Confidentiality-Preserving Control of Uplink Cellular Wireless Networks Using Hybrid ARQ

Yunus Sarikaya, Ozgur Ercetin, C. Emre Koksal

***Abstract*—We consider the problem of cross-layer resource allocation with information theoretic secrecy for uplink transmissions in time-varying cellular wireless networks. Particularly, each node in an uplink cellular network injects two types of traffic, confidential and open at rates chosen in order to maximize a global utility function while keeping the data queues stable and meeting a constraint on the secrecy outage probability. The transmitting node only knows the distribution of channel gains. Our scheme is based on Hybrid Automatic Repeat Request (HARQ) transmission with incremental redundancy. We prove that our scheme achieves a utility, arbitrarily close to the maximum achievable. Numerical experiments are performed to verify the analytical results, and to show the efficacy of the dynamic control algorithm.**

***Index Terms*—Physical Layer Security, Hybrid ARQ, Cross-layer Optimization**

I. Introduction

In recent years, there has been a significant interest in wireless information theoretic secrecy to provide unconditional security to communications in large-scale, dynamic and decentralized wireless networks. As an alternative to conventional cryptographic methods that can only provide computational security, information theoretic techniques are proposed to secure wireless networks without the need for secret keys. The foundations of physical layer secrecy have been initially developed in [1] and different variants of the problem have been revisited vastly. For example, in [2], [3], opportunistic secrecy was introduced on the single hop setting, which allows for the exploitation of channel variations due to fading to achieve secrecy. Achieving delay-limited secrecy and outage capacity of the wiretap channel were studied in [4]. The use of multiple antennas for secrecy has been considered in [5], [6] under various assumptions on the available transmitter channel state information (CSI). Multiuser communication with secrecy using cooperative jamming and relaying in the presence of eavesdropper was studied in [7], [8]. The design of the practical codes that approach the promised capacity limits was investigated in [9], [10]. In [11] the secrecy capacity scaling problem is addressed for multihop networks. Exploitation of path diversity in order to achieve secrecy from external eavesdroppers is studied in [12], [13]. Despite the significant progress in this area, most of the work has focused on physical layer techniques. The area of wireless information theoretic secrecy is still not well understood, as it relates to the design of wireless networks and its impact on network control and protocol development.

In this paper, we consider an uplink cellular wireless network in which each node generates both open and confidential information to be transmitted to the base station. When a node is transmitting a confidential packet, other legitimate nodes are considered as "internal eavesdroppers." In this setting, we assume that each node has the knowledge of merely the distribution of its associated uplink channel state as well as the cross channels between itself and every other node. Also a node does not receive any CSI from the base station apart from the 1-bit ACK/NAK signal indicating whether the transmission of the node is successful or not. We pose the problem as that of a network utility maximization in which information theoretic secrecy, *measured by equivocation*, is incorporated as a Quality of Service constraint. We develop a joint flow control and scheduling scheme, which is based on index policies, requiring very simple optimization problems to be solved in each slot. To accomplish reliability, we utilize an incremental redundancy HARQ scheme based on code puncturing. Our scheme relies on mutual information accumulation at each re-transmission. For confidential transmissions, we employ secure incremental redundancy HARQ developed in [14], which considers a block fading wire-tap channel with a single source-destination pair, and a single (external) eavesdropper. We engineer our scheme carefully to utilize resources efficiently and avoid secrecy outages to meet the secrecy outage constraint. Ultimately, we prove that our dynamic control scheme is optimal, i.e., it achieves the maximum utility, achievable by any flow control and scheduling scheme.

Note that, in many scenarios (e.g., tactical, financial, medical), confidentiality of communicated information between the nodes is necessary, so that data intended to 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.

Without confidential information, there has been a number of studies that develop cross-layer resource allocation solutions on HARQ-based transmissions. In [15] and [16], wireless routing with mutual information accumulation based coding is investigated with the aim of energy minimization. They conclude that obtaining optimal solution requires complex

This material is based upon work supported by the Marie Curie International Research Staff Exchange Scheme Fellowship PIRSES-GA-2010-269132 AGILENet within the 7th European Community Framework Programme.

Y. Sarikaya (email: sarikaya@su.sabanciuniv.edu) and O. Ercetin (email: oercetin@sabanciuniv.edu) are with the Department of Electronics Engineering, Faculty of Engineering and Natural Sciences, Sabanci University, 34956 Istanbul, Turkey.

C. E. Koksal (koksal@ece.osu.edu) is with the Department of Electrical and Computer Engineering at The Ohio State University, Columbus, OH.

and combinatorial networking decisions concerning which nodes participate in transmission, and which decode ordering to use. Thus, they propose greedy and heuristic algorithms resulting in suboptimal solutions. In [17], wireless scheduling with HARQ was investigated with the aim of minimizing the average of a cost function which was defined as an increasing function of the queue lengths. The solution to this problem was obtained for only specific types of cost functions by applying dynamic programming techniques. In [18] transmit power and modulation order adaptation strategies, based on semi-Markov decision process are investigated for the HARQ schemes over correlated Rayleigh fading channels. Here, the authors do not consider multi-user setting and their goal is to minimize transmission power, buffer delay and packet overflow. [19] aims to optimize the mapping between signal-to-interference-and-noise ratio (SINR) and modulation and coding scheme (MCS) to maximize the throughput by taking into account the type of HARQ scheme employed. [20] analyzes the interaction between TCP, Hybrid Automatic Repeat Request (HARQ) and scheduling techniques. [21] develops a cross-layer solution for downlink cellular systems with imperfect CSI at the transmitter by employing rateless codes. The problem in [21] is a constrained partial observed Markov decision problem (CPOMDP), which is known to be hard to solve. However, by using a modified Lyapunov drift method, they develop a dynamic network control scheme. The focus in all these works has solely been on the transmission of open messages and confidentiality of messages has not been a constraint.

In our previous work, we investigated the cross-layer resource allocation problem with confidentiality in a cellular wireless network, where users transmit information to the base station, secretly from the other users [22]. One of the main drawbacks of the cross-layer resource allocation algorithms such as the one proposed in [22] is that, instantaneous channel states between users and/or the base station are assumed to be available or they can be estimated fairly accurately. However, in general, neither the base station nor any other legitimate node in the network is aware of CSI of other nodes. CSI must be acquired (e.g., via pilot signal transmission) by consuming part of resources, which is otherwise used for data transmission. The overhead due to acquiring CSI increases with increasing number of users in the network. To avoid this overhead, in [23], we developed a solution, based on HARQ transmission with incremental redundancy. The solution scheme utilized an upper bound of the secrecy outage probability obtained by using Markov inequality, so that the amount of information leakage to the other nodes can be quantified independently over each time slot. Since Markov inequality is merely a bound, the constraint set over which the problem is solved, is tighter than it is necessary. Hence some performance is sacrificed. To that end, in this paper, we investigate the cross-layer resource allocation problem with confidentiality under a more realistic and practical network model as in [23], where both the users and the base station are oblivious to the instantaneous channel state information, and we obtain an optimal dynamic control algorithm.

Clearly, without exact instantaneous uplink CSI at the transmitter side, the wireless transmissions are prone to decoding errors, i.e., channel outages. Traditionally, reliability is accomplished via a standard automatic-repeat-request (ARQ) protocol, where, if a packet cannot be decoded, it is discarded and retransmitted again. However, hybrid ARQ (HARQ) schemes make use of forward error correction (FEC) coding so that the information collected from previous failed transmissions are combined to improve the likelihood of decoding success [24]. The main challenge involved in generalizing the network control with hybrid ARQ is encoding confidential and/or open messages over several blocks. This implies that the time-scales involved in the physical layer and the network layer cannot be decoupled, *eliminating the time-scale separation assumption*.

In recent studies, this challenge is overcome by introducing virtual queues for the messages, which are partially decoded or by giving scheduling decisions over many slots, i.e., T-slot scheduling [25]. However, this approach requires a feedback on instantaneous CSI from the receiver, informing the transmitting node about the accumulated information. The problem of dynamic network control without CSI is notoriously difficult even with only open packet arrivals. In order to design a cross-layer dynamic control algorithm for confidential communications, the rate of information leakage to other nodes in the network is required to be quantified over each slot independently. This leads to some unique technical issues that were not addressed in the existing studies on dynamic network resource allocation. To our best knowledge, our scheme is the first provably-optimal scheme that handles a hybrid traffic involving both open and confidential packets, without an instantaneous CSI. To achieve this, our approach overcomes a number of technical challenges. In particular:

- **(a)** Re-transmissions of the same confidential or open message are correlated with each other. We develop a novel queue model that eliminates the correlation between subsequent re-tranmissions of the same message.
- **(b)** The objective function of the associated NUM problem is coupled among the nodes in the network. In order to decompose the problem into that of a centralized scheduling sub-problem and independent flow control sub-problems solved by each node, we transformed our optimization formulation by introducing a new auxiliary variable and a corresponding constraint.

The rest of the paper is organized as follows. Section II describes the system model, where we give the channel model and a brief summary of incremental redundancy based HARQ for both confidential and open messages. In Section II-C, we characterize the achievable rate region and formulate the problem. In Section III, we formulate the problem as a network utility maximization (NUM) problem, and give solution by using dual decomposition. Section IV gives our novel queue model and our joint flow and scheduling algorithm. In Section V, we investigate the effects of the system parameters on the performance of the algorithm via numerical experiments. Section VI concludes this work by summarizing our contributions.

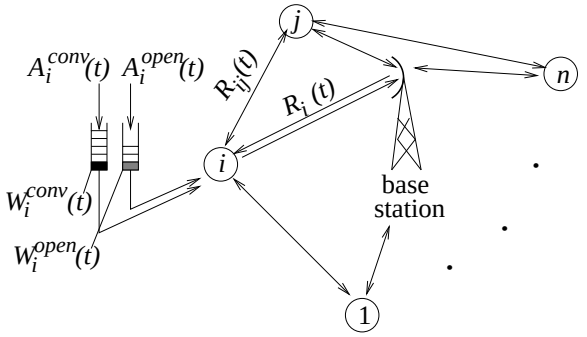


Fig. 1. Multiuser uplink communication system

II. System Model and Preliminaries

A. System Model

We consider a multiuser uplink network as illustrated in Fig. 1. The system consists of n nodes and a base station. The traffic injected by each of these nodes consists of both open and confidential packets. These packets are to be transmitted to the base station via an *unreliable* uplink channel. When a node is transmitting, every other node overhears the transmission over the associated cross channels. Hence, nodes treat each other as "internal eavesdroppers" when transmitting confidential information.

Traffic is assumed to be a mixture of confidential and open data, stored in separate buffers. Let λ_i^{conf} and λ_i^{open} represent input rates in bits per channel use with which confidential and open data are injected in node i, respectively. Let $U_i^{\text{conf}}(\lambda)$ and $U_i^{\text{open}}(\lambda)$ be the utility obtained by node i from the transmission of confidential and open information respectively at a rate of λ bits per channel use. We assume that $U_i^{\text{conf}}(0)=0$, $U_i^{\text{open}}(0)=0$, and $U_i^{\text{conf}}(\cdot)$ and $U_i^{\text{open}}(\cdot)$ are continuously differentiable, monotonically increasing and concave functions.

Time is slotted, and each slot has a length of N channel uses (physical layer symbols), where N is sufficiently large to allow for invoking random coding arguments. Both the main and the cross channels experience independent identically distributed (iid) block fading, in which the channel gain is constant over a slot and it is varying independently from slot to slot. Let $g_i(t)$ and $g_{ij}(t)$ be *instantaneous* complex channel gains of the uplink channel of node i and the cross channel between node i and node j in slot t, respectively. Let $\mathbf{z}_i(t)$ denote block of transmitted complex symbols of user i in slot t. Then, the corresponding blocks of received symbols at the base station $\mathbf{y}_i(t)$, and node j in slot t $\mathbf{y}_{ij}(t)$, are respectively defined as:

$$\mathbf{y}_i(t) = g_i(t)\mathbf{z}_i(t) + \mathbf{u}_i(t), \tag{1}$$

$$\mathbf{y}_{ij}(t) = g_{ij}(t)\mathbf{z}_i(t) + \mathbf{u}_{ij}(t), \tag{2}$$

where $\mathbf{u}_i(t)$ and $\mathbf{u}_{ij}(t)$ are circularly symmetric complex Gaussian noise sequences of the main and the cross channels, respectively. The instantaneous achievable rate of the uplink channel of node i, $R_i(t)$, is defined as the maximum achievable mutual information between the output symbols of node i and the input symbols at the base station over slot t. Likewise, we denote the rate of the cross channel between nodes i and j with $R_{ij}(t)$, which is the maximum mutual information possible between output symbols of node i and input symbols of node j over slot t. Note that there is no actual data transmission between any pair of nodes, but parameter $R_{ij}(t)$ will be necessary when we evaluate the secrecy uplink rates from node i to the base station. Even though our results are general for all distributions for the channel gains, in numerical evaluations we assume all channel gains to be *Gaussian* and the transmit power to be constant, identical to P over all slots t. We normalize the power gains such that the (additive Gaussian) noise has unit variance. Then, as $N \to \infty$,

$$R_i(t) = \log(1 + P|g_i(t)|^2),$$
$$R_{ij}(t) = \log(1 + P|g_{ij}(t)|^2)$$

bits/channel use.

Finally, we assume that transmitters do not have the knowledge of the instantaneous values of $g_i(t)$ and $g_{ij}(t)$, but their distributions are available[1].

B. Transmission Scheme and Secrecy

Due to the lack of the knowledge of the instantaneous values of $g_i(t)$ and $g_{ij}(t)$, to provide reliability and secrecy, we employ HARQ scheme based on mutual information. In this paper, we adopt the so called *incremental redundancy (INR)* HARQ which achieves high throughput efficiency by adapting its error correcting code redundancy to the varying channel conditions [24], [14][2]. Briefly, in INR HARQ scheme, only a selected number of coded symbols are transmitted at every slot. The selected number of coded symbols form a codeword of a punctured code. If a retransmission is requested, additional redundancy symbols are sent under possibly different channel conditions. An analysis of the throughput performance of different HARQ protocols is found in [24].

One should realize that, since instantaneous CSI is not available, one cannot choose the code rates based on a particular fading channel state. Instead, a particular HARQ scheme is chosen and the same code is used for each user at all times. Specifically, each node i has a confidential message $W_i^{\text{conf}} \in \{1,2,\ldots,2^{NC_i^{\text{conf}}}\}$ and open message $W_i^{\text{open}} \in \{1,2,\ldots,2^{NC_i^{\text{open}}}\}$, where C_i^{conf} and C_i^{open} denote the rates (to remain unchanged at all times) of confidential and open information respectively for node i. Every incoming open or confidential transport layer message into node i, $i=1,\ldots,n$, is encoded by using a mother code of length MN channel uses. The obtained codeword x_i is divided into M blocks each of length N channel uses and represented as $[x_i^1, x_i^2, \ldots, x_i^M]$. Let first transmission occur at time slot t_1, where node i sends the block x_i^1 under channel gain $g_i(t_1)$, which is then attempted to be decoded by the base station. If it can be decoded, the base station sends back an acknowledgement (ACK); otherwise, a negative acknowledgement (NAK) is sent.

[1]The distribution of main and cross channel gains can be inferred by node i from the received signals over the reverse channels, exploiting channel reciprocity, when the base station or nodes $j \neq i$ are transmitting.

[2]The dynamic control algorithm proposed in the subsequent sections can be easily modified for other HARQ schemes such as repetition-coding-based HARQ.

Depending on the scheduling policy which decides on the order of transmissions among the nodes in the network, a second transmission opportunity is given to node i at time slot t_2 under a possibly different channel gain realization $g_i(t_2)$. The transmitter sends the block x_i^2, and the base station attempts to decode by combining the previous block x_i^1 with x_i^2. Similarly, at each subsequent retransmission the base station attempts to decode the code by combining all received previous blocks of the same message. The procedure is repeated until the base station successfully decodes the message, the message is dropped by the transmitter, or all blocks of the mother code is transmitted. We assume that the number of blocks, M, is chosen sufficiently large to keep the probability of decoding failure due to exceeding the maximum number of retransmissions approximately identical to zero.

The main difference between the transmission of confidential and open messages with INR HARQ is that for confidential messages the mother code is designed to be a *Wyner code* of length MN [14]. Wyner code is constructed by a random binning strategy, which basically inserts a randomization message to the actual message to increase the level of secrecy [1]. Let $\mathscr{C}\left(\frac{C_i^{\text{code}}}{M},\frac{C_i^{\text{conf}}}{M},MN\right)$ be a Wyner code of size $2^{NC_i^{\text{code}}}$ codewords, generated to convey a confidential message set $\mathscr{W}_i^{\text{conf}}=\{1,2,\dots,2^{NC_i^{\text{conf}}}\}$. Thus, every codeword has a length of NC_i^{code} bits to convey NC_i^{conf} bits of confidential information. In the first transmission, the transmitted codeword, x_i^1, form a codeword of a punctured code of length N, $\mathscr{C}(C_i^{\text{code}},C_i^{\text{conf}},N)$. Similarly, after rth transmission of the confidential message, the combined codeword set, $[x_i^1,\dots,x_i^r]$ form a codeword of a punctured Wyner code of length rN, $\mathscr{C}\left(\frac{C_i^{\text{code}}}{r},\frac{C_i^{\text{conf}}}{r},rN\right)$.

After each re-transmission, both the base station and internal eavesdroppers accumulate information equal to the instantaneous main and cross channel rates at the slot the retransmission takes place. For example, let kth transmission of message W_i^{conf} from node i occur at slot t_k. Then, the mutual information gained by the base station during this re-transmission is $R_i(t_k)$. With INR HARQ, the accumulated mutual information at the base station after r re-transmissions is $\sum_{k=1}^r R_i(t_k)$. The message is correctly decoded by the base station after r transmissions, if the rate of information accumulation exceeds the code rate, i.e., $\sum_{k=1}^r R_i(t_k)>C_i^{\text{code}}$. Let $\rho_{(i,r)}^{\text{conf}}$ denote the probability of decoding failure of confidential message which is transmitted r times, i.e.,

$$\rho_{(i,r)}^{\text{conf}}=\mathbb{P}\left(\sum_{k=1}^r R_i(t_k)<C_i^{\text{code}}\right). \tag{3}$$

Similarly, the mutual information gained by node $j\neq i$ at the kth transmission of message W_i^{conf} at time t is $R_{ij}(t_k)$, and the total accumulated mutual information at node j after r transmissions is $\sum_{k=1}^r R_{ij}(t_k)$. Due to the lack of the knowledge of instantaneous cross channel gains, perfect secrecy cannot be ensured with probability 1 for confidential information. Note that $C_i^{\text{code}}-C_i^{\text{conf}}$ can be interpreted as the rate of the randomization message node i uses in the random binning scheme. A *secrecy outage* takes place after rth transmission of a message, if the total accumulated mutual information at one of the internal eavesdroppers exceeds the rate of the randomization message:

$$\sum_{k=1}^r R_{ij}(t_k)>C_i^{\text{code}}-C_i^{\text{conf}},$$

for some $j\neq i$. Let $\rho_{(i,r)}^{\text{secr}}$ denote the probability of secrecy outage of a message that is transmitted r times, i.e.,

$$\rho_{(i,r)}^{\text{secr}}=\mathbb{P}\left(\max_{j\neq i}\left\{\sum_{k=1}^r R_{ij}(t_k)\right\}>C_i^{\text{code}}-C_i^{\text{conf}}\right). \tag{4}$$

Note that the secrecy outage probability, $\rho_{(i,r)}^{\text{secr}}$, is an increasing function of the number of transmission attempts, r, since overhearing nodes obtain more information at each retransmission. In our problem, we will require that the probability of secrecy outage of each user i is below a given threshold, $\gamma_i,\ i=1,\dots,n$.

For the case of transmission of open messages, the transmitter encodes the information and cyclic redundancy check (CRC) bits by a mother code [24] with a fixed rate C_i^{open}. In each transmission, only the systematic part of the codeword and a selected number of parity bits are transmitted. Decoding is attempted at the receiver side by combining all previously transmitted codes. Let the kth transmission of open message from node i occur at slot t_k^o. If the accumulated information is larger than the fixed rate, $\sum_{k=1}^r R_i(t_k^o)>C_i^{\text{open}}$, the decoding of the open message is successful. Then, the decoding failure probability of the open message, which is transmitted r times is calculated as:

$$\rho_{(i,r)}^{\text{open}}=\mathbb{P}\left(\sum_{k=1}^r R_i(t_k^o)<C_i^{\text{open}}\right). \tag{5}$$

Given the encoding rates, $C_i^{\text{code}},C_i^{\text{conf}}$ and C_i^{open}, the probabilities in (3)-(5) can be easily calculated according to the known iid distributions of $R_i(t_k)$, $R_{ij}(t_k)$ and $R_i(t_k^o)$, $k=1,\dots,r$. and they are time-invariant[3].

As discussed in [26], it is possible to encode open information at a rate $C_i^{\text{code}}-C_i^{\text{conf}}$, jointly with the private information at rate C_i^{conf}. For that, during generation of mother code, one can simply replace the randomization message of the binning strategy of the achievability scheme with the open message, which is allowed to be decoded by other users.

C. Characterization of Achievable Rate Region

We call an arrival rate vector an *achievable rate* vector with respect to a set of given outage constraints $\gamma_1,\dots,\gamma_n$, if there exists a scheduling strategy and associated HARQ codes for each node such that all queues in the system remain stable and the long-term average rate of the occurrence of an outage (decoding or secrecy) event for each user i remains below γ_i. Here, we characterize the rates achievable in a multi-user communication system employing HARQ transmission scheme with incremental redundancy as described in the

[3]This assumption is reasonable for both slow fading and fast fading channel models in which the sequence of channel states over time slots for each node is iid, and so the probabilities are obtained by averaging over the channel distributions.

previous section. We characterize achievable rate regions of two different policies and then show the equivalence of both.

(1) Conventional policy: In this policy, the scheduler chooses a node to transmit, and the scheduled node transmits a message until it is successfully decoded by the base station. This policy is employed by the majority of works in the scope of the cross-layer control with HARQ [18], [25].

(2) Proposed policy: In this policy, each node groups its messages according to their transmission attempts, and scheduler selects a message from any of these groups.

To characterize the achievable rate region under the conventional scheduling policy, let us define a randomized policy, which schedules a confidential or open message of node i with probabilities π_i^{conf} and π_i^{open}, respectively and the transmission is repeated r times until a maximum retransmission limit is reached, or when a message transmitted r times previously is dropped with probability $d_{(i,r)}$. Let $\pi_{(i,r)}^{\text{conf}}$ and $\pi_{(i,r)}^{\text{open}}$ be the portion of all transmissions that node i is active in sending the confidential and open messages transmitted r times previously, respectively.

We present the achievable rate regions under the knowledge of the probabilities of secrecy outage and decoding failure of confidential messages transmitted $r-1$ times previously, $\rho_{(i,r)}^{\text{secr}}$, $\rho_{(i,r)}^{\text{conf}}$ and the probability of decoding failure of open messages transmitted $r-1$ times previously, $\rho_{(i,r)}^{\text{open}}$.

Proposition 1: The achievable rate region under the conventional policy, Γ, consists of all rates, λ_i^{conf} and λ_i^{open}, for which there exists probabilities, π_i^{conf} and π_i^{open}, and $d_{(i,r)}$ such that for all i

$$\pi_{(i,r)}^{\text{conf}} = \pi_{(i,r-1)}^{\text{conf}} \rho_{(i,r-1)}^{\text{conf}} (1 - d_{(i,r-1)}),\ \forall r = 2,\ldots,M, \tag{6}$$

$$\pi_{(i,r)}^{\text{open}} = \pi_{(i,r-1)}^{\text{open}} \rho_{(i,r-1)}^{\text{open}},\ \forall r = 2,\ldots,M, \tag{7}$$

$$\pi_i^{\text{conf}} = \sum_{r=1}^{M} \pi_{(i,r)}^{\text{conf}}, \tag{8}$$

$$\pi_i^{\text{open}} = \sum_{r=1}^{M} \pi_{(i,r)}^{\text{open}}, \tag{9}$$

$$1 \geq \sum_{i=1}^{n} \left(\pi_i^{\text{conf}} + \pi_i^{\text{open}} \right) \tag{10}$$

$$C_i^{\text{conf}} \gamma_i \geq C_i^{\text{conf}} \sum_{r=1}^{M} \pi_{(i,r)}^{\text{conf}} \rho_{(i,r)}^{\text{secr}} \left((1 - \rho_{(i,r)}^{\text{conf}}) + \rho_{(i,r)}^{\text{conf}} d_{(i,r)} \right), \tag{11}$$

$$\lambda_i^{\text{conf}} \leq C_i^{\text{conf}} \pi_{(i,1)}^{\text{conf}}, \tag{12}$$

$$\lambda_i^{\text{open}} \leq C_i^{\text{open}} \pi_{(i,1)}^{\text{open}}. \tag{13}$$

The necessity of the above conditions can be proven following the same approach in Theorem 3.8 in [27].

Conditions (6) and (7) represent that the messages should be transmitted until it is successfully decoded by the base station. (10) follows that only one node is allowed to transmit either confidential or open information at a given slot. A confidential message transmitted r times previously undergoes secrecy outage regardless of the final decodability of the confidential message at the destination, when one of the eavesdropper accumulates information at a rate exceeding the rate of randomized information. Hence, the probability that a confidential message transmitted r times, undergoes a secrecy outage, is $\rho_{(i,r)}^{\text{secr}} \left((1 - \rho_{(i,r)}^{\text{conf}}) + \rho_{(i,r)}^{\text{conf}} d_{(i,r)} \right)$. Condition (11) defines a secrecy outage constraint which can be interpreted as the portion of average confidential information intercepted by other nodes, γ_i. Conditions (12) and (13) represent the flow conservation constraints, i.e., the departure rates of the confidential and open messages should be larger than or equal to the corresponding arrival rates. Since the message is successively transmitted until encountering a successful decoding event of that message, it is convenient to use $\pi_{(i,1)}^{\text{conf}}$ and $\pi_{(i,1)}^{\text{open}}$ as the departure rates.

In the conventional policy, given that a node is scheduled to transmit, whether or not a successful transmission will occur in that slot is not an iid random variable but rather it depends on the number of times that the message is transmitted previously, which is characterized by the conditions (6) and (7). For that reason, nodes need to keep track of the number of times that the message is transmitted previously. Hence, the transmissions in subsequent time-slots under the conventional scheduling policy is temporally coupled. This coupling between successive transmission decisions eliminates the possibility of using standard dynamic control algorithms. Hence, we propose a novel scheduling approach where the messages are grouped according to the number of times they are transmitted, and the scheduler selects a message from any of these groups to transmit. Let us define a stationary policy that selects the confidential and open messages among all messages transmitted r times previously with probabilities $\hat{\pi}_{(i,r)}^{\text{conf}}$ and $\hat{\pi}_{(i,r)}^{\text{open}}$, respectively. In contrast to conventional policy where $\pi_{(i,r)}^{\text{conf}}$ and $\pi_{(i,r)}^{\text{open}}$ are dictated completely by the number of retransmissions of the transmitted message once node i is scheduled, now with the proposed policy at each slot we may serve a different message from a different user which was transmitted r times previously.

Proposition 2: The achievable rate region under the proposed policy, $\hat{\Gamma}$, consists of all rates, λ_i^{conf} and λ_i^{open}, for which there exists $\hat{\pi}_{(i,r)}^{\text{conf}}$ and $\hat{\pi}_{(i,r)}^{\text{open}}$, and $d_{(i,r)}$ such that for all i

$$C_i^{\text{conf}} \hat{\pi}_{(i,r)}^{\text{conf}} \geq C_i^{\text{conf}} \hat{\pi}_{(i,r-1)}^{\text{conf}} (1 - d_{(i,r-1)}) \rho_{(i,r-1)}^{\text{conf}},\ \forall r = 2,\ldots,M, \tag{14}$$

$$C_i^{\text{open}} \hat{\pi}_{(i,r)}^{\text{open}} \geq C_i^{\text{open}} \hat{\pi}_{(i,r-1)}^{\text{open}} \rho_{(i,r-1)}^{\text{open}},\ \forall r = 2,\ldots,M, \tag{15}$$

$$1 \geq \sum_{i=1}^{n} \sum_{r=1}^{M} \left(\hat{\pi}_{(i,r)}^{\text{conf}} + \hat{\pi}_{(i,r)}^{\text{open}} \right), \tag{16}$$

$$C_i^{\text{conf}} \gamma_i \geq C_i^{\text{conf}} \sum_{r=1}^{M} \hat{\pi}_{(i,r)}^{\text{conf}} \rho_{(i,r)}^{\text{secr}} \left((1 - \rho_{(i,r)}^{\text{conf}}) + \rho_{(i,r)}^{\text{conf}} d_{(i,r)} \right), \tag{17}$$

$$\lambda_i^{\text{conf}} \leq \hat{\pi}_{(i,1)}^{\text{conf}} C_i^{\text{conf}}, \tag{18}$$

$$\lambda_i^{\text{open}} \leq \hat{\pi}_{(i,1)}^{\text{open}} C_i^{\text{open}}. \tag{19}$$

Our subsequent algorithm development depends strictly on the achievable rate region as specified by Proposition 2. The sufficiency part for the network stability is proven in Section IV by constructing a dynamic stabilizing policy for any rate vector that is in the achievable rate region.

Conditions (14) and (15) represent retransmission constraints which implies that the messages for which the base

station fails to decode, should be transmitted in later time instants. (18) and (19) represent again the flow conservation constraints.

The importance of the Proposition 2 is that the message that is scheduled to transmit previously, corresponding to a particular user does not necessarily have priority over the users other messages, and the scheduler selects a message from any of these groups to transmit. More specifically, in the region specified by Proposition 2, we can construct a network that contains *virtual nodes* as shown in Section IV, which handle the messages the base station fails to decode. Specifically, in order to handle the messages undergoing a decoding failure event in a simple and effective way, we introduce queues that store the messages transmitted the same number of times previously. The intuition behind the introduction of these queues is to transform coupling introduced by the successive transmissions of the message into virtual nodes, and thus removing the need of the number of times a message is transmitted in making scheduling decisions. As we show in Section IV, the optimal solution can be obtained by using standard dynamic network control algorithms [27].

Proposition 3: The achievable rate region $\hat{\Gamma}$ defined in Proposition 2 is the same as Γ defined in Proposition 1.

The proof of Proposition 3 is provided in Appendix A.

We acknowledge that even though the region specified by Proposition 2 is the same as the one specified with Proposition 1, the base station now needs to store the transmitted parts of the messages until they are successfully decoded. Thus, each packet is assumed to have an appropriate header field with source and packet number identifiers so that the base station buffers the packets according to these identifiers. This creates a system with delayed successful transmission of the messages, which does not affect the rate region but may increase the average network delay.

III. Optimal Scheduling and Flow Control

Next, we formulate the problem as a static optimization problem. Using dual decomposition, we then obtain a dynamic solution to this problem and prove its optimality using stochastic Lyapunov techniques.

A. Network Utility Maximization

Our objective is to design a joint flow control and scheduling algorithm that maximizes the aggregate network utility, while keeping the probability of secrecy outage below a certain level. We assume that a node obtains a utility, only from messages successfully decoded by the base station. Recall that the base station may decide to drop a confidential message if its further retransmission of the message may violate the secrecy outage constraint of the node. Let μ_i^{drop} be the average rate of confidential information being dropped, i.e., $\mu_i^{\text{drop}} = C_i^{\text{conf}} \sum_{r=1}^{M} \pi_{(i,r)}^{\text{conf}} \rho_{(i,r)}^{\text{conf}} d_{(i,r)}$. Hence, the goodput of node i is $\lambda_i^{\text{conf}} - \mu_i^{\text{drop}}$ from which it obtains a utility of $U_i^{\text{conf}}(\lambda_i^{\text{conf}} - \mu_i^{\text{drop}})$. Also, node i obtains a utility of $U_i^{\text{open}}(\lambda_i^{\text{open}})$ from the transmission of open messages. In this paper, we consider the following problem:

$$(P): \quad \max \sum_{i=1}^{n} U_i^{\text{conf}}(\lambda_i^{\text{conf}} - \mu_i^{\text{drop}}) + U_i^{\text{open}}(\lambda_i^{\text{open}}) \qquad (20)$$
$$\text{subject to} \quad (14)-(19),$$

where the maximization is over the parameters $\pi_{(i,r)}^{\text{conf}}, \pi_{(i,r)}^{\text{open}}, d_{(i,r)}, \lambda_i^{\text{conf}}, \lambda_i^{\text{open}}$.

The optimization problem (P) is referred to as a Network Utility Maximization (NUM) problem, which is usually solved by decomposing it into a centralized scheduling sub-problem, and n independent flow control sub-problems solved by each node i. However, the objective function (20) is coupled among the nodes in the network, which in turn prohibits such a decomposition. The coupling is due to the parameter μ_i^{drop} depending on the scheduling decisions, which inevitably affects all the nodes in the system. The coupling in the objective function is usually harder to deal with than the coupling in the constraints, since the latter can be decomposed by using primal or dual decompositions (see [28] and the references therein). In order to address the coupling in the objective function, we introduce an auxiliary variable λ_i^{drop} corresponding to each μ_i^{drop}, and add an additional inequality constraint with respect to the auxiliary variable. Hence, we convert the coupling in the objective function to a coupling in the constraint, which can then be decoupled by dual decomposition and solved by introducing additional dual variable. The modified version of the optimization problem (20) is given as follows:

$$(Q): \quad \max \sum_{i=1}^{n} U_i^{\text{conf}}(\lambda_i^{\text{conf}} - \lambda_i^{\text{drop}}) + U_i^{\text{open}}(\lambda_i^{\text{open}}) \qquad (21)$$
$$\text{subject to} \quad (14)-(19),$$
$$\mu_i^{\text{drop}} \le \lambda_i^{\text{drop}}, \qquad (22)$$

for all i, where the maximization is over the parameters $\pi_{(i,r)}^{\text{conf}}, \pi_{(i,r)}^{\text{open}}, d_{(i,r)}, \lambda_i^{\text{conf}}, \lambda_i^{\text{open}}, \lambda_i^{\text{drop}}$. Note that the new decision variable λ_i^{drop} can be interpreted as the average rate of confidential information that is going to be dropped later by the node. Since the objective function (21) is a decreasing function of λ_i^{drop}, (22) is always active at the optimal point. Hence, the optimal solution of (P) is the same as that of (Q).

B. Dual Decomposition

Note that the objective function (21) is separable into individual user utility maximization problems, and due to the definition of the constraints in (14)-(19) and (22), there is no correlation among successive transmissions. Here, we solve the problem using dual decomposition method that is particularly appealing to our problem structure.

Let us first introduce dual variables $\{\mathbf{q}^{\text{conf}}, \mathbf{q}^{\text{open}}, \mathbf{q}^{\text{drop}}, \mathbf{k}\}$ to relax constraints in (14)-(19) and (22), respectively. Then we have the dual function as:

$$D(\mathbf{q}^{\text{conf}}, \mathbf{q}^{\text{open}}, \mathbf{q}^{\text{drop}}, \mathbf{k}) = \max_{\boldsymbol{\pi}, \mathbf{d}} L(\boldsymbol{\pi}^{\text{conf}}, \boldsymbol{\pi}^{\text{open}}, \mathbf{d}; \mathbf{q}^{\text{conf}}, \mathbf{q}^{\text{open}}, \mathbf{q}^{\text{drop}}, \mathbf{k}), \qquad (23)$$

where

$$
\begin{aligned}
&L(\boldsymbol{\pi}^{\text{conf}},\boldsymbol{\pi}^{\text{open}},\mathbf{d};\mathbf{q}^{\text{conf}},\mathbf{q}^{\text{open}},\mathbf{q}^{\text{drop}},\mathbf{k})\\
&=\sum_i\left(U_i^{\text{conf}}(\lambda_i^{\text{conf}}-\lambda_i^{\text{drop}})+U_i^{\text{open}}(\lambda_i^{\text{open}})\right)\\
&+q_{(i,1)}^{\text{conf}}\left(\pi_{(i,r)}^{\text{conf}}C_i^{\text{conf}}-\lambda_i^{\text{conf}}\right)+q_{(i,1)}^{\text{open}}\left(\pi_{(i,r)}^{\text{open}}C_i^{\text{open}}-\lambda_i^{\text{open}}\right)\\
&+C_i^{\text{conf}}\sum_{r=2}^{M}q_{(i,r)}^{\text{conf}}\left(\pi_{(i,r)}^{\text{conf}}-\pi_{(i,r-1)}^{\text{conf}}(1-d_{(i,r-1)})\rho_{(i,r-1)}^{\text{conf}}\right)\\
&+C_i^{\text{open}}\sum_{r=2}^{M}q_{(i,r)}^{\text{open}}\left(\pi_{(i,r)}^{\text{open}}-\pi_{(i,r-1)}^{\text{open}}\rho_{(i,r-1)}^{\text{open}}\right)-q_i^{\text{drop}}\left(\mu_i^{\text{drop}}-\lambda_i^{\text{drop}}\right)\\
&-k_iC_i^{\text{conf}}\sum_{r=1}^{M}\left(\pi_{(i,r)}^{\text{conf}}\rho_{(i,r)}^{\text{secr}}((1-\rho_{(i,r)}^{\text{conf}})+\rho_{(i,r)}^{\text{conf}}d_{(i,r)})\right). \qquad (24)
\end{aligned}
$$

Let $\boldsymbol{\lambda}^{\text{conf}}$,$\boldsymbol{\lambda}^{\text{open}}$, $\boldsymbol{\pi}$ and $\mathbf{d}$ represent the vectors of primal variables of the rates of flows of confidential and open traffic, the probabilities of scheduling and dropping, respectively; $\mathbf{q}^{\text{conf}}$, $\mathbf{q}^{\text{open}}$, $\mathbf{q}^{\text{drop}}$ and $\mathbf{k}$ represent the vectors of corresponding dual variables.

Let $\lambda_i^{\text{conf}^*}$, $\lambda_i^{\text{drop}^*}$ and $\lambda_i^{\text{open}^*}$ be the optimal rates of confidential, dropped and open information, respectively. Slater's condition in [29] states that, since the objective function is concave and the constraints are affine functions, the duality gap is zero and therefore $D(\mathbf{q}^{\text{conf}^*},\mathbf{q}^{\text{open}^*},\mathbf{q}^{\text{drop}^*},\mathbf{k}^*)=\sum_i\left(U_i^{\text{conf}}(\lambda_i^{\text{conf}^*}-\lambda_i^{\text{drop}^*})+U_i^{\text{open}}(\lambda_i^{\text{open}^*})\right)$ where

$$
\mathbf{q}^{\text{conf}^*},\mathbf{q}^{\text{open}^*},\mathbf{q}^{\text{drop}^*},\mathbf{k}^*\in \underset{q_{(i,r)}^{\text{conf}}\geq 0,q_{(i,r)}^{\text{open}}\geq 0,q_i^{\text{drop}}\geq 0,k_i\geq 0}{\operatorname{argmin}} D(\mathbf{q}^{\text{conf}},\mathbf{q}^{\text{open}},\mathbf{q}^{\text{drop}},\mathbf{k}).
$$

We are interested to obtain the optimal primal variables, i.e., $(\lambda_i^{\text{conf}^*},\lambda_i^{\text{drop}^*},\lambda_i^{\text{open}^*})$ as flow rates and $(\boldsymbol{\pi}^{\text{conf}^*},\boldsymbol{\pi}^{\text{open}^*},\mathbf{d}^*)$ as scheduling and dropping decisions. We notice that the dual function in (23) can be decomposed into the following subproblems:

$$
\begin{aligned}
D(\mathbf{q}^{\text{conf}},\mathbf{q}^{\text{open}},\mathbf{q}^{\text{drop}},\mathbf{k})=&D_1(\mathbf{q}^{\text{conf}},\mathbf{q}^{\text{open}},\mathbf{q}^{\text{drop}})\\
&+D_2(\mathbf{q}^{\text{conf}},\mathbf{q}^{\text{open}},\mathbf{q}^{\text{drop}},\mathbf{k})
\end{aligned}
$$

where

$$
\begin{aligned}
&D_1(\mathbf{q}^{\text{conf}},\mathbf{q}^{\text{open}},\mathbf{q}^{\text{drop}})=\max_{\lambda_i^{\text{conf}},\lambda_i^{\text{open}},\lambda_i^{\text{drop}}}\sum_i\Big(U_i^{\text{conf}}(\lambda_i^{\text{conf}}-\lambda_i^{\text{drop}})\\
&+U_i^{\text{open}}(\lambda_i^{\text{open}})\Big)-q_{(i,1)}^{\text{conf}}\lambda_i^{\text{conf}}-q_{(i,1)}^{\text{open}}\lambda_i^{\text{open}}+q_i^{\text{drop}}\lambda_i^{\text{drop}}, \qquad (25)
\end{aligned}
$$

$$
\begin{aligned}
&D_2(\mathbf{q}^{\text{conf}},\mathbf{q}^{\text{open}},\mathbf{q}^{\text{drop}},\mathbf{k})=\max_{\pi_{(i,r)}^{\text{conf}},\pi_{(i,r)}^{\text{open}},d_{(i,r)}}\sum_{r=1}^{M}q_{(i,r)}^{\text{conf}}\pi_{(i,r)}^{\text{conf}}C_i^{\text{conf}}\\
&-\sum_{r=2}^{M}\pi_{(i,r-1)}^{\text{conf}}(1-d_{(i,r-1)})\rho_{(i,r-1)}^{\text{conf}}C_i^{\text{conf}}+\sum_{r=1}^{M}q_{(i,r)}^{\text{open}}\pi_{(i,r)}^{\text{open}}C_i^{\text{open}}\\
&-\sum_{r=2}^{M}q_{(i,r)}^{\text{open}}\pi_{(i,r-1)}^{\text{open}}C_i^{\text{open}}\rho_{(i,r-1)}^{\text{open}}-q_i^{\text{drop}}\mu_i^{\text{drop}}\\
&-k_iC_i^{\text{conf}}\sum_{r=1}^{M}\left(\pi_{(i,r)}^{\text{conf}}\rho_{(i,r)}^{\text{secr}}((1-\rho_{(i,r)}^{\text{conf}})+\rho_{(i,r)}^{\text{conf}}d_{(i,r)})\right). \qquad (26)
\end{aligned}
$$

Subproblems (25) and (26) can be solved separately resulting in a cross-layer optimization algorithm for joint scheduling and flow control, to be showed in Section IV.

The dual problem can be solved using the subgradient projection method [30]. Let $\mathbf{Gq}^{\text{conf}}$, $\mathbf{Gq}^{\text{open}}$, $\mathbf{Gq}^{\text{drop}}$ and $\mathbf{Gk}$ be the subgradients of respective dual variables. Since primal variables $\boldsymbol{\pi}^{\text{conf}}$, $\boldsymbol{\pi}^{\text{open}}$ and $\mathbf{d}$ are obtained as a solution of maximization in dual objective function (23) at point $(q^{\text{conf}},q^{\text{open}},q^{\text{drop}},k)$, the subgradients of function (23) can be expressed as follows:

$$
Gq_{(i,r)}^{\text{conf}}=\begin{cases}\lambda_i^{\text{conf}}-\pi_{(i,r)}^{\text{conf}}C_i^{\text{conf}}, & \text{if } r=1\\ \pi_{(i,r-1)}^{\text{conf}}(1-d_{(i,r-1)})\rho_{(i,r-1)}^{\text{conf}}C_i^{\text{conf}}-\pi_{(i,r)}^{\text{conf}}C_i^{\text{conf}}, & \text{otherwise}\end{cases}, \qquad (27)
$$

$$
Gq_{(i,r)}^{\text{open}}=\begin{cases}\lambda_i^{\text{open}}-\pi_{(i,r)}^{\text{open}}C_i^{\text{open}}, & \text{if } r=1\\ \pi_{(i,r-1)}^{\text{open}}\rho_{(i,r-1)}^{\text{open}}C_i^{\text{open}}-\pi_{(i,r)}^{\text{conf}}C_i^{\text{open}}, & \text{otherwise}\end{cases}, \qquad (28)
$$

$$
Gq_i^{\text{drop}}=\mu_i^{\text{drop}}-\lambda_i^{\text{drop}}, \qquad (29)
$$

$$
Gk_i=\sum_{r=1}^{M}\pi_{(i,r)}^{\text{conf}}\rho_{(i,r)}^{\text{secr}}\left((1-\rho_{(i,r)}^{\text{conf}})+\rho_{(i,r)}^{\text{conf}}d_{(i,r)}\right)C_i^{\text{conf}}-\gamma_iC_i^{\text{conf}}. \qquad (30)
$$

The subgradient projection method finds the optimal solution by updating the dual variables in each iteration step t in the opposite direction of the subgradients:

$$
q_{(i,r)}^{\text{conf}}(t+1)=[q_{(i,r)}^{\text{conf}}(t)+\alpha Gq_{(i,r)}^{\text{conf}}]^+, \qquad (31)
$$

$$
q_{(i,r)}^{\text{open}}(t+1)=[q_{(i,r)}^{\text{open}}(t)+\alpha Gq_{(i,r)}^{\text{open}}]^+, \qquad (32)
$$

$$
q_i^{\text{drop}}(t+1)=[q_i^{\text{drop}}(t)+\alpha Gq_i^{\text{drop}}]^+, \qquad (33)
$$

$$
k_i(t+1)=[k_i(t)+\alpha Gk_i]^+, \qquad (34)
$$

where α is positive constant step size.

The dual decomposition approach only provides an intuition behind the solution, but the real network has dynamic arrivals. In Section IV, we present a complete solution which takes into account these dynamics, and establish its convergence and optimality.

C. Joint Encoding of Confidential and Open Information

In the case of joint encoding, a node can transmit $C_i^{\text{code}}-C_i^{\text{conf}}$ rate of open information upon successful transmission of a confidential message. Since open bits are used on the behalf of randomization bits, they should not be transmitted in the previous slots so that overhearing nodes do not have any information about the jointly encoded open bits. Thus, jointly encoded open bits are selected from newly arrived bits. In addition, we assume that by dropping confidential message, we drop jointly encoded open bits as well. To take into account joint encoding, we first need to modify condition (19) as:

$$
\sum_{r=1}^{M}\pi_{(i,r)}^{\text{conf}}\left(C_i^{\text{code}}-C_i^{\text{conf}}\right)\left((1-\rho_{(i,r)}^{\text{conf}})+\rho_{(i,r)}^{\text{conf}}d_{(i,r)}\right)+\pi_{(i,1)}^{\text{open}}C_i^{\text{open}}\geq\lambda_i^{\text{open}},\ \forall i, \qquad (35)
$$

Let $\mu_i^{\text{o,drop}}$ be the average rate of open information being dropped, i.e., $\mu_i^{\text{o,drop}}=\left(C_i^{\text{code}}-C_i^{\text{conf}}\right)\sum_{r=1}^{M}\pi_{(i,r)}^{\text{conf}}\rho_{(i,r)}^{\text{conf}}d_{(i,r)}$. Hence, node i obtains a utility of $U_i^{\text{open}}(\lambda_i^{\text{open}}-\mu_i^{\text{o,drop}})$ from the transmission of open messages and the transmission of jointly encoded confidential messages. By following the same steps in Section III-A, we obtain the optimization problem with joint encoding as follows:

$$(J): \quad \max \sum_{i=1}^{n} U_i^{\text{conf}}(\lambda_i^{\text{conf}} - \lambda_i^{\text{drop}}) + U_i^{\text{open}}(\lambda_i^{\text{open}} - \lambda_i^{\text{o,drop}}) \tag{36}$$

$$\text{subject to} \quad (14)-(18),(22),(35),$$
$$\mu_i^{\text{o,drop}} \le \lambda_i^{\text{o,drop}}, \tag{37}$$

for all i, where the maximization is over the parameters $\pi_{(i,r)}^{\text{conf}}, \pi_{(i,r)}^{\text{open}}, d_{(i,r)}, \lambda_i^{\text{conf}}, \lambda_i^{\text{open}}, \lambda_i^{\text{drop}}, \lambda_i^{\text{o,drop}}$. Note that the newly added decision variable $\lambda_i^{\text{o,drop}}$ can be interpreted as the average rate of open information that is going to be jointly dropped with confidential information later by the node.

Based on the given optimization problem (J), the Lagrangian function of (Q) defined in (24) should be modified as:

$$\begin{aligned}
&L(\boldsymbol{\pi}^{\text{conf}}, \boldsymbol{\pi}^{\text{open}}, \mathbf{d}; \mathbf{q}^{\text{conf}}, \mathbf{q}^{\text{open}}, \mathbf{q}^{\text{drop}}, \mathbf{k}) \\
&= \sum_i \left(U_i^{\text{conf}}(\lambda_i^{\text{conf}} - \lambda_i^{\text{drop}}) + U_i^{\text{open}}(\lambda_i^{\text{open}} - \lambda_i^{\text{o,drop}}) \right) \\
&- q_i^{\text{o,drop}} \left(\mu_i^{\text{o,drop}} - \lambda_i^{\text{o,drop}} \right) + q_{(i,1)}^{\text{conf}} \left(\pi_{(i,r)}^{\text{conf}} C_i^{\text{conf}} \right) \\
&+ q_{(i,1)}^{\text{open}} \left(\pi_{(i,r)}^{\text{open}} C_i^{\text{open}} + \sum_{r=1}^{M} \pi_{(i,r)}^{\text{conf}} \pi_{(i,r)}^{\text{conf}} \left(C_i^{\text{code}} - C_i^{\text{conf}} \right) - \lambda_i^{\text{open}} \right) \\
&+ C_i^{\text{conf}} \sum_{r=2}^{M} q_{(i,r)}^{\text{conf}} \left(\pi_{(i,r)}^{\text{conf}} - \pi_{(i,r-1)}^{\text{conf}} (1 - d_{(i,r-1)}) \rho_{(i,r-1)}^{\text{conf}} \right) \\
&+ C_i^{\text{open}} \sum_{r=2}^{M} q_{(i,r)}^{\text{open}} \left(\pi_{(i,r)}^{\text{open}} - \pi_{(i,r-1)}^{\text{open}} \rho_{(i,r-1)}^{\text{open}} \right) - q_i^{\text{drop}} \left(\mu_i^{\text{drop}} - \lambda_i^{\text{drop}} \right) \\
&- k_i C_i^{\text{conf}} \sum_{r=1}^{M} \left(\pi_{(i,r)}^{\text{conf}} \rho_{(i,r)}^{\text{secr}} ((1 - \rho_{(i,r)}^{\text{conf}}) + \rho_{(i,r)}^{\text{conf}} d_{(i,r)}) \right).
\end{aligned} \tag{38}$$

where $q_i^{\text{o,drop}}$ is a dual variable to relax constraint in (37). Based on modified Lagrangian function in (38), it is straightforward to modify subproblems in (25) and (26) and subgradient in (28). In addition, the dual variable $q_i^{\text{o,drop}}$ is updated in each iteration step t as:

$$q_i^{\text{o,drop}}(t+1) = [q_i^{\text{o,drop}}(t) + \alpha \left(\mu_i^{\text{o,drop}} - \lambda_i^{\text{o,drop}} \right)]^+ \tag{39}$$

With the above modifications, it is straightforward to generalize all subsequent development to handle the scenario with joint encoding of open and confidential messages.

IV. Queue Model and Dynamic Control

In this section, we relate each subproblem derived from the dual decomposition with a functionality of wireless networks such as scheduling and flow control. The solution given by (26) gives the steady state probabilities of transmissions from each node. However, the cross-layer algorithm presented here is a simple index policy, which observes the current state and makes a decision dynamically.

A. Queuing Model

We can associate each of the dual variables $(\mathbf{q}^{\text{conf}}, \mathbf{q}^{\text{open}})$ with a queue. These queues are obtained by simply making the change of variable at the update of dual variables as

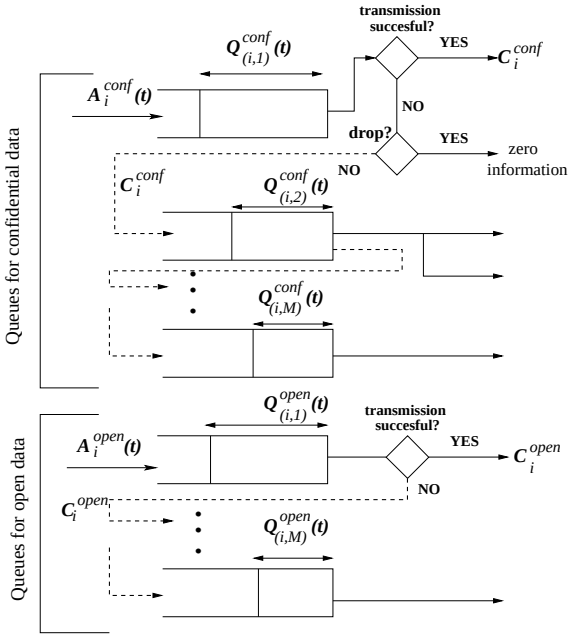


Fig. 2. Queue model

$\alpha Q_{(i,r)}^{\text{conf}}(t) = q_{(i,r)}^{\text{conf}}(t)$ and $\alpha Q_{(i,r)}^{\text{open}}(t) = q_{(i,r)}^{\text{open}}(t)$. Note that these queues store codewords of messages having been transmitted the same number of times, i.e., $Q_{(i,r)}^{\text{conf}}(t)$ and $Q_{(i,r)}^{\text{open}}(t)$ denote the sizes of the queues storing codewords for confidential and open messages respectively, of node i that are already transmitted $r-1$ times by time slot t as illustrated in Fig. 2. Since the maximum number of transmission attempts is M, there are a total of $2M$ queues at each node. By definition, $Q_{(i,1)}^{\text{conf}}(t)$ and $Q_{(i,1)}^{\text{open}}(t)$ refer to the sizes of queues storing packets not transmitted yet by slot t. In addition, at each time slot, nodes decide how much confidential and open information they admit to their respective queues. Hence, the arrivals to these queues are exogenous with rates $A_i^{\text{conf}}(t)$ and $A_i^{\text{open}}(t)$ bits per channel use, respectively. We assume that arrival processes are stationary and ergodic, and the arrival rates, $A_i^{\text{conf}}(t)$ and $A_i^{\text{open}}(t)$ have long-term average rates λ_i^{conf} and λ_i^{open} respectively, i.e., $\lambda_i^{\text{conf}} \triangleq \mathbb{E}\left[A_i^{\text{conf}}(t)\right]$ and $\lambda_i^{\text{open}} \triangleq \mathbb{E}\left[A_i^{\text{open}}(t)\right]$ and the maximum number of arrivals are bounded by finite numbers, $A_i^{\text{conf,max}}$ and $A_i^{\text{open,max}}$. Arrivals to all other queues are triggered by a NAK feedback received from the base station due to a decoding failure of a previous transmission attempt. For example, after the transmission of the codeword x_i^r, if the base station fails to decode the message, the codeword x_i^{r+1} is inserted into the next queue $r+1$. Note that all codewords x_i^r , $r = 1, \ldots, M$ are generated from the same mother code. For ease of exposition, we call these codewords as packets of the same message.

At each time slot, the length of each of the $2M$ queues, and the secrecy outage and decoding failure probabilities are observed. Based on this information, a node and one of its $2M$ queues is scheduled and the head of line packet from this queue is transmitted. Let $\mathcal{S}_{(i,r)}^{\text{conf}}(t)$ and $\mathcal{S}_{(i,r)}^{\text{open}}(t)$, be indicator variables representing the scheduler decision.

Specifically, $\mathcal{S}^{\text{conf}}_{(i,r)}(t)=1$ if a packet at the head of line of the rth queue storing confidential codewords of node i is scheduled to be served, and $\mathcal{S}^{\text{conf}}_{(i,r)}(t)=0$ otherwise. Likewise, $\mathcal{S}^{\text{open}}_{(i,r)}(t)=1$ if a packet at the head of line of the rth queue storing open messages of node i is scheduled to be served, and $\mathcal{S}^{\text{open}}_{(i,r)}(t)=0$ otherwise. By definition, $\sum_{i=1}^{n}\sum_{r=1}^{M}\mathcal{S}^{\text{conf}}_{(i,r)}(t)+\mathcal{S}^{\text{open}}_{(i,r)}(t)\leq 1$ for all $t>0$. Recall that, $\pi^{\text{conf}}_{(i,r)}$ and $\pi^{\text{open}}_{(i,r)}$ are the steady-state scheduling probability of the confidential and open messages that are transmitted $r-1$ times. These probabilities are the long-term averages of the aforementioned scheduling decisions, i.e., $\pi^{\text{conf}}_{(i,r)}=\lim_{t\to\infty}\frac{1}{t}\sum_{\tau=0}^{t}\mathcal{S}^{\text{conf}}_{(i,r)}(\tau)$ and $\pi^{\text{open}}_{(i,r)}=\lim_{t\to\infty}\frac{1}{t}\sum_{\tau=0}^{\tau}\mathcal{S}^{\text{open}}_{(i,r)}(\tau)$. Similarly, let $\mathscr{D}_{(i,r)}(t)$ be an indicator variable taking value of 1 if node i decides to drop the head of line packet in its rth confidential queue at slot t, and 0 otherwise. Then, $d_{(i,r)}=\lim_{t\to\infty}\frac{1}{t}\sum_{\tau=0}^{t}\mathscr{D}_{(i,r)}(\tau)$.

Also, let $\mathscr{F}^{\text{conf}}_{(i,r)}(t)$ and $\mathscr{F}^{\text{open}}_{(i,r)}(t)$ denote indicator variables for the decoding success/failure of a packet from the rth confidential and open queues respectively, transmitted in slot t. Precisely, $\mathscr{F}^{\text{conf}}_{(i,r)}(t)=1$ if a confidential message in its rth transmission attempt cannot be decoded by the base station, i.e., a NAK feedback is received. Similarly, $\mathscr{F}^{\text{open}}_{(i,r)}(t)=1$ if an open message in its rth transmission attempt cannot be decoded by the base station in slot t. We note that the long-term averages of $\mathscr{F}^{\text{conf}}_{(i,r)}(t)$ and $\mathscr{F}^{\text{open}}_{(i,r)}(t)$ give the probabilities of decoding failure at the rth transmission attempt of a confidential and open message, respectively, i.e., $\rho^{\text{conf}}_{(i,r)}=\lim_{t\to\infty}\frac{1}{t}\sum_{\tau=0}^{t}\mathscr{F}^{\text{conf}}_{(i,r)}(\tau)$ and $\rho^{\text{open}}_{(i,r)}=\lim_{t\to\infty}\frac{1}{t}\sum_{\tau=0}^{t}\mathscr{F}^{\text{open}}_{(i,r)}(\tau)$.

The dynamics of confidential and open traffic queues, $Q^{\text{conf}}_{(i,1)}(t)$ and $Q^{\text{open}}_{(i,1)}(t)$ are given as follows:

$$Q^{\text{conf}}_{(i,1)}(t+1)=\left[Q^{\text{conf}}_{(i,1)}(t)-\mathcal{S}^{\text{conf}}_{(i,1)}(t)C^{\text{conf}}_{i}\right]^{+}+A^{\text{conf}}_{i}(t), \quad (40)$$

$$Q^{\text{open}}_{(i,1)}(t+1)=\left[Q^{\text{open}}_{(i,1)}(t)-\mathcal{S}^{\text{open}}_{(i,1)}(t)C^{\text{open}}_{i}\right]^{+}+A^{\text{open}}_{i}(t), \quad (41)$$

where $[x]^{+}=\max(0,x)$.

The dynamics of other confidential and open traffic queues, for $r\neq 1$, are as follows:

$$Q^{\text{conf}}_{(i,r)}(t+1)=\left[Q^{\text{conf}}_{(i,r)}(t)-\mathcal{S}^{\text{conf}}_{(i,r)}(t)C^{\text{conf}}_{i}\right]^{+}+\mathcal{S}^{\text{conf}}_{(i,r-1)}(t)\mathscr{F}^{\text{conf}}_{(i,r-1)}(t)(1-\mathscr{D}_{(i,r-1)}(t))C^{\text{conf}}_{i}, \quad (42)$$

$$Q^{\text{open}}_{(i,r)}(t+1)=\left[Q^{\text{open}}_{(i,r)}(t)-\mathcal{S}^{\text{open}}_{(i,r)}(t)C^{\text{open}}_{i}\right]^{+}+\mathcal{S}^{\text{open}}_{(i,r-1)}(t)\mathscr{F}^{\text{open}}_{(i,r-1)}(t)C^{\text{open}}_{i}. \quad (43)$$

Comparing (31)-(32) with (40)-(43), we can deduce the relationships of queue lengths with the corresponding dual variables as $Q^{\text{conf}}_{(i,r)}(t)=q^{\text{conf}}_{(i,r)}(t)/\alpha$ and $Q^{\text{open}}_{(i,r)}(t)=q^{\text{open}}_{(i,r)}(t)/\alpha$. In addition, we can relate the dual variables $q^{\text{drop}}_{i}(t)$ and $k_i(t)$ with virtual queues representing the secrecy outage and dropping constraints in (17) and (22) as:

$$K_i(t+1)=\left[K_i(t)+C^{\text{conf}}_{i}\left(\sum_{r=1}^{M}\mathcal{S}^{\text{conf}}_{(i,r)}(t)\rho^{\text{secr}}_{(i,r)}\left((1-\mathscr{I}^{\text{conf}}_{(i,r)}(t))+\mathscr{I}^{\text{conf}}_{(i,r)}(t)\mathscr{D}_{(i,r)}(t)\right)-\gamma_i\right)\right]^{+}, \quad (44)$$

$$Q^{\text{drop}}_{i}(t+1)=\left[Q^{\text{drop}}_{i}(t)-A^{\text{drop}}_{i}(t)+C^{\text{conf}}_{i}\sum_{r=1}^{M}\mathcal{S}^{\text{conf}}_{(i,r)}(t)\mathscr{F}^{\text{conf}}_{(i,r)}(t)\mathscr{D}_{(i,r)}(t)\right]^{+}. \quad (45)$$

The arrivals and departures to the queue defined by (44) are the number of the confidential bits undergoing secrecy outage and the number of confidential bits allowed to undergo outage as given by the outage constraint, respectively. Similarly, the arrivals to the queue in (45) are confidential bits that are going to be dropped in subsequent slots, and departures are confidential bits actually dropped in the current slot. The state of the virtual queue at any given point is an indicator on the amount by which we have exceeded the allowable outage constraint. Thus, the larger the state of these queues, the more conservative our dynamic algorithm has to get toward meeting these constraints. In the long run, we should guarantee strong stability of the virtual queues, which in turn guarantees the constraints to be satisfied [27].

B. Cross-layer optimization algorithm

With the queueing model described in the previous section, we can use the queue length information instead of dual variables to solve the optimization problem presented in (21). Furthermore, our proposed scheme is based on simple index policies, involving the solution of simple optimization problems that depend only on the instantaneous state of the system. Note that, even though the secrecy outage and decoding failure probabilities are static, the information in real confidential and open queues, and virtual queues are dynamically changing over each time slot.

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

(1) Flow control: For some $\alpha>0$, each node i injects $A^{\text{conf}}_{i}(t)$, and $A^{\text{open}}_{i}(t)$ bits of confidential and open information to real queues $Q^{\text{conf}}_{(i,1)}(t)$ and $Q^{\text{open}}_{(i,1)}(t)$ respectively. Also, node i adds $A^{\text{drop}}_{i}(t)$ virtual bits into virtual queue $Q^{\text{drop}}_{i}(t)$. We choose these parameters as the solution of:

$$\left(A^{\text{conf}}_{i}(t),A^{\text{drop}}_{i}(t),A^{\text{open}}_{i}(t)\right)=\underset{A^{\text{conf}}\geq 0,A^{\text{drop}}\geq 0,A^{\text{open}}\geq 0}{\text{argmax}}\left\{\frac{1}{\alpha}\left[U^{\text{conf}}_{i}(A^{\text{conf}}-A^{\text{drop}})+U^{\text{open}}_{i}(A^{\text{open}})\right]-Q^{\text{conf}}_{i}(t)A^{\text{conf}}-Q^{\text{open}}_{i}(t)A^{\text{open}}+Q^{\text{drop}}_{i}(t)A^{\text{drop}}\right\}$$

(2) Scheduling: Select a node i, and one of its confidential ($\mathcal{S}^{\text{conf}}_{(i,r)}(t)=1$) or open ($\mathcal{S}^{\text{open}}_{(i,r)}(t)=1$) queues for transmission. If the transmission is from a confidential data queue but NAK feedback is received from the base station, determine whether to drop the confidential message ($\mathscr{D}_{(i,r)}(t)=1$) or not. We choose these parameters as the solution of:

$$\left(\mathcal{S}^{\text{conf}}_{(i,r)}(t),\mathcal{S}^{\text{open}}_{(i,r)}(t),\mathscr{D}_{(i,r)}(t)\right)=\underset{\mathcal{S}^{\text{conf}},\mathcal{S}^{\text{open}},\mathscr{D}}{\text{argmax}}\left\{\sum_{k=1}^{M}\left(Q^{\text{conf}}_{(i,k)}(t)\mathcal{S}^{\text{conf}}_{(i,k)}(t)C^{\text{conf}}_{i}+Q^{\text{open}}_{(i,k)}(t)\mathcal{S}^{\text{open}}_{(i,k)}(t)C^{\text{open}}_{i}\right)\right.$$

$$-\sum_{k=1}^{M-1}\Big(Q^{\text{conf}}_{(i,k+1)}(t)\mathcal{S}^{\text{conf}}_{(i,k)}(t)\mathscr{I}^{\text{conf}}_{(i,k)}(t)(1-\mathscr{D}_{(i,k)}(t))C_i^{\text{conf}}$$
$$+Q^{\text{open}}_{(i,k+1)}(t)\mathcal{S}^{\text{open}}_{(i,k)}(t)\mathscr{I}^{\text{open}}_{(i,k)}(t)C_i^{\text{open}}\Big)$$
$$-Q_i^{\text{drop}}(t)\sum_{k=1}^{M}\mathcal{S}^{\text{conf}}_{(i,k)}(t)\mathscr{I}^{\text{conf}}_{(i,k)}(t)\mathscr{D}_{(i,k)}(t)C_i^{\text{conf}}-K_i(t)C_i^{\text{conf}}$$
$$\left(\sum_{k=1}^{M}\mathcal{S}^{\text{conf}}_{(i,k)}(t)\rho^{\text{secr}}_{(i,k)}\Big((1-\mathscr{I}^{\text{conf}}_{(i,k)}(t))+\mathscr{I}^{\text{conf}}_{(i,k)}(t)\mathscr{D}_{(i,k)}(t)\Big)-\gamma_i\right)\Bigg\},$$

where $\sum_{i=1}^{n}\sum_{k=1}^{M}\mathcal{S}^{\text{conf}}_{(i,k)}(t)+\mathcal{S}^{\text{open}}_{(i,k)}(t)=1$. The queues in each node are updated with respect to the ACK/NAK feedback received from the base station. If $\mathcal{S}^{\text{conf}}_{(i,r)}(t)=1$ and NAK feedback is received from the base station, $\mathscr{D}_{(i,r)}(t+1)$ is determined as follows:

$$\mathscr{D}_{(i,r)}(t+1)=\begin{cases}1, & \text{if } Q^{\text{conf}}_{(i,r+1)}(t+1)>Q_i^{\text{drop}}(t+1)\\ & \qquad\qquad +K_i(t+1)\rho^{\text{secr}}_{(i,r)}\\ 0, & \text{otherwise.}\end{cases}$$

For all other cases, $\mathscr{D}_{(i,r)}(t+1)=0$.

Theorem 1: If $C_i^{\text{conf}}<\infty$ and $C_i^{\text{open}}<\infty$ for all i, and $A_i^{\text{conf}}(t)<A_i^{\text{conf,max}}<\infty$ and $A_i^{\text{open}}(t)<A_i^{\text{open,max}}<\infty$ for all i,t then for some given $\alpha>0$ the proposed dynamic control algorithm satisfies:

$$\sum_{i=1}^{n}U_i^{\text{conf}}(\lambda_i^{\text{conf}}-\lambda_i^{\text{drop}})+U_i^{\text{open}}(\lambda_i^{\text{open}})\geqslant U^*-B\alpha$$
$$\limsup_{T\to\infty}\frac{1}{T}\sum_{\tau=0}^{T-1}\sum_{i=1}^{n}\mathbb{E}\left[Q^{\text{conf}}_{(i,1)}(\tau)\right]\leqslant\frac{B+(\bar{U}-U^*)/\alpha}{\varepsilon_1}$$
$$\limsup_{T\to\infty}\frac{1}{T}\sum_{\tau=0}^{T-1}\sum_{i=1}^{n}\mathbb{E}\left[Q^{\text{open}}_{(i,1)}(\tau)\right]\leqslant\frac{B+(\bar{U}-U^*)/\alpha}{\varepsilon_2},$$

where

$$\lambda_i^{\text{conf}}=\liminf_{T\to\infty}\frac{1}{T}\sum_{\tau=0}^{T-1}A_i^{\text{conf}}(\tau),$$
$$\lambda_i^{\text{drop}}=\liminf_{T\to\infty}\frac{1}{T}\sum_{\tau=0}^{T-1}A_i^{\text{drop}}(\tau),$$
$$\lambda_i^{\text{open}}=\liminf_{T\to\infty}\frac{1}{T}\sum_{\tau=0}^{T-1}A_i^{\text{open}}(\tau),$$

$B,\varepsilon_1,\varepsilon_2>0$ are constants, and U^* is the optimal aggregate utility, i.e., the solution of the problem in (21)-(22) and $\bar{U}$ is the maximum possible aggregate utility.

Proof: The proof of Theorem 1 is given in Appendix B. ■

According to Theorem 1, there is a trade-off in choosing the parameter α, i. e., smaller values achieve a solution closer to the optimal, but at the same time increases the aggregate queue length. Note that, Theorem 1 gives performance bounds for the separate encoding. However, the performance bounds with joint encoding can be obtained by following similar approach done in Theorem 1.

Discussion: Our cross-layer algorithm relies on the assumption that only one user is scheduled to transmit to the base station while other users behave as passive eavesdroppers. However, the same model can be extended to a multi-user scheduling setting where a number of users can transmit at the same time slot. Multiple users accessing to the same channel can be modeled as medium access control (MAC) channel. For the MAC channel, the achievable confidential rates can be found as in [31]. The results in [31] show that the achievable rates of each transmitting node depend on the set of active nodes, i.e., the nodes which are actively transmitting in slot t. More precisely, if we allow simultaneous scheduling of multiple nodes, the possible number of schedules grow exponentially with the number of active users. Furthermore, for any given set of scheduled users, the number of rate allocations depend on the order of decoding for the associated MAC channel. Consequently, the set of possible rate allocations for each active user grows super-exponentially with the number of active users. Thus, the number of queues defined for each schedule and the complexity of the scheduling algorithm increase fairly significantly. Even if multi-user scheduling have potential to improve the network performance, one needs to take into account the increased complexity as well as the performance improvement when designing the system.

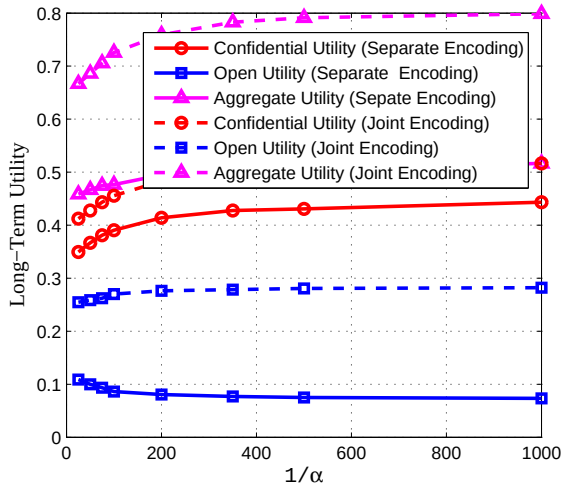
V. Numerical Results

In our numerical evaluations, we consider an uplink wireless cellular network consisting of four nodes and a single base station. The uplink channel between a node and the base station, and the cross-channels between pairs of nodes are modeled as iid Rayleigh fading Gaussian channels. The power gains of the channels are exponentially distributed with the probability density function (PDF) $f(h_i)=(1/\overline{h_i})e^{-h_i/\overline{h_i}}$, and the cross-channel between node i and node j has the PDF $f(h_{ij})=(1/\overline{h_{ij}})e^{-h_{ij}/\overline{h_{ij}}}$, where $\overline{h_i}$ and $\overline{h_{ij}}$ are the average channel gains of the uplink channel and the cross-channel between node i and node j, respectively. Let $\overline{h_i}$ and $\overline{h_{ij}}$ be chosen at random, uniformly distributed in the intervals $[6,10]$, and $[0.5,2]$, respectively. The normalized transmit power is taken as $P=1$ in every slot and for all nodes.

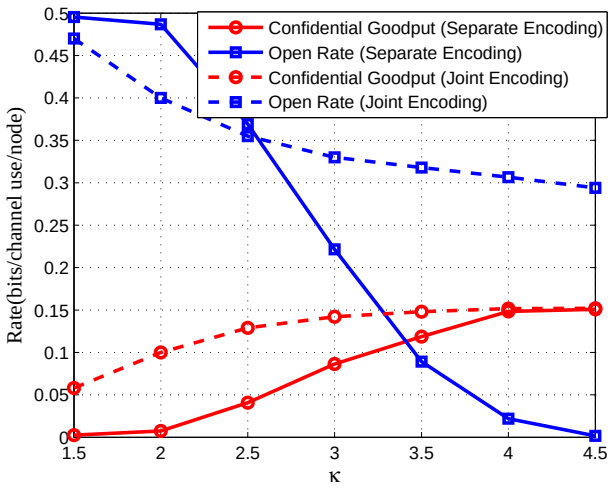
We consider logarithmic confidential and open utility functions where the confidential utility is chosen to be κ times the open utility for a given rate[4]. More precisely, $U_i^{\text{open}}(x)=\frac{1}{\kappa}U_i^{\text{conf}}(x)=\log(1+x)$. We take $\kappa=3.5$ in all experiments except for the one investigating the effect of κ. In addition, we select encoding rates as $C_i^{\text{code}}=3$, $C_i^{\text{conf}}=1$, and $C_i^{\text{open}}=3$ for all i in all experiments except for the one inspecting the effect of C_i^{code}. The rates depicted in the graphs are average per node rates calculated as the total rates achieved by the network divided by the number of nodes. The unit of the plotted rates is bits/channel-use/node. We simulate both control algorithm presented in Section IV-B (we refer to this policy as Algorithm with Separate Encoding) and its joint encoding version where the randomization message is selected from open bits (we refer to this policy as Algorithm with Joint Encoding).

In Fig. 3a, we investigate the effect of system parameter $\frac{1}{\alpha}$ in our dynamic control algorithms. We take $\gamma=0.25$ for all nodes. As expected, the total utility increases with increasing $\frac{1}{\alpha}$ and Fig. 3a shows that the long-term utilities for $\frac{1}{\alpha}>200$ converges to their optimal values fairly closely verifying the results in Theorem 1 for both algorithms with separate and

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

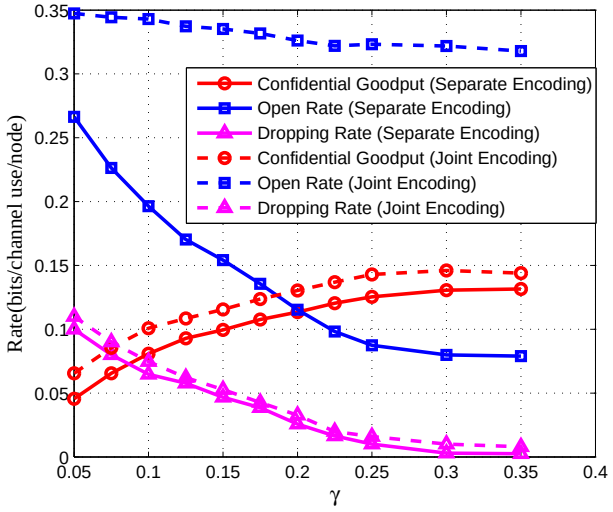


(a) Long-term Utility vs. $1/\alpha$

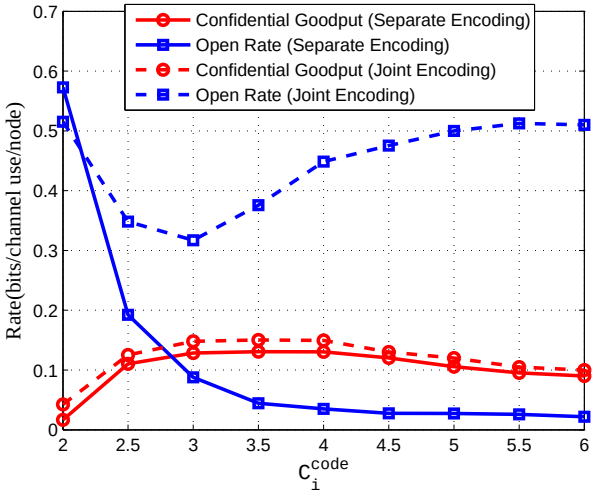


(b) confidential and open rates vs. κ

Fi



(a) confidential and open rates vs. γ



(b) confidential and open rates vs. C_i^{code}

Fig. 4. Numerical results with respect to parameters γ and C_i^{code}.

joint encoding. In addition, as expected, we obtain higher utility with joint encoding since one can utilize additional resources by using open bits instead of randomization bits.

For the rest of the experiments, we take $\frac{1}{\alpha} = 200$. Fig. 3b analyzes the effect of κ, which can also be interpreted as the ratio of utility of confidential and open transmissions taking place at the same rate. We call this ratio *confidential utility gain*. As expected, the confidential goodput increases while the open rate decreases as the confidential utility gain increases. Interestingly, for small values of confidential utility gain, the confidential rate is approximately zero for the algorithm with separate encoding. This is due to fact that confidential transmissions consume more resources, and thus, open transmission is more preferable with comparable utility gains. On the other hand, for the algorithm with joint encoding, the confidential rate is non-zero even with small κ values since resources is utilizes more efficiently by encoding open bits jointly with confidential bits. On the other hand, when confidential utility gain is high, system favors confidential transmissions to maximize the total network utility for both algorithms.

Fig. 4a illustrates the effect of the secrecy outage probability constraint, γ. As seen from Fig. 4a, algorithms with separate and joint encoding exhibits similar behaviors with increasing γ except that the algorithm with joint encoding achieves higher open rate as expected. Confidential goodput increases with increasing γ. This is because for low γ values, in order to satisfy a tight secrecy outage constraint, a larger fraction of confidential messages are dropped. Meanwhile, open rate decreases with increasing γ, since there is a smaller number of transmission opportunities left for open messages with more confidential information being transmitted by the node. Starting around $\gamma = 0.25$, the secrecy outage constraint becomes inactive, since the constraint is realized with strict inequality.

We finally investigate the effect of encoding rate C_i^{code} for $\gamma = 0.25$ in Fig. 4b. Initially, confidential goodput increases with increasing encoding rate C_i^{code} for both control

algorithms. Note that for small randomization rates, i.e., $C_i^{\text{code}} - C_i^{\text{conf}}$, other nodes can accumulate information on the confidential messages over the cross-channels. Hence, the probability of secrecy outages is high, and the transmitter drops confidential messages more frequently in order to satisfy the given secrecy outage constraint γ. As randomization rate increases, the confidential goodput increases until $C_i^{\text{code}} = 3$. Note that, any further increase in C_i^{code} results in a decrease in confidential goodput, since the base station needs to collect more information to successfully decode the message, which in turn increases the probability of decoding failures. This result clearly exhibits a *tradeoff between secrecy and reliability*. Transmitter needs to add sufficient randomization to ensure perfect secrecy, but beyond a certain point, too much randomization harms the reliability of the communication. Meanwhile, open rate decreases with increasing C_i^{code} for the algorithm with separate encoding, since, as C_i^{code} increases, nodes use more resources to transmit confidential messages, and a smaller number of transmission opportunities remain for open transmissions. Differently, for the algorithm with joint encoding, with increasing C_i^{code}, a node can jointly encode increasing number of open bits with confidential bits. After $C_i^{\text{code}} = 3$, this increase of jointly encoded open bits dominates the decrease in transmission opportunities for open transmissions, which results in increasing open rate with increasing C_i^{code} .

VI. Conclusion

We considered the problem of resource allocation in wireless cellular networks where nodes have both open and confidential information to be transmitted to the base station over time-varying uplink channels. All nodes in the network are considered as internal eavesdroppers from which the confidential information needs to be protected. Unlike other works in the literature, we develop a provably-optimal scheme that handles a hybrid traffic involving both open and confidential packets, without an instantaneous CSI. Given only the statistical distribution of main and cross-channels, we have developed a reliable cross-layer dynamic control algorithm based on HARQ transmission with incremental redundancy. We believe our new technique also contributes to the field of network control [27], [32], even without confidential information transmissions, since it enables the use of Lyapunov techniques in the analysis of the schemes such as HARQ, which is based on encoding information over many blocks.

As a future direction, we will investigate the implementation of our dynamic control algorithm with HARQ in a multi-hop setting, where the confidential and open messages between multiple source destination pairs are carried cooperatively via intermediate relay nodes.

Appendix A
Proof of Proposition 3

Here, we provide the proof of Proposition 3 for the confidential messages by identifying the achievable rate regions for confidential messages, but it can be shown in a similar way for the open messages. Let $\boldsymbol{\lambda}^{\text{conf}}$ be the rate vector defined as $\left[\lambda_1^{\text{conf}}, \ldots, \lambda_n^{\text{conf}}\right]$. First, we show that if $\boldsymbol{\lambda}^{\text{conf}} \in \Gamma$, then it should lie in $\hat{\Gamma}$ as well. This can be shown directly by determining $\hat{\pi}_{(i,1)}^{\text{conf}}$ which is equal to (or larger than) $\pi_{(i,1)}^{\text{conf}}$, since the departure rates are completely characterized by $\hat{\pi}_{(i,1)}^{\text{conf}}$ and $\pi_{(i,1)}^{\text{conf}}$. Note that, with conventional policy given the control decisions, π_i^{conf} and $d_{(i,r)}$, we uniquely obtain $\pi_{(i,r)}$ using (6) and (8) as:

$$\pi_{(i,r)}^{\text{conf}} = \pi_i^{\text{conf}} \frac{\prod_{n=1}^{r-1} \rho_{(i,n)}^{\text{conf}} (1 - d_{(i,n)})}{1 + \sum_{m=1}^{M-1} \prod_{n=1}^{m} \rho_{(i,n)}^{\text{conf}} (1 - d_{(i,n)})} \tag{46}$$

Suppose that (14) is realized with equality. Then, if the stationary random scheduling decision of the proposed policy, $\hat{\pi}_{(i,r)}^{\text{conf}}$, is selected such that $\hat{\pi}_{(i,r)}^{\text{conf}} = \pi_{(i,r)}^{\text{conf}}$, where $\pi_{(i,r)}^{\text{conf}}$ is obtained in (46), $\boldsymbol{\lambda}^{\text{conf}} \in \hat{\Gamma}$ as well.

The other direction can be shown by proving that for any $\boldsymbol{\lambda}^{\text{conf}} + \varepsilon_1 \in \hat{\Gamma}$, $\boldsymbol{\lambda}^{\text{conf}} + \varepsilon_2 \in \Gamma$, and $\varepsilon_2 \leq \varepsilon_1$.

Since $\boldsymbol{\lambda}^{\text{conf}} + \varepsilon_1 \in \hat{\Gamma}$, we have

$$\lambda_i^{\text{conf}} + \varepsilon_1 \leq C_i^{\text{conf}} \hat{\pi}_{(i,1)}^{\text{conf}}$$

Let $\varepsilon \geq 0$ be a variable reflecting the slack in inequality (14):

$$\hat{\pi}_{(i,r)}^{\text{conf}} = \hat{\pi}_{(i,r-1)}^{\text{conf}} \rho_{(i,r-1)}^{\text{conf}} (1 - d_{(i,r-1)}) + \varepsilon, \tag{47}$$

Now, we need to determine whether there exists $\pi_{(i,1)}^{\text{conf}}$ referring to the departure rate such that λ_i^{conf} is in the region specified by Γ. By letting $\sum_{r=1}^{M} \hat{\pi}_{(i,r)}^{\text{conf}} = \sum_{r=1}^{M} \pi_{(i,r)}^{\text{conf}}$, we have that (10) and (8) satisfied, and by using (6) for $\pi_{(i,r)}^{\text{conf}}$ and (47) for $\hat{\pi}_{(i,r)}^{\text{conf}}$, we obtain $\pi_{(i,1)}^{\text{conf}}$ as:

$$\pi_{(i,1)}^{\text{conf}} = \hat{\pi}_{(i,1)}^{\text{conf}} + \frac{(M-1)\varepsilon}{1 + \sum_{m=1}^{M-1} \prod_{n=1}^{m} \rho_{(i,n)}^{\text{conf}} (1 - d_{(i,n)})},$$

where M is the maximum number of times that a message can be retransmitted. By letting $\varepsilon_2 = \varepsilon_1 - \frac{C_i^{\text{conf}}(M-1)\varepsilon}{1+\sum_{m=1}^{M-1} \prod_{n=1}^{m} \rho_{(i,n)}^{\text{conf}} (1-d_{(i,n)})}$, we have

$$\lambda_i^{\text{conf}} + \varepsilon_2 \leq C_i^{\text{conf}} \pi_{(i,1)}^{\text{conf}}.$$

Thus, we have $\boldsymbol{\lambda}^{\text{conf}} + \varepsilon_2 \in \Gamma$. Notice that, the second term of ε_2 is non-negative implying that ε_2 is always equal to or smaller than ε_1. Furthermore, in the first part, we prove that for $\boldsymbol{\lambda}^{\text{conf}} \in \Gamma$, $\boldsymbol{\lambda}^{\text{conf}} \in \hat{\Gamma}$ as well, so ε_2 cannot have a negative value. As $\varepsilon_1 \to 0$, ε_2 and ε approach zero as well, which proves that in the boundary of the region $\hat{\Gamma}$, (14) is realized with equality, and $\Gamma = \hat{\Gamma}$.

Appendix B
Proof of Theorem 1

The optimality of the algorithm can be shown by applying the Lyapunov optimization theorem [27]. Before restating this theorem, we define the following parameters. Let $\mathbf{B}(t) = (B_1(t), \ldots, B_K(t))$ be the backlog process of the queues in a given queuing system, and let our objective be the maximization of a scalar valued concave function $g(\cdot)$ of time average of another process $\mathbf{R}(t)$ while keeping $\mathbf{B}(t)$ finite. Also define $\Delta(\mathbf{B}(t)) = \mathbb{E}\left[L(\mathbf{B}(t+1)) - L(\mathbf{B}(t)) | \mathbf{B}(t)\right]$ as the drift of some appropriate Lyapunov function $L(\cdot)$.

Theorem 2: (Lyapunov Optimization) [27] For the scalar valued concave function $g(\cdot)$, if there exists positive constants V, ε, W, such that for all blocks t and all unfinished work vector $\mathbf{B}(t)$ the Lyapunov drift satisfies:

$$\Delta(\mathbf{B}(t)) - V\mathbb{E}\left[g(\mathbf{R}(t))|\mathbf{B}(t)\right] \leq W - Vg^* - \varepsilon\sum_{i=1}^{K} B_i(k), \quad (48)$$

then the time average utility and queue backlog satisfy:

$$\liminf_{t\to\infty} g(\bar{r}(t)) \geq g^* - \frac{W}{V} \quad (49)$$

$$\limsup_{t\to\infty} \frac{1}{t}\sum_{\tau=0}^{t-1}\sum_{i=1}^{K}\mathbb{E}\left[B_i(\tau)\right] \leq \frac{W+V(\bar{g}-g^*)}{\varepsilon}, \quad (50)$$

where $\bar{r}(t) = \frac{1}{t}\sum_{\tau=0}^{t-1}\mathbb{E}\left[\mathbf{R}(\tau)\right]$, g^* is the optimal value of $g(\cdot)$ and $\bar{g} = \limsup_{t\to\infty}\frac{1}{t}\sum_{\tau=0}^{t-1}\mathbb{E}\left[g(\mathbf{R}(\tau))\right]$.

The proof of Theorem 2 can be found in [27]. Let $\mathbf{Q}(t) = (Q^{\text{conf}}_{(1,1)}(t),\ldots,Q^{\text{conf}}_{(1,M)}(t),\ldots,Q^{\text{conf}}_{(n,M)}(t),$ $Q^{\text{open}}_{(1,1)}(t),\ldots,Q^{\text{open}}_{(1,M)}(t),\ldots,Q^{\text{open}}_{(n,M)}(t),$ $Q^{\text{drop}}_{1}(t),\ldots,Q^{\text{drop}}_{n}(t),K_1(t),\ldots,K_n(t))$ be a vector of all real and virtual queues in the system. We consider a quadratic Lyapunov function of the form:

$$L(\mathbf{Q}(t)) = \frac{1}{2}\sum_{i=1}^{n}\left[\sum_{r=0}^{M}\left((Q^{\text{conf}}_{(i,r)}(t))^2 + (Q^{\text{open}}_{(i,r)}(t))^2\right) + (Q^{\text{drop}}_{i}(t))^2 + (K_i(t))^2\right].$$

Also we define the one-step expected Lyapunov drift, $\Delta(\mathbf{Q}(t))$ as: $\Delta(\mathbf{Q}(t)) = \mathbb{E}\left[L(t+1) - L(t)|\mathbf{Q}(t)\right]$.

The following lemma provides an upper bound on $\Delta(\mathbf{Q}(t))$.

Lemma 1:

$$\begin{aligned}
\Delta(\mathbf{Q}(t)) \leq\ & B - \sum_{i=1}^{n}\mathbb{E}\left[Q^{\text{conf}}_{(i,1)}(t)(\mathcal{S}^{\text{conf}}_{(i,1)}(t)C^{\text{conf}}_{i} - A^{\text{conf}}_{i}(t))\right] \\
& - \sum_{i=1}^{n}\sum_{r=2}^{M}\mathbb{E}\left[Q^{\text{conf}}_{(i,r)}(t)C^{\text{conf}}_{i}(\mathcal{S}^{\text{conf}}_{(i,r)}(t) - \mathcal{S}^{\text{conf}}_{(i,r-1)}\mathscr{F}^{\text{conf}}_{(i,r-1)}(t)(1-\mathscr{D}_{(i,r-1)}(t))\right] \\
& - \sum_{i=1}^{n}\mathbb{E}\left[Q^{\text{open}}_{(i,1)}(t)(\mathcal{S}^{\text{open}}_{(i,1)}(t)C^{\text{open}}_{i} - A^{\text{open}}_{i}(t))\right] \\
& - \sum_{i=1}^{n}\sum_{r=2}^{M}\mathbb{E}\left[Q^{\text{open}}_{(i,r)}(t)C^{\text{open}}_{i}(\mathcal{S}^{\text{open}}_{(i,r)}(t) - \mathcal{S}^{\text{open}}_{(i,r-1)}\mathscr{F}^{\text{open}}_{(i,r-1)})\right] \\
& - \sum_{i=1}^{n}\mathbb{E}\left[Q^{\text{drop}}_{i}(t)\left(\sum_{r=1}^{M}\mathcal{S}^{\text{conf}}_{(i,r)}(t)\mathscr{F}_{(i,r)}(t)\mathscr{D}_{(i,r)}(t)C^{\text{conf}}_{i} - A^{\text{drop}}_{i}(t)\right)\right] \\
& - \sum_{i=1}^{n}\mathbb{E}\left[K_i(t)C^{\text{conf}}_{i}\left(\sum_{r=1}^{M}\mathcal{S}^{\text{conf}}_{(i,r)}(t)\rho^{\text{secr}}_{(i,r)}\left((1-\mathscr{F}^{\text{conf}}_{(i,r)}(t)) + \mathscr{F}^{\text{conf}}_{(i,r)}(t)\mathscr{D}_{(i,r)}\right) - \gamma_i\right)\right]
\end{aligned} \quad (51)$$

where $B > 0$ is a constant. Note that all expectations are conditioned on $\mathbf{Q}(t)$.

Proof: In an interference-limited practical wireless system both the transmission power and the transmission rate is bounded. We assume that the confidential and open arrival rates are also bounded by $A_i^{\text{conf,max}}$, $A_i^{\text{open,max}}$. By following simple algebraic manipulations one can obtain a bound for the difference $(Q^{\text{conf}}_{(i,1)}(t+1))^2 - (Q^{\text{conf}}_{(i,1)}(t))^2$.

$$\begin{aligned}
&\frac{(Q^{\text{conf}}_{(i,1)}(t+1))^2 - (Q^{\text{conf}}_{(i,1)}(t))^2}{2} \\
&= \left(\left[Q^{\text{conf}}_{(i,1)}(t) - \mathcal{S}^{\text{conf}}_{(i,1)}(t)C^{\text{conf}}_{i}\right]^{+} + A^{\text{conf}}_{i}(t)\right)^2/2 - (Q^{\text{conf}}_{(i,1)}(t))^2/2 \\
&\leq (C^{\text{conf}}_{i})^2/2 + (A^{\text{conf}}_{i}(t))^2/2 - Q^{\text{conf}}_{(i,1)}(t)[\mathcal{S}^{\text{conf}}_{(i,1)}(t)C^{\text{conf}}_{i} - A^{\text{conf}}_{(i,1)}(t)] \\
&\leq B_1 - Q^{\text{conf}}_{(i,1)}(t)[\mathcal{S}^{\text{conf}}_{(i,1)}(t)C^{\text{conf}}_{i} - A^{\text{conf}}_{(i,1)}(t)] \\
&\text{where } B_1 = \frac{(C^{\text{conf}}_{i})^2 + (A^{\text{conf,max}}_{i})^2}{2}
\end{aligned}$$

The bounds for other types of queues in the system can be derived in a similar fashion. The derivations of these bounds are omitted for brevity. Summing up all bounds, we obtain the result given in (51). ∎

Theorem 2 suggests that a good control strategy is the one that minimizes the following:

$$\Delta^U(t) = \Delta(t) - \frac{1}{\alpha}\mathbb{E}\left[\sum_i U^{\text{conf}}_i\left(A^{\text{conf}}_i(t) - A^{\text{drop}}_i(t)\right) + U^{\text{open}}_i(A^{\text{open}}_i(t))|\mathbf{Q}(t)\right] \quad (52)$$

where $U^{\text{conf}}_i(t)$ and $U^{\text{open}}_i(t)$ are confidential and open utility obtained in slot t. By using (51), we may obtain an upper bound for (52).

$$\begin{aligned}
&\Delta^U(t) < \text{RHS of (51)} \\
&- \frac{1}{\alpha}\mathbb{E}\left[\sum_i U^{\text{conf}}_i\left(A^{\text{conf}}_i(t) - A^{\text{drop}}_i(t)\right) + \sum_i U^{\text{open}}_i(A^{\text{open}}_i(t))|\mathbf{Q}(t)\right]
\end{aligned} \quad (53)$$

Our proposed dynamic network control algorithm is designed such that it minimizes the right hand side of (53). If the arrival rates and the secrecy outage parameter, γ_i, are in the feasible region, it has been shown in [27] that there must exist a stationary scheduling and rate control policy that chooses the users independent of queue backlogs. Let U^* be the optimal value of the objective function of the problem (21)-(22) obtained by the aforementioned stationary policy. Also let $\lambda_i^{\text{conf}^*}$, $\lambda_i^{\text{open}*}$, $\lambda_i^{\text{drop}^*}$, be optimal traffic arrival rates, and the confidential goodput and packet dropping rates found as the solution of the same problem. Note that the expectations on the right hand side of (53) can be written separately due to independence of backlogs with scheduling and rate control policy. Also, since the rates are in the achievable rate region, i.e., arrival rates are strictly interior of the rate region, there must exist a stationary scheduling and rate allocation policy that is independent of queue backlogs which satisfies the following:

$$\begin{aligned}
&C^{\text{conf}}_i\pi^{\text{conf}}_{(i,1)} \geq \lambda_i^{\text{conf}^*} + \varepsilon_1\ ,\ C^{\text{open}}_i\pi^{\text{open}}_{(i,1)} \geq \lambda_i^{\text{open}^*} + \varepsilon_2\ , \\
&\mu^{\text{drop}}_i + \varepsilon_3 \geq \lambda_i^{\text{drop}^*}\ \text{, and} \\
&C^{\text{conf}}_i\gamma_i \geq C^{\text{conf}}_i\sum_{r=1}^{M}\pi^{\text{conf}}_{(i,r)}\rho^{\text{secr}}_{(i,r)}\left((1-\rho^{\text{conf}}_{(i,r)}) + \rho^{\text{conf}}_{(i,r)}d_{(i,r)}\right) + \varepsilon_4
\end{aligned} \quad (54)$$

Recall that our proposed policy minimizes RHS of (53), and thus, any other stationary policy has a higher RHS value. By using optimal stationary policy, we can obtain an upper bound for the RHS of our proposed policy. Inserting (54) into (53) and using the independence of queue backlogs with scheduling and rate policy, we obtain the following bound:

$$\begin{aligned}
RHS <\ & B - \sum_i \varepsilon_1\mathbb{E}\left[Q^{\text{conf}}_{(i,1)}(t)\right] - \sum_i \varepsilon_2\mathbb{E}\left[Q^{\text{open}}_{(i,1)}(t)\right] - \sum_i \varepsilon_3\mathbb{E}\left[Q^{\text{drop}}_{i}(t)\right] \\
& - \sum_i \varepsilon_4\mathbb{E}\left[K_i(t)\right] - V\mathbb{E}\left[\sum_i U^{\text{conf}}_i(A^{\text{conf}}_i(t) - A^{\text{drop}}_i(t)) + U^{\text{open}}_i(A^{\text{open}}_i(t))\right]
\end{aligned}$$

$$< B - \sum_i \varepsilon_1 \mathbb{E}\left[Q^{\text{conf}}_{(i,1)}(t)\right] - \sum_i \varepsilon_2 \mathbb{E}\left[Q^{\text{open}}_{(i,1)}(t)\right] - \sum_i \varepsilon_3 \mathbb{E}\left[Q^{\text{drop}}_i(t)\right] - \sum_i \varepsilon_4 \mathbb{E}\left[K_i(t)\right] - \frac{U^*}{\alpha}. \quad (55)$$

where (55) follows from Jensen's inequality together with concavity of $U_i^{\text{conf}}(.)$ and $U_i^{\text{open}}(.)$, and $U^* = \sum_i U_i^{\text{conf}}(\lambda_i^{\text{conf}^*} - \lambda_i^{\text{drop}^*}) + U_i^{\text{open}}(\lambda_i^{\text{open}^*})$. This is exactly in the form of Lyapunov Optimization Theorem given in Theorem 2, and hence, we can obtain bounds on the performance of the proposed policy and the sizes of queue backlogs as given in Theorem 1. ■

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1380, Oct. 1975.

[2] 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.

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

[4] 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, pp. 1–9.

[5] A. Khisti and G. W. Wornell, "Secure transmissions with multiple antennas: The misome wiretap channel," *IEEE Trans. Inf. Theory*, vol. 7, pp. 3088–3014, July 2010.

[6] S. Shaffiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of gaussian mimo wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, pp. 4033–4039, Sept. 2009.

[7] 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, no. 3, pp. 4033–4039, March 2010.

[8] G. Zheng, L. Choo, and K. Wong, "Optimal Cooperative Jamming to Enhance Physical Layer Security Using Relay," *IEEE Trans. on Signal Processing*, vol. 59, no. 3, March 2011.

[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] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J. Merolla, "Ldpc based secret key agreement over gaussian wiretap channel," in *Proc. IEEE Intl. Symposium on Information Theory*, Seattle, WA, Sep. 2011, pp. 1179–1183.

[11] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inform. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[12] N. Cai and R. Yeung, "Secure network coding," in *Proc. IEEE Int. Symposium Inform. Theory*, Lausanne, Switzerland, June 2002, p. 323.

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

[14] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the Throughput of Secure Hybrid-ARQ Protocols for Gaussian Block-Fading Channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, March 2009.

[15] R. Urgaonkar and M. J. Neely, "Optimal routing with mutual information accumulation in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 9, pp. 1730–1737, Sep. 2012.

[16] T. Girici and A. C. Kazez, "Energy efficient routing with mutual information accumulation," *Proc. Intl. Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, pp. 425–430, May 2012.

[17] J. Huang, R. A. Berry, and M. L. Honig, "Wireless scheduling with hybrid arq," *IEEE Trans. on Wireless Communications*, vol. 4, no. 6, pp. 2801–2810, Nov. 2005.

[18] A. K. Karmokar, D. V. Djonin, and V. K. Bhargava, "Cross-Layer Rate and Power Adaptation Strategies for IR-HARQ Systems over Fading Channels with Memory: A SMDP-Based Approach," *IEEE Trans. on Communications*, vol. 56, no. 8, pp. 1352–1365, Aug. 2008.

[19] H. T. Zheng and H. Viswanathan, "Optimizing the ARQ performance in downlink packet data systems with scheduling," *IEEE Trans. on Wireless Communications*, vol. 4, pp. 495–506, Mar. 2005.

[20] M. Assaad and D. Zeghlache, "Cross-Layer design in HSDPA system to reduce the TCP effect," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 614–625, Mar. 2006.

[21] Y. Sun, C. E. Koksal, S. J. Lee, and N. B. Shroff, "Network control without csi using rateless codes for downlink cellular systems." in *Proc. IEEE Conf. Computer Communications (Infocom)*, Turin, Italy, 2013.

[22] C. E. Koksal, O. Ercetin, and Y. Sarikaya, "Control of wireless networks with secrecy," *IEEE/ACM Trans. on Networking*, vol. 21, no. 1, pp. 215–225, Feb. 2013.

[23] Y. Sarikaya, O. Ercetin, and C. E. Koksal, "Wireless network control with privacy using hybrid arq," in *Proc. IEEE Intl. Symposium on Information Theory*, Cambridge, MA, July 2012, pp. 1142–1146.

[24] S. Lin, J. D. J. Costello, and M. J. Miller, "Automatic-repeat-request error control schemes," *IEEE Communications Magazine*, vol. 22, pp. 5–16, Dec. 1984.

[25] J. Yang, Y. Liu, and S. C. Draper, "Optimal scheduling policies with mutual information accumulation in wireless networks." in *Proc. IEEE Conf. Computer Communications (Infocom)*, 2012, pp. 1062–1070.

[26] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[27] L. Georgiadis, M. J. Neely, and L. Tassiulas, "Resouce Allocation and Cross-layer Control in Wireless Networks," *Foundations and Trends in Networking*, vol. 1, no. 1, pp. 1–144, 2006.

[28] D. P. Palomar and M. Chiang, "A Tutorial on Decomposition Methods for Network Utility Maximization," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 8, pp. 1439–1451, June 2007.

[29] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York, NY: Cambridge University Press, 2004.

[30] D. P. Bertsekas and J. N. Tsitsiklis, *Parallel and Distributed Computation: Numerical Methods*. Upper Saddle Rive, NJ: Prentice-Hall, 1989.

[31] Y. Liang and H. V. Poor, "Generalized multiple access channels with confidential messages," in *Proc. IEEE Intl. Symposium on Information Theory*, Seattle, WA, July 2006, pp. 952–956.

[32] X. Lin and N. B. Shroff, "Utility maximization for communication networks with multipath routing," *IEEE Trans. on Automatic Control*, vol. 51, no. 5, pp. 766–781, May 2006.

Yunus Sarikaya received the BS and MS degrees in telecommunications engineering from Sabanci University, Istanbul, Turkey, in 2006 and 2008, respectively. He was a visiting scholar at The Ohio State University, OH. He is currently PhD student in electrical engineering at Sabanci University.

His research interests include optimal control of wireless networks, stochastic optimization and information theoretical security.

Ozgur Ercetin received the BS degree in electrical and electronics engineering from the Middle East Technical University, Ankara, Turkey, in 1995 and the MS and PhD degrees in electrical engineering from the University of Maryland, College Park, in 1998 and 2002, respectively. Since 2002, he has been with the Faculty of Engineering and Natural Sciences, Sabanci University, Istanbul. He was also a visiting researcher at HRL Labs, Malibu, CA, Docomo USA Labs, CA, and The Ohio State University, OH. His research interests are in the field of computer and communication networks with emphasis on fundamental mathematical models, architectures and protocols of wireless systems, and stochastic optimization.

C. Emre Koksal Can Emre Koksal (S96M03SM13) received the B.S. degree in Electrical Engineering from the Middle East Technical University in 1996, and the S.M. and Ph.D. degrees from MIT in 1998 and 2002, respectively, in Electrical Engineering and Computer Science. He was a Postdoctoral Fellow at MIT until 2004, and a Senior Researcher at EPFL until 2006. Since then, he has been with the Electrical and Computer Engineering Department at Ohio State University, currently as an Associate Professor. His general areas of interest are wireless communication, communication networks, information theory, stochastic processes, and financial economics.

He is the recipient of the National Science Foundation CAREER Award in 2011, the OSU College of Engineering Lumley Research Award in 2011, and the co-recipient of an HP Labs - Innovation Research Award in 2011. The paper he co-authored was a best student paper candidate in MOBICOM 2005. Currently, he is an Associate Editor for IEEE Transactions on Information Theory, IEEE Transactions on Wireless Communications, and Elsevier Computer Networks.