Dynamic Network Control for Confidential Multi-hop Communications

Yunus Sarikaya, Ozgur Ercetin
Faculty of Natural Science and Engineering
Sabanci University, Istanbul, Turkey
Email: {sarikaya,oercetin}@sabanciuniv.edu

C. Emre Koksal
Department of Electrical and Computer Engineering
The Ohio State University, Columbus, OH
Email: koksal@ece.osu.edu

***Abstract*—We consider the problem of resource allocation and control of multihop networks in which multiple source-destination pairs communicate confidential messages, secretly from the intermediate nodes. We pose the problem as that of network utility maximization, into which confidentiality is incorporated as an additional quality of service constraint. We develop a simple, and yet optimal dynamic control algorithm which combines flow control, routing and end-to-end secrecy-encoding. In order to achieve confidentiality, our scheme exploits multipath diversity and temporal diversity due to channel variability. Our end-to-end dynamic encoding scheme encodes confidential messages over many packets, to be combined at the ultimate destination for recovery. We also evaluated our scheme numerically under various conditions to show its efficacy.**

I. Introduction

In some scenarios (e.g., tactical, financial, medical), confidentiality of communicated information between the nodes is necessary, so that data intended to (or originated from) a node is not shared by any other node. Even in scenarios in which confidentiality is not necessary, it may be dangerous to assume that nodes will always remain uncompromised. Keeping different nodes' information confidential can be viewed as a precaution to avoid a captured node from gaining access to information from other uncaptured nodes.

In this paper, we consider wireless networks in which messages are carried between the source destination pairs cooperatively in a multi-hop fashion via intermediate nodes. In a multihop network, as data packets are transferred, intermediate nodes obtain all or part of the information through directly forwarding data packets or overhearing the transmission of nearby nodes. This poses a clear problem when transferring confidential messages. In this paper, we build efficient algorithms for confidential multiuser communication over multihop wireless networks without the source-destination pairs having to share any secret key a priori. The metric we use to measure the confidentiality is the mutual information leakage rate to the relay nodes, i.e., the *equivocation rate*. We require this rate to be arbitrarily small with high probability and impose this in the resource allocation problem via an additional constraint.

To provide the basic intuition behind our approaches and how the source nodes can achieve confidentiality from the relay nodes, consider the following simple example of a diamond network given in Fig. 1. Let the source node have a single bit of information to be transmitted to the destination node, with *perfect secrecy* (with 0 mutual information leaked) from the relay nodes r_1 and r_2. The issue is that, the source cannot transmit this bit directly over one of the possible paths (through r_1 or r_2), since either r_1 or r_2 would obtain it, violating the confidentiality constraint. This problem can be solved by adding random noise (i.e., randomization bit) on the information bit, and sending the noise and the noise corrupted message over different paths, which can then be combined at the destination. The details of the process is as follows:

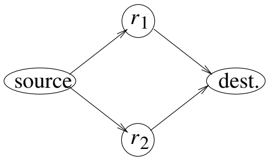


Fig. 1. Diamond network

(1) Let b denote the information bit. The source generates a noise bit N at random, with $\mathbb{P}(N=0)=\mathbb{P}(N=1)=\frac{1}{2}$.
(2) Source node transmits N to relay r_1 and $b\oplus N$ to relay r_2. Then, the relay nodes forward these bits to the destination.
(3) Destination node reconstructs the original bit by a simple xor operation: $b=N\oplus(b\oplus N)$.

Note that with the information available to the relay nodes, there is no way that they can make an educated guess about the information bit, since they have *zero* mutual information: $I(b;N)=I(b;N\oplus b)=0$. Full confidentiality is achieved here at the expense of halving of the data rate, i.e., for each information bit the source has, the network has to carry two bits to the destination. Furthermore, one can see that the existence of multiple paths from the source to the destination is crucial to achieve perfect secrecy. However, a source cannot route the confidential information arbitrarily over the relay nodes. Hiding information from the other nodes can be made possible with a careful design of end-to-end coding, data routing on top of other network mechanisms, flow control and scheduling in order for an efficient resource utilization. Clearly, the example is highly simplistic and ignores many important issues, which we explicitly consider in this paper. In particular:
(a) To achieve confidentiality, one needs to encode blocks of information over multiple packets. We develop a novel adaptive end-to-end encoding scheme, which takes feedback from the network and chooses the appropriate code rates to maintain confidentiality for each block of data.
(b) In a multihop network, each node possibly overhears the same information as it is transmitted over multiple hops. We take into account such accumulation of information over multiple transmissions. Thus, we need to go beyond the scenario

This work was supported in part by European Commission under Marie Curie IRSES grant PIRSES-GA-2010-269132 AGILENet.

given in Fig. 1, in which the paths are disjoint and each intermediate node has only one path crossing.

(c) We combine a variety of strategies developed in the context of information theoretic secrecy with major networking mechanisms such as flow control and routing. Such a unifying framework is non-existent in the literature as it pertains to multihop information transmission. For that purpose, we model the entire problem as that of a network utility maximization, in which confidentiality is incorporated as an additional constraint and develop the associated dynamic flow control, routing, and scheduling mechanisms.

(d) We take into account wireless channel variations in our scheduling and routing policies as well as end-to-end encoding scheme for confidentiality. For that purpose, we assume *instantaneous* channel state information (CSI) at the transmitters.

(e) Our *attacker model* is that of a passive one: while each attacker can overhear all the information transmitted and received by a single node, it is not capable of changing the content of the information the node forwards, nor does it inject phantom messages into the network. In our model, intermediate nodes are entities, compliant with network operations as they properly execute algorithms, but the messages need to be kept confidential from them.

We address the problem in two parts. In the first part, we ignore the delay issue and consider the possibility of encoding over very long blocks of information in order to maximize the confidential data throughput. For any given encoding rate (not necessarily optimized for the network conditions), we provide a dynamic network control scheme that achieves a utility, close to the maximum achievable utility (for those particular encoding rates), subject to *perfect* secrecy constraint, i.e., guaranteeing with probability 1 that an arbitrarily low mutual information is leaked to the intermediate nodes on the confidential message. The main challenges involved in generalizing the network control problem to multihop networks with confidentiality are dynamic end-to-end encoding and multipath routing. The confidential message is encoded over many blocks, which implies that the time-scale involved in physical-layer resource allocation cannot be decomposed from the time scales involved in network-layer resource allocation, eliminating the time-scale separation assumption of standard dynamic control algorithms. This leads to some unique technical issues that were not addressed in the existing studies on network resource allocation. In addition, the existing schemes for wireless multihop networks are not concerned with how information ought to be spatially distributed in the network [1], [2]. Additional "virtual" queues are defined for the leaked information to other nodes in the network to make sure that information from the source node is sufficiently spatially distributed in the network. Hence, unlike the standard multihop dynamic algorithm where the objective is to only increase end-to-end flow rates, in our problem increasing the flow rate and keeping confidentiality of the messages appear as two conflicting objectives.

Next, we consider practical delay requirements for each user, which eliminates the possibility of encoding over an arbitrarily long block. Due to finite codewords, subsequent packets associated with a given secrecy-encoded message cannot be decoupled, eliminating the possibility using standard dynamic control algorithms. For the same reason, achieving perfect secrecy for all confidential messages is not possible. Consequently, we define the notion of *secrecy outage*, and impose a probabilistic constraint on the probability that a message experiences a secrecy outage. This time, we also develop a dynamic policy to choose the encoding rates for each message, based on the instantaneous channel state information, queue states and secrecy outage requirements. We observe that proposed scheme approaches the optimal rates asymptotically, with increasing block size. Finally, we numerically characterize the performance of dynamic control algorithms with respect to several network parameters.

Here, it first must be stressed that even though the flow control is distributed, the scheduling is still assumed to be centralized in this paper. The reason why we design centralized algorithm is that the centralized algorithm provides an upper bound of network performance and a benchmark to evaluate performance of distributed algorithms. However, we note that the results of this work can be extended to distributed implementations using the approach in [3] at the expense of sacrificing some confidential data throughput. The key idea in [3] is to introduce regulators at each node, one for each flow passing through the node. Regulators are mainly utilized to limit arrivals based on the knowledge of average arrival rate. The packets are first queued at the regulator, and they are transferred from the regulator to the corresponding queue only when the size of the regulator is positive. Additionally, we need to keep a virtual queue, which keep track of how much information is accumulated at intermediate nodes. This time, regulators limit the arrival process, and normal and virtual queues are responsible for determining scheduling.

In the following, we develop our dynamic network control for confidential multi-hop communications by focusing on wireless networks. However, as will be discussed later, the proposed framework and developed concepts can be readily applicable to wired networks as well.

II. Related Work

Since the pioneering work of Wyner [4], there has been a wide interest on the variations of the wiretap channel and how to provide secrecy in various cases, mainly under the single hop setting. To give a few examples on the single hop setting, in [5], [6], opportunistic secrecy was introduced, which allows for the exploitation of channel variations due to fading to achieve secrecy, even when the eavesdropper has a higher average signal-to-noise ratio (SNR). Achieving delay-limited secrecy and outage capacity of the wiretap channel were studied in [7]. Multiuser communication with secrecy using cooperative jamming and relaying in the presence of eavesdropper was studied in [8]. The design of the practical codes that approach the promised capacity limits was investigated in [9]. Confidential multihop communication is also considered to some limited extent. In [10], [11] the secrecy capacity scaling problem is addressed. Exploitation of path diversity in order to achieve confidentiality from external eavesdroppers is studied in [12], [13] and for confidentiality via mobility in [14].

Despite the significant progress in information theoretic secrecy, most of the work has focused on physical layer techniques. Therefore, our understanding of the interplay between the confidentiality requirements and the critical functionalities of wireless networks, such as scheduling, routing, and congestion control remains unlimited. Recently, in [15], we have investigated the cross-layer resource allocation problem with confidentiality in a cellular wireless network, where users transmit information to the base station, confidentially from the other users. To our best knowledge, multihop network control with confidentiality has not been investigated before.

III. System Model

We consider a multi-hop wireless network with K source-destination node pairs communicating with each other via intermediate relay nodes. Let S and D be the set of information ingress and egress nodes in the network, respectively. There is no direct connection between the nodes in S and D, and messages from a source node are relayed by intermediate nodes in the network to the intended destination node. For ease of exposition, we consider a set of logical links, L, connecting the nodes in the network, i.e., nodes i and j can communicate only if link $(i,j) \in L$.

All nodes in the network are legitimate nodes. However, each source node in S aims to keep its information confidential from all other nodes in the network except the intended destination node in D. To that end, a source node precodes its message, divides it into multiple pieces, and sends separate pieces over different paths to the destination. Henceforth, none of the intermediate relay nodes in the network will accumulate sufficient amount of information to decode the confidential message.

We assume every channel to be iid block fading, with a block size of N_1 channel uses (physical-layer symbols). We denote the instantaneous achievable rate of the channel between nodes i and j in block t by $R_{ij}(t)$, where $R_{ij}(t)$ is the maximum mutual information between the output symbols of node i and input symbols of node j. Even though our results are general for all channel state distributions, in numerical evaluations, we use Gaussian channels, as will be described in Section VII.

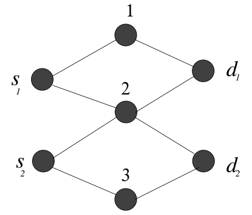


Fig. 2. A diamond shaped multi-hop multi-path network.

We assume the wireless transceivers to operate in a half duplex fashion, i.e., a node cannot transmit and receive simultaneously. Hence, two links sharing a common ingress or egress node cannot be active simultaneously. We define a set of links that can transmit simultaneously as a *set of concurrently active links* indexed by e. Also, let E be the collection of all sets of concurrently active links. Set E depends on the assumed interference model. For example, consider a sample multi-hop network as shown in Fig 2 with node-exclusive interference model. Examples of set of concurrently active links include $\{(s_1,1),(s_2,3),(2,d_1)\}$, $\{(s_1,1),(s_2,3),(2,d_2)\}$, $\{(s_1,2),(1,d_1),(3,d_2)\}$, and $\{(s_2,2),(1,d_1),(3,d_2)\}$. At the beginning of every block, the scheduler chooses a particular set of concurrently active links. We use indicator variable $\mathscr{I}_e(t)$ to represent the scheduler decision, where $\mathscr{I}_e(t)$ is one if set e is scheduled for transmission in block t, and it is zero otherwise. By definition, $\sum_{e\in E} \mathscr{I}_e(t) \leq 1$ for all $t > 0$.

There are K different flows in the network, one for each source-destination node pair. Each flow in the network is identified by the index of its ingress node, and thus, the network flow problem considered in this work can be modeled as a multi-commodity flow problem. Let $\mathscr{I}_{ij}^s(t)$ be the indicator function taking a value of 1 if link (i,j) carries commodity s in block t. Hence, the total flow rate of commodity s over link (i,j) in block t is:

$$\mu_{ij}^s(t) = \begin{cases} R_{ij}(t), & \text{if } (i,j) \in e, \mathscr{I}_e(t) = 1, \mathscr{I}_{ij}^s(t) = 1 \\ 0, & \text{otherwise} \end{cases}. \quad (1)$$

Due to broadcast nature of wireless communications, transmissions are overheard by unintended receivers. At every transmission, overhearing neighboring nodes and the node which receives information from the active link accumulate information for each commodity s. Let k be a node overhearing a transmission of commodity s over link (i,j), i.e., there is a link $(i,k) \in L$. Then, whenever node k is not active transmitting or receiving, i.e., no link originating or terminating at node k is scheduled, it accumulates $f_k^s(t) = \min(R_{ik}(t), \max_{j\neq i} \mu_{ij}^s(t))$ bits of information over block t, since overhearing information cannot exceed the actual transmitted information. We assume that the centralized scheduler has the reach to instantaneous channel state information, i.e., $R_{ij}(t)$ is available causally.

Discussion: The perfect secrecy of multihop wireless communications relies on the fact that individual links experience statistically independent fading. The random channel variations are then exploited by opportunistic algorithms such as the control algorithms presented in Section V and VI. These control algorithms can also be used in a wired network setting, wherein the random variations in the links are due to the congestion control and buffer management mechanisms. The main differences in a wired network setting are: All links can be concurrently active, which in turn relaxes the scheduling constraints to complete set of links in the network; and the capacities of the links are constant, i.e., $R_{ij}(t) = R_{ij}$, for all t.

IV. End-to-End Achievable Confidential Rates

In this section, we analyze the achievable confidential data rate for a given source-destination pair, when the sequence of scheduling and routing decisions are given. Assume that depending on the message length, and routing decisions the entire session for commodity s lasts for N_s blocks, i.e., the destination node receives the complete message at the end of N_s blocks counted from the beginning of the first block the source node started its transmission. This corresponds to a total of $N = N_1 N_s$ channel uses.

Each source node s has a confidential message $W_s \in \{1,\ldots,2^{NR_s^{\text{priv}}}\}$ to be transmitted to an intended destination over

N channel uses. Let the vector of symbols received by node k be $\mathbf{Y}_k^s$. To achieve *perfect secrecy*, the following constraint must be satisfied by node s: for all k,

$$\frac{1}{N} I(W_s, \mathbf{Y}_k^s) \leq \varepsilon, \quad \text{as } N \to \infty. \tag{2}$$

As will be shown shortly, for a given scheduling and routing policy, source s achieves a confidential data rate $R_s^{priv} = \min_{j \neq s} \left\{ R_s - \mathbb{E}\left[f_j^s(t) \right] \right\}$, where R_s is the transmission rate of node s. To achieve this set of rates, we use a secrecy-encoding strategy based on random coding and binning [16] described in the proof of the following theorem.

Theorem 1: Given scheduling and routing decisions, $\mathscr{I}_e(t)$, $\mathscr{I}_{ij}^s(t)$ for all $t > 0$ and for all $(i,j) \in L$, a confidential data rate of

$$R_s^{priv} = \mathbb{E}\left[\sum_{(s,i) \in L} \mu_{si}(t) \right] - \max_{\forall j \neq s} \left\{ \mathbb{E}\left[f_j^s(t) \right] \right\}, \tag{3}$$

is achievable for source s.

The proof of this theorem is in Appendix A. One can notice that, if there exists a node j through which all possible paths between a given source s and its destination are passing, then $R_s^{priv} = 0$ for that source s, since $\mathbb{E}\left[f_j^s(t) \right]$ is identical to $\mathbb{E}\left[\sum_{(s,i) \in L} \mu_{si}(t) \right]$ for that node, j. This underlines the necessity of the existence of multiple paths between a source-destination pair in order for them to achieve non-zero confidential data rate.

Note that, to achieve this confidential data rate of R_s^{priv}, the rate of data, composed of the actual confidential bits and the randomization bits to confuse the intermediate nodes, carried over the network is R_s, which is lower bounded as:

$$R_s \geq \mathbb{E}\left[\sum_{(s,i) \in L} \mu_{si}(t) \right] - \delta, \tag{4}$$

as with probability 1 as $N_1, N_s \to \infty$ for any given $\delta > 0$. This follows directly from strong law of large numbers as

$$\lim_{N_1, N_s \to \infty} \frac{1}{N_s} \sum_{t=1}^{N_s} \sum_{(s,i) \in L} \mu_{si}(t) = \mathbb{E}\left[\sum_{(s,i) \in L} \mu_{si}(t) \right]$$

with probability 1, where the expectation is over the achievable rates of all links $(s,i) \in L$.

Before finalizing this section, note that the rate provided in Theorem 1 is achieved as the number of blocks $N_s \to \infty$. This implies that, encoding for confidentiality is done over an infinitely-long sequence of blocks[1]. In the next section, we provide network mechanisms to maximize a utility function over infinitely many blocks. Following that, we incorporate a more practical constraint of encoding over a finite number of blocks, imposing a hard limit on the decoding delay.

V. Multihop Network Control with Confidentiality

In this section, our objective is to determine a joint scheduling and routing algorithm that maximizes aggregate network utility while achieving perfect secrecy over infinitely many blocks. Initially, we assume that messages are incoming to a source node encoded a priori at a given rate that is not necessarily optimal. More precisely, confidential message of source s is encoded with a fixed rate code $C(2^{NR_s}, 2^{N\alpha_s R_s}, N)$, where the confidential information rate of the encoded packet is $R_s^{priv} = \alpha_s R_s$. We assume end-to-end confidential data rates, $\{\alpha_s R_s,\ s \in S\}$, to lie in the region of achievable end-to-end confidentiality.

Let $U_s(x)$ be utility obtained by source s when the confidential transmission rate is x bits/channel use. We assume that $U_s(\cdot)$ is a continuously differentiable, increasing and strictly concave function. There is an infinite backlog at the transport layer, which contains the secrecy-encoded messages. In each block, source node s determines the amount of encoded information admitted to its queue at the network level. Let $A_s(t)$ be the amount of traffic injected into the queue of source s at block t, and $x_s = \lim_{N_s \to \infty} \frac{1}{N_s} \sum_t A_s(t)$ be long term rate. Our objective is to support the traffic demand to achieve a long term confidential rate that maximizes the sum of utilities of the sources.

The arrival rate, x_s should combine both the confidential information and the randomization bits. Hence, for the arrival rate of x_s, the confidential information rate is $\alpha_s x_s$, and source s attains a long term expected utility of $U_s(\alpha_s x_s)$. Recall that the rate of information obtained by any intermediate node should not exceed the randomization rate, $(1-\alpha_s)x_s$, to ensure perfect secrecy. To that end, we consider the following optimization problem:

$$\max_{A_s(t), \mathscr{I}_e(t), \mathscr{I}_{ji}^s(t)} \sum_{s \in S} U_s(\alpha_s x_s) \tag{5}$$

$$\text{s.t. } x_s \leq \mathbb{E}\left[\sum_{\{i | (s,i) \in L\}} \mu_{si}(t) \right], \forall s \in S \tag{6}$$

$$\mathbb{E}\left[\sum_{\{j | (i,j) \in L\}} \mu_{ij}^s(t) \right] - \mathbb{E}\left[\sum_{\{j | (j,i) \in L\}} \mu_{ji}^s(t) \right] \geq 0, \forall\ i \notin S, D \tag{7}$$

$$\mathbb{E}\left[f_j^s(t) \right] \leq (1-\alpha_s)x_s, \forall s \in S, \forall j \notin S, D, \tag{8}$$

where the expectations are over all channel realizations and scheduling decisions. Constraint (6) ensures the stability of the queues at the source nodes; Constraint (7) is the flow conservation constraint at the intermediate nodes; and Constraint (8) is the confidentiality constraint, which ensures that the information obtained by any of the intermediate nodes does not exceed the rate of the randomization message $(1-\alpha_s)x_s$.

To solve the optimization problem (5)-(8), we employ a cross-layer dynamic control algorithm based on the stochastic network optimization framework developed in [17] . This framework allows the solution of a long-term stochastic optimization problem without requiring the explicit characterization of the achievable rate regions.

Let $Q_s(t)$ denote the queue size at ingress node s. Each intermediate node keeps separate queues $Q_i^s(t)$ for each commodity s. The dynamics of the queues are as follows:

$$Q_s(t+1) = \left[Q_s(t) - \sum_{\{i | (s,i) \in L\}} \mu_{si}(t) \right]^+ + A_s(t),$$

$$Q_i^s(t+1) = \left[Q_i^s(t) - \sum_{\{j | (i,j) \in L\}} \mu_{ij}^s(t) \right]^+ + \sum_{\{j | (j,i) \in L\}} \mu_{ji}^s(t),\ \forall i \neq S, D,$$

[1] The number of blocks need to be large enough for sufficient averaging of the variations in the channels.

where $[.]^+$ denotes the projection of the term to $[0,+\infty]$. The constraint in (8) can be represented by a virtual queue, strong stability of which ensures that the constraint is also satisfied [17], i.e., the perfect secrecy is achieved in our case:

$$Z_j^s(t+1) = \left[Z_j^s(t) + f_j^s(t) - (1-\alpha_s)A_s(t)\right]^+ \tag{9}$$

Note that to perform the update in (9), nodes need to have access to instantaneous CSI of all neighboring nodes.

Control Algorithm 1: The algorithm executes the following steps in each block t:

(1) **Flow control:** For some $H > 0$, each source s injects $A_s(t)$ bits into its queues, where

$$A_s(t) = \operatorname*{argmax}_{A} \left\{ HU_s(\alpha_s A) - Q_s(t)A + \sum_{j \notin S} Z_j^s(t)(1-\alpha_s)A \right\}.$$

(2) **Scheduling:** In each block, t, the scheduler chooses the set of links e if $\mathscr{I}_e(t) = 1$ and flow s on the link $(i,j) \in e$ if $\mathscr{I}_{ij}^s(t) = 1$, where

$$(s,e) = \operatorname*{argmax}_{s\in S, e\in E} \left\{ \sum_{(i,j)\in e} (Q_i^s(t) - Q_j^s(t))\mu_{ij}^s(t) - \sum_{j \notin S,D} Z_j^s(t) f_j^s(t) \right\}$$

Optimality of Control Algorithm: Now, we present our main result showing that our proposed dynamic control algorithm can achieve a performance arbitrarily close to the optimal solution while keeping the queue backlogs bounded.

Theorem 2: If $R_{ij}(t) < \infty$ for all (i,j) links and for all t blocks, then control algorithm satisfies:

$$\liminf_{t\to\infty} \frac{1}{t} \sum_{\tau=0}^{t-1} \sum_{s\in S} \mathbb{E}\left[U_s(\tau)\right] \geqslant U^* - \frac{B}{H}$$

$$\limsup_{t\to\infty} \frac{1}{t} \sum_{\tau=0}^{t-1} \sum_{s\in S} \mathbb{E}\left[Q_s(\tau)\right] \leqslant \frac{B + H(\bar{U} - U^*)}{\varepsilon_1}$$

$$\limsup_{t\to\infty} \frac{1}{t} \sum_{\tau=0}^{t-1} \sum_{s\in S} \sum_{i \notin S,D} \mathbb{E}\left[Q_i^s(\tau)\right] \leqslant \frac{B + H(\bar{U} - U^*)}{\varepsilon_2}$$

where $B, \varepsilon_1, \varepsilon_2$ are positive constants, U^* is the optimal aggregate utility, i.e., the solution of (5-8), and $\bar{U}$ is the maximum possible instantaneous aggregate utility.

Due to space limitations, here we omit the proof, which can be found in our technical report [18]. This theorem shows that it is possible to get arbitrarily close to the optimal utility by choosing H sufficiently large at the expense of proportionally increased average queue sizes.

Discussion: Before we finalize the section, we would like to note that, in this problem we considered a given confidentiality encoding rate. The nature of the problem did not allow us to further maximize over R_s and R_s^{priv}, since we encode information over infinitely many blocks. Consequently, encoding needs to be done at the beginning of the entire session and data that is injected into the source queues are already confidentiality-encoded at the given rates. Hence, the confidentiality encoding rate cannot be changed dynamically during the session, as a response to the network state information observed. However, clearly the maximum accumulated utility is a function of the rate pair R_s, R_s^{priv}. One can ask the question, for which set of pairs, is the sum utility maximized? In Section VII, we numerically evaluate the best rate selection and provide the associated performance as an upper bound for our scheme.

VI. Confidential Multihop Network Control with a Finite Decoding Delay Constraint

In this section, we consider the more practical case where there is a hard constraint on the number of blocks a given confidential message is encoded, i.e., $N_s < \infty$. The entire data including actual confidential bits and the randomization bits sent by source s is $N_s R_s$, where R_s is defined as before. Note that since the number of blocks is finite, the message can be decoded at the destination with a finite delay. We assume that the length of the message $N_s R_s$ is determined a priori based on the required end-to-end delay between the source and destination nodes.

Secrecy outages can be completely avoided in the infinite-block scenario, since the network mechanisms can react to an undesirably large rate of accumulation at a given node at a time scale faster than the number of blocks across which the message is encoded. However, here, the reaction time may be too slow and the accumulated information at a node may already exceed the threshold for perfect secrecy. Consequently, we define the notion of *secrecy outage*, and impose a probabilistic constraint on the event that a message experiences a *secrecy outage*. In particular, we assume that, each source has the knowledge of the amount accumulated information at each node for its message, so it can identify the occurrence of the event of secrecy outage. On the other hand, unlike the infinite-block case, each of the messages encoded over finite number of blocks, k, can be encoded with a different confidential rate $R_s^{k,priv}$, determined based on the history of prior messages experiencing secrecy outages. Thus, a scheme can adaptively vary its confidential data rate to improve the performance.

As in Section V, our objective is to maximize aggregate long-term confidential utility of K source-destination pairs. Let x_s^p be the average rate of confidential messages injected into the queue of the source node s, $p_s^{out}(R_s^{k,priv})$ be the secrecy outage probability of the message k of source node s when encoded with confidentiality rate $R_s^{k,priv}$, and γ_s be the maximum allowable portion of actual confidential bits experiencing secrecy outage. We consider the solution of the following optimization problem:

$$\max_{R_s^{k,priv}, \mathscr{I}_e(t), \mathscr{I}_{ji}^s(t)} \sum_{s\in S} U(x_s^p) \tag{10}$$

$$\text{s. t. } x_s^p \le \mathbb{E}\left[R_s^{k,priv}\right] \tag{11}$$

$$\mathbb{E}\left[R_s^{k,priv} p_s^{out}(R_s^{k,priv})\right] \le \gamma_s \mathbb{E}\left[R_s^{k,priv}\right] \tag{12}$$

$$\mathbb{E}\left[\sum_{\{j|(i,j)\in L\}} \mu_{ij}^s(t)\right] - \mathbb{E}\left[\sum_{\{j|(j,i)\in L\}} \mu_{ji}^s(t)\right] \ge 0, \tag{13}$$

where Constraint (11) ensures that the long-term service rate is larger than the long-term arrival rate; Constraint (12) ensures that the portion of the actual confidential bits experiencing secrecy outage is lower than γ_s; and Constraint (13) is for the flow conservation at intermediate nodes.

Once again, we employ a cross-layer dynamic control algorithm based on the stochastic network optimization framework to solve the optimization problem (10-13). Clearly, in this problem, subsequent scheduling decisions are correlated with each other, since the message is encoded over finite number of

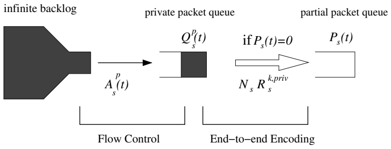


Fig. 3. Queues in a source node used for Control Algorithm 2.

blocks, and thus, the optimality of dynamic control algorithms cannot be claimed. In the following, we develop a sub-optimal solution which performs scheduling by treating the messages as if they are infinite length messages, but at the same time chooses confidential encoding rates of individual messages by keeping account of information experiencing secrecy outages.

The source node s has two separate queues operating at two different time scales as illustrated in Fig.3. The first queue stores the confidential information that has been neither secrecy-encoded nor transmitted in previous blocks. Let $Q_s^p(t)$ denote the length of the confidential information queue at block t. In every block t, $A_s^p(t)$ confidential bits are admitted into the queue, where x_s^p is the long term average rate of admitted confidential bits. Departures from this queue occur only when a new secrecy-encoded message is created. Let $k_s(t)$ be the number of secrecy-encoded messages created by block t. The $k(t)$th confidential message is encoded with rate $R_s^{k_s(t),priv}$, so the actual confidential bits in the message is $N_s R_s^{k_s(t),priv}$ whereas the complete length of the encoded message including the randomization bits is always $N_s R_s$ for every secrecy-encoded message. Once a new confidential message is created, it is admitted to the second queue, which stores the bits of partially transmitted confidential message $k_s(t)$. Let $P_s(t)$ denote the size of this partial message queue at block t. The departures from this queue may occur at any block t depending on the outcome of the scheduling and routing decisions. A new secrecy-encoded message is admitted to the queue only when the partial message queue has emptied, i.e., $P_s(t) = 0$. Hence, $k_s(t+1) = k_s(t) + 1$, if $P_s(t) = 0$.

$$Q_s^p(t+1) = \begin{cases} \left[Q_s^p(t) - N_s R_s^{k_s(t+1),priv}\right]^+ + A_s^p(t) & \text{if } P_s(t) = 0, \\ Q_s^p(t) + A_s^p(t), & \text{otherwise} \end{cases},$$

$$P_s(t+1) = \begin{cases} N_s R_s & \text{if } P_s(t) = 0 \\ \left[P_s(t) - \sum_{i|(s,i)\in L} \mu_{si}(t)\right]^+ & \text{otherwise} \end{cases}.$$

At every intermediate node, there is a queue for each source s. Let $Q_i^s(t)$ denote the size of the queue at intermediate node j for source s.

$$Q_i^s(t+1) = \left[Q_i^s(t) - \sum_{j|(i,j)\in L} \mu_{ij}^s(t)\right]^+ + \sum_{j|(j,i)\in L} \mu_{ji}^s(t).$$

In order to determine the occurrence of secrecy outages, each source keeps track of accumulated information at each intermediate node. Let $Z_i^s(t)$ be the number of bits that must be accumulated by intermediate node i to decode the $k(t)$th confidential message of source s at block t. Note that a secrecy outage occurs in $k(t)$th message, if $Z_i^s(t) = 0$ for any intermediate node i.

$$Z_i^s(t+1) = \begin{cases} (R_s - R_s^{k_s(t+1),priv})N_s & \text{if } P_s(t) = 0 \\ [Z_i^s(t) - f_i^s(t)]^+ & \text{otherwise} \end{cases}.$$

The constraint in (12) can be represented by a virtual queue, strong stability of which ensures that the constraint is also satisfied. The virtual queue keeps account of confidential information experiencing secrecy outages. Hence, there is only an arrival of $R_s^{k,priv}$ if kth message has undergone secrecy outage.

$$V_s^{k+1} = \begin{cases} \left[V_s^k + R_s^{k,priv} - \gamma_s R_s^{k,priv}\right]^+ & \text{if outage in } k\text{th message} \\ \left[V_s^k - \gamma_s R_s^{k,priv}\right]^+ & \text{if no outage in } k\text{th message} \end{cases}.$$

Control Algorithm 2 (with Finite Encoding Block):
For each source s:

(1) End-to-end Encoding: At every generation of new confidential message, i.e., $P_s(t) = 0$, let $k_s(t+1) = k_s(t) + 1$, and determine end-to-end confidential encoding rate:

$$R_s^{k_s(t+1),priv} = \underset{r}{\text{argmax}} \left\{ Q_s^p(t) - V_s^{k_s(t)} \left(r p_s^{out}(r) - r\gamma_s \right) \right\}$$

(2) Flow control: At each block t, for some $H > 0$, each source s injects $A_s^p(t)$ confidential bits into its queues

$$A_s^p(t) = \underset{a}{\text{argmax}} \left\{ HU_s(a) - Q_s^p(t)a \right\}.$$

(3) Scheduling: At each block, t , the scheduler chooses the set of links e if $\mathscr{I}_e(t) = 1$ and flow s on the link $(i,j) \in e$ if $\mathscr{I}_{ij}^s(t) = 1$, where

$$(s,e) = \underset{s\in S, e\in E}{\text{argmax}} \left\{ \sum_{(s,i)\in e} \left(\frac{R_s}{R_s^{k_s(t),priv}} Q_s^p(t) + P_s(t) - Q_i^s(t) \right) \mu_{si}(t) \right.$$
$$\left. + \sum_{(i,j)\in e} \left(Q_i^s(t) - Q_j^s(t) \right) \mu_{ij}^s(t) - \sum_{j\notin S,D} Z_j^s(t) f_j^s(t) \right\}$$

where $Q_s^p(t)$ is multiplied by $R_s / R_s^{k_s(t),priv}$ in order to normalize it to the size of other queues in the network.

Note that secrecy outage probability $p_s^{out}(R)$ can only be calculated if the scheduling decisions are known a priori. Since this is not the case, we use an estimate of secrecy outage probability as discussed in Section VII.

VII. Numerical Results

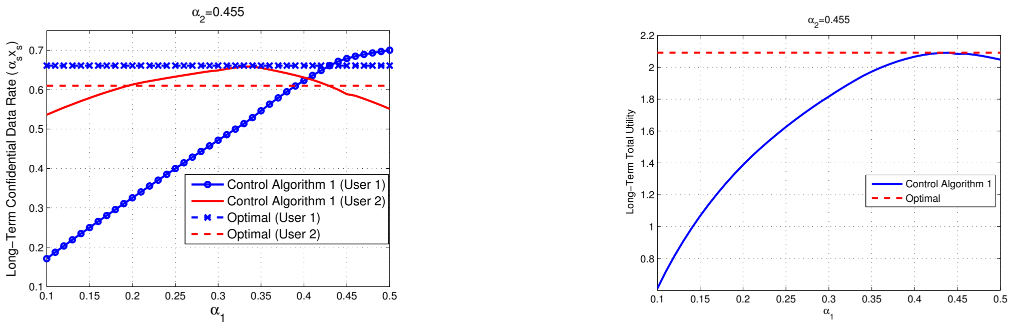
In our numerical experiments, we have considered the network depicted in Fig. 2. The channels between nodes are modeled as iid Rayleigh fading Gaussian channels. The noise normalized transmit power is taken as constant and identical to $P = 1$ in every block and for all nodes. Let the power gain of the channel between nodes i and j be $h_{ij}(t)$ at block t. Then, as $N_1 \to \infty$, $R_{ij}(t) = \log(1 + Ph_{ij}(t))$. The power gains of the channels are exponentially distributed, where the means of the link are as given in Table I. We consider a logarithmic utility function as $U_s(t) = \kappa + \log(A_s^p(t))^2$, where $A_s^p(t)$ is the confidential information admitted in block t. Note that, $A_s^p(t) = \alpha_s A_s(t)$ for the control algorithm presented in Section V. We take $\kappa = 3$ and $H = 100$ in all experiments.

TABLE I
Mean channel gains

$(s_1, 1)$	$(s_1, 2)$	$(s_2, 2)$	$(s_2, 3)$	$(1, d_1)$	$(2, d_1)$	$(2, d_2)$	$(3, d_2)$
6	8	10	4	8	6	4	6

In Fig. 4a-4b, we investigate the performance of dynamic control algorithm presented in Section V. For the network

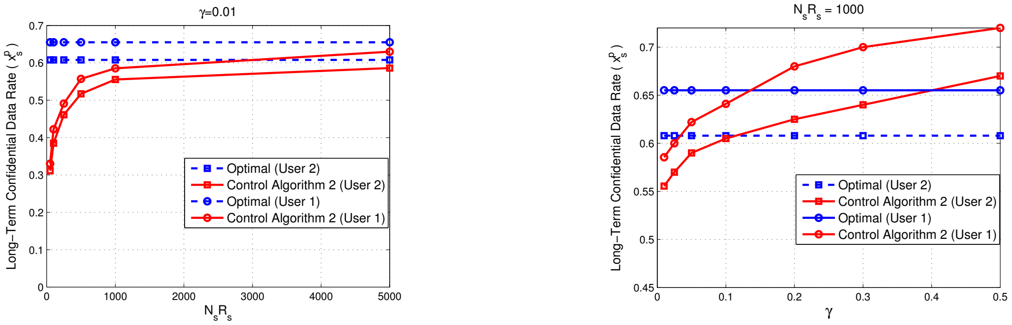
[2] We utilize logarithmic utility function to provide proportional fairness.



(a) α_1 vs Long-Term Confidential Data Rate $(\alpha_s x_s)$

(b) α_1 vs Long-term Total Utility

Fig. 4. Performance evaluation of Control Algorithm 1 presented in Section V.



(a) N_sR_s vs Long-Term Confidential Data Rate (x_s^p)

(b) γ vs Long-Term Confidential Data Rate (x_s^p)

Fig. 5. Performance evaluation of Control Algorithm 2 presented in Section VI.

depicted in Fig. 2, we numerically obtain the encoding rates resulting in maximum long-term total utility for source s, α_s^*. Specifically, we obtain $\alpha_1^* = 0.435$ and $\alpha_2^* = 0.455$ which corresponds to long-term average arrival rates $x_1^* = 1.52$ and $x_2^* = 1.34$, respectively. In the experiments, we fix $\alpha_2 = \alpha_2^*$ and vary the value of α_1 to analyze the effect of α_s on the confidential data rates and total utility. From Fig. 4a, we first notice that, long-term confidential data rate of source s_1 increases with increasing α_1, since source s_1 sends more confidential information for each encoded message. It is interesting to note that long-term confidential data rate of source s_2 increases initially with increasing α_1. This is because for low α_1 values, in order to satisfy fairness between sources, source s_1 admits more packets to its queue (e.g., $x_1 = 1.71$, when $\alpha_1 = 0.1$), and hence its queue size becomes higher. As a result, scheduling decisions are given according to emphasis of the stability of source s_1's queue, and thus the long-term arrival rate of source s_2 is lower when α_1 is smaller (e.g., $x_2 = 1.18$ when $\alpha_1 = 0.1$). However, when α_1 is high, the emphasis on the scheduling decisions is to satisfy the perfect secrecy, and source s_1 should divide its transmission over the paths more equally at the expense of lower long-term arrival rates, x_1 and x_2. Fig. 4b depicts the relationship between α_1 and the long-term total utility. As expected, the total utility increases with increasing α_1 until $\alpha_1 = \alpha_1^*$. As α_1 increases, there is a gain due to incorporating more confidential information into each encoded message of source s_1. However, when α_1 is high, long-term arrival rates of both sources decrease as indicated previously. Thus, when $\alpha_1 > \alpha_1^*$, the loss due to decrease in x_1 and x_2 dominates the gain due to increasing α_1.

We next analyze the performance of control algorithm presented in Section VI. In numerical experiments, we estimate $p_s^{out}(R)$ with $\frac{R^2}{(R_s)^2}$ for $0 < R < R_s$. In Fig. 5a, the effect of increasing N_sR_s on the long-term confidential data rate, x_s^p, is shown. We first take the confidentiality outage parameter, $\gamma_s = 0.01$, for all users. Fig. 5a depicts that when $N_sR_s = 50$ [3], the long-term confidential data rate has reduced by approximately 50% compared to the optimal rates obtained for $N_s \to \infty$. However, the confidential data rate increases with increasing N_sR_s, and it gets close to the optimal confidential data rates, $\alpha_s^* x_s^*$, when N_sR_s is large enough, i.e., $N_sR_s = 5000$. This is due to fact that when the transmission of a message takes smaller number of blocks, the portion of confidential bits inserted into the codeword, $R_s^{k,priv}/R_s$, gets smaller to satisfy the confidentiality constraint. In addition, as the N_sR_s increases, the correlation between subsequent packets associated with a given secrecy-encoded message decreases, so iid approximation of control algorithm presented in Section VI becomes more accurate. Finally, we investigate the effect of confidentiality outage parameter, $\gamma_s = \gamma$ for all sources, on x_s^p. Fig. 5b shows that when the confidentiality outage constraint is relaxed, i.e., γ is increased, the long-term confidential data rate increases. This result is expected, since sources can insert more confidential information into the encoded message, $R_s^{k,priv}$, with a higher secrecy outage parameter. Note that, the optimal confidential data rates is obtained for the case where there is no secrecy outages. Thus, after $\gamma = 0.15$, the long-term confidential data rates exceeds the optimal confidential data rates.

[3] If the average rate in a block t is 0.5 bits/channel use, the message is approximately transmitted in 100 blocks.

VIII. Conclusion

In this paper, we obtained achievable confidential data rate regions of wireless multihop networks, where the message is encoded over long blocks of information. Then, we designed a dynamic control algorithm for a given encoding rate and we prove that our algorithm achieves utility arbitrarily close to the maximum achievable utility. Next, we described a sub-optimal algorithm for the system, where the messages are encoded over finite number of blocks. The simulation results verify the efficacy of the algorithms, and we show that the proposed algorithm asymptotically approaches the optimal rates.

As a future direction, we will investigate distributed version of our dynamic control algorithms, where the scheduler decision is given according to local information. We will also consider the case, where transmitters only obtain imperfect channel state information of the links.

References

[1] Y. Chen, R. Hwang, and Y. Lin, "Multipath qos routing with bandwidth guarantee," in *Proc. IEEE Global Telecommunications Conf.*, vol. 4, Sep. 2001.

[2] X. Lin and N. B. Shroff, "Utility maximization for communication networks with multipath routing," *IEEE Transactions on Automatic Control*, vol. 51, pp. 766–781, May 2006.

[3] L. Bui, A. Eryilmaz, R. Srikant, and X. Wu, "Joint asynchronous congestion control and distributed scheduling for multi-hop wireless networks," *Proc. IEEE INFOCOM*, pp. 1–12, April 2006.

[4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–138, Oct. 1975.

[5] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4687–4698, Oct. 2008.

[6] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2470–2492, June 2008.

[7] O. Gungor, J. Tan, C. E. Koksal, H. E. Gamal, and N. B. Shroff, "Joint power and secret key queue management for delay limited secure communication," in *Proc. IEEE Conf. Computer Communications (Infocom)*, (San Diego, CA), March 2010.

[8] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. on Signal Processing*, vol. 58, pp. 4033–4039, March 2010.

[9] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevic, "Secure nested codes for type ii wiretap channels," in *Proc. IEEE Information Theory Workshop*, (Lake Tahoe, CA), Sep. 2011.

[10] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inform. Theory*, vol. 58, pp. 3000–3015, May 2012.

[11] C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Secret communication in large wireless networks without eavesdropper location information," in *Proc. IEEE Conf. Computer Communications (Infocom)*, (Orlando, FL), pp. 1152–1160, March 2012.

[12] N. Cai and R. Yeung, "Secure network coding," in *Proc. IEEE Int. Symposium Inform. Theory*, (Lausanne, Switzerland), June 2002.

[13] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, pp. 612–613, Nov. 1979.

[14] W. Lou, W. Liu, and Y. Fang, "Spread: enhancing data confidentiality in mobile ad hoc networks," in *Proc. IEEE Conf. Computer Communications (Infocom)*, pp. 2404–2413, March 2004.

[15] C. E. Koksal, O. Ercetin, and Y. Sarikaya, "Control of wireless networks with secrecy," *IEEE/ACM Trans. on Networking*. to appear.

[16] A. E. Gamal and Y. Kim, *Network Information Theory*. Cambridge University Press, 2011.

[17] L. Georgiadis, M. J. Neely, and L. Tassiulas, "Resource allocation and cross-layer control in wireless networks," *Foundations and Trends in Networking*, vol. 1, no. 1, 2006.

[18] Y. Sarikaya, O. Ercetin, and C. E. Koksal, "Dynamic network control for confidential multi-hop communications." http://www.arxiv.org/abs/1301.1002, Jan. 2013.

Appendix A
Proof of Theorem 1

To begin, node s generates $2^{N(R_s-\delta)}$ random binary sequences. Then, it assigns each random binary sequence to one of $2^{NR_s^{\text{priv}}}$ bins, so that each bin contains exactly $2^{N(R_s-R_s^{priv}-\delta)}$ binary sequences. We call the sequences associated with a bin, the *randomization sequences* of that bin. Each bin of source s is one-to-one matched with a confidential message $w \in \{1,\dots,2^{NR_s^{\text{priv}}}\}$ randomly and this selection is revealed to the destination and all nodes before the communication starts. Then, the stochastic encoder of node s selects one of the randomization sequences associated with each bin at random, independently and uniformly over all randomization sequences associated with that bin. Whenever a message is selected by node s, this particular randomization message is used. This selection is not revealed to any of the nodes nor to the destination.

Let us denote the randomization sequence of message W_s as W_s^r for source s, and the transmitted vector of channel symbols as $\mathbf{X_s} = [X_s(1),\dots,X_s(N_s)]$, where $X_s(t)$ represents the transmitted vector of N_1 symbols in block t. The received signal at intermediate *relay* node j is $\mathbf{Y_j^s} = [Y_j^s(1),\dots,Y_j^s(N_s)]$, where $Y_j^s(t)$ represents the received vector of symbols at node j in block t. Also, the received signal at overhearing neighbor node i is $\mathbf{Z_i^s} = [Z_i^s(1),\dots,Z_i^s(N_s)]$. Assume that there are n overhearing neighbor nodes of source s. The equivocation analysis follows directly for a given scheduling/routing decision. For any given intermediate node j, conditional entropy is given as

$$
\begin{aligned}
&H(W_s|Y_j^s) = I(W_s;Z_1^s,\dots,Z_n^s|Y_j^s) + H(W_s|Z_1^s,\dots.,Z_n^s) \\
&\geq I(W_s;Z_1^s,\dots,Z_n^s|Y_j^s) && (14)\\
&= I(W_s,W_s^r;Z_1^s,\dots Z_n^s|Y_j^s) - I(W_s^r;Z_1^s,\dots,Z_n^s|Y_j^s,W_s) && (15)\\
&= I(W_s,W_s^r;Z_1^s,\dots Z_n^s|Y_j^s) - H(W_s^r|Y_j^s,W_s) + H(W_s^r|Z_1^s,\dots,Z_n^s,W_s) \\
&\geq I(W_s,W_s^r;Z_1^s,\dots,Z_n^s|Y_s) - H(W_s^r|Y_j^s,W_s) && (16)\\
&\geq I(W_s,W_s^r;Z_1^s,\dots,Z_n^s|Y_j^s) - N\varepsilon_1 && (17)\\
&= I(X_s,Z_1^s,\dots,Z_n^s|Y_j^s) - I(X_s,Z_1^s,\dots,Z_n^s|Y_j^s,W_s,W_s^r) - N\varepsilon_1 && (18)\\
&\geq I(X_s;Z_1^s,\dots,Z_n^s|Y_j^s) - N(\varepsilon_1+\varepsilon_2) && (19)\\
&= I(X_s,Z_1^s,\dots,Z_n^s) - I(X_s;Y_j^s) - N(\varepsilon_1+\varepsilon_2) && (20)\\
&\geq \sum_{t=1}^{N_2}\Big[I(X_s(t);Z_1^s(t),\dots,Z_n^s(t)) - I(X_s(t);Y_j^s(t))\Big] - N(\varepsilon_1+\varepsilon_2) && (21)\\
&\geq N\left[\left(\mathbb{E}\left[\sum_{(s,i)\in L}\mu_{si}(t)\right]-\delta\right) - \mathbb{E}\left[f_j^s(t)\right] - (\varepsilon_1+\varepsilon_2+\varepsilon_3)\right] && (22)
\end{aligned}
$$

with probability 1, for any positive $(\varepsilon_1,\varepsilon_2,\varepsilon_3)$ triplet and arbitrarily small δ, as $N_1,N_2 \to \infty$. Here, (15) is by the chain rule, (17) follows from the application of Fano's equality, (18) follows from the chain rule and that $(W_s,W_s^r) \leftrightarrow X_s \leftrightarrow (Z_1^s,\dots.,Z_n^s,Y_j^s)$ forms a Markov chain, (19) holds since $I(X_s,Z_1^s,\dots,Z_n^s|Y_j^s,W_s,W_s^r) \leq N\varepsilon_2$ as the transmitted symbols sequence X_s is determined w.p.1 given (Y_j^s,W_s,W_s^r), (20) follows from the chain rule, (21) holds since the fading processes are iid, and finally (22) follows from strong law of large numbers. ■