Rate Allocation for Multipath Routing in Wireless Multihop Networks with Security Constraints Based on Erasure Channel Modeling

Jinho Choi, *Senior Member, IEEE*

***Abstract*—Multipath routing can offer various advantages for wireless multihop networks. Among those advantages, in this paper, we focus on an advantage of multipath routing for security using the notion of information-theoretic security. We formulate an optimization problem that maximizes the transmission rate from a source node to a destination node with information-theoretic security constraints to avoid eavesdropping that can be carried out at some nodes within a wireless multihop network. Binary erasure channel (BEC) modeling is employed to model wireless links that suffer from fading and interference. It is shown that the proposed throughput maximization problem is a linear optimization problem and the optimal rate allocation can be found by standard optimization techniques. We also study performance analysis including an asymptotic analysis to see whether or not multipath routing (with equal rate allocation) could be secure in terms of an information-theoretic security point of view. Through performance analysis, we can show that multipath routing can provide not only more secure routing against eavesdropping, but also a higher throughput as more multipaths are available.**

***Index Terms*—Rate allocation, multipath routing, wireless multihop networks, security, binary erasure channel (BEC).**

I. Introduction

PATH diversity has been investigated for routing to provide various advantages. Traffic dispersion has been utilized to alleviate the effects of traffic bursts and reduce queueing delay and probability of packet loss [1]. Redundant dispersity routing is studied in [2], [3] to mitigate delay and packet loss at the cost of sending more data through the network. Multipath routing for wireless multihop networks (e.g., wireless ad hoc or mesh networks) has been extensively investigated as it can be robust against failure of some wireless links (due to fading or interference) and offer the flexibility for load balancing. In [4], [5], multipath routing with maximally disjoint paths is considered to prevent some nodes from being congested by splitting traffics into multiple paths. In [6], multipath routing is exploited for efficient and reliable video communications over wireless multihop networks. While various multipath routing protocols have been developed as an effective means for reliable transmissions in wireless multihop networks (see [7], [8] for comparison and the reference therein), there are also skeptical views on multipath routing. In [9], it is shown that multipath routing could be less effective than single-path routing unless the number of multipaths is sufficiently large. Furthermore, it is pointed out in [10] that multipath routing can suffer from the interference in wireless multihop networks due to broadcasting nature of wireless communications.

Despite the skeptical views above, multipath routing is still important to overcome the inherent unreliability of wireless links in wireless multihop networks. Exploiting the notion of diversity coding in [11], a robust multipath routing scheme that transmits blocks of a coded packet through different disjoint paths[1] is proposed in [12]. The size of each block per path is optimized to maximize the probability of successful transmission based on the binary erasure channel (BEC) modeling for each path [12] [13].

Multipath routing could be more secure than single-path routing to defend against intruders as intruders should need more resources to disrupt data transmissions [14]. As discussed in [16], [15], the security issue is more serious in wireless multihop networks. While most multipath routing schemes consider malicious nodes which can stop or disrupt communications in wireless multihop networks, in this paper, we study a different security issue where some nodes become eavesdroppers in multipath routing. Eavesdropper nodes[2] (ENs) can behave normally and forward packets from a source node (SN) to a destination node (DN). Thus, there is no means to check whether or not some nodes on multipaths are ENs, although each pair of SN and DN does not want that ENs can succeed to decode the message from SN to DN. Multipath routing is more secure than single-path routing against eavesdropping as that against intruders' attack in [14]. Although strong cryptographic protocols can be used, eavesdropping becomes easier as only one link along a single-path is to be wiretapped in single-path routing. On the other hand, for multipath routing, since more links are to be wiretapped for eavesdropping, intruders need more resources and effort.

With three nodes (SN, DN, and EN), a security problem can be formulated with a wiretap channel model to address a fundamental security limit in terms of information theory in [17]. In the context of wireless communications, recently, information-theoretic security (ITS) has been extensively in-

Paper approved by M. Motani, the Editor for Network Information Theory and Cooperative Protocols of the IEEE Communications Society. Manuscript received July 16, 2010; revised July 3 and December 28, 2011.

This work was supported by ESPRC-DSTL under Grant EP/H011919/1.

J. Choi is with the College of Engineering, Swansea University, Singleton Park, Swansea, SA2 8PP, UK (e-mail: j.choi@swansea.ac.uk).

Digital Object Identifier 10.1109/TCOMM.2012.061412.100422

[1] We use the terms path (or multipath) and route interchangeably throughput this paper.

[2] A node whose incoming link is wiretapped becomes an EN without any intention.

vestigated (e.g., see [18] and references therein). It is noteworthy that we have a different assumption in this paper from the conventional wireless wiretap channel model. In [18], eavesdroppers are usually unknown receivers to SN (thus, wiretap channels are also unknown) and the secure capacity is of interest, while eavesdroppers are some of existing nodes in multipath in this paper. Since the characteristics of the wireless links between nodes are assumed to be known, we have a different challenging problem: maximizing the throughput from SN to DN by finding optimal rates to disjoint multiple paths subject to a certain ITS constraint to ensure that any EN(s) cannot decode a message from SN to DN successfully. In order to characterize the wireless links between nodes, the BEC model is employed as in [12], [13] and their erasure error probabilities are assumed to be known for the throughput optimization problem.

The main contribution of the paper is two-fold: *i)* BEC-based modeling of wireless multihop networks is derived to effectively employ ITS constraints; *ii)* a throughput maximization problem is formulated with ITS constraints and performance analysis is carried out for secure multipath routing. We show that the throughput maximization problem is a linear optimization problem that can be solved by standard optimization techniques. Through performance analysis, it is shown that multipath routing can provide not only more secure routing against eavesdropping, but also a higher throughput as more multipaths are available.

The rest of the paper is organized as follows. In Section II, we review related work. Section III presents the system model with some key properties of the multihop network where each wireless link is modeled by erasure channels. Throughput maximization problems with ITS constraints are derived in Section IV. Performance analysis and numerical results are presented in Sections V and VI, respectively. Finally, we conclude the paper with some remarks in Section VII.

II. Related Work

Multipath routing has been investigated in terms of security in the literature, e.g. [14], [19], [20], [21], [22], [23]. While unreliable wireless links are considered in [19], [20], links between nodes are assumed to be reliable to study multipath routing for improving security against eavesdropping or attacking links in [14], [21], [22], [23]. Thus, the work in the paper is more closely related to [19], [20]. In [19], with wireless links of one of two states, good or bad, with a certain probability, a routing problem is formulated to minimize the maximum security risk by assigning optimal probabilities for routes. In [20], it is proposed to distribute secure information among several independent multipaths for a certain level of security with redundancy. One of the key differences between the proposed approach in this paper and the approaches in [19], [20] is the channel model. As mentioned earlier, the BEC model is adopted for wireless links and this allows us to study secure multipath routing from an information-theoretic point of view [18]. Another main difference is that we can consider a stream of data packets so that an optimal transmission rate can be decided to each path according to a throughput maximization problem. If the probability of path for routing in [19] is considered as a (average) transmission rate to a path, the problems in [19] can be re-formulated using the approach in this paper from an information-theoretic point of view. However, this issue is not addressed in this paper and will be considered as a further research issue.

TABLE I
List of Symbols

	Defined in Section II
K	the number of disjoint multipaths
L_k	the number of links of the kth multipath
$R_{\rm in}$	the input rate at source node
$R_{\rm out}(R_1, \ldots, R_K)$	the output rate at destination node
R_k	the allocated input rate to the kth multipath
ϵ	erasure probability
ϵ_k	the erasure probability of the kth multipath
$\epsilon_{k,l}$	the erasure probability of the lth link of the kth multipath
	Defined in Section III
r_k	the normalized input rate to the kth multipath
$\mathbf{r}$	the rate vector
$\mathbf{u}_k$	the constraint vector of the kth multipath
$\psi = \frac{R_{\rm out}(R_1,\ldots,R_K)}{R_{\rm in}}$	throughput
	Defined in Section IV
$\beta = 1 - \epsilon$	non-erasure probability
$\beta_k = 1 - \epsilon_k$	non-erasure probability of the kth path
$\beta_{k,l} = 1 - \epsilon_{k,l}$	non-erasure probability of the lth link of the kth path
$\bar{\epsilon}$	the maximum erasure probability
$\alpha_{K,L}(\mathbf{r})$	the probability of no ITS routing with K multipaths and L wireless link per each multipath for given rate allocation $\mathbf{r}$
$\bar{\alpha}_{K,L}$	upper-bound on $\alpha_{K,L}(\mathbf{r})$
$I(a)$	rate function
	Defined in Section IV
$P_{\rm its}(K, L)$	probability of successful ITS routing
$\psi_{\rm eq}$	throughput with equal rate allocation
$\psi_{\rm its}$	throughput with optimal rate allocation with ITS constraint

III. System Model

For convenience, we list the symbols and notations used in this paper as follows. The superscript $\rm T$ stands for the transpose. The kth element of vector $\mathbf{x}$ is denoted by $[\mathbf{x}]_k$. $[\mathbf{A}]_{l,k}$ represents the (l, k)th element of a matrix $\mathbf{A}$. A vector of all 0's is denoted by $\mathbf{0}$ and a vector of all 1's is denoted by $\mathbf{1}$. The statistical expectation is denoted by $\mathbb{E}[\cdot]$ and $\Pr(\mathcal{A})$ stands for the probability of a random event $\mathcal{A}$. The symbol $\Leftrightarrow$ is used for the biconditional of two statements. In addition, the list of key symbols used in the paper is shown in Table I.

Throughout this paper, we assume that disjoint multipaths have been built between a pair of SN to DN for multipath routing. To characterize a wireless link between two connected nodes with a certain unreliability due to impairments such as fading and interference, we use the BEC model. Note that BEC is also employed to model multipaths in [12]. In addition, in [24], the BEC model for wireless links in wireless networks is considered to find the capacity for multicasting. To allow the rate allocation to multipaths, we will generalize the BEC model in this section. Throughout this paper, we also assume that coded packets are transmitted through multipaths as in [12] using diversity coding in [11].

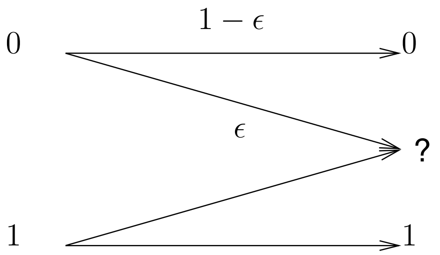


Fig. 1. Binary erasure channel model (in the figure, ϵ denotes the erasure probability and ? denotes the erasure state).

A. Multipath Routing

Suppose that there is a wireless multihop network consisting of multiple nodes. We consider a pair of SN and DN with multipath routing (throughout this paper, we only consider one pair of SN and DN). It is assumed that there are K multipaths from SN to DN and there is no common link between multiple paths. That is, we have K disjoint multipaths from SN to DN. SN can allocate different input transmission rates to multipaths and the input transmission rate to the kth path is denoted by R_k in bits per second (bps) per Hz (bps/Hz). Thus, the total input transmission rate becomes $\sum_{k=1}^K R_k$. For convenience, denote by $R_{\text{in}} = \sum_{k=1}^K R_k$ the input transmission rate. A coded packet is divided into multiple subpackets, say N subpackets. If N_k subpackets are transmitted through the kth path, the allocated input rate to the kth path is

$$R_k = \frac{N_k}{N} R_{\text{in}}, \tag{1}$$

if the original coded packet is transmitted at a rate of R_{in}. Since each wireless link is not reliable, there would be subpacket losses. However, at DN, if we can have a sufficient number of subpackets, we could decode and recover the original message sent by SN. This approach is proposed in [12].

Note that we only consider the case that a codeword (or coded packet) of length N is divided into K sub-codewords as in (1) in this paper. There could be other approaches to transmit codewords with multipath routing. For example, a codeword can be duplicated K times for K multipaths (i.e., the same codeword is transmitted through all the multipaths). A different coding strategy for multipath routing could result in a different rate allocation and ITS. Although we do not investigate in this paper, it would be interesting to consider optimal secure coding strategies with multipath routing in the future.

B. BEC Modeling for Multipaths in Multihop Networks

Each wireless link is characterized or modeled by BEC with the associated erasure probability as shown in Fig. 1. For binary input, the channel capacity or spectral efficiency of this wireless link is $1-\epsilon$, where ϵ is the erasure probability. Suppose that the input transmission rate can be arbitrary. For an input transmission rate of R, if the output transmission rate becomes $R(1-\epsilon)$ (in bps/Hz), where ϵ is the erasure probability per bit, this wireless link with BEC modeling can be characterized by two parameters, (R, ϵ) and is referred to as the scalable erasure channel (SEC) of (R, ϵ) throughout this paper.

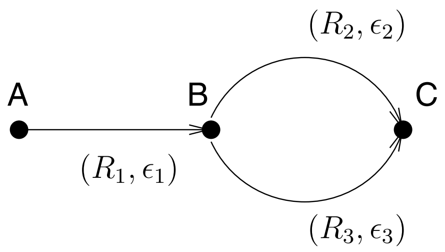


Fig. 2. A network of 3 nodes with serial and parallel connections.

Property 1. *Suppose that two links are serially connected. The erasure probabilities of the first and second links are denoted by ϵ_1 and ϵ_2, respectively. Then, if the input transmission rate is R to the first link, the serial composite link becomes a SEC of $(R, 1-(1-\epsilon_1)(1-\epsilon_2))$.*

Property 2. *Suppose that there are two parallel links between two nodes, where each link is a SEC of (R_n, ϵ_n), $n = 1, 2$. Then, the parallel composite link is a SEC of $(R_1 + R_2, \frac{R_1}{R_1+R_2}\epsilon_1 + \frac{R_2}{R_1+R_2}\epsilon_2)$.*

Example 1. Consider a network shown in Fig. 2. Based on Property 2, we can see that the parallel composite link from node B and C becomes a SEC of $(R_2 + R_3, \epsilon_{BC})$, where $\epsilon_{BC} = \frac{R_2}{R_2+R_3}\epsilon_2 + \frac{R_3}{R_2+R_3}\epsilon_3)$. The composite link from node A and C is now a serial composite link. Based on Property 1, it becomes a SEC of $(R_1, 1-(1-\epsilon_1)(1-\epsilon_{BC}))$.

As shown above, any path consisting of (combinations of) parallel and serial connections can be represented as a path consisting of a certain number of serially connected wireless links based on the SEC model. Thus, throughout the paper, we have the following assumption.

L1) There are K disjoint multipaths from SN and DN and the kth path from SN to DN consists of serially connected L_k wireless links.

Property 3. *Suppose that there are K disjoint multipaths from SN to DN and each link within the network is modeled as a SEC. The input transmission rate to the kth path is R_k from SN. Then, each path becomes a SEC and the erasure probability of the kth path can be expressed as $\epsilon_k = 1 - \prod_{q=1}^{L_k}(1-\epsilon_{k,q})$, where $\epsilon_{k,q}$ is the erasure probability of the qth wireless link of the kth path. The overall composite link from SN to DN becomes a SEC of $(\sum_{k=1}^K R_k, \sum_{k=1}^K \frac{R_k}{\sum_{q=1}^K R_q}\epsilon_k)$.*

As a consequence of Property 3, we can find the output transmission rate, denoted by $R_{\text{out}}(R_1, \ldots, R_K)$, which is a function of $R_1, \ldots, R_K$, as follows:

$$R_{\text{out}}(R_1, \ldots, R_K) = R_{\text{in}} \left(1 - \sum_{k=1}^K \frac{R_k}{\sum_{q=1}^K R_q}\epsilon_k\right), \tag{2}$$

where $\sum_{k=1}^K R_k = R_{\text{in}}$. If the code rate for coded packets is less than $R_{\text{out}}(R_1, \ldots, R_K)/R_{\text{in}}$, we can assume that the coded packets can be successfully decoded at DN. In [12], the maximization of the successful transmission probability is considered by optimizing rates[3] to multipaths.

IV. Throughput Maximization by Rate Allocation with ITS Constraints

In this section, we discuss throughput maximization problems with ITS constraints to find optimal rates to multipaths. It is assumed that any node in the multipaths can be an eavesdropper to derive ITS constraints. ITS constraints can also be generalized if multiple nodes are cooperative to decode the message from SN as a group of cooperative eavesdroppers.

A. Problem Formulation

We can find the input transmission rates to K multipaths to maximize the total output transmission rate. For example, we can formulate the following optimization problem to maximize the output transmission rate:

$$\{R_1^*, \ldots, R_K^*\} = \arg \max_{R_k, k=1,2,\ldots,K} R_{\text{out}}(R_1, \ldots, R_K)$$
$$\text{subject to } \sum_{k=1}^{K} R_k \le R_{\text{in}}. \tag{3}$$

Using Property 3, this problem could be easily solved using an inequality derived from (2) as follows:

$$\begin{aligned} R_{\text{out}}(R_1, \ldots, R_K) &= R_{\text{in}} \left(1 - \sum_{k=1}^{K} \frac{R_k}{\sum_{q=1}^{K} R_q} \epsilon_k \right) \\ &\le \bar{R}_{\text{out}} \overset{\triangle}{=} R_{\text{in}}(1 - \min_k \epsilon_k). \end{aligned} \tag{4}$$

The upper-bound on $R_{\text{out}}(R_1, \ldots, R_K)$ in (4) can be achieved by choosing a single path (among K multipaths) that is the path of the lowest erasure probability, $\min_k \epsilon_k$. From this, we can see that the optimal solution of the problem in (3) is given by

$$R_k^* = \begin{cases} R_{\text{in}}, & \text{if } k = k^* = \arg\min_q \epsilon_q; \\ 0, & \text{otherwise.} \end{cases} \tag{5}$$

That is,

$$\begin{aligned} &\max_{R_1 + \cdots + R_K \le R_{\text{in}}} R_{\text{out}}(R_1, \ldots, R_K) \\ &= R_{\text{out}}(0, \ldots, 0, R_k^* = R_{\text{in}}, 0, \ldots, 0) = \bar{R}_{\text{out}}. \end{aligned}$$

If the code rate is decided to be less than $\bar{R}_{\text{out}}/R_{\text{in}} = 1 - \epsilon_{k^*}$, coded packets transmitted through the k^*th path can be reliably decoded at DN. In general, as K increases (i.e., more multipaths are available), the output transmission rate could increase and this gain is called multiroute path selection (MRPS) diversity gain [25] [26]. A similar approach can also be found in a multiuser wireless system where the user who has the best channel is chosen to access a common channel [27].

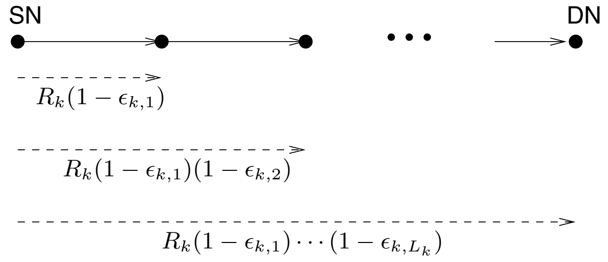

SN
DN
$R_k(1-\epsilon_{k,1})$
$R_k(1-\epsilon_{k,1})(1-\epsilon_{k,2})$
$R_k(1-\epsilon_{k,1})\cdots(1-\epsilon_{k,L_k})$

Fig. 3. The channel capacity for a serially connected path (as the first node has the highest capacity among all the nodes on the path, this node becomes the best node to be the EN).

Although the solution in (5) can maximize the output transmission rate, this solution could be vulnerable to eavesdropping. Suppose that a node on the k^*th path becomes an EN, say the qth node. Since the output transmission rate from SN to this EN is higher than or equal to that from SN to DN as

$$R_{\text{in}} \prod_{l=1}^{q} (1 - \epsilon_{k^*,l}) \ge \bar{R}_{\text{out}} = R_{\text{in}} \prod_{l=1}^{L_{k^*}} (1 - \epsilon_{k^*,l}), \text{ for all } q \le L_k,$$

this EN can successfully decode the signal from SN. This confirms that single-path routing is not preferable in terms of ITS.

In multipath routing, we may not be able to know which node is an EN. Thus, it would be the best to consider the worst case. As illustrated in Fig. 3, the first node on any path can achieve the highest output transmission rate among all the nodes on the path, because

$$(1 - \epsilon_{k,1}) \ge \prod_{l=1}^{q} (1 - \epsilon_{k,l}), \ 1 \le q \le L_k.$$

If an EN is closer to the SN, it can receive less degaded signals and better chance to decode coded signals successfully. Thus, as the worst case, we can assume that an EN is the first node on a path, although it may not be true. Under this assumption, ITS routing can be considered and it can be secure even if the eavesdropper is the first node on a path (the worst case). Furthermore, if the eavesdropper's location is known, we can simply exclude the path where the eavesdropper presents. Otherwise, we need to consider the worst case and distribute traffics to multipaths according to optimal rates to keep a certain level of security which results from ITS constraints. Consequently, we assume that the first nodes on multipaths are potential ENs throughout this paper (while the multipaths where the eavesdropers present, if any, are excluded). To avoid successful decoding by any EN, ITS constraints need to be included in the output rate maximization problem for secure transmission from SN to DN.

If a rate allocation of $(R_1, \ldots, R_K)$ satisfies

$$\max_k R_k(1 - \epsilon_{k,1}) < R_{\text{out}}(R_1, \ldots, R_K), \tag{6}$$

this rate allocation is called information-theoretic secure. For a given set of multipaths, if there exists a rate allocation that is information-theoretic secure, this multipath routing is called ITS routing in this paper.

For convenience, define the (normalized) throughput as

$$\psi = \frac{R_{\text{out}}(R_1, \ldots, R_K)}{R_{\text{in}}} = 1 - \sum_{k=1}^{K} r_k \epsilon_k, \tag{7}$$

[3] In [12], a packet is divided into multiple blocks and these blocks are transmitted through multipaths. In our context, the numbers of blocks for each path are actually equivalent to the transmission rates for each path.

where $r_k = \frac{R_k}{\sum_{q=1}^{K} R_q}$ is the normalized (input) rate to the kth path. Clearly, ψ becomes the throughput of a given set of multipaths from SN and DN when $R_{\text{in}} = 1$. For convenience, we normalize the input transmission rate to be unity (in this case, $R_k = r_k$ for all k). To make clear that ψ is a function of the r_k's, it will be denoted by $\psi(r_1, r_2, \ldots, r_K)$ hereafter. The throughput maximization problem with ITS constraints is given by

$$\{r_1^*, r_2^*, \ldots, r_K^*\} = \arg\max_{\{r_1,r_2,\ldots,r_K\}} \psi(r_1, r_2, \ldots, r_K)$$
$$\text{subject to} \left\{ \begin{array}{ll} \sum_{k=1}^{K} r_k & = 1; \\ \max_k r_k(1-\epsilon_{k,1}) & < \psi(r_1, r_2, \ldots, r_K); \\ r_k & \geq 0,\ k = 1, 2, \ldots, K. \end{array} \right. \quad (8)$$

The first constraint results from the rate normalization. The second constraint is the ITS constraint from (6), and the third constraint makes sure that the rates are non-negative.

Let $\mathbf{r} = [r_1\ r_2\ \ldots\ r_K]^{\mathrm{T}}$ and

$$[\mathbf{u}_k]_q = \left\{ \begin{array}{ll} 1 - \epsilon_{k,1} + \epsilon_k, & \text{if } q = k; \\ \epsilon_q; & \text{otherwise.} \end{array} \right. \quad (9)$$

We can now formulate the problem in (8) as a linear optimization problem.

Problem 1. *The problem in* (8) *becomes the following linear optimization problem:*

$$\mathbf{r}^* = \arg\min_{\mathbf{r}} \mathbf{c}^{\mathrm{T}}\mathbf{r}$$
$$\textit{subject to} \left\{ \begin{array}{ll} \mathbf{1}^{\mathrm{T}}\mathbf{r} & = 1 \\ \mathbf{U}^{\mathrm{T}}\mathbf{r} & < \mathbf{1} \\ \mathbf{r} & \geq \mathbf{0} \end{array} \right. \quad (10)$$

where

$$\mathbf{c} = [\epsilon_1\ \epsilon_2\ \ldots\ \epsilon_K]^{\mathrm{T}}$$
$$\mathbf{U} = [\mathbf{u}_1\ \mathbf{u}_2\ \ldots\ \mathbf{u}_K]. \quad (11)$$

In (10), the inequality between vectors is componentwise inequality. It is straightforward to show that $\mathbf{c}^{\mathrm{T}}\mathbf{r} = 1 - \psi(r_1, \ldots, r_K)$. Each element of the second constraint, i.e. $\mathbf{U}^{\mathrm{T}}\mathbf{r} < \mathbf{1}$, is given by

$$\mathbf{u}_k^{\mathrm{T}}\mathbf{r} < 1,\ k = 1, 2, \ldots, K.$$

It can be shown that

$$\mathbf{u}_k^{\mathrm{T}}\mathbf{r} < 1 \Leftrightarrow r_k(1 - \epsilon_{k,1}) < \psi(r_1, \ldots, r_K).$$

Therefore, the second constraint in (8) is equivalent to the second constraint in (10). That is,

$$\max_k r_k(1 - \epsilon_{k,1}) < \psi(r_1, \ldots, r_K) \Leftrightarrow \mathbf{U}^{\mathrm{T}}\mathbf{r} < \mathbf{1}.$$

This shows that the optimization problem in (8) is equivalent to that in (10).

Note that the strict inequality in $\mathbf{U}^{\mathrm{T}}\mathbf{r} < \mathbf{1}$ can be relaxed as $\mathbf{U}^{\mathrm{T}}\mathbf{r} \leq \mathbf{1}$ in a linear solver. In this case, $\mathbf{U}^{\mathrm{T}}\mathbf{r} \leq \mathbf{1}$ is referred to as the *relaxed* ITS constraint.

Example 2. *Suppose that $K = 2$ and $L_k = 3$ for all k. Let $\epsilon_{1,l} = 0.1$ and $\epsilon_{2,l} = 0.15$. Then, we have $\epsilon_1 = 0.271$ and $\epsilon_2 = 0.3859$. Using the linear programming, we can find the solution as follows:*

$$\mathbf{r}^* = [0.7822\ 0.2178]^{\mathrm{T}}.$$

The throughput is $\psi(r_1^*, r_2^*) = 0.704$. Since $r_1^*(1 - \epsilon_{1,1}) = 0.704 \leq \psi(r_1^*, r_2^*)$ and $r_2^*(1 - \epsilon_{2,1}) = 0.196 < \psi(r_1^*, r_2^*)$, we can see that the (relaxed) ITS constraint is satisfied. To keep the ITS constraint strict in the above example, the optimality can be sacrificed. For example, we can set $r_1 = 0.78$ and $r_2 = 0.22$. That is, the rate to the second path increases to keep the ITS constraint strictly. As a result, we have $r_1(1 - \epsilon_{1,1}) = 0.702 < \psi(r_1, r_2) = 0.7037$ and $r_2(1 - \epsilon_{2,1}) = 0.1870 < \psi(r_1, r_2) = 0.7037$. Thus, if the first node of the firth path is an EN, it fails to decode the coded packet as its output rate is 0.702. Since the other nodes have lower output rates, they all fail to decode successfully.

Note that the ITS is different from that used in [18] where a strict information security is imposed. Clearly, a different information security requirment results in a different ITS constraint and needs to be further studied in the future.

B. Generalization with Multiple Cooperative ENs

Suppose that there are multiple cooperative ENs, say m ENs. To efficiently decode the message from SN, multiple ENs should be cooperative and distributed over m paths. Thus, in this subsection, we assume that there are m paths on which the first nodes are ENs. However, it is assumed that these m paths are not known to SN.

Consider a set of m ENs that collaborate to decode the message from the SN. Define the set of the indexes of m different multipaths as

$$\mathcal{I}_m = \{(k_1, k_2, \ldots, k_m) :\ k_p \neq k_q,\ \text{for all } p \neq q\}.$$

Then, we can show that

$$M_m = |\mathcal{I}_m| = \left(\begin{array}{c} K \\ m \end{array} \right).$$

Denote by $\mu^m(i)$ the ith element of $\mathcal{I}_m$. Clearly, $\mu^m(i)$ is an index set for m multipaths. Furthermore, denote by $\mu_j^m(i)$ the index for the jth path on $\mu^m(i)$. That is, $\mu^m(i) = (\mu_1^m(i), \mu_2^m(i), \ldots, \mu_m^m(i))$. With m cooperative ENs, the ITS constraint becomes

$$\max_{\mu^m(i) \in \mathcal{I}_m} \sum_{j=1}^{m} r_{\mu_j^m(i)} \left(1 - \epsilon_{\mu_j^m(i),1}\right) < \psi(r_1, r_2, \ldots, r_K). \quad (12)$$

If a rate allocation satisfies (12), it is called information-theoretic secure with m ENs.

To build a linear optimization problem with the ITS constraint in (12), define (13). Then, we can generalize the throughput maximization problem in (10) with m cooperative ENs as follows.

Problem 2. *The throughput maximization problem when there are m cooperative ENs becomes the following linear optimization problem:*

$$\mathbf{r}^* = \arg\min_{\mathbf{r}} \mathbf{c}^{\mathrm{T}}\mathbf{r}$$
$$\textit{subject to} \left\{ \begin{array}{ll} \mathbf{1}^{\mathrm{T}}\mathbf{r} & = 1 \\ \mathbf{U}_{(m)}^{\mathrm{T}}\mathbf{r} & < 1 \\ \mathbf{r} & \geq 0, \end{array} \right. \quad (14)$$

where

$$\mathbf{U}_{(m)} = [\mathbf{u}_{(m),1}\ \mathbf{u}_{(m),2}\ \ldots\ \mathbf{u}_{(m),M_m}]. \quad (15)$$

$$[\mathbf{u}_{(m),i}]_q = \begin{cases} 1-\epsilon_{\mu_j^m(i),1}+\epsilon_{\mu_j^m(i)}, & \text{if } q=\mu_j^m(i),\ j=1,2,\ldots,m; \\ \epsilon_q; & \text{otherwise.} \end{cases} \tag{13}$$

By including more constraints as shown in (14), we can find the optimal rate allocation for multipath routing when there are multiple cooperative ENs. However, the linear programming does not scale well with m because the number of constraints grows quickly with m and a feasible solution may not exist for a large m. It is noteworthy that the optimal rate vector $\mathbf{r}^*$ is obtained without knowing the location of ENs by taking into account the worst case as discussed earlier.

V. Performance Analysis

It is certainly desirable to understand the performance of the rate allocation from the throughput maximization problem with ITS constraints under realistic environments. For example, there could be interference between the wireless links if they share a common channel (i.e., multiple access channels). Furthermore, the erasure probability could be determined in a different way for each wireless link. Unfortunately, these practical aspects may not allow simple and intuitive analysis for the performance of the rate allocation developed in Section IV. Thus, for tractable analysis, we consider the following symmetric assumptions:

A1) Assume that the erasure event of each wireless link is independent and the erasure probability is the same and denoted by ϵ.

A2) Assume that $L_k = L$ for all the paths.

Under **A1**) and **A2**), the throughput is given by

$$\psi(r_1, r_2, \ldots, r_K) = 1 - \sum_{q=1}^{K} r_q(1-\beta^L), \tag{16}$$

where $\beta = 1-\epsilon$. From this and $\sum_{q=1}^{K} r_q = 1$, with one EN (i.e., $m = 1$), the ITS constraint becomes

$$\max_k r_k \beta < \psi(r_1, r_2, \ldots, r_K) = \beta^L. \tag{17}$$

The throughput maximization problem reduces to

$$\begin{aligned} &\min\nolimits_{\mathbf{r}} \mathbf{c}^{\mathrm{T}}\mathbf{r} = \epsilon \min\nolimits_{\mathbf{r}} \mathbf{1}^{\mathrm{T}}\mathbf{r} \\ &\text{subject to } \ \mathbf{1}^{\mathrm{T}}\mathbf{r} = 1, \quad \mathbf{r} < \beta^{L-1}\mathbf{1}. \end{aligned} \tag{18}$$

For any $\mathbf{r}$ satisfying $\mathbf{1}^{\mathrm{T}}\mathbf{r} = 1$, we have $\mathbf{c}^{\mathrm{T}}\mathbf{r} = \epsilon$ and it can be an optimal solution (there could be infinitely many optimal solutions). For example, if a feasible solution exists, the following rate allocation becomes an optimal solution:

$$r_k^* = \frac{1}{K}, \ k = 1, 2, \ldots, K. \tag{19}$$

This shows that the equal rate allocation is optimal under the symmetric conditions (i.e., **A1**) and **A2**)) and this solution is valid if $r_k^* = \frac{1}{K} < (1-\epsilon)^{L-1}$. Thus, for the equal rate allocation, we can derive the following condition for ϵ:

$$\epsilon < 1 - \frac{1}{K^{\frac{1}{L-1}}}.$$

As mentioned earlier, there are also other optimal solutions. However, since the equal rate allocation is easy to analyze, we focus on it in the rest of the section.

A general result with m cooperative ENs with the equal rate allocation can be given as follows.

Theorem 1. *Under the symmetric conditions in* **A1**) *and* **A2**)*, if there are m cooperative ENs, the equal rate allocation (i.e., $r_k^* = 1/K$ for all k) becomes an optimal solution when the following condition is satisfied:*

$$\epsilon < \bar{\epsilon} = 1 - \left(\frac{m}{K}\right)^{\frac{1}{L-1}}. \tag{20}$$

Proof: Under the symmetric conditions in **A1**) and **A2**), the optimal rate is $r_k^* = \frac{1}{K}$. Then, for the ITS constraint, from (17), we have the following inequality:

$$\frac{m}{K}\beta < \beta^L.$$

Then, it follows

$$\frac{m}{K} < \beta^{L-1} = (1-\epsilon)^{L-1}. \tag{21}$$

From this inequality, the upper-bound on ϵ in (20) can be obtained. This completes the proof. ■

The condition in (20) can also be used as a sufficient condition for ITS routing when the erasure probabilities are different. It can be shown that if

$$\max_k \epsilon_k < \bar{\epsilon} = 1 - \left(\frac{m}{K}\right)^{\frac{1}{L-1}},$$

the multipath routing can be ITS routing.

From (21), we can show that

$$K > \frac{m}{(1-\epsilon)^{L-1}}.$$

This implies that the number of multipaths, K, should grow linearly as m increases when ϵ and L are fixed for ITS routing. In addition, K needs to grow exponentially with L for fixed ϵ and m. Note that the throughput decreases exponentially with L as $\psi = \beta^L = (1-\epsilon)^L$ from (16).

So far, we have considered the rate allocation when the erasure probabilities are known. If the erasure probabilities are not known, we are unable to find the optimal rate allocation as in (14). In this case, with a suboptimal rate allocation, which is the equal rate allocation, we are interested in finding the probability that the multipath routing with equal rate allocation is ITS routing or no ITS routing. To find this probability, we consider the following assumption.

A1′) Assume that the erasure event of each wireless link is independent and the erasure probability of each wireless link, $\epsilon_{k,l}$, is independent and identically distributed (iid). For convenience, let $F(x) = \Pr(\beta_{k,l} \le x)$, where $\beta_{k,l} = 1 - \epsilon_{k,l}$.

We assume that there is one EN, i.e., $m = 1$, for further analysis. For convenience, denote by $\alpha_{K,L}(\mathbf{r})$ the probability of no ITS routing with K multipaths and L wireless link per each multipath for given rate allocation $\mathbf{r}$. With a single EN, we have

$$\alpha_{K,L}(\mathbf{r}) = \Pr\left(\max_k r_k\beta_{k,1} > 1 - \sum_{k=1}^{K} r_k(1 - \prod_{l=1}^{L}\beta_{k,l})\right). \tag{22}$$

Let

$$\bar{\alpha}_{K,L} = \min_{\mathbf{r}} \alpha_{K,L}(\mathbf{r}).$$

Since the equal rate allocation is suboptimal, we have the following upper bound on $\bar{\alpha}_{K,L}$:

$$\bar{\alpha}_{K,L} \le \bar{\alpha}^{(\mathrm{eq})}_{K,L} = \Pr\left(\max_k \beta_{k,1} > \sum_{k=1}^{K}\prod_{l=1}^{L}\beta_{k,l}\right). \tag{23}$$

Theorem 2. *Suppose that $F(0) = 0$. For a fixed and finite L, under* **A1′**) *and* **A2**)*, we have*

$$\lim_{K\to\infty} \bar{\alpha}^{(\mathrm{eq})}_{K,L} = 0. \tag{24}$$

Proof: Let $c_{k,L} = e^{-(L-1)v_{k,L}}$, where $v_{k,L} = -\frac{1}{L-1}\sum_{l=2}^{L}\log\beta_{k,l}$. Then, from (23), we can show that

$$\begin{aligned}\bar{\alpha}^{(eq)}_{K,L} &= \Pr(\max_k \beta_{k,1} > \sum_{k=1}^{K} c_{k,L}\beta_{k,1})\\ &\le \Pr\left(\frac{\max_k \beta_{k,1}}{\sum_{k=1}^{K}\beta_{k,1}} > \min_k c_{k,L}\right).\end{aligned} \tag{25}$$

According to [28], since $\mathbb{E}[\beta_{k,1}] \le 1 < \infty$, it follows that

$$\lim_{K\to\infty} \frac{\max_k \beta_{k,1}}{\sum_{k=1}^{K}\beta_{k,1}} = 0 \ w.p.1. \tag{26}$$

Furthermore, since $F(0) = 0$, $c_{k,L} > 0$ w.p. 1 for a finite L. Thus,

$$\lim_{K\to\infty} \bar{\alpha}^{(\mathrm{eq})}_{K,L} \le 0. \tag{27}$$

This completes the proof. ■

The result in Theorem 2 shows that the equal rate allocation for the multipath routing becomes information-theoretic secure if the number of multipaths approaches infinity when the number of nodes on paths, L, is fixed and finite. This is a natural consequence as the output transmission rate to any EN on a path approaches 0 when the input transmission rate per path, say R_k, approaches 0 for $K \to \infty$. with a finite input rate $R_{\mathrm{in}} < \infty$. However, if L also increases when K increases, it is not clear whether or not the multipath routing could be ITS routing. (Note that when L increases, it is necessary that the input transmission rate, R_{in} also increases so that the output transmission rate does not go to zero.) Therefore, we need to consider the probability of no ITS routing for the case where both K and L increase.

Theorem 3. *Suppose that* **A1′**) *and* **A2**) *hold. Let $Y_{k,l} = -\log\beta_{k,l}$. Under A1′), $Y_{k,l}$ becomes iid. Denote by $I(a)$ and μ the rate function and mean of $Y_{k,l}$, respectively. If i) there exists $a > \mu$ satisfies*

$$\mu < I(a) \tag{28}$$

and ii) K and L approach infinity such as

$$\lim_{K,L\to\infty} \frac{K}{e^{L\eta}} = c > 0, \tag{29}$$

where c is a finite constant and $\eta \in (\mu, I(a))$, we have

$$\lim_{K,L\to\infty} \bar{\alpha}^{(\mathrm{eq})}_{K,L} = 0. \tag{30}$$

Proof: See Appendix A. ■

The result in Theorem 3 shows that the multipath routing with equal rate allocation could be ITS routing when both K and L approach infinity. In order the multipath routing to be ITS routing, as shown in (29), K should grow faster than L, in particularly, K should grow exponentially with L.

Note that the rate function of a random variable, X, is defined as [29]

$$I(a) = \sup_{s\ge 0}(sa - \log\mathbb{E}[e^{sX}]). \tag{31}$$

We present an example where the condition in (28) holds as follows.

Example 3. *Suppose that*

$$\epsilon_{k,l} = \begin{cases} 0, & w.p.\ p_0;\\ \bar{\epsilon}, & w.p.\ 1-p_0,\end{cases}$$

where $0 < \bar{\epsilon} < 1$ and $0 < p_0 < 1$. Then, we have

$$\mu = \mathbb{E}[-\log(1-\epsilon_{k,l})] = (1-p_0)\log\frac{1}{1-\bar{\epsilon}}.$$

Furthermore,

$$I(a) = \max_{s\ge 0}\left(a - \frac{1}{1-\bar{\epsilon}}\right)s + \log\frac{1}{1-p_0}.$$

Thus, if $a > \frac{1}{1-\bar{\epsilon}}$, $I(a) = \infty$. From this, we can easily verify that there exists $\eta \in (\mu, I(a))$ for $a > \frac{1}{1-\bar{\epsilon}} \ge \mu$.

VI. Numerical Results

In this section, we consider three different routing schemes: the optimal single-path routing (that maximizes the throughput), the multipath routing with equal rate allocation, and the proposed optimal multipath routing with ITS constraints. To find the optimal solution, we use a MATLAB function, linprog.m as an optimizer. For simulations, the erasure probabilities for wireless link are randomly generated for each run according to the following uniform distribution:

$$f(\epsilon_{k,l}) = \begin{cases} \frac{1}{\epsilon_{\max}}, & 0 \le \epsilon_{k,l} < \epsilon_{\max};\\ 0, & \epsilon_{\max} \le \epsilon_{k,l} \le 1,\end{cases}$$

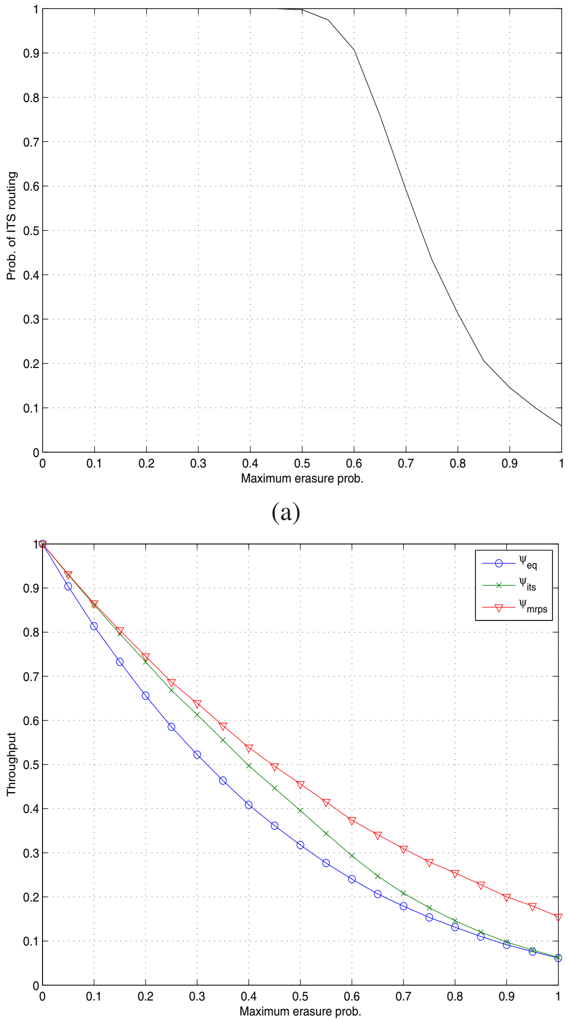
where $0 < \epsilon_{\max} \le 1$ is the maximum erasure probability. In order to find the throughput and probability of no ITS routing, average values of 4000 runs are used.

The throughput of the optimal single-path routing based on MRPS is denoted by $\psi_{\mathrm{mrps}} = \bar{R}_{\mathrm{out}}/R_{\mathrm{in}}$ according to (4). In addition, the throughputs of the multipath routing with equal rate allocation and the proposed optimal multipath routing with the ITS constraint are given by

$$\begin{aligned}\psi_{\mathrm{eq}} &= \psi\left(\frac{1}{K}, \frac{1}{K}, \dots, \frac{1}{K}\right);\\ \psi_{\mathrm{its}} &= \psi\left(r_1^*, r_2^*, \dots, r_K^*\right),\end{aligned}$$

respectively. Note that the solution of the optimal rate allocation for ITS routing may not exist. In this case, we have the equal rate allocation. Thus, we have

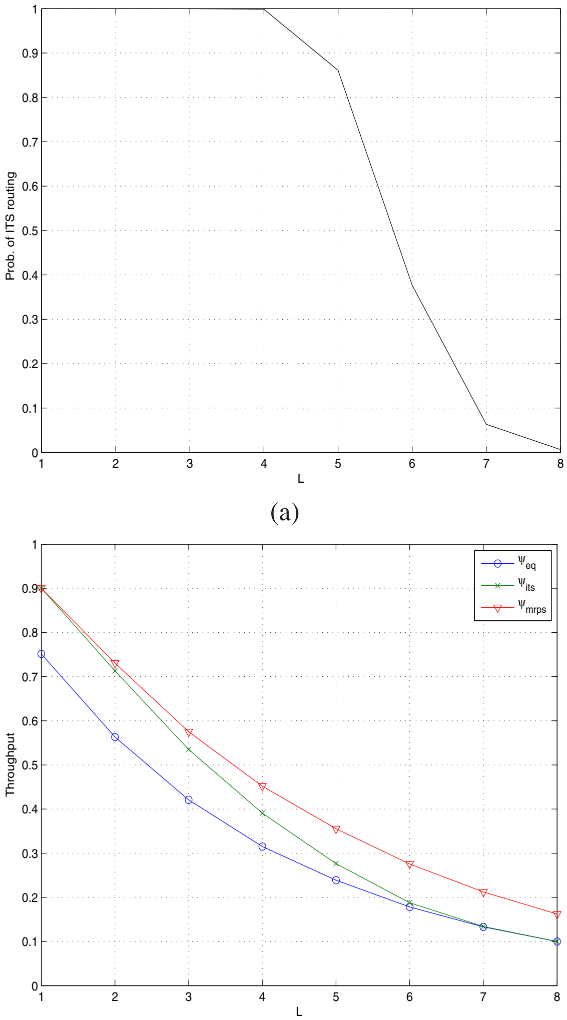
$$\psi_{\mathrm{mrps}} \ge \psi_{\mathrm{its}} \ge \psi_{\mathrm{eq}}. \tag{32}$$



(a)

(b)

Fig. 4. Probability of successful ITS routing and throughputs for various values of the maximum erasure probability with one EN (i.e., $m = 1$) when $K = L = 4$: (a) Probability of successful ITS routing; (b) Throughputs of various rate allocations.



(a)

(b)

Fig. 5. Probability of successful ITS routing and throughputs for various values of L with one EN (i.e., $m = 1$) when $K = 4$ and $\epsilon_{\max} = 0.5$: (a) Probability of successful ITS routing; (b) Throughputs of various rate allocations.

It is noteworthy that as mentioned earlier, MRPS can provide the best throughput, but it is vulnerable to eavesdropping as an eavesdropper that is a node on the selected path can decode the message from SN to DN. Therefore, although the throughput can be lower, it would be secure to employ ITS routing.

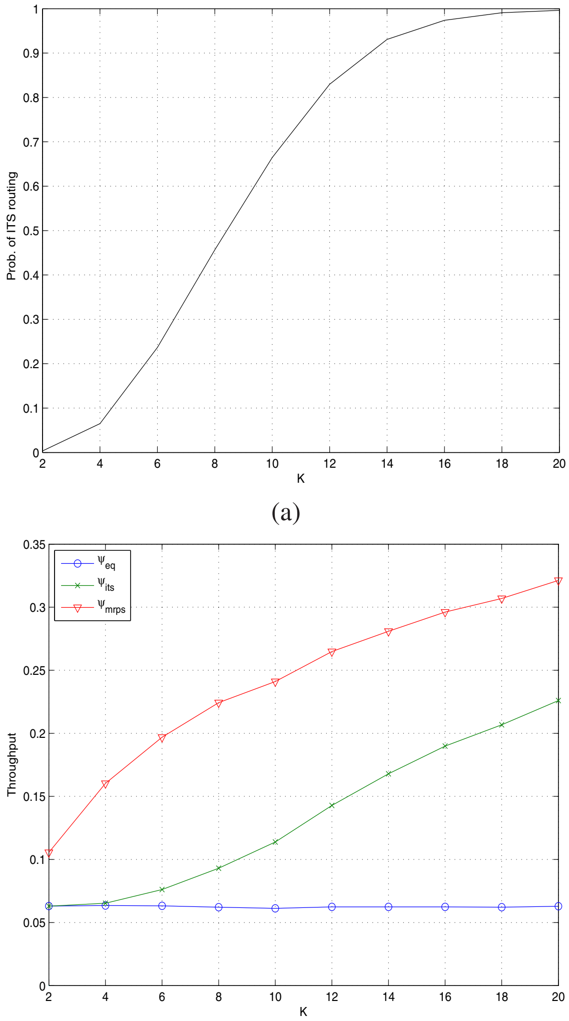
Together with the throughput, we are also interested in the probability of successful ITS routing, which is denoted by $P_{\text{its}}(K, L)$. Clearly, from (22), we have

$$P_{\text{its}}(K, L) = 1 - \alpha_{K,L}(\mathbf{r}^*).$$

Fig. 4 shows $P_{\text{its}}(K, L)$ and the throughputs when $K = L = 4$ and $m = 1$ for various values of the maximum erasure probability, $\epsilon_{\max}$. As $\epsilon_{\max}$ increases, the reliability of wireless link decreases. This results in the decrease of the throughputs with $\epsilon_{\max}$ for all routing schemes. As $\epsilon_{\max}$ approaches 1, there would be more cases where the optimal rate allocation for ITS routing does not exist. Thus, $P_{\text{its}}(K, L)$ decreases with $\epsilon_{\max}$ as shown in Fig. 4 (a). As expected, Fig. 4 (b) shows that the throughput of ITS routing is lower than that of MRPS at the cost of secure transmissions. The throughput of ITS routing is higher than that of multipath routing with equal rate allocation, ψ_{eq}, due to the throughput maximization.

Fig. 5 shows $P_{\text{its}}(K, L)$ and the throughputs for various values of L when $K = 4$, $m = 1$, and the maximum erasure probability is $\epsilon_{\max} = 0.5$. For a fixed K, the paths become less reliable as L increases. From this, we can see that the throughput and $P_{\text{its}}(K, L)$ decrease with L. Note that, as mentioned earlier, in the optimal rate allocation for ITS routing, if the solution does not exist, we assume that the equal rate allocation is used. Thus, as $P_{\text{its}}(K, L)$ approaches 0, ψ_{its} approaches ψ_{eq}. This behavior is seen in both Figs. 4 (b) and 5 (b).

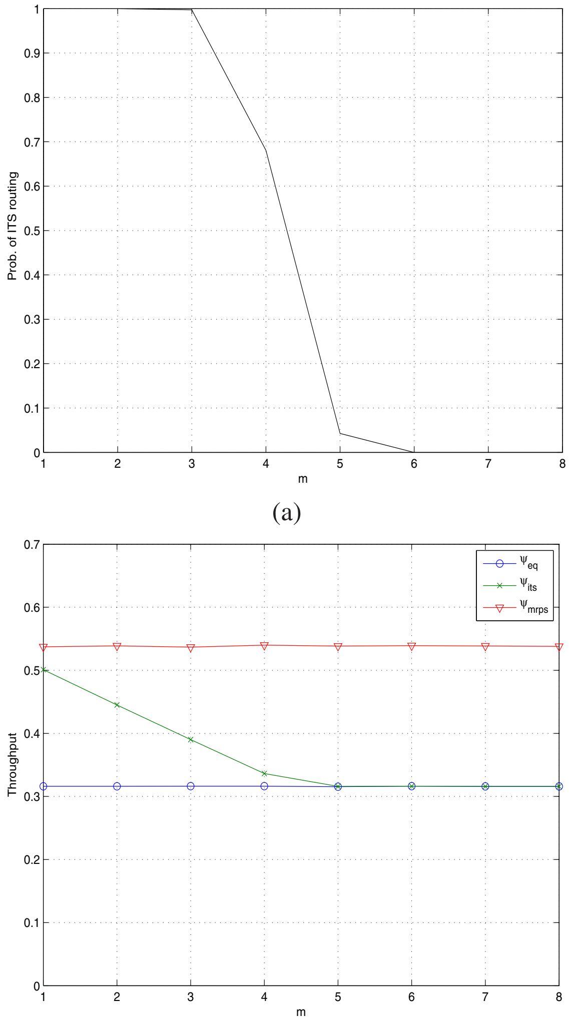
It is expected that the probability of no ITS routing decreases with K when L is fixed through Theorem 2. In other words, $P_{\text{its}}(K, L)$ increases with K. Furthermore, as more multipaths are available, the throughput should also increase with K. In Fig. 6, we present $P_{\text{its}}(K, L)$ and the throughputs for various values of K when $L = 4$, $m = 1$, and the maximum erasure probability is $\epsilon_{\max} = 1$. As expected, the throughput is improved for a large K as shown in Fig. 6



(a)

(b)

Fig. 6. Probability of successful ITS routing and throughputs for various values of K with one EN (i.e., $m = 1$) when $L = 4$ and $\epsilon_{\max} = 1$: (a) Probability of ITS routing; (b) Throughputs of various rate allocations.



(a)

(b)

Fig. 7. Probability of successful ITS routing and throughputs for various values of m when $K = 10$ and $L = 4$ and $\epsilon_{\max} = 0.5$: (a) Probability of ITS successful routing; (b) Throughputs of various rate allocations.

(b) except for the multipath routing with equal rate allocation. Since the throughput is normalized, it will not increase with K for the equal rate allocation as the transmission rate per each path decreases. However, for the optimal single-path routing based on MRPS, the throughput of the best route (that can have the highest throughput among all the possible routes) increases with the number of multipaths, thanks to the MRPS diversity gain [25]. The MRPS diversity gain can also be observed in multipath routing when the optimal rate allocation is used. In Fig. 6 (b), we can see that ψ_{its} also increases with K. From this, we can conclude that the proposed throughput maximization with ITS constraints can provide not only a higher probability of ITS routing, but also a higher throughput as more multipaths are available.

Fig. 7 shows the impact of the number of cooperative ENs, m, where $P_{\text{its}}(K, L)$ and the throughputs for various values of m are presented when $K = 10$ and $L = 4$, and the maximum erasure probability is $\epsilon_{\max} = 0.5$. We can see that $P_{\text{its}}(K, L)$ and ψ_{its} decrease with m as it is more difficult to find the optimal rate allocation for ITS routing for a larger m. If the ITS constraint is not used, the throughput should remain the same regardless the value of m. Thus, ψ_{mrps} and ψ_{eq} become invariant with respect to m as shown in Fig. 7 (b).

VII. Concluding Remarks

In this paper, we studied multipath routing with the SEC modeling for each wireless link in wireless multihop networks. Adopting the notion of ITS, we formulated a throughput maximization problem with ITS constraints as a linear optimization problem to assign optimal rates to multipaths which can be found by solving the linear optimization problem. Coded packets can be divided to transmit over multipaths according to the optimal rates, which results in ITS routing. Although the throughput of ITS routing is lower than that of MRPS which is the maximum ouput transmission rate without ITS constraints, it is more secure against eavesdropping. We studied performance analysis in order to understand ITS routing. It was shown that the equal rate allocation (where all multipaths of an equal transmission rate are used) becomes optimal under symmetric conditions. Asymptotic behaviors of the multipath routing with equal rate allocation had been analyzed for a large number of multipaths. We observed that the optimal rate allocation for ITS routing can provide not only a higher probability of ITS routing, but also a higher throughput as more multipaths are available.

Simulation results showed that the throughput and probability of ITS routing increase with the number of multipaths, K, and decrease with the length of multipaths, L. Furthermore, it was shown that the probability of ITS routing rapidly decreases with the number of potential eavesdropping nodes.

Various problems related to the modeling for wireless links in multihop networks and security issues remain open. For example, the interference between two wireless links closely located should be taken into account. The ITS constraint could be relaxed if the locations of ENs are known or the probability that a node is EN is known.

Appendix

Appendix A: Proof of Theorem 3

Define the following event: $\mathcal{A} = \{\prod_{l=2}^{L} \beta_{k,l} \geq z^{L-1}, \forall k\}$ for a constant $0 < z < 1$. Thus, we have

$$\begin{aligned}\bar{\alpha}^{(\mathrm{eq})}_{K,L} &= \Pr\left(\max_k \beta_{k,1} > \sum_{k=1}^{K} \beta_{k,1} \prod_{l=2}^{L} \beta_{k,l}\right) \\ &\leq \Pr\left(\max_k \beta_{k,1} > \sum_{k=1}^{K} \beta_{k,1} \prod_{l=2}^{L} \beta_{k,l} \;\middle|\; \mathcal{A}\right) \Pr(\mathcal{A}) + \Pr(\mathcal{A}^c) \\ &\leq \Pr\left(\max_k \beta_{k,1} > \sum_{k=1}^{K} \beta_{k,1} z^{L}\right) \Pr(\mathcal{A}) + \Pr(\mathcal{A}^c), \end{aligned} \tag{33}$$

where $\mathcal{A}^c$ denotes the complement set of $\mathcal{A}$.

First, let us focus on $\Pr(\mathcal{A})$. Since $\beta_{k,l}$ is iid, we have

$$\begin{aligned}\Pr(\mathcal{A}) &= \left(\Pr\left(\prod_{l=2}^{L} \beta_{k,l} \geq z^{L-1}\right)\right)^{K} \\ &= \left(\Pr\left(\frac{1}{L-1}\sum_{l=2}^{L} Y_{k,l} \leq a\right)\right)^{K} \\ &= \left(1 - \Pr\left(\frac{1}{L-1}\sum_{l=2}^{L} Y_{k,l} > a\right)\right)^{K},\end{aligned}$$

where $Y_{k,l} = -\log \beta_{k,l}$ and $a = -\log z$. If L is sufficiently large, using large deviations [29], it can be given by

$$\Pr\left(\frac{1}{L-1}\sum_{l=2}^{L} Y_{k,l} > a\right) = e^{-(L-1)I(a)}, \tag{34}$$

for $a > \mu$, where $I(a)$ is the rate function of $Y_{k,l}$. Thus, when $a > \mu$, we have

$$\Pr(\mathcal{A}) = \left(1 - e^{-(L-1)I(a)}\right)^{K}, \tag{35}$$

for a large L. From this, if

$$\lim_{K,L\to\infty} \frac{K}{e^{(L-1)I(a)}} = \lim_{K,L\to\infty} \frac{K}{e^{LI(a)}} = c_1 \tag{36}$$

where c_1 is a constant, we can show that

$$\lim_{K,L\to\infty} \Pr(\mathcal{A}) = e^{-c_1}. \tag{37}$$

Next, we focus on $\Pr\left(\max_k \beta_{k,1} > \sum_{k=1}^{K} \beta_{k,1} z^{L-1}\right)$. We can show that

$$\Pr\left(\max_k \beta_{k,1} > \sum_{k=1}^{K} \beta_{k,1} z^{L-1}\right) = \Pr\left(\max_k \beta_{k,1} > \phi_K K z^{L-1}\right), \tag{38}$$

where $\phi_K = \frac{\sum_{k=1}^{K} \beta_{k,1}}{K}$. Since $\beta_{k,l}$ are iid, it can be shown that

$$\begin{aligned}&\Pr\left(\frac{\max_k \beta_{k,1}}{\phi_K} > K z^{L-1}\right) \\ &= \Pr\left(\frac{\max_k \beta_{k,1}}{\phi_K} > K z^{L-1} \;\middle|\; |\phi_K - \phi| \leq \delta\right) \Pr(|\phi_K - \phi| \leq \delta) \\ &+ \Pr\left(\frac{\max_k \beta_{k,1}}{\phi_K} > K z^{L-1} \;\middle|\; |\phi_K - \phi| > \delta\right) \Pr(|\phi_K - \phi| > \delta) \\ &\leq \Pr\left(\max_k \beta_{k,1} > K z^{L-1}(\phi - \delta)\right) \Pr(|\phi_K - \phi| \leq \delta) \\ &+ \Pr(|\phi_K - \phi| > \delta)\end{aligned} \tag{39}$$

for $0 < \delta < 1$, where $\phi = \mathbb{E}[\beta_{k,l}]$. Since $a = -\log z$ and $a > \mu$, we have

$$K z^{L-1} = \frac{K}{e^{(L-1)a}} < \frac{K}{e^{(L-1)\mu}}. \tag{40}$$

If K and L approach infinity according to (29), we have

$$\lim_{K,L\to\infty} \frac{K}{e^{LI(a)}} = c_1 = 0;$$
$$\lim_{K,L\to\infty} \frac{K}{e^{(L-1)\mu}} = \lim_{K,L\to\infty} \frac{K}{e^{L\mu}} = 0.$$

This implies that

$$\lim_{K,L\to\infty} \Pr(\mathcal{A}) = 1;$$
$$\lim_{K,L\to\infty} \Pr\left(\frac{\max_k \beta_{k,1}}{\phi_K} > K z^{L-1}\right) = 0. \tag{41}$$

Noting that, as $K \to \infty$,

$$\Pr(|\phi_K - \phi| > \delta) \to 0$$
$$\Pr(|\phi_K - \phi| \leq \delta) \to 1$$

in (39), we can conclude that

$$\lim_{K,L\to\infty} \bar{\alpha}^{(\mathrm{eq})}_{K,L} = 0. \tag{42}$$

This completes the proof.

References

[1] E. Gustafsson and G. Karlsson, "A literature survey on traffic dispersion," *IEEE Network*, vol. 11, pp. 28–36, Mar. 1997.

[2] N. F. Maxemchuk, "Dispersity routing," in *Proc. 1975 IEEE ICC*, pp. 41.

[3] N. F. Maxemchuk, "Dispersity routing in store-and-forward networks," Ph.D. dissertation, University of Pennsylvania.

[4] S. J. Lee and M. Gerla, "AODV-BR: backup routing in ad hoc networks," in *Proc. 2000 IEEE WCNC*, vol. 3, pp. 1311–1316.

[5] S.-J. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks," in *Proc. 2001 IEEE ICC*, pp. 3201–3205.

[6] S. Kompella, S. Mao, Y. T. Hou, and H. D. Sherali, "Optimal multipath routing for performance guarantees in multi-hop wireless networks," in *Proc. 2007 IEEE WCNC*, pp. 3987–3992.

[7] G. Parissidis, V. Lenders, M. May, and B. Plattner, "Multi-path routing protocols in wireless mobile ad hoc networks: a quantitative comparison," in *Proc. 2006 International Conf. NEW2AN*, pp. 313–326.

[8] S. Mueller, R. P. Tsang, and D. Ghosal, "Multipath routing in mobile ad hoc networks: issues and challenges," *Performance Tools Appl. Netw. Syst.: Revised Tut. Lectures*, pp. 209–234, 2004.

[9] Y. Ganjali and A. Keshavarzian, "Load balancing in ad hoc networks: single-path routing vs. multi-path routing," in *Proc. 2004 IEEE INFOCOM*, pp. 1120–1125.

[10] S. Waharte and R. Boutaba, "Totally disjoint multipath routing in multihop wireless networks," in *Proc. 2006 IEEE ICC*, pp. 5576–5581.

[11] E. Ayanoglu, C.-L. I, R. D. Gitlin, and J. E. Mazo, "Diversity coding for transparent self-healing and fault-tolerant communication networks," *IEEE Trans. Commun.*, vol. 41, no. 11, pp. 1677–1686, Nov. 1993.

[12] A. Tsirigos and Z. J. Haas, "Multipath routing in the presence of frequent topological changes," *IEEE Commun. Mag.*, vol. 39, pp. 132–138, Nov. 2001.

[13] A. Tsirigos and Z. J. Haas, "Analysis of multipath routing—part I: the effect on the packet delivery ratio," *IEEE Trans. Wireless Commun.*, vol. 3, no. 1, pp. 138–146, Jan. 2004.

[14] P. P. C. Lee, V. Misra, and D. Rubenstein, "Distributed algorithms for secure multipath routing in attack-resistant networks," *IEEE Trans. Netw.*, vol. 15, no. 6, pp. 1490–1501, Dec. 2007.

[15] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, "SecMR—a secure multipath routing protocol for ad hoc networks," *Ad Hoc Netw.*, vol. 5, pp. 87–99, 2007.

[16] P. Papadimitratos and Z. J. Hass, "Secure data communication in mobile ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 343–356, Feb. 2006.

[17] A. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[18] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory* vol. 54, no. 6, pp. 2515–2534, June 2008.

[19] L. Chen and J. Leneutre, "On multipath routing in multihop wireless networks: security, performance, and their tradeoff," *EURASIP J. Wireless Commun. Netw.*, 2009 (doi: 10.1155/2009/946493).

[20] W. Lou, W. Liu, and Y. Fang, "Spread: improving network security by multipath routing," in *Proc. 2003 IEEE MILCOM*, pp. 808–813.

[21] S. Bohacek, J. P. Hespanha, K. Obraczka, J. Lee, and C. Lim, "Enhancing security via stochastic routing," in *Proc. 2002 IEEE ICCCN*, pp. 58–62.

[22] J. Yang and S. Papavassiliou, "Improving network security by multipath traffic dispersion," in *Proc. 2001 IEEE MILCOM*, pp. 34–38.

[23] M. S. Siddiqui, S. O. Amin, J. H. Kim, and C. S. Hong, "MHRP: a secure multi-path hybrid routing protocol for wireless mesh network," in *Proc. 2007 IEEE MILCOM*, pp. 1–7.

[24] A. F. Dana, R. Gowaikar, R. Palanki, B. Hassibi, and M. Effros, "Capacity of wireless erasure networks," *IEEE Trans. Inf. Theory* vol. 52, no. 3, pp. 789–804, Mar. 2006.

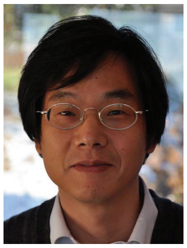
[25] M. Souryal, B. Vojcic, and R. Pickholtz, "Ad hoc, multihop CDMA networks with route diversity in a Rayleigh fading channel," in *Proc. 2001 IEEE MILCOM*, pp. 1003–1007.

[26] M. Park, J. G. Andrews, and S. M. Nettles, "Wireless channel-aware ad hoc cross-layer protocol with multi-route path selection diversity," in *Proc. 2003 IEEE VTC – Fall*, pp. 2197–2201.

[27] R. Knopp and P. A. Humblet, "Information capacity and power control in single-cell multiuser communications," in *Proc. 1995 IEEE ICC*, pp. 331–335.

[28] G. L. O'Brien, "A limit theorem for sample maxima and heavy branches in Galton-Watson trees," *J. Appl. Prob.* vol. 17, pp. 539–545, 1980.

[29] A. Shwartz and A. Weiss, *Large Deviations for Performance Analysis: Queues, Communication, and Computing*. Chapman & Hall, 1995.



Jinho Choi was born in Seoul, Korea. He received B.E. (magna cum laude) degree in electronics engineering in 1989 from Sogang University, Seoul, and the M.S.E. and Ph.D. degrees in electrical engineering from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, in 1991 and 1994, respectively. He is now with the College of Engineering, Swansea University, United Kingdom, as a Professor/Chair of Wireless. His research interests include wireless communications and array/statistical signal processing. He authored two books published by Cambridge University Press in 2006 and 2010. Prof. Choi received the 1999 Best Paper Award for Signal Processing from EURASIP, 2009 Best Paper Award from WPMC (Conference), and is a Senior Member of IEEE. Currently, he is an Associate Editor of IEEE COMMUNICATIONS LETTERS and an Editor of *Journal of Communications and Networks* (JCN) since 2005 and served an Associate Editor of IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY from 2005 to 2007 and ETRI journal.