Control of Multi-Hop Wireless Networks with Security Constraints

Qiuming Liu [†,‡], Li Yu [†], Jun Zheng [†]
[†] School of Electronic Information and Communications,
Huazhong University of Science and Technology, Wuhan, China, 430074
[‡] School of Soft Engineering, Jiangxi University of Science and Technology, Nanchang, China, 330013
E-Mail: liuqiuming@hust.edu.cn; hustlyu@hust.edu.cn; junzheng@hust.edu.cn;

***Abstract*—We consider a control problem in wireless multi-hop networks in which source-destination pairs desire to secure communication. Specifically, a control algorithm is proposed based on the stochastic network optimization to maximize a global utility function, subject to end-to-end secrecy transmission and network stability. To achieve secure communication, we firstly exploit an independent randomization encoding strategy to guarantee the multi-hops secrecy transmission. Then, the control algorithm is decomposed into flow control, routing and resource allocation. Based on the control algorithm, each node makes decisions on the arrival confidential data as well as the users and links. The numerical analysis illustrates that the proposed algorithm can achieve a utility result, arbitrarily close to optimal value.**

I. Introduction

Wireless ad hoc network is a decentralized type of wireless networks which consists of a set of nodes. Each node communicates with each other over a wireless channel using multi-hop transmission. Due to the broadcast characteristics of wireless channel, the confidential message is susceptible to eavesdropping. This motivates us to consider secrecy as a quality of service (QoS) constraint in the process of network design. Since Wyner [1] opened a pioneer work to solve the security problem in wireless channel, lots of works have been devoted to secrecy issue. Liang *et al.* [2] studied a single hop wireless network in which the base station attempted to transmit confidential message securely to multiuser, they proposed a dynamic control algorithm to obtain the maximization of network utility. In [3], Koksal *et al.* also studied a secure wireless network, in which an optimal cross-layer resource allocation algorithm is proposed to maximize the network utility function. Later, Wang *et al.* [4] studied the scheduling problem in cellular network, they developed an effective scheduling policy, jointly considering the security and network stability, to maximize the secrecy rate. The secrecy scheduling in wireless network has been extensively investigated, such as OFDMA-based network [5], [6] and cognitive wireless network [7], [8], [9], [10]. Although these security control algorithms obtained good network performance, most of them were designed for one-hop wireless network. Few works have been done on multi-hop wireless networks. In [11], [12], the authors developed an optimal control for multi-hop wireless network. To maximize the throughput of network, a dynamic strategy was proposed to make decision in each slot. However, they did not consider the secure communication constraint. In [13], [14], the authors, relaxed the assumptions on designing control policy, investigated the secrecy capacity scaling law problem in large scale multi-hop networks. There are a few number of works on control algorithm in wireless multi-hop networks with secure communication constraint. In [15], a dynamic control policy is developed in multi-hop line network. Recently, Sarikaya *et al.* [16] considered a general multi-hop network topology. They proposed a dynamic encoding strategy to encode the confidential data by exploiting multi-path transmission at the expense of sacrificing the data rate, where the channel block is asymptotically large. Based on the stochastic network optimization [17], a control policy, combining flow control, routing and resource allocation, was developed to choose encoding rate for each confidential message, such that the network utility function is maximized. However, the works mentioned above either focused on one-hop wireless network scenario or employed multi-path transmission to guarantee the secrecy in multi-hop wireless networks.

In this paper, we address the control problem in multi-hop wireless network with the constraint of secure communication. In particular, we design a control algorithm to achieve a utility, closed to the maximum utility value, subject to secrecy communication and network stabilization. The control algorithm gives a control decision in each slot to choose confidential message. We exploit an independent randomization encoding strategy to displace the multi-path transmission strategy in [16]. In addition, We are aimed to maximize the long-term average utility value, while in [16], the control algorithm is based on the separation of time scales. According to the stochastic network optimization, the control algorithm can be decomposed into flow control, routing and resource allocation. We also prove that the performance of control algorithm can arbitrarily close to the optimal utility result.

The rest of the paper is organized as follows. Section II introduces the system model and the problem formulation. The independent randomization encoding strategy is presented in section III. In section IV, we develop a control algorithm to solve the formulated problem, and the performance of proposed algorithm is analyzed in section V. Section VI evaluates the algorithm. Finally, the paper is concluded in section VII.

978-1-5090-5935-5/17/$31.00 ©2017 IEEE

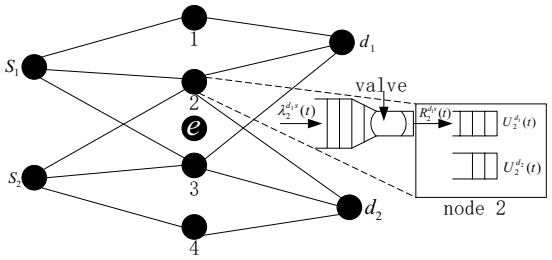


Fig. 1. Multi-hop network

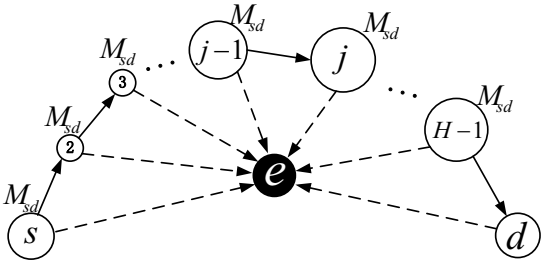


Fig. 2. Multi-hop secure transmission

II. System Models and Problem Formulation

A. System Models

We consider a wireless multi-hop network with M legitimate nodes or users and L links connecting the nodes. For a link $l \in \{1, 2, ..., L\}$, we define $T(l)$ and $D(l)$ as the transmitter and receiver of link l, respectively. As shown in Fig. 1, each node communicates with its destination via intermediate relay nodes. Let E be the set of eavesdroppers in the network. Each source node desires to securely transmit its message against the eavesdroppers. The network operates on a time-slotted model, in which the slot is normalized to integral unit $t \in \{0, 1, 2, ...\}$. We also assume the wireless channel is an independent and identically distributed (i.i.d) block fading channel. Let $\vec{S}(t) = (S_1(t), ..., S_L(t))$ be the channel state vector of network in slot t, and $S_l(t)$ is the channel state of link l. We note that $S_l(t)$ consists of N channels where N is sufficiently large, such that we can exploit an independent randomization encoding strategy to guarantee the end-to-end secrecy communication. Let $R_l(t)$ denote the achievable rate on link l in slot t, and $\bar{R}_l^e(t)$ be the maximum overhearing rate of eavesdropper e. We assume the network can obtain the perfect instantaneous Channel State Information (CSI) including legitimate nodes and eavesdroppers. Since the network consists multiple flows and each for a particular source-destination pair, we identify each flow by its destination node $c \in \{1, ..., M\}$. In each slot t, let $\lambda_n^{cs}(t)$ be the confidential data arrived at node n and destined for node c, and it is bounded by $\lambda_n^{c\max}$. A control valve determines $R_n^{cs}(t)$ confidential data to admit the network. Thus, the network flow problem is regarded as a multi-commodity problem. For each commodity c, $Q_n^c(t)$ represents its backlog at node n. If $c = n$, $Q_n^n(t) = 0$ for all n and t.

Due to the broadcast characteristics of wireless channel, message is overheard by eavesdroppers. Thus, for each transmission, we need to encode the message to secure from the eavesdroppers. The encoder uses the Wyner's encoding scheme [1], Specifically, in each slot, for a link l, the transmitter, according to $R_l(t)$ and $\bar{R}_l^e(t)$, chooses $R_n^s(t)$ (may contain multiple commodities) confidential message from its arrival data. Then an independent randomization encoding strategy is employed to provide secrecy. Since the data rate of link l is $R_l(t)$ and the maximum eavesdropper's rate is $\bar{R}_l^e(t)$, the output confidential message rate $R_l^s(t)$ should be no larger than secrecy channel capacity $R_l(t) - \bar{R}_l^e(t)$, and if $R_l(t) - \bar{R}_l^e(t) < 0$, $R_l^s(t) = 0$, such that we can guarantee the secrecy from the eavesdropper in one hop transmission. In Section III, we will discuss that the confidential message can be securely transmitted over the entire multi-hop path if we exploit the independent randomization encoding strategy.

B. Problem Formulation

We are aimed to develop a control algorithm to stable the network and guarantee the end-to-end secrecy communication. Specifically, in each slot, the controller determines the rate of confidential message admitted to the network, and decides which user can be transmitted on the links. To evaluate the performance of the proposed algorithm, we define a set of utility function $U_n^c(\bar{r}_n^{cs})$, which represents the "satisfaction" received by sending confidential message from node n to node c and $\bar{r}_n^{cs}$ bits/slot is the time average confidential message rate. We also assume the utility function is a concave and non-decreasing function. Thus, the optimization problem can be formulated as follows:

$$\begin{aligned} \text{Maximize}: \quad & \sum_{n,c} U_n^c(\bar{r}_n^{cs}) \\ \text{Subject to}: \quad & 0 \le R_n^{cs}(t) \le \lambda_n^{cs}(t) \ \text{ for all } (n,c) \end{aligned} \tag{1}$$

where $\lambda_n^{cs}(t)$ is the confidential data generated by node n to node c in slot t. The constraint indicates that the admitted confidential data is less than the generated data. $\bar{r}_n^{cs}$ is the achievable long-term average confidential data rate, which is defined as follows:

$$\bar{r}_n^{cs} \triangleq \lim_{t\to\infty} \frac{1}{t} \sum_{\tau=0}^{t-1} \mathbb{E}\{R_n^{cs}(\tau)\}, \tag{2}$$

where $R_n^{cs}(t)$ is the confidential data rate selected in each slot t.

III. Secure Multi-Hop Transmission Strategy

In each hop transmission, we employ a codebook to encode the confidential message according to the maximal eavesdropper's rate R_e^*. The end-to-end confidential message is secured against from the eavesdroppers if

- The error probability of decoding the confidential message at each hop can be made arbitrarily small as $N \to \infty$, and

$$
\begin{aligned}
I(M_{s,d};\mathbf{Y}_e) &= I(M_{s,d};\mathbf{Y}_e(1),...,\mathbf{Y}_e(H)) \\
&\overset{(a)}{\leq} I(M_{s,d};\mathbf{Y}_{e_1^*},...,\mathbf{Y}_{e_H^*}) \\
&= I(M_{s,d},M_1^x,...,M_H^x;\mathbf{Y}_{e_1^*},...,\mathbf{Y}_{e_H^*}) - I(M_1^x,...,M_H^x;\mathbf{Y}_{e_1^*},...,\mathbf{Y}_{e_H^*}|M_{s,d}) \\
&\overset{(b)}{\leq} I(\mathbf{X}_1,...,\mathbf{X}_H;\mathbf{Y}_{e_1^*},...,\mathbf{Y}_{e_H^*}) - H(M_1^x,...,M_H^x|M_{s,d}) + H(M_1^x,...,M_H^x|\mathbf{Y}_{e_1^*},...,\mathbf{Y}_{e_H^*},M_{s,d}) \\
&\overset{(c)}{=} \sum_{i=1}^{H} I(\mathbf{X}_1,...,\mathbf{X}_H;\mathbf{Y}_{e_i^*}|\mathbf{Y}_{e_1^*},...,\mathbf{Y}_{e_{i-1}^*}) - H(M_1^x,...,M_H^x) + \sum_{i=1}^{H} H(M_i^x|M_{s,d},\mathbf{Y}_{e_1^*},...,\mathbf{Y}_{e_H^*},M_1^x,...,M_{i-1}^x) \\
&= \sum_{i=1}^{H}\Bigg[I(\mathbf{X}_i;\mathbf{Y}_{e_i^*}|\mathbf{Y}_{e_1^*},...,\mathbf{Y}_{e_{i-1}^*}) + I(\mathbf{X}_1,...,\mathbf{X}_{i-1},\mathbf{X}_{i+1},...,\mathbf{X}_H;\mathbf{Y}_{e_i^*}|\mathbf{Y}_{e_1^*},...,\mathbf{Y}_{e_{i-1}^*},\mathbf{X}_i) - NR_i^x \\
&\quad + N\frac{\epsilon_1}{H} + H(M_i^x|\mathbf{Y}_{e_i^*},M_{s,d})\Bigg] \\
&\overset{(d)}{\leq} \sum_{i=1}^{H}\left[H(\mathbf{Y}_{e_i^*}|\mathbf{Y}_{e_1^*},...,\mathbf{Y}_{e_{i-1}^*}) - H(\mathbf{Y}_{e_i^*}|\mathbf{Y}_{e_1^*},...,\mathbf{Y}_{e_{i-1}^*},\mathbf{X}_i) - NR_i^x + N\frac{\epsilon_1+\epsilon_2}{H}\right] \\
&\overset{(e)}{\leq} \sum_{i=1}^{H}\left[H(\mathbf{Y}_{e_i^*}) - H(\mathbf{Y}_{e_i^*}|\mathbf{X}_i) - NR_i^x + N\frac{\epsilon_1+\epsilon_2}{H}\right] \\
&= \sum_{i=1}^{H}\left[I(\mathbf{X}_i;\mathbf{Y}_{e_i^*}) - NR_i^x + N\frac{\epsilon_1+\epsilon_2}{H}\right] \\
&\overset{(f)}{\leq} \sum_{i=1}^{H}\left[NI(X_i;Y_{e_i^*}) - NR_i^x + N\frac{\epsilon_1+\epsilon_2}{H}\right] \\
&= N(\epsilon_1+\epsilon_2)
\end{aligned}
\tag{3}
$$

- The message leakage rate of eavesdropper over the entire path, i.e., $\frac{I(M_{s,d};\mathbf{Y}_e)}{N}$, can be made arbitrarily small $\forall e \in E$ as $N \to \infty$ for almost all source and destination pairs.

For a given source and destination pair (s,d), as shown in Fig.2, the message $M_{s,d}$ is assumed to transmit H hops to its destination. During the transmission, the scheduler observes the CSI of eavesdropper when considering the secrecy encoding. If $\frac{I(M_{s,d};\mathbf{Y}_e(1),\mathbf{Y}_e(2),...,\mathbf{Y}_e(H))}{N}$ can be made arbitrarily small, then the second condition can be satisfied, where $\mathbf{Y}_e$ is the hop h's observation vector at eavesdropper $e \in E$.

To secure the confidential message, we develop a secrecy codebook for each hop's transmission. The secrecy codebook is designed according to the possible maximum rate of eavesdropper. For a given hop i, the secrecy encoder generates $2^{N(R_i+R_i^x-\frac{\epsilon_1}{H})}$ codewords each entry with i.i.d $\mathcal{CN}(0,P)$, where R_i is the achievable rate of hop i, R_i^x ($R_i^x = \max\{0, R_i - R_e^*\}$) is the corresponding confidential message rate and $\epsilon_1 > 0$ is some constant. Then these codewords are distributed into 2^{NR_i} bins. Let $(M_{s,d}, M_i^x)$ denote a codeword, where $M_{s,d}$ is the confidential message (bin index), and M_i^x is the randomization message (codeword index). Before transmitting the confidential message $M_{s,d}$, the secrecy encoder of hop i randomly and uniformly selects a codeword in the bin of $M_{s,d}$. In addition, along the multi-hop path, each transmitter do the secrecy encoding independently and randomly, i.e., if hop $i \neq j$, then the codeword of M_i^x is independent of that of M_j^x. Let $\mathbf{Y}_{e_i^*}$ be the observation of eavesdropper e^* in the hop i, $\mathbf{X}_i(M_{s,d}, M_i^x)$ denote the selected codeword, and $\mathbf{X}_i$ be the transmitted symbols of transmitter i. Omitting the indices $(M_{s,d}, M_i^x)$ and setting $R_i^x = I(X_i; Y_{e_i^*})$, we have Equation (3).

In Equation (3), the step (a) holds since $\mathbf{Y}_{e^*}$ is a worse set of observations with respect to that of $\mathbf{Y}_e(i)$. (b) is based on the Markov chain $\{M_{s,d}, M_1^x, ..., M_H^x\} \to \{\mathbf{X}_1, ..., \mathbf{X}_H\} \to \{\mathbf{Y}_{e_1^*}, ..., \mathbf{Y}_{e_H^*}\}$, (c) is due to the independence between $M_{s,d}$ and M_i^x, step d holds since $R_i^x \leq I(X_i; Y_{e_i^*})$ and the eavesdropper can decode randomization message given the bin index (Fano's inequality) as well as the second term of summation is zero. Specifically, let $P_{e,e_i^*} \triangleq Pr\{\hat{M}_i^x \neq M_i^x\}$ be the decoding error probability, where $\hat{M}_i^x$ denotes the estimate of M_i^x given $(\mathbf{Y}_{e_i^*}, M_{s,d})$. Then we have

$$
H(M_i^x|\mathbf{Y}_{e_i^*}, M_{s,d}) \leq N\left(\frac{H(P_{e,e_i^*})}{N} + P_{e,e_i^*}R_i^x\right) \leq N\frac{\epsilon_2}{H}, \tag{4}
$$

with some $\epsilon_2 \to 0$ as $N \to \infty$, (e) is due to the fact that the entropy is not increased with conditioning and $H(\mathbf{Y}_{e_i^*}|\mathbf{Y}_{e_1^*},...,\mathbf{Y}_{e_{i-1}^*},\mathbf{X}_i) = H(\mathbf{Y}_{e_i^*}|\mathbf{X}_i)$, and (f) follows that $I(\mathbf{X}_i;\mathbf{Y}_{e_i^*}) = \sum_{t=1}^{N} I(\mathbf{X}_i; Y_{e_i^*}(t)|Y_{e_i^*}(1),...,Y_{e_i^*}(t-1)) \leq \sum_{t=1}^{N} H(Y_{e_i^*}(t)) - H(Y_{e_i^*}(t)|X_i(t)) = NI(X_i;Y_{e_i^*})$.

Let $\epsilon = \epsilon_1 + \epsilon_2$, we have, for any given $\epsilon > 0$, $\frac{I(M_{s,d};\mathbf{Y}_e)}{N} < \epsilon$ as $N \to \infty$.

IV. Control of Multi-Hop Network with Secrecy

A dynamic control algorithm is developed to deliver the confidential message to its destination over multi-hop routing. In particular, the network makes control decision every slot:

- Resource allocation: Choose a confidential message rate vector $\vec{R}^s(t) = (R_1^s(t), ..., R_L^s(t))$.
- Routing/scheduling: for each link l and each commodity c, $R_l^{cs}(t)$ should satisfy $\sum_c R_l^{cs}(t) \le R_l(t) - \bar{R}_l^e(t)$.

For a node n, the confidential message arrival process of commodity c is $\lambda_n^{cs}(t)$, which is bounded by $\lambda_n^{c\max}$. In each slot t, a control valve chooses $R_n^{cs}(t)$ confidential data of the arrival rate $\lambda_n^{cs}(t)$, such that we can stabilize the network. Let Ω_n and Θ_n be the set of of all links l such that $T(\Omega_n) = n$ and $D(\Theta_n) = n$, respectively. Thus, in each slot t, the queue evolution $Q_n^c(t)$ can be represented as:

$$Q_n^c(t+1) \le \max\left[Q_n^c(t) - \sum_{l\in\Omega_n} R_l^{cs}(t), 0\right] + \sum_{l\in\Theta_n} R_l^{cs}(t) + R_n^{cs}(t) \tag{5}$$

Definition: Queue Stable: A queue $Q(t)$ is defined to be strongly stable with random arrival and service rate if:

$$\limsup_{t\to\infty} \frac{1}{t}\sum_{\tau=0}^{t-1} \mathbb{E}\{Q(\tau)\} < \infty. \tag{6}$$

The control algorithm can be separated into flow control, routing and resource allocation executed in each slot t.

Multi-hop Secrecy Control Algorithm (MSCA):

- **Flow control**: In each slot t, observing the queue length $Q_n^c(t)$ of each commodity $c \in \{1, ..., N\}$, node n selects $R_n^{cs}(t)$ confidential message to solve the following optimization problem:

$$\text{Maximize}: \sum_{c=1}^{N}\left[VU_n^c(R_n^{cs}(t)) - 2R_n^{cs}(t)Q_n^c(t)\right] \tag{7}$$

$$\text{Subject to}: \ 0 \le R_n^{cs}(t) \le \lambda_n^{cs}(t) \tag{8}$$

  where $V > 0$ is a constant which influences the performance of the control algorithm.
- **Routing and Scheduling**: For each link l and node n, the scheduler observes the queue length in all neighboring nodes j of node n (where $tran(l) = n$, $rec(l) = j$). Let $W_l^c(t) = Q_{tran(l)}^c(t) - Q_{rec(l)}^c(t)$ denote the differential queue length of commodity c. The largest differential queue length over link l is $W_l^*(t) \triangleq \max_{[c|l\in\mathcal{L}_c]}\{W_l^c(t), 0\}$, then the message commodity of $c_l^*(t)$ is chosen to transmit on link l if $W_l^*(t) > 0$, where $c_l^*(t)$ is the maximizing commodity.
- **Resource Allocation**: observing the current channel state $\vec{S}(t)$, a confidential rate vector $\vec{R}^s(t)$ is chosen to maximize $\sum_l W_l^*(t)R_l^s(t)$ with the constraint $R_l^s(t) \le R_l(t) - \bar{R}_l^e(t)$. The optimal confidential rate of $R_l^s(t)$ is assigned to commodity $c_l^*(t)$ on link l.

V. Algorithm Performance

The proposed control algorithm can achieve a performance arbitrarily close to the optimal result while keeping the queue length stable, and we have:

Theorem 1. *If $R_l^{cs} < \infty$ for all link l, then for any $V > 0$, the MSCA algorithm satisfies:*

$$\overline{\sum_{n,c} Q_n^c} \le \frac{BM + VU_{\max}}{2\lambda_{sym}}, \tag{9}$$

$$\liminf_{t\to\infty} \sum_{n,c} U_n^c(\bar{r}_n^{cs}(t)) \ge \sum_{n,c} U_n^c(r_n^{*cs}) - \frac{BM}{V}, \tag{10}$$

where λ_{sym} is the maximum confidential arrival rate for all sessions (n,c) and $\lambda_{sym} \triangleq \sum_{n=1}^{M}\lambda_n^{c\max}$, $B \triangleq \frac{1}{M}\sum_{n=1}^{M}[(\lambda_n^{c\max} + R_{n,\max}^{in,s})^2 + (R_{n,\max}^{out,s})^2]$, and $R_{n,\max}^{out,s} \triangleq \max_{\vec{S}}\sum_{l\in\Omega_n} R_l^s$, $R_{n,\max}^{in,s} \triangleq \max_{\vec{S}}\sum_{l\in\Theta_n} R_l^s$ which are the maximum confidential rates out of and into node n. $\lambda_n^{c\max}$ is the maximum confidential rate admitted to the queue. r_n^{*cs} is the optimal solution of (1) *subject to constraint, and:*

$$\overline{\sum_{n,c} Q_n^c} \triangleq \limsup_{t\to\infty} \frac{1}{t}\sum_{\tau=0}^{t-1}\left[\sum_{n,c}\mathbb{E}\{Q_n^c(\tau)\}\right], \tag{11}$$

$$\bar{r}_n^{cs}(t) \triangleq \frac{1}{t}\sum_{\tau=0}^{t-1}\mathbb{E}\{R_n^{cs}(\tau)\}. \tag{12}$$

The proof of Theorem 1 follows from the stochastic network optimization [17], which can stabilize the network and maximize utility functions simultaneously.

Let $\underline{Q}(t) = (Q_n^c(t))$ be the queue backlogs and define a Lyapunov function $L(\underline{Q}(t)) = \sum_{n,c}(Q_n^c(t))^2$. The selection of confidential message rate $R_n^{cs}(t)$ is a process influencing the system, and assume the selected rate are bounded, such that $\sum_{n,c} U_n^c(R_n^{cs}(t)) \le U_{\max}$ for all t. Let U^* be the "target utility" value of utility functions, which is non-negative and concave. Observing the queue length vector $\underline{Q}(t)$, the conditional Lyapunov drift $\Delta\underline{Q}(t)$ can be defined as:

$$\Delta\underline{Q}(t) \triangleq \mathbb{E}\{L(\underline{Q}(t+1)) - L(\underline{Q}(t))|\underline{Q}(t)\}, \tag{13}$$

where the conditional expectation is regard to the random on-step queuing evolutions on the condition of current queue $\underline{Q}(t)$.

Lemma 1. *For positive constants V, θ and B, if the Lyapunov drift satisfies:*

$$\Delta(\underline{Q}(t)) - V\sum_{n,c}\mathbb{E}\{U_n^c(R_n^{cs}(t))|\underline{Q}(t)\} \le B - \theta\sum_{n,c} Q_n^c(t) - VU^*, \tag{14}$$

then time average utility and queues satisfies:

$$\limsup_{t\to\infty}\frac{1}{t}\sum_{\tau=0}^{t-1}\sum_{n,c}\mathbb{E}\{Q_n^c(\tau)\} \le \frac{B + VU_{\max}}{\theta}, \tag{15}$$

$$\liminf_{t\to\infty}\sum_{n,c}\{U_n^c(\bar{r}_n^{cs}(t))\} \ge U^* - \frac{B}{V}, \tag{16}$$

where $\bar{r}_n^{cs}(t)$ is defined in (2)*.*

Proof. Assume (14) holds. Taking expectations over the distribution of $\underline{Q}(t)$ and substituting $\Delta(\underline{Q}(t))$ in (13) yields:

$$\begin{aligned}&\mathbb{E}\{L(\underline{Q}(t+1)) - L(\underline{Q}(t))\} - V\sum_{n,c}\mathbb{E}\{U_n^c(R_n^{cs}(t))\}\\&\leq B - \theta\sum_{n,c}\mathbb{E}\{Q_n^c(t)\} - VU^*,\end{aligned} \tag{17}$$

where $\theta \triangleq \sum_{n,c}\mathbb{E}\left\{\sum_{l\in\Omega_n} R_l^{cs}(t) - \sum_{l\in\Theta_n} R_l^{cs}(t) - R_n^{cs}(t)\right\}$ which is bounded. For all timeslots t, Equation (17) always holds. Given a positive integer K and summing (17) over $t \in \{0,1,2,\ldots,K-1\}$ yields:

$$\begin{aligned}&\mathbb{E}\{L(\underline{Q}(K))\} - \mathbb{E}\{L(\underline{Q}(0))\} - V\sum_{\tau=0}^{K-1}\sum_{n,c}\mathbb{E}\{U_n^c(R_n^{cs}(\tau))\}\\&\leq BK - \theta\sum_{\tau=0}^{K-1}\sum_{n,c}\mathbb{E}\{Q_n^c(\tau)\} - VKU^*.\end{aligned} \tag{18}$$

Since the Lyapunov function is non-negativity and $\sum_{n,c} U_n^c(R_n^{cs}(\tau)) \leq U_{\max}$, each term of (18) divides $K\theta$ and we rearrange (18) to obtain:

$$\frac{1}{K}\sum_{\tau=0}^{K-1}\sum_{n,c}\mathbb{E}\{Q_n^c(\tau)\} - \frac{\mathbb{E}\{L(\underline{Q}(0))\}}{K\theta} \leq \frac{B + VU_{\max}}{\theta}. \tag{19}$$

Letting $K \to \infty$ and taking the $\limsup$, we achieve the queue bound (15).

Similarly, rearranging (18) and dividing by $K\theta$, we have the utility bound:

$$\sum_{n,c}\frac{1}{K}\sum_{\tau=0}^{K-1}\mathbb{E}\{U_n^c(R_n^{cs}(\tau))\} \geq U^* - \frac{B + E\{L(\underline{Q}(0))\}/K}{V}. \tag{20}$$

Due to the concavity of utility function $U_n^c(r)$, using Jensen's inequality, we have $\frac{1}{K}\sum_{\tau=0}^{K-1}\mathbb{E}\{U_n^c(R_n^{cs}(\tau))\} \leq U_n^c\left(\frac{1}{K}\sum_{\tau=0}^{K-1}\mathbb{E}\{R_n^{cs}(\tau)\}\right)$. Substituting it into (20) and taking the $\liminf$ as $K \to \infty$, we have the result in (16). □

Lemma 1 indicates that the control algorithm needs to greedily minimize the following drift and penalty:

$$\Delta(\underline{Q}(t)) - V\sum_{n,c}\mathbb{E}\{U_n^c(R_n^{cs}(t))|\underline{Q}(t)\}. \tag{21}$$

The MSCA control algorithm is indeed greedily to minimize the above drift. Firstly, for all queues (n,c), according to the evolution of queue backlog in (5), the Lyapunov drift can be expressed as:

$$\begin{aligned}\Delta(\underline{Q}(t)) \leq& MB - 2\sum_{n,c}Q_n^c(t)\mathbb{E}\{\sum_{l\in\Omega_n}R_l^{cs}(t)\\&- \sum_{l\in\Theta_n}R_l^{cs}(t) - R_n^{cs}(t)|\underline{Q}(t)\}.\end{aligned} \tag{22}$$

We add the conditional penalty $\sum_{n,c}\mathbb{E}\{VU_n^c(R_n^{cs})|\underline{Q}(t)\}$ to the both side of (22), and define function $\Psi(\underline{Q}(t))$ and $\Phi(\underline{Q}(t))$ as follows:

$$\Psi(\underline{Q}(t)) \triangleq \sum_{n,c}\mathbb{E}\{VU_n^c(R_n^{cs}(t)) - 2Q_n^c(t)R_n^{cs}(t)|\underline{Q}(t)\}, \tag{23}$$

$$\Phi(\underline{Q}(t)) \triangleq 2\sum_{n,c}Q_n^c(t)\mathbb{E}\{\sum_{l\in\Omega_n}R_l^{cs}(t) - \sum_{l\in\Theta_n}R_l^{cs}(t)|\underline{Q}(t)\}. \tag{24}$$

Then, the Equation (22) can be rewritten as:

$$\begin{aligned}&\Delta(\underline{Q}(t)) - V\sum_{n,c}\mathbb{E}\{U_n^c(R_n^{cs}(t))|\underline{Q}(t)\}\\&\leq MB - \Psi(\underline{Q}(t)) - \Phi(\underline{Q}(t)).\end{aligned} \tag{25}$$

Observing the queue backlog matrix $\underline{Q}(t)$ at time t, the MSCA control algorithm is proposed to greedily minimize the right hand side (RHS) of (25) over all flow control options, routing schemes and resource allocation strategies. Thus, We have the following Lemma:

Lemma 2. *The $\Psi(\underline{Q}(t))$ and $\Phi(\underline{Q}(t))$ function satisfy:*

$$\Psi^{MSCA}(\underline{Q}(t)) \geq \sum_{n,c}[VU_n^c(r_n^{*cs}) - 2Q_n^c(t)r_n^{*cs}], \tag{26}$$

$$\Phi^{MSCA}(\underline{Q}(t)) \geq 2\sum_{n,c}Q_n^c(t)\mathbb{E}\{\sum_{l\in\Omega_n}R_l^{*cs} - \sum_{l\in\Theta_n}R_l^{*cs}\}, \tag{27}$$

where (r_n^{*cs}) are any possible confidential rates that satisfy (1) *for all n, and (R_l^{*cs}) are any possible (potentially randomized) decisions on routing and resource allocation.*

The flow control algorithm (7) maximizes $\Psi(\underline{Q}(t))$ over all feasible selection on $R_n^{cs}(t)$. In addition, $\Phi(\underline{Q}(t))$ is maximized by the routing and resource allocation policy. Switching the summation, we have:

$$\Phi(\underline{Q}(t)) = 2\sum_{l}\sum_{c}\mathbb{E}\{R_l^{cs}(t)|\underline{Q}(t)\}[Q_{tran(l)}^c(t) - Q_{rec(l)}^c(t)]. \tag{28}$$

Therefore, let $\Phi^{MSCA}(\underline{Q}(t))$ denote the function values at time t decided by the rate selection $R_l^{cs}(t)$ based on MSCA algorithm, and $\Phi^*(\underline{Q}(t))$ be function values at time t achieved by any feasible rate $R_l^{*cs}(t)$ (possible via randomization), then from (28) we have:

$$\begin{aligned}\Phi^*(\underline{Q}(t)) &\leq 2\sum_{l}\sum_{c}\mathbb{E}\{R_l^{*cs}(t)|\underline{Q}(t)\}W_l^*(t)\\&\leq \Phi^{MSCA}(\underline{Q}(t)),\end{aligned} \tag{29}$$

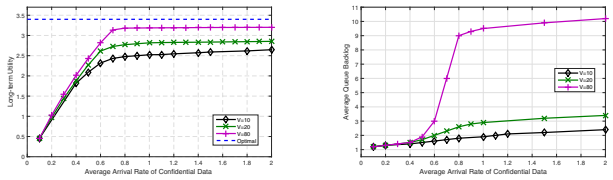
where $W_l^*(t) = \max[Q_{tran(l)}^c(t) - Q_{rec(l)}^c(t), 0]$.

VI. Numerical Results

For the network model presented in Fig. 1, we consider i.i.d Rayleigh fading channels between nodes. The ratio of transmit power and noise has been normalized to 1. Let $h_{i,j}$ be the power gain between node i and j, which follows exponential distribution and the mean of each link is presented in Table

TABLE I
MEAN CHANNEL GAIN

(S_1,1)	(S_1,2)	(S_1,3)	(1,d_1)	(2,d_1)	(3,d_1)
6	8	10	8	6	4
(S_2,2)	(S_2,3)	(S_2,4)	(2,d_2)	(3,d_2)	(4,d_2)
6	8	10	8	6	4
(S_1,e)	(S_2,e)	(1,e)	(2,e)	(3,e)	(4,e)
3	2	1	1	2	3



(a) (b)

Fig. 3. Numerical results: (a) Long-term utility versus average arrival rate of confidential data. (b) Average queue backlog versus average arrival rate of confidential data

I. The achievable rate between node i and j is $R_{i,j}(t) = \log(1+h_{i,j}(t))$ and the rate of eavesdropper $R_{i,e}(t) = \log(1+h_{i,e}(t))$. The utility function is a logarithmic utility function, i.e., $U_n^c(t) = \kappa + \log(R_n^{cs}(t))$, where $\kappa = 3$ and $R_n^{cs}(t)$ is the confidential rate selected by node n in slot t. We assume the confidential data arrival process for each user follows an i.i.d Bernoulli process with rate λ.

In the simulation, the maximum average confidential data arrival rate is 2 bit/s, since the bandwidth is assumed to be one. Choosing the parameter $V \in \{10, 20, 80\}$, we have Fig. 3, where each value is collected by running 5000 times. Fig. 3(a) shows the impact of increasing average confidential data arrival rate on the utility function and Fig. 3(b) depicts the average queue backlog in the network. For a fixed V, when the arrival rate is low, Fig. 3(a) indicates that the utility function linearly increases with the average admission confidential rate. The reason is that, if the arrival confidential rate is low, almost all the arrival confidential data can be admitted. When the arrival confidential rate larger than the secrecy channel capacity, the average admitted confidential rate turns into saturation. Not surprisingly, as the parameter V increases, we observe that the utility function grows closer to the optimal value. While in Fig. 3(b), the average queue backlog is increased with V dramatically. It indicates that the transmission delay is increased with V. Thus, the choice of V is indeed a tradeoff between average utility and short-term system performance. To achieve both large utility and low delay, we may employ V to be a variable.

VII. CONCLUSION

In this paper, we consider the control problem of multi-hop wireless network with security constraint. To guarantee the confidentiality in multi-hop transmission, we proposed an independent randomization encoding strategy in each hop. Using the stochastic network optimization, we develop a dynamic control algorithm involved flow control, routing and resource allocation. The proposed control algorithm achieves utility arbitrarily close to the optimal utility. Numerical results show that the value of utility approaches to the optimum, while the average queue backlog increases very fast. Thus, how to make a tradeoff between performance and queue backlog is subject to future research.

ACKNOWLEDGMENT

This work was supported in part by National Natural Science Foundation of China (No. 61231010) and Foundation of Jiangxi Educational Committee (Grant No. GJJ160626).

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] Y. Liang, H. V. Poor, and L. Ying, "Secure communications over wireless broadcast networks: Stability and utility maximization," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 682–692, 2011.

[3] C. E. Koksal, O. Ercetin, and Y. Sarikaya, "Control of wireless networks with secrecy," in *2010 Conference Record of the Forty Fourth Asilomar Conference on Signals, Systems and Computers*, Nov 2010, pp. 47–51.

[4] X. Wang, Y. Chen, L. Cai, and J. Pan, "Scheduling in a secure wireless network," in *INFOCOM, 2014 Proceedings IEEE*, 2014, pp. 2184–2192.

[5] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and subcarrier allocation for physical-layer security in ofdma-based broadband wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 693–702, 2011.

[6] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation for secure ofdma systems," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 6, pp. 2572–2585, July 2012.

[7] X. Zhu, B. Yang, C. Chen, and L. Xue, "Cross-layer scheduling for ofdma-based cognitive radio systems with delay and security constraints," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 12, pp. 5919–5934, 2015.

[8] X. Kang, Y. C. Liang, A. Nallanathan, H. K. Garg, and R. Zhang, "Optimal power allocation for fading channels in cognitive radio networks: Ergodic capacity and outage capacity," in *Vehicular Technology Conference, 2008. Vtc Spring*, 2008, pp. 1544–1548.

[9] M. Elkashlan, L. Wang, T. Q. Duong, and G. K. Karagiannidis, "On the security of cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 8, pp. 3790–3795, 2015.

[10] X. Xu, B. He, W. Yang, and X. Zhou, "Secure transmission design for cognitive radio networks with poisson distributed eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 373–387, 2015.

[11] M. J. Neely, E. Modiano, and C. P. Li, "Fairness and optimal stochastic control for heterogeneous networks," *IEEE/ACM Transactions on Networking (TON)*, vol. 16, no. 2, pp. 396–409, 2008.

[12] R. L. Cruz and A. V. Santhanam, "Optimal routing, link scheduling and power control in multihop wireless networks," in *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428)*, vol. 1, March 2003, pp. 702–711 vol.1.

[13] J. Zhang, L. Fu, and X. Wang, "Asymptotic analysis on secrecy capacity in large-scale wireless networks," *IEEE/ACM Transactions on Networking*, vol. 22, no. 1, pp. 66–79, 2014.

[14] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 3000–3015, 2009.

[15] X. He and A. Yener, "End-to-end secure multi-hop communication with untrusted relays," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 1–11, 2013.

[16] Y. Sarikaya, C. E. Koksal, and O. Ercetin, "Dynamic network control for confidential multi-hop communications," *IEEE/ACM Transactions on Networking*, vol. 24, no. 2, pp. 1181–1195, April 2016.

[17] M. Neely, "Stochastic network optimization with application to communication and queueing systems," *Synthesis Lectures on Communication Networks*, vol. 3, no. 1, p. 211, 2010.