf{x})$ at $\mathbf{x}^\star$, for any $\epsilon>0$, there is a neighborhood $\mathcal{B}(\epsilon)$ centered at $\mathbf{x}^\star$ such that any $\mathbf{x}\in\mathcal{B}(\epsilon)$ has the property of $|h(\mathbf{x})-h(\mathbf{x}^\star)|<\epsilon$. Moreover, since $\mathcal{S}$ is a convex set, we have $\text{vol}\left(\mathcal{B}(\epsilon)\cap\mathcal{S}\right)>0$. Now we can write

$$\begin{aligned}
\lim_{L\to\infty} -\frac{\log(H(L))}{L} &\leq \lim_{L\to\infty} -\frac{1}{L}\log\left(\oint_{\mathcal{S}\cap\mathcal{B}(\epsilon)} e^{-Lh(\mathbf{x})}d\mathbf{x}\right)\\
&\leq \lim_{L\to\infty} -\frac{1}{L}\log\left(e^{-L(h(\mathbf{x}^\star)+\epsilon)}\oint_{\mathcal{S}\cap\mathcal{B}(\epsilon)} d\mathbf{x}\right)\\
&= h(\mathbf{x}^\star)+\epsilon.
\end{aligned} \tag{47}$$

Making ϵ arbitrarily small, results (46) and (47) prove the lemma.

APPENDIX E
PROOF OF LEMMA IV

According to Lemma I, $u_j(x)$ is increasing and convex for $\forall 1 \leq j \leq J$. Thus, the objective function $f(\beta) = \sum_{j=1}^{J} \gamma_j u_j(\frac{\beta_j}{\eta_j})$ is also convex, and the region $\mathcal{S}_T$ is determined by J convex inequality constraints and one affine equality constraint. Hence, in this case, KKT conditions are both necessary and sufficient for solution [31]. In other words, if there exist constants ϕ_j and ν such that

$$\frac{\gamma_j}{\eta_j} l_j(\frac{\beta_j^\star}{\eta_j}) - \phi_j - \nu = 0 \quad \forall 1 \leq j \leq J \tag{48}$$

$$\phi_j \left[\eta \mathbb{E}\{x_j\} - \beta_j^\star\right] = 0 \quad \forall 1 \leq j \leq J \tag{49}$$

then the point $\beta^\star$ is a global minimum.

Now, we prove that either $\beta_j^\star = \eta_j \mathbb{E}\{x_j\}$ for all $1 \leq j \leq J$, or $\beta_j^\star > \eta_j \mathbb{E}\{x_j\}$ for all $1 \leq j \leq J$. Let us assume the opposite is true, and there are at least two elements of the vector $\beta^\star$, indexed with k and m, which have the values of $\beta_k^\star = \eta_k \mathbb{E}\{x_k\}$ and $\beta_m^\star > \eta_m \mathbb{E}\{x_m\}$ respectively. For any arbitrary $\epsilon > 0$, the vector $\beta^{\star\star}$ can be defined as below

$$\beta_j^{\star\star} = \begin{cases} \beta_j^\star + \epsilon & \text{if } j = k \\ \beta_j^\star - \epsilon & \text{if } j = m \\ \beta_j^\star & \text{otherwise.} \end{cases} \tag{50}$$

Then, we have

$$\begin{aligned} \lim_{\epsilon \to 0} \frac{f(\beta^{\star\star}) - f(\beta^\star)}{\epsilon} &= \lim_{\epsilon \to 0} \frac{1}{\epsilon} \left\{ \gamma_k u_k \left(\frac{\beta_k^\star + \epsilon}{\eta_k} \right) + \gamma_m u_m \left(\frac{\beta_m^\star - \epsilon}{\eta_m} \right) - \gamma_m u_m \left(\frac{\beta_m^\star}{\eta_k} \right) \right\} \\ &\overset{(a)}{=} \lim_{\epsilon \to 0} \frac{\gamma_k}{\eta_k} l_k \left(\frac{\beta_k^\star + \epsilon'}{\eta_k} \right) - \frac{\gamma_m}{\eta_m} l_m \left(\frac{\beta_m^\star + \epsilon''}{\eta_m} \right) \\ &= -\frac{\gamma_m}{\eta_m} l_m \left(\frac{\beta_m^\star}{\eta_m} \right) < 0 \end{aligned} \tag{51}$$

where $\epsilon', \epsilon'' \in [0, \epsilon]$, and (a) follows from Taylor's theorem. Thus, moving from $\beta^\star$ to $\beta^{\star\star}$ decreases the function which contradicts the assumption of $\beta^\star$ being the global minimum.

Out of the remaining possibilities, the case where $\beta_j^\star = \eta_j \mathbb{E}\{x_j\}$ ($\forall 1 \leq j \leq J$) obviously agrees with Lemma IV for the special case of $\nu = 0$. Therefore, the lemma can be proved assuming $\beta_j^\star > \eta_j \mathbb{E}\{x_j\}$ ($\forall 1 \leq j \leq J$). Then, equation (49) turns into $\phi_j = 0$ ($\forall 1 \leq j \leq J$). By rearranging equation (48) and using the condition $\sum_{j=1}^{J} \beta_j = \alpha$, Lemma IV is proved.

APPENDIX F
PROOF OF THEOREM II

The parameter ν is obviously a function of the vector η. Differentiating equation (29) with respect to η_k gives us

$$\frac{\partial \nu}{\partial \eta_k} = -\frac{v_k \left(\frac{\nu \eta_k}{\gamma_k} \right) + \frac{\nu \eta_k}{\gamma_k} v_k' \left(\frac{\nu \eta_k}{\gamma_k} \right)}{\sum_{j=1}^{J} \frac{\eta_j^2}{\gamma_j} v_j' \left(\frac{\nu \eta_j}{\gamma_j} \right)} \tag{52}$$

where $v_j(x) = l_j^{-1}(x)$, and $v_j'(x)$ denotes its derivative with respect to its argument. The objective function can be simplified as

$$g(\eta) = \sum_{j=1}^{J} \gamma_j u_j(\frac{\beta_j^\star}{\eta_j}) = \sum_{j=1}^{J} \gamma_j u_j \left(v_j(\frac{\nu \eta_j}{\gamma_j}) \right). \tag{53}$$

$\nu^\star$ is defined as the value of ν corresponding to $\eta^\star$. It is easy to show that $\nu^\star > 0$. Let us assume the opposite is true ($\nu^\star \leq 0$). Then, according to Lemma I, we have $v_j(\frac{\nu^\star \eta_j}{\gamma_j}) \leq \mathbb{E}\{x_j\}$ for all j which results in $g(\eta^\star) = 0$. However, it is possible to achieve a positive value of $g(\eta)$ by setting $\eta_j = 1$ for the one vector which has the property of $\mathbb{E}\{x_j\} < \alpha$, and setting $\eta_j = 0$ for the rest. Thus, $\eta^\star$ can not be the maximal point. This contradiction proves the fact that $\nu^\star > 0$.

At the first step, we prove that $\eta_j^\star > 0$ if $\mathbb{E}\{x_j\} < \alpha$. Assume the opposite is true for an index $1 \leq k \leq J$. Since $\sum_{j=1}^{J} \eta_j^\star = 1$, there should be at least one index m such that $\eta_m^\star > 0$. For any arbitrary $\epsilon > 0$, the vector $\eta^{\star\star}$ can be defined as below

$$\eta_j^{\star\star} = \begin{cases} \epsilon & \text{if } j = k \\ \eta_j^\star - \epsilon & \text{if } j = m \\ \eta_j^\star & \text{otherwise.} \end{cases} \tag{54}$$

$\nu^{\star\star}$ is defined as the corresponding value of ν for the vector $\eta^{\star\star}$. Based on equation (52), we can write

$$\begin{aligned} \Delta\nu &= \nu^{\star\star} - \nu^\star \qquad (55) \\ &= \frac{v_m\left(\frac{\nu^\star \eta_m^\star}{\gamma_m}\right) + \frac{\nu^\star \eta_m^\star}{\gamma_m} v_m'\left(\frac{\nu^\star \eta_m^\star}{\gamma_m}\right) - \mathbb{E}\{x_k\}}{\sum_{j=1}^{J} \frac{\eta_j^{\star 2}}{\gamma_j} v_j'\left(\frac{\nu^\star \eta_j^\star}{\gamma_j}\right)} \epsilon + O(\epsilon^2). \end{aligned}$$

Then, we have

$$\begin{aligned} \lim_{\epsilon \to 0} \frac{g(\eta^{\star\star}) - g(\eta^\star)}{\epsilon} &= \lim_{\epsilon \to 0} \frac{1}{\epsilon} \left\{ \frac{\nu^{\star 2} \eta_k^\star}{\gamma_k} v_k'\left(\frac{\nu^\star \eta_k^\star}{\gamma_k}\right) \epsilon - \frac{\nu^{\star 2} \eta_m^\star}{\gamma_m} v_m'\left(\frac{\nu^\star \eta_m^\star}{\gamma_m}\right) \epsilon + \nu^\star \Delta\nu \sum_{j=1}^{J} \frac{\eta_j^{\star 2}}{\gamma_j} v_j'\left(\frac{\nu^\star \eta_j^\star}{\gamma_j}\right) + O(\epsilon^2) \right\} \\ &\overset{(a)}{=} \nu^\star \left\{ v_m\left(\frac{\nu^\star \eta_m^\star}{\gamma_m}\right) - \mathbb{E}\{x_k\} \right\} \end{aligned} \tag{56}$$

where (a) follows from (55). If the value of (56) is positive for an index m, moving in that direction increases the objective function which contradicts with the assumption of $\eta^\star$ being a maximal point . If the value of (56) is non-positive for all indexes m whose $\eta_m^\star > 0$, we can write

$$\mathbb{E}\{x_k\} \geq \sum_{m=1}^{J} \eta_m^\star v_m\left(\frac{\nu^\star \eta_m^\star}{\gamma_m}\right) = \alpha \tag{57}$$

which obviously contradicts the assumption of $\mathbb{E}\{x_k\} < \alpha$.

At the second step, we prove that $\eta_j^\star = 0$ if $\mathbb{E}\{x_j\} \geq \alpha$. Assume the opposite is true for an index $1 \leq r \leq J$. Since $\sum_{j=1}^{J} \eta_j^\star = 1$, we should have $\eta_s^\star < 1$ for all other indices s. For any arbitrary $\epsilon > 0$, the vector $\eta^{\star\star\star}$ can be defined as below

$$\eta_j^{\star\star\star} = \begin{cases} \eta_j^\star - \epsilon & \text{if } j = r \\ \eta_j^\star + \epsilon & \text{if } j = s \\ \eta_j^\star & \text{otherwise.} \end{cases} \tag{58}$$

$\nu^{\star\star\star}$ is defined as the corresponding value of ν for the vector $\eta^{\star\star\star}$. Based on equation (52), we can write

$$\begin{aligned} \Delta\nu &= \nu^{\star\star\star} - \nu^\star \\ &= \frac{v_r\left(\frac{\nu^\star \eta_r^\star}{\gamma_r}\right) + \frac{\nu^\star \eta_r^\star}{\gamma_r} v_r'\left(\frac{\nu^\star \eta_r^\star}{\gamma_r}\right) - v_s\left(\frac{\nu^\star \eta_s^\star}{\gamma_s}\right) - \frac{\nu^\star \eta_s^\star}{\gamma_s} v_s'\left(\frac{\nu^\star \eta_s^\star}{\gamma_s}\right)}{\sum_{j=1}^{J} \frac{\eta_j^{\star 2}}{\gamma_j} v_j'\left(\frac{\nu^\star \eta_j^\star}{\gamma_j}\right)} \epsilon + O(\epsilon^2). \end{aligned} \tag{59}$$

Then, we have

$$\lim_{\epsilon\to 0}\frac{g(\eta^{\star\star\star})-g(\eta^{\star})}{\epsilon} = \lim_{\epsilon\to 0}\frac{1}{\epsilon}\left\{\frac{\nu^{\star 2}\eta_s^{\star}}{\gamma_s}v_s'\left(\frac{\nu^{\star}\eta_s^{\star}}{\gamma_s}\right)\epsilon-\frac{\nu^{\star 2}\eta_r^{\star}}{\gamma_r}v_r'\left(\frac{\nu^{\star}\eta_r^{\star}}{\gamma_r}\right)\epsilon+\ \nu^{\star}\Delta\nu\sum_{j=1}^{J}\frac{\eta_j^{\star 2}}{\gamma_j}v_j'\left(\frac{\nu^{\star}\eta_j^{\star}}{\gamma_j}\right)+O(\epsilon^2)\right\}$$
$$\stackrel{(a)}{=} \nu^{\star}\left\{v_r\left(\frac{\nu^{\star}\eta_r^{\star}}{\gamma_r}\right)-v_s\left(\frac{\nu^{\star}\eta_s^{\star}}{\gamma_s}\right)\right\} \tag{60}$$

where (a) follows from (59). If the value of (60) is positive for an index s, moving in that direction increases the objective function which contradicts with the assumption of $\eta^{\star}$ being a maximal point . If the value of (60) is non-positive for all indices s whose $\eta_s^{\star}>0$, we can write

$$\mathbb{E}\{x_r\}<v_r\left(\frac{\nu^{\star}\eta_r^{\star}}{\gamma_r}\right)\le\sum_{s=1}^{J}\eta_s^{\star}v_s\left(\frac{\nu^{\star}\eta_s^{\star}}{\gamma_s}\right)=\alpha \tag{61}$$

which obviously contradicts the assumption of $\mathbb{E}\{x_r\}\ge\alpha$.

Now that the boundary points are checked, we can safely use the KKT conditions [31] for all $1\le k\le J$ where $\mathbb{E}\{x_k\}<\alpha$ to find the maximum η.

$$\zeta = \frac{\nu^{\star 2}\eta_k^{\star}}{\gamma_k}v_k'\left(\frac{\nu^{\star}\eta_k^{\star}}{\gamma_k}\right)+\nu^{\star}\sum_{j=1}^{J}\frac{\eta_j^{\star 2}}{\gamma_j}v_j'\left(\frac{\nu^{\star}\eta_j^{\star 2}}{\gamma_j}\right)\frac{\partial\nu}{\partial\eta_k}|_{\nu=\nu^{\star}}$$
$$\stackrel{(a)}{=} -\nu^{\star}v_k\left(\frac{\nu^{\star}\eta_k^{\star}}{\gamma_k}\right) \tag{62}$$

where ζ is a constant independent of k, and (a) follows from (52). Using the fact that $\sum_{j=1}^{J}\eta_j=1$ with equations (29) and (62) gives us

$$\zeta=-\alpha\nu^{\star}$$
$$\nu^{\star}=\sum_{\mathbb{E}\{x_j\}<\alpha}\gamma_j l_j(\alpha). \tag{63}$$

Combining equations (62) and (63) proves the theorem.

Appendix G

Discrete Analysis of One Path

$Q(n,k,l)$ is defined as the probability of having exactly k errors out of the n packets sent over the path l. Since we temporarily focus on one path, the index l can be dropped in this section. Depending on the initial state of the channel, $P_g(n,k)$ and $P_b(n,k)$ are defined as the probabilities of having k errors out of the n packets when we start the transmission in good or bad states respectively. It is easy to see

$$Q(n,k)=\pi_g P_g(n,k)+\pi_b P_b(n,k). \tag{64}$$

$P_g(n,k)$ and $P_b(n,k)$ can be computed from the following recursive equations

$$P_b(n,k) = \pi_{b|b}P_b(n-1,k-1)+\pi_{g|b}P_g(n-1,k-1)$$
$$P_g(n,k) = \pi_{b|g}P_b(n-1,k)+\pi_{g|g}P_g(n-1,k) \tag{65}$$

with the initial conditions

$$P_g(n,k)=0 \qquad \text{for } k\le n$$
$$P_b(n,k)=0 \qquad \text{for } k>n$$
$$P_g(n,k)=0 \qquad \text{for } k<0$$
$$P_b(n,k)=0 \qquad \text{for } k\le 0 \tag{66}$$

where $\pi_{s_2|s_1}$ is the probability of the channel being is in the state $s_2 \in \{g, b\}$ provided that it has been in the state $s_1 \in \{g, b\}$ when the last packet was transmitted. $\pi_{s_2|s_1}$ has the following values for different combinations of s_1 and s_2 [1]

$$\begin{aligned} \pi_{g|g} &= \pi_g + \pi_b \, e^{-\dfrac{\mu_g + \mu_b}{S_l}} \\ \pi_{b|g} &= 1 - \pi_{g|g} \\ \pi_{b|b} &= \pi_b + \pi_g \, e^{-\dfrac{\mu_g + \mu_b}{S_l}} \\ \pi_{g|b} &= 1 - \pi_{b|b} \end{aligned} \tag{67}$$

where S_l denotes the transmission rate on path l.

The recursive equations (65) can be solved with the complexity of $O\left(k(n-k)\right)$ which give us $Q(n, k, l)$ according to equation (64).

Appendix H
Discrete Analysis of One Type

When there are n packets to be distributed over L_j identical paths of type j, even distribution is obviously the the optimum allocation. However, since the integer n may be indivisible by L_j, the L_j dimentional vector $\mathbf{N}$ is defined as below

$$N_l = \begin{cases} \lfloor \dfrac{n}{L_j} \rfloor + 1 & \text{for } 1 \leq l \leq \text{Rem}(n, L_j) \\ \\ \lfloor \dfrac{n}{L_j} \rfloor & \text{for Rem}(n, L_j) < l \leq L_j \end{cases} \tag{68}$$

where $\text{Rem}(a, b)$ denotes the remainder of dividing a by b. $\mathbf{N}$ represents the closest integer vector to even distribution.

$E^{\mathbf{N}}(k, l)$ is defined as the probability of having exactly k erasures among the n packets transmitted over the identical paths 1 to l with the allocation vector $\mathbf{N}$. $E^{\mathbf{N}}(k, l)$ can be computed recursively as

$$\begin{aligned} E^{\mathbf{N}}(k, l) &= \sum_{i=0}^{k} E^{\mathbf{N}}(k-i, l-1) Q(N_l, i, l) \\ E^{\mathbf{N}}(k, 1) &= Q(N_1, k, 1) \end{aligned} \tag{69}$$

where $Q(n, k, l)$ is defined in appendix G and shown to be computed with the complexity of $O(k(n-k))$. According to the definitions, it is obvious that $Q_j(n, k) = E^{\mathbf{N}}(k, L_j)$ which can be calculated with the complexity of $O(k^2 n)$ using dynamic programming.

APPENDIX I
PROOF OF LEMMA V

The lemma is proved by induction on j. The case of $j = 1$ is obviously true as $\hat{P}_e(n, k, 1) = P_e^{opt}(n, k, 1)$. Let us assume this statement is true for $j = 1$ to $J - 1$. Then for $j = J$, we have

$$\begin{aligned}
& \hat{P}_e(n, k, J) \\
\overset{(a)}{\leq} \quad & \sum_{i=0}^{N_J} Q_J(N_J^{opt}, i)\hat{P}_e(n - N_J^{opt}, k - i, J - 1) \\
\overset{(b)}{\leq} \quad & \sum_{i=0}^{N_J} Q_J(N_J^{opt}, i)P_e^{opt}(n - N_J^{opt}, k - i, J - 1) \\
\overset{(c)}{\leq} \quad & \sum_{i=0}^{N_J} Q_J(N_J^{opt}, i)P_e^{\mathbf{N}^{opt}}(k - i, J - 1) \\
\overset{(d)}{=} \quad & P_e^{\mathbf{N}^{opt}}(k, J) = P_e^{opt}(n, k, J)
\end{aligned}$$

where $\mathbf{N}^{opt}$ denotes the optimum allocation of n packets among the J types of paths. (a) follows from the recursive equation (32), and (b) is the induction assumption. (c) comes from the definition of $P_e^{opt}(n, k, l)$, and (d) is a result of equation (33).

APPENDIX J
PROOF OF THEOREM III

First, we compute the asymptotic behavior of $Q_j(n, k)$, for n growing proportionally to L_j $(n = n'L_j)$ and $k > n\mathbb{E}\{x_j\}$. Here, we can apply Sanov Theorem [28], [32] as n and k are discrete variables and n' is constant.

Sanov's Theorem. Let $X_1, X_2, \ldots, X_n$ be i.i.d. discrete random variables from an alphabet set $\mathcal{X}$ with the size of $|\mathcal{X}|$ and probability mass function (pmf) $Q(x)$. Let $\mathcal{P}$ denote the set of pmf's in $\mathbb{R}^{|\mathcal{X}|}$, i.e. $\mathcal{P} = \left\{\mathbf{P} \in \mathbb{R}^{|\mathcal{X}|} |\ P(i) \geq 0,\ \sum_{i=1}^{|\mathcal{X}|} P(i) = 1\right\}$. Also, let $\mathcal{P}_n$ denote the subset of $\mathcal{P}$ corresponding to all possible empirical distributions of $\mathcal{X}$ in n observations [32], i.e. $\mathcal{P}_n = \{\mathbf{P} \in \mathcal{P}|\ \forall i,\ nP(i) \in \mathbb{Z}\}$. For any dense and closed set [30] of pmf's $E \subseteq \mathcal{P}$, the probability that the empirical distribution of n observations belongs to the set E is equal to

$$\mathbb{P}\{E\} = \mathbb{P}\{E \cap \mathcal{P}_n\} \doteq e^{-nD(\mathbf{P}^\star||\mathbf{Q})} \tag{70}$$

where $\mathbf{P}^\star = \underset{\mathbf{P} \in E}{\operatorname{argmin}} D(\mathbf{P}||\mathbf{Q})$ and $D(\mathbf{P}||\mathbf{Q}) = \sum_{i=1}^{|\mathcal{X}|} P(i) \log \frac{P(i)}{Q(i)}$.

Going back to our problem, assume that $\mathbf{P}$ is defined as the empirical distribution of the number of errors in each path, i.e. $\forall i,\ 1 \leq i \leq n',\ P(i)$ shows the ratio of the total paths which contain exactly i lost packets. Similarly, $\forall i,\ 1 \leq i \leq n',\ Q(i)$ denotes the probability of exactly i packets being lost out of the n' packets trasnmitted on a path of type j. The sets E, E_{out} are also defined as follows

$$\begin{aligned}
E \quad &= \quad \{\mathbf{P} \in \mathcal{P}| \sum_{i=0}^{n'} iP(i) \geq \beta\} \qquad (71) \\
E_{out} \quad &= \quad \{\mathbf{P} \in \mathcal{P}| \sum_{i=0}^{n'} iP(i) = \beta\}
\end{aligned}$$

where $\beta = \dfrac{k}{n}$. Knowing E and E_{out} are dense sets, we can compute $Q_j(n, k)$ as

$$Q_j(n, k) \overset{(a)}{=} \mathbb{P}\{E_{out}\} \overset{(b)}{\doteq} e^{-L_j \underset{\mathbf{P} \in E_{out}}{\min} D(\mathbf{P}||\mathbf{Q})} \overset{(c)}{\doteq} e^{-L_j \underset{\mathbf{P} \in E}{\min} D(\mathbf{P}||\mathbf{Q})} \overset{(d)}{\doteq} e^{-\gamma_j L u_j(\frac{k}{n})} \tag{72}$$

where (a) follows from the definition of $Q_j(n,k)$, and (b) results from the Sanov Theorem. Knowing the fact that the Kullback Leibler distance $D(\mathbf{P},\mathbf{Q})$ is a convex function of $\mathbf{P},\mathbf{Q}$ [32], we conclude that its minimum over the convex set E either lies on an interior point which is a global minimum of the function over the whole set $\mathcal{P}$ or is located on the boundry of E. However, we know that the global minimum of Kullback Leibler distance occurs at $\mathbf{P}=\mathbf{Q}\notin E$. This results in (c). Finally, (d) follows from (17).

1) We prove the first part of the theorem by induction on J. When $J=1$, the statement is correct for both cases of $\frac{K}{N}>\mathbb{E}\{x_1\}$ and $\frac{K}{N}\leq\mathbb{E}\{x_1\}$, remembering the fact that $\hat{P}_e(n,k,1)=P_e^{opt}(n,k,1)$ and $u_1(x)=0$ for $x\leq\mathbb{E}\{x_1\}$.

Now, Lut us assume the first part of the theorem is true for $j=1$ to $J-1$. We try to prove the same statemenet for J as well. The proof can be divided to two different cases, depending on whether $\frac{K}{N}$ is larger than $\mathbb{E}\{x_J\}$ or vice versa.

1.1) $\dfrac{K}{N}>\mathbb{E}\{x_J\}$

According to the definition, the value of $\hat{P}_e(n,k,J)$ is computed by taking a minimization over n_J. Now, we show that for any value of n_J, the corresponding term in the minimization is asymptotically at least equal to $P_e^{opt}(n,k,J)$.

First, we show the statement for $\epsilon L\leq n_J\leq N(1-\epsilon)$ and any constant $\epsilon\leq\min\left\{\gamma_j,1-\frac{K}{N}\right\}$. Defining $i_J=\lfloor n_J\frac{K}{N}\rfloor$, we have

$$\begin{aligned}\frac{i_J}{n_J}&=\frac{K}{N}+O(\frac{1}{L}),\\ \frac{K-i_J}{N-n_J}&=\frac{K}{N}+O(\frac{1}{L})\end{aligned}\tag{73}$$

as ϵ is constant and $K,N=O(L)$. Hence, we have

$$\begin{aligned}\sum_{i=0}^{n_J}Q_J(n_J,i)\hat{P}_e(N-n_J,K-i,J-1)&\geq Q_J(n_J,i_J)\hat{P}_e(N-n_J,K-i_J,J-1)\\ &\overset{(a)}{\doteq} e^{-L\sum_{j=1}^{J}\gamma_j u_j\left(\frac{K}{N}+O\left(\frac{1}{L}\right)\right)}\\ &\overset{(b)}{\doteq} e^{-L\sum_{j=1}^{J}\gamma_j u_j\left(\frac{K}{N}\right)}\end{aligned}\tag{74}$$

where (a) follows from (72) and the induction assumption, and (b) follows from the fact that u_j's are differentiable functions.

For $0\leq n_J\leq\epsilon L$, since $\epsilon<\gamma_j$, the number of packets assigned to the paths of type J is less that the number of such paths. Thus, one packet is allocated to n_J of the paths, and the rest of the paths of type J are not used. Defining $\pi_{b,J}$ as the probability of a path of type J being in the bad state, we can write

$$Q_J(n_J,n_J)=\pi_{b,J}^{n_J}=e^{-n_J\log\left(\frac{1}{\pi_{b,J}}\right)}.\tag{75}$$

Therefore, for $0 \leq n_J \leq \epsilon L$, we have

$$
\begin{aligned}
\sum_{i=0}^{n_J} Q_J(n_J, i)\hat{P}_e(N-n_J, K-i, J-1) &\geq Q_J(n_J, n_J)\hat{P}_e(N-n_J, K-n_J, J-1) \\
&\doteq e^{-L\sum_{j=1}^{J-1}\gamma_j u_j\left(\frac{K-n_J}{N-n_J}\right) - n_J \log\left(\frac{1}{\pi_{b,J}}\right)} \\
&\overset{(a)}{\geq} e^{-L\epsilon\log\left(\frac{1}{\pi_{b,J}}\right) - L\sum_{j=1}^{J-1}\gamma_j u_j\left(\frac{K}{N}\right)} \\
&\overset{(b)}{\doteq} e^{-L\sum_{j=1}^{J-1}\gamma_j u_j\left(\frac{K}{N}\right)} \geq e^{-L\sum_{j=1}^{J}\gamma_j u_j\left(\frac{K}{N}\right)}
\end{aligned} \tag{76}
$$

where (a) follows from the fact that $\frac{K-n_J}{N-n_J} \leq \frac{K}{N}$, and (b) results from the fact that we can put ϵ as small as possible.

Finally, we prove the statement for the case $n_J > N(1-\epsilon)$. In this case, we have

$$
\begin{aligned}
\sum_{i=0}^{n_J} Q_J(n_J, i)\hat{P}_e(N-n_J, K-i, J-1) &\geq Q_J(n_J, K)\hat{P}_e(N-n_J, 0, J-1) \\
&\overset{(a)}{\geq} e^{-L\gamma_J u_J\left(\frac{K}{N(1-\epsilon)}\right)} \\
&\overset{(b)}{\dot{\geq}} e^{-L\sum_{j=1}^{J}\gamma_j u_j\left(\frac{K}{N}\right)}
\end{aligned} \tag{77}
$$

where (a) follows from the fact that ϵ is small enough such that $\epsilon < 1 - \frac{K}{N}$ and the fact that $\hat{P}_e(n, 0, j) = 1$, for all n, j, and putting ϵ small enough results in (b).

Inequalities (74), (76), and (77) result in

$$
\hat{P}_e(N, K, J) \;\dot{\geq}\; e^{-L\sum_{j=1}^{J}\gamma_j u_j(\alpha)} \tag{78}
$$

Combining (78) with Lemma V proves the first part of Theorem III for the case when $\frac{K}{N} > \mathbb{E}\{x_J\}$.

1.2) $\frac{K}{N} \leq \mathbb{E}\{x_J\}$

For any $0 < \epsilon < \min\left\{\gamma_J, 1 - \frac{K}{N}\right\}$ and for all values of $\epsilon L < n_J \leq N(1-\epsilon)$, we define i_J as $i_J = \lceil n_J \mathbb{E}\{x_J\}\rceil$. We have

$$
\begin{aligned}
\frac{i_J}{n_J} &= \mathbb{E}\{x_J\} + O\left(\frac{1}{L}\right) \geq \mathbb{E}\{x_J\} \\
\frac{K-i_J}{N-n_J} &< \frac{K}{N} + O\left(\frac{1}{L}\right)
\end{aligned} \tag{79}
$$

Hence,

$$
\begin{aligned}
\sum_{i=0}^{n_J} Q_J(n_J, i)\hat{P}_e(N-n_J, K-i, J-1) &\geq Q_J(n_J, i_J)\hat{P}_e(N-n_J, K-i_J, J-1) \\
&\overset{(a)}{\doteq} e^{-L\gamma_J u_J(\mathbb{E}\{x_J\}) - L\sum_{j=1}^{J-1}\gamma_j u_j\left(\frac{K-i_J}{N-n_J}\right)} \\
&\overset{(b)}{\geq} e^{-L\gamma_J u_J(\mathbb{E}\{x_J\}) - L\sum_{j=1}^{J-1}\gamma_j u_j\left(\frac{K}{N} + O\left(\frac{1}{L}\right)\right)} \\
&\overset{(c)}{\doteq} e^{-L\sum_{j=1}^{J}\gamma_j u_j\left(\frac{K}{N}\right)}
\end{aligned} \tag{80}
$$

where (a) follows from (72) and the induction assumption. (b) is based on (79), and (c) results from $u_J\left(\mathbb{E}\{x_J\}\right)=0$.

For $0 \le n_J \le \epsilon L$, the analysis of section 1.1 and inequality (76) are still valid. For $n_J > (1-\epsilon)N$, we set $i_J = \lceil \mathbb{E}\left\{x_J\right\} n_J \rceil$. Now, we can write

$$\begin{aligned} \sum_{i=0}^{n_J} Q_J(n_J,i)\hat{P}_e(N-n_J,K-i,J-1) &\geq Q_J(n_J,i_J)\hat{P}_e(N-n_J,K-i_J,J-1) \\ &\overset{(a)}{\geq} e^{-L\gamma_J u_J\left(\mathbb{E}\left\{x_J\right\}+\frac{1}{(1-\epsilon)L}\right)} \\ &\doteq 1 \end{aligned} \tag{81}$$

where (a) follows from the fact that $K \le \mathbb{E}\left\{x_J\right\} n_J$ and the fact that $\hat{P}_e(n,k,j)=1$, for $k \le 0$.

Hence, inequalities (76), (80), and (81) result in

$$\hat{P}_e(N,K,J) \;\dot{\geq}\; e^{-L\sum_{j=1}^{J}\gamma_j u_j(\alpha)} \tag{82}$$

which proves the first part of Theorem III for the case of $\frac{K}{N} \le \mathbb{E}\{x_J\}$ when combined with Lemma V.

2) We prove the second and the third parts of the theorem by induction on j while the total number of path types, J, is fixed. The proof of the statements for the base of the induction, $j=J$, is similar to the proof of the induction step, from $j+1$ to j. Hence, we just give the proof for the induction step. Assume the second and third parts of the theorem are true for $m=J$ to $j+1$. We prove the same statemenets for j. The proof is divided into two different cases, depending on whether $\frac{K}{N}$ is larger than $\mathbb{E}\{x_J\}$ or vice versa.

Before we proceed further into the proofs, it is helpful to introduce two new parameters N' and K' as

$$\begin{aligned} N' &= N - \sum_{m=j+1}^{J} \hat{N}_j \\ K' &= K - \sum_{m=j+1}^{J} K_j. \end{aligned}$$

According to the above definitions and the induction assumptions, it is obvious that

$$\frac{K'}{N'} = \frac{K}{N} + o(1) = \alpha + o(1).$$

2.1) $\dfrac{K}{N} > \mathbb{E}\{x_j\}$

First, by contradiction, it will be shown that for small enough values of $\epsilon > 0$, we have $\hat{N}_j > \epsilon N'$. Let us assume the opposite is true ($\hat{N}_j \le \epsilon L$). Then, we can write

$$\begin{aligned} \hat{P}_e(N',K',j) &\overset{(a)}{=} \sum_{i=0}^{\hat{N}_j} \hat{P}_e(N'-\hat{N}_j,K'-i,j-1)Q_j(\hat{N}_j,i) \\ &\geq \hat{P}_e(N'-\hat{N}_j,K',j-1)Q_j(\hat{N}_j,\hat{N}_j) \\ &\overset{(b)}{\doteq} Q_j(\hat{N}_j,\hat{N}_j)e^{-L\sum_{r=1}^{j-1}\gamma_r u_r\left(\frac{K'-\hat{N}_j}{N'-\hat{N}_j}\right)} \\ &\overset{(c)}{\geq} e^{-Ln_0\left(1-\sum_{r=j+1}^{J}\eta_r\right)\epsilon\log\left(\frac{1}{\pi_{b,j}}\right)-L\sum_{r=1}^{j-1}\gamma_r u_r\left(\frac{K'}{N'}\right)} \\ &\overset{(d)}{\dot{>}} e^{-L\sum_{r=1}^{j}\gamma_r u_r(\alpha)} \end{aligned} \tag{83}$$

where (a) follows from equation (33) and step (2) of our suboptimal algorithm, (b) is resulted from the first part of Theorem III, and (c) can be justified with similar arguments to those of inequality (76). (d) is obtained assuming ϵ is small enough such that the corresponding term in the exponent is stricly less than $L\gamma_j u_j\left(\frac{K'}{N'}\right)$ and also the fact that $\frac{K'}{N'} = \alpha + o(1)$. The result (83) is obviously in contradiction with the first part of Theorem III, proving that $\hat{N}_j > \epsilon L$.

Now, we show that for the small enough values of ϵ, if $\hat{N}_j > (1-\epsilon)N'$ happens, for all the other types of paths $1 \leq r \leq j-1$, we have $\mathbb{E}\{x_r\} > \alpha$. In such a case, we observe $\frac{\hat{N}_j}{N'} = 1 + o(1)$, verifying Theorem III. Let us assume $\hat{N}_j > (1-\epsilon)N'$. Hence,

$$\begin{aligned}\hat{P}_e(N', K', j) &= \sum_{i=0}^{\hat{N}_j} \hat{P}_e(N' - \hat{N}_j, K' - i, j-1) Q_j(\hat{N}_j, i) \\ &\dot{\geq} \hat{P}_e(N' - \hat{N}_j, 0, j-1) Q_j(\hat{N}_j, K') \\ &\overset{(a)}{\doteq} e^{-L\gamma_j u_j\left(\frac{K'}{(1-\epsilon)N'}\right)}\end{aligned} \tag{84}$$

where (a) follows from the fact that $\hat{P}_e(n, 0, j) = 1$, for all values of n, j, and the fact that $\hat{N}_j \geq (1-\epsilon)N'$. Applying (84) and knowing the fact that $\hat{P}_e(N', K', j) \doteq e^{-L\sum_{r=1}^{j}\gamma_r u_r(\alpha)}$, we conclude $\mathbb{E}\{x_r\} > \alpha$, for all values of $1 \leq r \leq j-1$.

$\hat{P}_e(N', K', j)$ can be written as

$$\begin{aligned}\hat{P}_e(N', K', j) &= \min_{0 \leq N_j \leq N'} \sum_{i=0}^{N_j} \hat{P}_e(N' - N_j, K' - i, j-1) Q_j(N_j, i) \\ &\overset{(a)}{\doteq} \min_{\epsilon N' \leq N_j \leq (1-\epsilon)N'} \max_{\mathbb{E}\{x_j\}N_j < i \leq N_j} e^{-L\gamma_j u_j\left(\frac{i}{N_j}\right) - L\sum_{r=1}^{j-1}\gamma_r u_r\left(\frac{K'-i}{N'-N_j}\right)} \\ &\doteq e^{-L \max_{\epsilon N' \leq N_j \leq (1-\epsilon)N'} \min_{\mathbb{E}\{x_j\}N_j < i \leq N_j} \gamma_j u_j\left(\frac{i}{N_j}\right) + \sum_{r=1}^{j-1}\gamma_r u_r\left(\frac{K'-i}{N'-N_j}\right)} \\ &\overset{(b)}{\doteq} e^{-L \max_{\epsilon \leq \lambda_j \leq (1-\epsilon)} \min_{\mathbb{E}\{x_j\}\lambda_j < \beta_j \leq \lambda_j} \gamma_j u_j\left(\frac{\beta_j}{\lambda_j}\right) + \sum_{r=1}^{j-1}\gamma_r u_r\left(\frac{\alpha-\beta_j}{1-\lambda_j}\right)}.\end{aligned} \tag{85}$$

Here, (a) follows from the fact that $\hat{N}_j$ is bounded as $\epsilon N' \leq \hat{N}_j \leq (1-\epsilon)N'$, and that for values of $i < \mathbb{E}\{x_j\}N_j$, we have $Q_j(N_j, i) \dot{\leq} Q_j(N_j, \mathbb{E}\{x_j\}N_j) \doteq 1$ and $P_e(n, k, j)$ is a decreasing function of k. β_j and λ_j are defined as $\beta_j = \frac{i}{N'}$ and $\lambda_j = \frac{N_j}{N'}$. (b) follows from the fact that for any real values of $\left(\beta_j^0, \lambda_j^0\right)$, the term corresponding to $\left(i^0 = \lfloor \beta_j N' \rfloor, N_j^0 = \lfloor \lambda_j N' \rfloor\right)$ is exponentially equal to the term corresponding to $\left(\beta_j^0, \lambda_j^0\right)$. Hence, the discrte to continuous relaxation is valid.

Let us define $\left(\beta_j^*, \lambda_j^*\right)$ as the values of (β_j, λ_j) which solve the max-min problem in (85). Differentiating the exponent in equation (85) with respect to β_j and λ_j gives us

$$\begin{aligned}\frac{\gamma_j}{\lambda_j^*} l_j\left(\frac{\beta_j^*}{\lambda_j^*}\right) - \sum_{\substack{r=1,\\ \mathbb{E}\{x_r\}<\zeta}}^{j-1} \frac{\gamma_r}{1-\lambda_j^*} l_r(\zeta) &= 0 \\ -\frac{\gamma_j \beta_j^*}{\lambda_j^{*2}} l_j\left(\frac{\beta_j^*}{\lambda_j^*}\right) + \sum_{\substack{r=1,\\ \mathbb{E}\{x_r\}<\zeta}}^{j-1} \frac{\gamma_r(\alpha - \beta_j^*)}{(1-\lambda_j^*)^2} l_r(\zeta) + \left(\frac{\gamma_j}{\lambda_j^*} l_j\left(\frac{\beta_j^*}{\lambda_j^*}\right) - \sum_{\substack{r=1,\\ \mathbb{E}\{x_r\}<\zeta}}^{j-1} \frac{\gamma_r}{1-\lambda_j^*} l_r(\zeta)\right) \frac{\partial \beta_j^*}{\partial \lambda_j}\Big|_{\lambda_j=\lambda_j^*} &= 0\end{aligned} \tag{86}$$

where $\zeta = \dfrac{\alpha - \beta_j^*}{1-\lambda_j^*}$. Solving the above equations gives the unique optimmum solution (β_j^*, λ_j^*) as

$$\begin{aligned} \beta_j^* &= \alpha\lambda_j^* \\ \lambda_j^* &= \frac{\gamma_j l_j(\alpha)}{\displaystyle\sum_{r=1,\alpha>\mathbb{E}\{x_r\}}^{j} l_r(\alpha)} \end{aligned} \tag{87}$$

Hence, the integer parameters $K_j, \hat{N}_j$ defined in the suboptimal algorithm has to satisfy $\frac{K_j}{N'} = \beta_j^* + o(1)$ and $\frac{\hat{N}_j}{N'} = \lambda_j^* + o(1)$, respectively. Based on the induction assumption, it is easy to show that

$$\frac{N'}{N} = \frac{\displaystyle\sum_{r=1,\mathbb{E}\{x_r\}<\alpha}^{j} \gamma_r u_r(\alpha)}{\displaystyle\sum_{r=1,\mathbb{E}\{x_r\}<\alpha}^{J} \gamma_r u_r(\alpha)} \tag{88}$$

which completes the proof for the case of $\mathbb{E}\{x_j\} < \frac{K}{N}$.

2.2) $\dfrac{K}{N} \leq \mathbb{E}\{x_j\}$

In this case, we show that $\frac{\hat{N}_j}{N} = o(1)$. Defining $i_j = \lceil \mathbb{E}\{x_j\}\hat{N}_j \rceil$, we have

$$\frac{K' - i_j}{N' - \hat{N}_j} = \alpha - (\mathbb{E}\{x_j\} - \alpha)\frac{\hat{N}_j}{N' - \hat{N}_j} + o(1). \tag{89}$$

Now, we have

$$\begin{aligned} \hat{P}_e(N', K', j) &= \sum_{i=0}^{\hat{N}_j} \hat{P}_e(N' - \hat{N}_j, K' - i, j-1) Q_j(\hat{N}_j, i) \\ &\geq \hat{P}_e(N' - \hat{N}_j, K' - i_j, j-1) Q_j(\hat{N}_j, i_j) \\ &\overset{(a)}{\doteq} e^{-L\gamma_j u_j\left(\mathbb{E}\{x_j\} + o(1)\right) - L\sum_{r=1}^{j-1}\gamma_r u_r\left(\alpha - (\mathbb{E}\{x_j\} - \alpha)\frac{\hat{N}_j}{N' - \hat{N}_j}\right)} \\ &\doteq e^{-L\sum_{r=1}^{j-1}\gamma_r u_r\left(\alpha - (\mathbb{E}\{x_j\} - \alpha)\frac{\hat{N}_j}{N' - \hat{N}_j}\right)} \end{aligned} \tag{90}$$

where (a) follows from the first part of Theorem III and (72). On the other hand, according to the result of the first part of Theorem III, we know

$$\hat{P}_e(N', K', j) \doteq e^{-L\sum_{r=1}^{j-1}\gamma_r u_r(\alpha)}. \tag{91}$$

Comparing (90) and (91) and knowing that $\mathbb{E}\{x_j\} > \alpha$, we conclude $\frac{\hat{N}_j}{N'} = o(1)$. Noting (88), we have $\frac{\hat{N}_j}{N} = o(1)$ which proves the theorem.

References

[1] J.C. Bolot, S. Fosse-Parisis, and D. Towsley, "Adaptive FEC-based error control for Internet telephony," in *IEEE INFOCOM, Proc. IEEE Vol. 3*, 1999, pp. 1453–1460.

[2] T. Nguyen and A. Zakhor, "Multiple Sender Distributed Video Streaming," *IEEE transactions on multimedia*, vol. 6, no. 2, pp. 315– 326, 2004.

[3] H. Han, S. Shakkottai, C.V. Hollot, R. Srikant, and D. Towsley, "Multi-Path TCP: A Joint Congestion Control and Routing Scheme to Exploit Path Diversity in the Internet," *IEEE/ACM Transactions on Networking*, vol. 14, no. 6, pp. 1260 – 1271, 2006.

[4] T. Nguyen and A. Zakhor , "Path diversity with forward error correction (pdf) system for packet switched networks," in *IEEE INFOCOM Proc. IEEE Vol. 1*, 2003, pp. 663– 672.

[5] S. Mao, S.S. Panwar, and Y.T. Hou, "On optimal partitioning of realtime traffic over multiple paths," in *INFOCOM 2005, Proc. IEEE Vol. 4*, 2005, pp. 2325–2336.

[6] J. Han, D. Watson, and F. Jahanian, "An Experimental Study of Internet Path Diversity," *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 4, pp. 273 – 288, 2006.

[7] David Eppstein, "Finding the k shortest paths," in *Proc. 35th Symp. Foundations of Computer Science*, 1994, pp. 154–165.

[8] Richard G. Ogier, Vlad Rutenburg, and Nauchum Shacham, "Distributed Algorithms for Computing Shortest Pairs of Disjoint Paths," *IEEE transactions on information theory*, vol. 39, no. 2, pp. 443– 455, 1993.

[9] David G. Andersen, *Resilient Overlay Networks*. Master's Thesis, Massachusetts Institute of Technology, 2001.

[10] B-G Chun, R. Fonseca, I. Stoica, and J. Kubiatowicz, "Characterizing Selfishly Constructed Overlay Routing Networks," in *IEEE INFOCOM*, 2004, pp. 1329–1339.

[11] Roger Karrer, and Thomas Gross, "Multipath Streaming in Best-Effort Networks," in *Proc. of the IEEE International Conference on Communications (ICC'03)*, 2003.

[12] J.G. Apostolopoulos, T. Wong, W. Tan, and S.J. Wee, "On Multiple Description Streaming with Content Delivery Networks," in *IEEE INFOCOM, Proc. IEEE Vol. 3*, 2002, pp. 1736 – 1745.

[13] J. Chakareski and B. Girod, "Rate-distortion optimized packet scheduling and routing for media streaming with path diversity," in *Proc. IEEE Data Compression Conference*, 2003, pp. 203– 212.

[14] Ron M. Roth, *Introduction to Coding Theory*, 1st ed. Cambridge University Press, 2006.

[15] W. T. Tan and A. Zakhor, "Video Multicast Using Layered FEC and Scalable Compression," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 11, no. 3, pp. 373–386, 2001.

[16] L. Dairaine, L. Lancrica, J. Lacan, and J. Fimes, "Content-Access QoS in Peer-to-Peer Networks Using a Fast MDS Erasure Code," *Elsevier Computer Communications*, vol. 28, no. 15, pp. 1778–1790, 2005.

[17] X. H. Peng, "Erasure-control Coding for Distributed Networks," *IEE Proceedings on Communications*, vol. 152, pp. 1075 – 1080, 2005.

[18] N. Alon, J. Edmonds, and M. Luby, "Linear Time Erasure Codes with Nearly Optimal Recovery," in *IEEE Symposium on Foundations of Computer Science, Proc. IEEE Vol. 3*, 1995, pp. 512–519.

[19] J. Justesen , "On the complexity of decoding Reed-Solomon codes," *IEEE transactions on information theory*, vol. 22, no. 2, pp. 237– 238, 1993.

[20] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Efficient Erasure Correcting Codes," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 569–584, 2001.

[21] A. Shokrollahi, "Raptor Codes," *IEEE Transactions on Information Theory*, vol. 52, no. 6, pp. 2551–2567, 2006.

[22] R. Koetter and M. Medard , "An algebraic approach to network coding," *IEEE transactions on Networking*, vol. 11, no. 5, pp. 782– 795, 2003.

[23] P. A. Chou, Y. Wu, and K. Jain, "Practical Network Coding ," in *51st Allerton Conference on Communication, Control and Computing*, 2003.

[24] C. Gkantsidis and P. R. Rodriguez, "Network coding for large scale content distribution," in *IEEE INFOCOM, Proc. IEEE Vol. 4*, 2005, pp. 2235–2245.

[25] J. Padhye, V. Firoiu, D.F Towsley, and J.F. Kurose, "Modeling TCP Reno performance: a simple model and its empirical validation," *IEEE/ACM Transactions on Networking*, vol. 8, no. 2, pp. 133 – 145, 2000.

[26] M. Yajnik, S.B. Moon, J.F. Kurose, and D.F. Towsley , "Measurement and Modeling of the Temporal Dependence in Packet Loss," in *IEEE INFOCOM Proc. IEEE Vol. 1*, 1999, pp. 345–352.

[27] P. Rossi, G. Romano, F. Palmieri, and G. Iannello , "A Hidden Markov Model for Internet Channels," in *IEEE International Symposium on Signal Processing and Information Technology*, 2003.

[28] Amir Dembo and Ofer Zeitouni, *Large Deviations Techniques and Applications*, 2nd ed. New York: Springer, 1998.

[29] R. G. Gallager, *Information Theory and Reliable Communication*, 1st ed. New York, NY, USA: John Wiley & Sons, 1968.

[30] J. L. Kelley, *General Topology*. Springer, 1975.

[31] S. Boyd and L. Vandenberghe, *Convex Optimization*, 1st ed. Cambridge, UK: Cambridge University Press, 2004.

[32] T. Cover and J. Thomas, *Elements of Information Theory*, 1st ed. New York: Wiley, 2006.