Distributed Opportunistic Scheduling with QoS Constraints for Wireless Networks with Hybrid Links

Wenguang Mao, Xudong Wang, and Shanshan Wu

***Abstract*—Opportunistic scheduling for a wireless network with hybrid links is studied in this paper. Specifically, two link types are considered: a link of the first type always has a much lower transmission rate than a link of the second type. To avoid starvation in the first type of links, two link types must be treated differently in opportunistic scheduling, and quality of service (QoS) constraints such as maximum delay or minimum throughput must be imposed on the first link type. Considering QoS constraints, a distributed opportunistic scheduling scheme is derived based on the optimal stopping theory. Two scenarios are considered for the QoS-oriented opportunistic scheduling scheme. In the first scenario, all links within the same link type follow the same rate distribution. Thus, QoS constraints are imposed on the entire link type. In the second scenario, links of the first type follow heterogeneous rate distributions. Thus, QoS requirements need to be imposed on links with the worst performance. Performance results show that the new opportunistic scheduling scheme outperforms the existing ones in most scenarios.**

***Index Terms*—distributed opportunistic scheduling, quality of service, hybrid links, optimal stopping theory.**

I. Introduction

It is common that wireless links in a network have heterogeneous characteristics such as transmission rates and QoS requirements. Such links are called *hybrid links* in this paper. One factor leading to link heterogeneity involves application-specific requirements for different links. For example, some applications (e.g., control message transmissions in the smart grid or cognitive radio networks) impose a strong requirement on the security, and physical layer techniques [1][2][3] are applied to ensure perfect secrecy in corresponding links (called *secure links*) [4][5]. Since perfect secrecy comes at the cost of degrading channel capacity [6][7], secure links have much lower transmission rates as compared to other links (called *regular links*). Due to security concern, secure links may also demand stringent QoS guarantee. For ease of explanation throughout this paper, we use *secure links* and *regular links* to represent two link types that follow significantly different rate distributions.

Packet transmissions in a network with hybrid links can be conducted in two different approaches: 1) following a pure random access medium access control (MAC) protocol; 2) based on a scheduling scheme. The former approach is simple and easy to implement, but may lead to low throughput in a network with hybrid links due to the presence of performance anomaly [8], i.e., the wireless medium is extensively occupied by low rate transmissions on secure links. Therefore, the latter approach is necessary to improve the network throughput. Among existing scheduling schemes, opportunistic scheduling is considered as the most effective to exploit fluctuations in channel conditions to produce significant throughput gains for the entire network [9][10][11]. The key idea of opportunistic scheduling is explained as follows: given a transmission opportunity, if a link with the highest transmission rate is selected, the maximum throughput can be achieved. Unfortunately, these opportunistic scheduling schemes rely on the existence of the central controller (e.g., the base station in cellular networks), and hence are hard to implement in ad hoc networks or wireless mesh networks, where such a central node is not readily available. To address this issue, several distributed opportunistic scheduling schemes are proposed [12]-[21], which utilized local information to determine whether to take transmission opportunities or not. However, the quality of service (QoS) of interested links are not taken into account in these schemes. Recently, a distributed opportunistic scheduling scheme considering the delay QoS is developed in [21] based on the scheme in [16]. However, this scheme is not applicable to hybrid links, as it cannot guarantee QoS requirements for a specific type of links (e.g., secure links) and at the same time maximize the overall throughput. So far, there is a lack of effective distributed opportunistic scheduling to support a network with hybrid links.

In order to treat hybrid links separately and also support QoS requirements of a specific type of links, a new distributed opportunistic scheduling scheme is proposed in this paper. It is developed based on the optimal stopping theory and considering two type of links: secure links and regular links. Compared with existing opportunistic scheduling schemes, the new scheduling scheme is distinct with following features: 1) the system overall throughput is maximized under various QoS constraints of a specific link type (e.g., secure links); 2) it can be implemented as a double-threshold scheduling policy, i.e., one threshold for each link type, and then a link determines its transmission opportunity based on this threshold; 3) the rate heterogeneity among the same type of links is also taken into account to improve QoS of links with low channel quality. Simulations are carried out to evaluate the new opportunistic scheduling scheme. Performance results verify the optimality of our scheme and demonstrate that QoS of secure links can be effectively guaranteed under both homogeneous and heterogeneous rate distribution scenarios. Moreover, results also show that our scheme outperforms the existing ones in most cases.

The contribution of this paper is the development of a new distributed scheduling framework that treats multiple types of links separately in an efficient way and effectively satisfies their own QoS requirements. Also, in our framework, various patterns of QoS constraints, such as delay requirement, throughput requirement, or both, are considered. Moreover, the link heterogeneity among the same type of links is taken into account in the framework, which effectively avoids the starvation of the links with low channel quality.

The rest of the paper is organized as follows. The related work is summarized in Section II. The system model for our opportunistic scheduling is explained in Section III. The QoS-oriented opportunistic scheduling scheme under the scenarios of homogeneous and heterogeneous rate distributions is derived in Section IV and Section V, respectively. Performance results are presented in Section VI. Further discussions about our scheme are provided in Section VII. The paper is concluded in Section VIII.

II. Related Work

Opportunistic scheduling is an effective way to utilize the fluctuation of channel conditions to enhance the network throughput performance. Several opportunistic scheduling schemes (e.g., [9][10][11]) have been proposed for a network with a central controller. However, these schemes are not applicable to wireless mesh/ad hoc networks where such controller does not exist. To solve this problem, several distributed opportunistic scheduling schemes are proposed [12]-[21]. These schemes exploit local information to determine whether to take transmission opportunities.

In [12], an opportunistic distributed scheduling is developed and its capacity is investigated based on Point Process Approximation. It is shown that the capacity approaches that of a centralized system where the best link is always selected to transmit. In this paper, the author focuses on uplink traffic in a multiple-access channel, while we consider peer-to-peer traffic in an ad hoc network. In [13], a channel-aware ALOHA protocol is developed, where the nodes only transmit their packets when their channel gains are above a given threshold. Also, other channel-aware ALOHA schemes are designed according to decentralized channel state information in [14][15]. Based on the optimal stopping theory [22], a distributed opportunistic scheduling is derived in [16] to maximize the system overall throughput. In [17], the author investigates the stopping policy when the channel qualities for different transmission periods are correlated. In [18], the author proposes a distributed opportunistic scheduling scheme exploiting game theory. In this scheme, an effective mechanism is designed to combat the issue of user selfishness. Although these schemes utilize opportunistic transmissions to improve the network throughput in a distributed manner, none of them takes into account the quality of service (QoS) of interested links. Thus, these schemes are not applicable to scenarios studied in this paper.

Distributed opportunistic scheduling schemes proposed in [19], [20] and [21] are most related to the scheme developed in this paper. In [19] and [20], an opportunistic scheduling scheme is developed to maximize the proportionally fair allocation. Based on the control theory, the scheme adapts to the variation of network load and can dynamically drive the system to the optimal operation point. This scheme is different from ours in the following points. First, the scheme considers the fairness. Although ensuring fairness is beneficial to improve QoS of the links with low transmission rates, it cannot directly guarantee a specific QoS requirement on such links (e.g., the delay is less than a specific value or the throughput is greater than a specific value). In contrast, our scheme directly focuses on the QoS. Second, the proportionally fair allocation is maximized in their scheme, instead of the overall throughput of the network as our scheme. In [21], an opportunistic scheduling scheme considering delay QoS is developed based on the scheme proposed in [16]. In this scheme, network centric delay constraints and individual delay constraints are satisfied based on different strategies. However, this scheme is not suitable for a network with hybrid links, for two reasons: 1) A network-centric delay constraint cannot guarantee the QoS requirements of one specific type of links; 2) If the individual delay constraint is applied to each link, the overall throughput is not maximized.

To the best of our knowledge, the optimal stopping theory [22] is first introduced to derive distributed opportunistic scheduling schemes in [16][21]. The framework of derivations in this paper is based on the work in [16][21] but makes the following nontrivial and important extensions. First, in our model, two types of links, which have different rate distribution functions, different QoS requirements, and different transmission durations, are considered [23]. To meet their QoS requirements, two types of links need to be treated differently in the mathematical derivations, which leads to a double threshold stopping policy. Furthermore, the strategies for handling two types of links in this paper can be easily extended to support multiple types of links with various QoS requirements. Second, in our derivations we consider both the delay constraints and the throughput constraints, which leads to different derivations to obtain the scheduling scheme. For instance, it is required to design more complicated profit functions[1] for opportunistic scheduling with throughput constraints. Third, in our model, link heterogeneity among the same type of links is taken into account. In this case, we set constraints on a subset of one type of links, instead of the whole set of links, which complicates the process of deriving the optimal stopping thresholds and the maximum expected profit equation[2].

III. System Model

In this paper, we focus on a single-hop ad hoc network where all nodes can hear each other, as previous work [16][18][19][21]. Such network model is common in various communication scenarios such as wireless sensor networks [24] and body area networks [25]. Moreover, a single-hop network can serve as a building block for general multihop networks. A common and practical approach for managing packet transmissions in a multihop network is to divide the whole

[1] The profit is defined in Appendix B.

[2] See Section IV-A

network into several single-hop sub-networks and coordinate transmissions among these sub-networks using hierarchical methods [26]. In each sub-network, the scheduling schemes developed for single-hop networks are adopted. Hence, the study on single-hop networks also benefits the data transmissions in general multihop networks.

The carrier sensing is enforced: if an ongoing transmission is detected in the medium, a node will postpone its own packets. Moreover, two types of links between nodes in this network are considered: 1) secure links for transmitting critical messages with physical layer security; 2) regular links for other messages. Note that the links considered in this paper are virtual. Thus, a secure link and a regular link can have the same source and destination nodes. In this case, these two links share a common physical link.

When the transmission medium is sensed idle, a node contends the channel slot by slot with a fixed access probability (i.e., p-persistent mechanism). To this ends, the node transmits a pilot packet to its destination node at the beginning of certain time slot. If two or more nodes contend the channel in the same time slot, a collision occurs (denoted by "C" in Fig. 1). If only one node sends a pilot packet to the channel, the destination will successfully receive it and reply a confirmation packet. In this case, the contention is successful (denoted by "S" in Fig. 1). Note that the confirmation packet is transmitted in the same time slot with the pilot packet. Thus, the size of a time slot is set larger than the total length of a pilot packet and a confirmation packet. If none of nodes transmits a pilot packet, the channel remains idle (denoted by "I" in Fig. 1).

If a node successfully captures the channel, instead of proceeding to data packet transmissions directly, it needs to detect current channel quality and follow a decision rule to determine whether or not a packet can be transmitted: if the current channel quality is low, the node skips the transmission opportunity to avoid the situation where the wireless medium is occupied by a low-rate transmission, as shown in Fig. 1. For this purpose, the node needs to know the current channel quality and determine the decision rule. The channel from the source to the destination is measured by the destination using the preamble sequence in the pilot packet, and the results are carried back by the confirmation packet. The decision rule is derived based on the optimal stopping theory [22] such that the network throughput is maximized under the constraints of QoS requirements. If the opportunity is dropped, the contention process restarts in the next time slot. Otherwise, the node starts its data transmissions. The transmission can last multiple time slots as shown in Fig. 1, and we assume that the channel condition remains unchanged during the transmission process (i.e., block-fading channel). In addition, we assume that the channel conditions during different transmission periods are independent, which is the same in the previous work [19], [21].

To clearly present our opportunistic scheduling scheme, several parameters are defined below. As shown in Fig 1, a time slot has a length of t, and data transmission durations for secure links and regular links are assumed constant and denoted by D_s and D_r, respectively. There are M nodes in the network. For the sake of clarity, we assume that each node has exactly one secure link and one regular link. However, the derivation presented in Section IV and VI can be directly applied to general cases. Given a time slot, node m contends the channel for its secure link and regular link with the probability (i.e., the persistent factor) equal to $p_{s,m}$ and $p_{r,m}$ respectively. Furthermore, the probability that the secure link of node m wins the channel contention, i.e., $P_{s,m}$, is given by

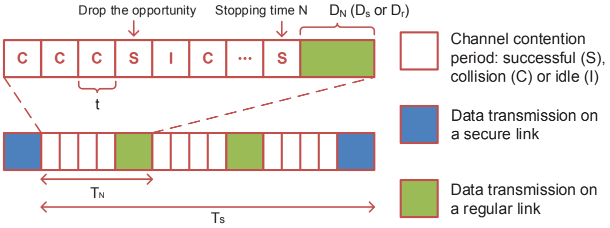

Drop the opportunity
Stopping time N
D_N (D_s or D_r)
C
C
C
S
I
C
···
S
t
T_N
T_s
Channel contention period: successful (S), collision (C) or idle (I)
Data transmission on a secure link
Data transmission on a regular link

Fig. 1. The diagram for channel contention and data transmission.

$$P_{s,m} = p_{s,m} \prod_{i \neq m} (1 - p_{s,i} - p_{r,i}). \tag{1}$$

Thus, P_s, defined as the probability that any secure link successfully contends the channel, can be calculated by $\sum P_{s,m}$. $P_{r,m}$ and P_r are defined for regular links in a similar way. In addition, the transmission rates on the secure link and the regular link of node m follow the distributions with cumulative (probability) density function $F_{s,m}(r)$ $(f_{s,m}(r))$ and $F_{r,m}(r)$ $(f_{r,m}(r))$, respectively. As [19] and [21], these distribution functions are assumed known. Moreover, for the mathematical tractability, we assume that $F_{s,m}(r)$ and $F_{r,m}(r)$ are differentiable, and $f_{s,m}(r)$ and $f_{r,m}(r)$ are greater than zero for any $r > 0$. These assumptions are valid for commonly used rate distribution models [27]. For convenience, let R_s denote the transmission rate on any secure link. The distribution of R_s, i.e., $F_s(r)$, is given by

$$F_s(r) = \sum_m \frac{P_{s,m}}{P_s} F_{s,m}(r). \tag{2}$$

For regular links, R_r and $F_r(r)$ are defined similarly.

As shown in Fig. 1, if a node successfully contends the channel at time N and decides to transmit a data packet, then we call N a stopping time. Given a stopping time N, T_N denotes the total time for this transmission round, including contention period and packet transmission time D_N. Here, D_N is equal to D_s if the transmission is on a secure link, and is equal to D_r for the transmission on a regular link. Also, R_N is used to denote the transmission rate of the node. If the transmission in this round is on a secure link, R_N^s is used to denote the transmission rate (i.e., $R_N = R_N^s$). The time between two successive transmissions on secure links is denoted by T_s, which also stands for the delay of secure links. Apparently, the choice of stopping time has influence on T_s.

IV. Opportunistic Scheduling with Homogeneous Rate Distributions

To maximize the system overall throughput under various QoS constraints for secure links, we develop a new distributed

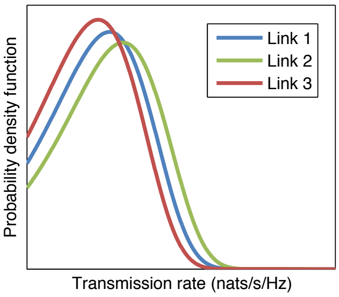


Fig. 2. The rate distributions of different links in the homogeneous scenario.

opportunistic scheduling scheme based on the optimal stopping theory. First, the homogeneous rate distribution scenario is considered, where the rate distributions of secure links are identical to each other. In this case, the overall performance of all secure links can effectively reflect that of each individual link, since each link contributes equally to the overall performance. Thus, in this section, we consider secure links as a whole and set overall QoS constraints on all these links. As soon as the overall QoS of secure links is satisfied, corresponding QoS for each individual link is also guaranteed.

In practice, the developed scheduling scheme is useful in two scenarios: 1) the rate distributions of secure links are close to each other, as shown in Fig. 2; 2) the rate distributions are different, but only the overall QoS of secure links needs to be satisfied.

A. Opportunistic Scheduling with Throughput Constraint

We define ζ as the set of stopping times as follows:

$$\zeta \triangleq \{N : N \geqslant 1, E[T_N] \leq \infty\}.$$

Also, let θ_s denote the throughput on all secure links, and α stand for the minimum throughput requirement. The maximization of overall throughput under the throughput constraint can be formulated as

$$\max_{N\in\zeta}\frac{E[R_N D_N]}{E[T_N]},\ \text{subject to } \theta_s = \frac{E[R_N^s D_s]}{E[T_s]} \geq \alpha.$$

Note that a distributed opportunistic scheduling that maximizes the overall throughput under QoS constraints is derived in [21] based on optimal stopping theory, but the solution therein is not applicable in our scenarios for two reasons. First, there exist two different types of links in our problem, and the constraint presented in our formula is applied to one type of links instead of to all links. This leads to different stopping policies for two types of links. Also, in [21], only the delay constraint is considered, while in our problem the throughput constraint is also studied. Hence, a new derivation is needed.

Let x^* denote the maximum throughput under the throughput constraint. According to Theorem 6.1 in [22], the optimization problem formulated previously is equivalent to

$$\max_{N\in\zeta} E[R_N D_N] - x^* E[T_N],$$

subject to

$$\alpha E[T_s] - E[R_N^s D_s] \leq 0.$$

The formulated optimization problem is a constrained one. To solve this problem, we convert it into an unconstrained one through the method of Lagrange multipliers. As proved in Appendix A, the constraint qualification is satisfied in our problem, In this case, the solution for the original problem also maximizes the converted problem and the Karush-Kuhn-Tucker (KKT) condition holds [28]. As a result, we can find the optimal solution for the original problem by solving the converted problem. If there are more than one solutions for the converted problem, we select the one that maximizes the original objective function.

Based on the method of Lagrange multipliers [29], the optimization problem is converted to

$$\max_{N\in\zeta} E[R_N D_N] - x^* E[T_N] - \lambda(\alpha E[T_s] - E[R_N^s D_s]), \quad (3)$$

where λ is the Lagrange multiplier. By solving this problem, the following proposition can be derived.

Proposition 4.1: The optimal stopping rule for secure links and regular links is a double-threshold policy. The threshold for secure links is ϕ_s, and that for regular links is ϕ_r. If a secure link wins the channel contention, it does not skip the transmission opportunity only if $R_s \geq \phi_s$; if a regular link successfully captures the channel, it takes the transmission opportunity when $R_r \geq \phi_r$. The optimal thresholds for secure links and regular links are given by

$$\begin{cases} \phi_s = \frac{x^*+\lambda\alpha}{1+\lambda}, \\ \phi_r = x^* + \lambda\alpha. \end{cases} \quad (4)$$

The proof can be found in Appendix B. According to the proposition, it can be shown that $\phi_s < x^* < \phi_r$. Thus packets on regular links can be sent only when the current transmission rate is greater than the system expected throughput, while messages on secure links are transmitted even if the transmission rate is less than the throughput value. Such discrimination between two types of links is helpful to favor the transmissions on secure links and hence provides the QoS on these links.

In Proposition 4.1, the optimal thresholds ϕ_s and ϕ_r are expressed in terms of (x^*, λ). Hence, further calculation of ϕ_s and ϕ_r requires the knowledge of (x^*, λ). The procedure for determining (x^*, λ) is presented as follows.

According to the definition of profit given in Appendix B, the maximum expected profit L^* can be expressed as

$$\begin{aligned} L^* \ = \ & P_s E[\max(R_s D_s + \lambda R_s D_s - x^* D_s - \lambda\alpha D_s, L^*) \\ & -kt(x^* + \lambda\alpha)] + P_r E[\max(R_r D_r + \lambda E[R_N^s D_s] \\ & -x^* D_r - \lambda\alpha D_r - \lambda\alpha E[T_s], L^*) - kt(x^* + \lambda\alpha)], \quad (5) \end{aligned}$$

where k is the number of time slots before the first successful channel contention. Note that the first expectation in the right hand side of Eq. (5) denotes the maximum expected profit when the first successful channel contention is won by a secure link, while the second expectation stands for the maximum expected profit when a regular link takes the first successful channel contention. Since L^* is zero as explained in Appendix B, Eq. (5) can be simplified as

$$t(x^*+\lambda\alpha) = D_s P_s(1+\lambda)E[(R_s-\phi_s)^+] + D_r P_r E[(R_r-\phi_r)^+],$$

where $(\cdot)^+$ denotes $\max\{\cdot, 0\}$. In addition, according to KKT conditions, we have $\lambda(E[R_N^s D_s] - \alpha E[T_s]) = 0$, where

$$\begin{cases} E[R_N^s D_s] = \frac{\int_{\phi_s}^{\infty} r\mathrm{d}F_s(r)}{\int_{\phi_s}^{\infty} \mathrm{d}F_s(r)} D_s, \\ E[T_s] = \frac{t+P_r(1-F_r(\phi_r))D_r}{P_s(1-F_s(\phi_s))} + D_s. \end{cases} \tag{6}$$

The first expression in Eq. (6) is based on the fact that all transmissions on secure links are conducted with the rates greater than ϕ_s, while the second expression can be derived in a similar way as Appendix C. Combining the maximum expected profit equation, KKT conditions, and Eq. (4), (x^*, λ) is calculated with the Levenberg-Marquardt algorithm (LMA) [30], a numerical method to solve non-linear equations.Theoretically the convergence speed of LMA is similar to that of widely known Gauss-Newton method. However, in practice, the implementations of LMA are proved more efficient in most scenarios [30]. Matlab [31] provides a built-in function that implements the LMA algorithm. We use this function to solve the above equations to obtain (x^*, λ). Following that, the optimal threshold pair (ϕ_s, ϕ_r) can be calculated based on Eq. (4).

It is necessary to emphasize that throughput constraint α is effective only when it falls into a specific range. If α is too small, the optimal thresholds derived from previous equations will be equal to those in the unconstrained case. In this scenario, the throughput constraint is inactive. If α is too large, the constraint cannot be satisfied even if skipping all regular transmissions. To characterize the lower bound and the upper bound for α, we have the following proposition.

Proposition 4.2: The effective range for throughput requirement α is given by $\theta_s^L \leq \alpha \leq \theta_s^U$, where θ_s^U is the maximum throughput of secure links when $\phi_r = \infty$, and it can be determined by

$$\theta_s^U = \frac{P_s \int_{\theta_s^U}^{\infty} r\mathrm{d}F_s(r)}{\frac{t}{D_s} + P_s(1 - F_s(\theta_s^U))}.$$

Also, θ_s^L is the throughput of secure links when the threshold pair is equal to the optimal one (i.e. (ϕ^*, ϕ^*)[3]) for the unconstrained case, and it is given by

$$\theta_s^L = \frac{P_s D_s \int_{\phi^*}^{\infty} r\mathrm{d}F_s(r)}{t + P_s D_s(1 - F_s(\phi^*)) + P_r D_r(1 - F_r(\phi^*))}.$$

The detailed proof of this proposition can be found in Appendix D. As the rate distributions of secure links improve, the throughput of secure links with $\phi_r = \infty$, i.e., θ_s^U, increases due to higher link rate for each transmission. Also, the throughput of secure links with $(\phi_s, \phi_r) = (\phi^*, \phi^*)$, i.e., θ_s^L, enhances because secure links get more transmission opportunities. Thus , according to the proposition, both upper bound and lower bound of the effective range for α will increase with better rate distributions of secure links.

B. Opportunistic Scheduling with Delay Constraint

In this subsection, an opportunistic scheduling scheme with delay constraint is studied. Similar to the network-wide average delay defined in [21], the delay studied in this subsection is imposed on the set of all secure links instead of a specific secure link. Specifically, the delay imposed on the set of secure links (denoted by T_s) is defined as the time between two successive transmissions on any secure links, as shown in Fig. 1. In contrast, the delay on a secure link of node m (denoted by $T_{s,m}$) is defined as the time between two successive transmissions on this link. In homogeneous cases, if there are n secure links in total, the average delay on a specific secure link is about n times as that on the set of all secure links, i.e., $E[T_{s,m}] = nE[T_s]$. Based on this relationship, we can set the delay constraint imposed on the set of all secure links (i.e., T_s) according to the delay requirement of individual secure link.

Let σ_s stand for the average delay of secure links, and β denote the delay requirement. Thus, we formulate the problem as

$$\max_{N \in \zeta} \frac{E[R_N D_N]}{E[T_N]}, \text{ subject to } \sigma_s = E[T_s] \leq \beta.$$

As discussed in Section IV-A, the previous optimization problem is equivalent to

$$\max_{N \in \zeta} E[R_N D_N] - x^* E[T_N] - \mu(E[T_s] - \beta),$$

where μ is the Lagrange multiplier. By solving this problem, the optimal threshold pair can be derived as

$$\begin{cases} \phi_s = x^* + \mu - \frac{\mu\beta}{D_s}, \\ \phi_r = x^* + \mu. \end{cases}$$

To further calculate (ϕ_s, ϕ_r), following equations are needed:

$$t(x^* + \mu) = P_s D_s E[(R_s - \phi_s)^+] + P_r D_r E[(R_r - \phi_r)^+],$$

and

$$\mu(E[T_s] - \beta) = 0,$$

where the first equation is the maximum expected profit equation and the second one is from KKT conditions [29]. The derivation of above equations and the calculation of the optimal thresholds follow the similar framework presented in Section IV-A and Appendix B. In addition, similar with throughput constraint, delay requirement β also has an effective range as described in the following proposition.

Proposition 4.3: The delay constraint β has a lower effective bound β^L and an upper effective bound β^U. β^L is the minimal possible average delay for secure links, and is given by $\beta^L = \frac{t}{P_s} + D_s$. β^U is the average delay for secure traffic when the thresholds for secure links and regular links are set to these (i.e., ϕ^* for both types of links) in the unconstrained case, and it can be determined by

$$\beta^U = \frac{t + P_r(1 - F_r(\phi^*))D_r}{P_s(1 - F_s(\phi^*))} + D_s.$$

Proof: For the lower bound, T_s includes time period t/P_s for at least one round successful channel contention and packet transmission time D_s. Hence, the minimum achievable delay requirement is $\frac{t}{P_s} + D_s$. For the upper bound, if delay requirement β is greater than β^U, then the optimal threshold pair for the unconstrained case is located in the feasible domain, which indicates that this optimal solution is also

[3] In the unconstrained scenario, the thresholds for secure links and regular links are identical.

the one for the constrained problem. In this case, the delay constraint is inactive. ■

According to the proposition, the lower bound of the effective range is determined by access probabilities of secure links and unrelated to rate distributions, while the upper bound decreases as the rate distributions of secure links improve.

C. Opportunistic Scheduling with Throughput and Delay Constraints

In some scenarios, both throughput and delay requirements are imposed. In this case, the problem for maximizing the overall throughput can be formulated as

$$\max_{N\in\zeta}\frac{E[R_N D_N]}{E[T_N]},$$

subject to

$$\theta_s=\frac{E[R_N^s D_s]}{E[T_s]}\geq\alpha\ \text{ and }\ \sigma_s=E[T_s]\leq\beta.$$

As discussed in Section IV-A, the above optimization problem is equivalent to

$$\max_{N\in\zeta}E[R_N D_N]-x^*E[T_N]-\lambda(\alpha E[T_s]-E[R_N^s D_s]) \\ -\mu(E[T_s]-\beta),$$

where λ and μ are the Lagrange multipliers. By solving this problem, the optimal stopping rule is derived. Similar to the case of a single constraint (e.g. throughput or delay), this rule is also a double-threshold stopping policy, and the optimal thresholds are given by

$$\begin{cases}\phi_s=\frac{x^*+\lambda\alpha+\mu-\frac{\mu\beta}{D_s}}{1+\lambda},\\ \phi_r=x^*+\lambda\alpha+\mu.\end{cases}$$

The calculation of above thresholds requires the knowledge of (x^*,λ,μ), which can be determined with the following equations:

$$\begin{aligned}t(x^*+\lambda\alpha+\mu) &= P_sD_s(1+\lambda)E[(R_s-\phi_s)^+] \\ &\quad +P_rD_rE[(R_r-\phi_r)^+],\end{aligned}\tag{7}$$

and

$$\begin{cases}\lambda(E[R_N^s D_s]-\alpha E[T_s])=0,\\ \mu(E[T_s]-\beta)=0.\end{cases}\tag{8}$$

Eq. (7) is the maximum expected profit equation, while Eq. (5) and Eq. (8) are from KKT conditions.

Similar to single constraint scenarios, there exists an area where both throughput requirement α and delay requirement β are effective. To characterize this area, we have the following proposition.

Proposition 4.4: For a given delay requirement β, the effective range for α is bounded by

$$\left[\frac{\int_{\phi_s^L}^{\infty}r\mathrm{d}F_s(r)}{\beta(1-F_s(\phi_s^L))}D_s,\ \frac{\int_{\phi_s^H}^{\infty}r\mathrm{d}F_s(r)}{\beta(1-F_s(\phi_s^H))}D_s\right],$$

where

$$\begin{cases}\phi_s^L=F_s^{-1}(1-\frac{t+P_rD_r}{P_s(\beta-D_s)}),\\ \phi_s^H=F_s^{-1}(1-\frac{t}{P_s(\beta-D_s)}).\end{cases}$$

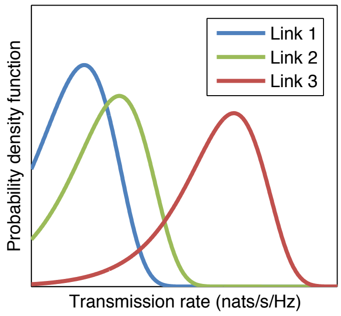


Fig. 3. The rate distributions of different links in heterogeneous scenarios.

The detailed proof is given in Appendix E. When α lies on the left side of the range given in the proposition, the throughput constraint is less tight than the delay constraint. In this case, the throughput constraint is inactive. When α is greater than the upper bound of the range, the throughput requirement imposes a stronger constraint on the problem. In this case, the delay constraint is inactive.

V. Opportunistic Scheduling with Heterogeneous Rate Distributions

In this section, the heterogeneous rate distribution scenario is considered, where the rate distribution of a secure link can be significantly different from those of other secure links, as shown in Fig. 3. In this scenario, the overall performance of secure links cannot reflect that of each individual link. Actually, if we consider all secure links as a whole as previous sections, the opportunistic scheduling scheme will provide more transmission opportunities to links with good link quality and cause the starvation of links with poor channel quality, which leads to unacceptable QoS for these links. To avoid this situation, we set QoS constraints for secure links with the worst link conditions instead of putting QoS requirements on the whole set of secure links.

A. Worst link analysis

The basic idea behind our scheme for heterogeneous scenarios is to set QoS constraints on the secure links with the worst performance instead of on the whole set of secure links. Hence, before imposing QoS constraints, we need to identify such links. Considering the secure link of node m, the average delay of this link, i.e., $E[T_{s,m}]$, can be expressed as

$$E[T_{s,m}]=\frac{\Delta}{P_{s,m}(1-F_{s,m}(\phi_s))},\tag{9}$$

where

$$\Delta=t+\sum_i P_{s,i}(1-F_{s,i}(\phi_s))D_s+\sum_i P_{r,i}(1-F_{r,i}(\phi_r))D_r.$$

The derivation of this expression can be found in Appendix C. According to the above equation, the numerators of delay expressions for all secure links are exactly the same. Therefore, the secure link with the worst delay can be determined if we can find a link with the minimum denominator value in its

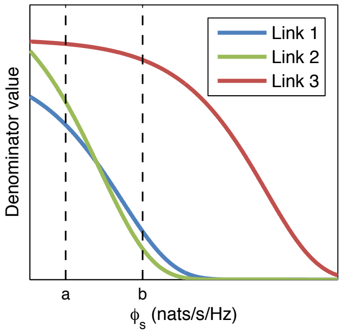


Fig. 4. The value of denominators in delay expressions for secure links.

delay expression. Furthermore, if the worst link is identified and the delay QoS constraint is set on the link, the delay of any other secure links will also meet this QoS requirement, since these links have better delay performance as compared to the worst link.

However, in some scenarios such link cannot be determined without the knowledge of the threshold for secure links. This can be explained with the following example. Consider three secure links with heterogeneous rate distributions. The denominator values in their delay expressions under different thresholds of secure links (i.e., ϕ_s) are plotted in Fig. 4. If the threshold is equal to a, the denominator of Link 1 has the minimum value, and hence Link 1 is the worst link; if the threshold is equal to b, Link 2 is the worst in delay. Namely, with different thresholds ϕ_s, the link that experiences the worst delay performance is different. Therefore, unless we know the threshold of secure links, we cannot determine the secure link with the worst delay performance.

In this case, instead of identifying a unique secure link that experiences the worst performance, we consider all links that *potentially* become the worst link in an interested range of ϕ_s. We call these links *potential-worst links*. In the previous example, both Link 1 and Link 2 can be the worst link under different thresholds of secure links. Therefore, Link 1 and Link 2 are both potential-worst links. However, Link 3 has evidently better quality than Link 1 and Link 2 and never experiences the worst delay performance. Therefore, Link 3 does not belong to the set of potential-worst links. Generally, potential-worst links have relatively poor channel quality. To help these links to achieve an acceptable performance, we treat these links as a group and set QoS constraints on the group.

B. Opportunistic scheduling with the delay constraint on potential-worst links

We define ξ as the set that consists of all potential-worst secure links. Furthermore, the delay on the set of potential-worst links is defined as the time between two successive transmissions on links belonging to this set. For convenience, T_{pw} is used to denote this delay.

To avoid the starvation on potential-worst links, we set the delay requirement on these links as $E[T_{pw}] \leqslant \gamma$. Therefore, the problem of maximizing the overall throughput under the delay constraint can be formulated as

$$\max_{N\in\zeta} \frac{E[R_N D_N]}{E[T_N]}, \text{ subject to } \; E[T_{pw}] \leq \gamma,$$

where ζ denotes the set of stopping times. As discussed in Section IV-A, the previous optimization problem is equivalent to

$$\max_{N\in\zeta} \; E[R_N D_N] - x^* E[T_N] - \omega(E[T_{pw}] - \gamma),$$

where ω is the Lagrange multiplier. By solving this optimization problem, we can derive the following proposition.

Proposition 5.1: The optimal stopping rule that maximizes the overall throughput under the delay constraint on potential-worst links is a double-threshold policy, and the optimal threshold pair is given by

$$\begin{cases} \phi_s = x^* + \omega - \frac{\sum_{i\in\xi} P_{s,i}}{P_s} \frac{\gamma\omega}{D_s}, \\ \phi_r = x^* + \omega. \end{cases}$$

Also, the value of (x^*, ω) can be determined with the following equations

$$\begin{cases} t(x^* + \omega) = P_s D_s E[(R_s - \phi_s)^+] + P_r D_r E[(R_r - \phi_r)^+] \\ \qquad\qquad + \frac{(P_s - \sum_{i\in\xi} P_{s,i})(\sum_{i\in\xi} P_{s,i})\gamma\omega}{P_s} F_\Delta, \\ \omega\left(E[T_{pw}] - \gamma\right) = 0, \end{cases}$$

where F_Δ denotes the difference between the value of the rate distribution function of non-potential-worst secure links at ϕ_s (i.e., $F_{s,nw}(\phi_s)$) and that of potential-worst links (i.e., $F_{s,pw}(\phi_s)$). The proof of this proposition can be found in Appendix F.

C. Discussion

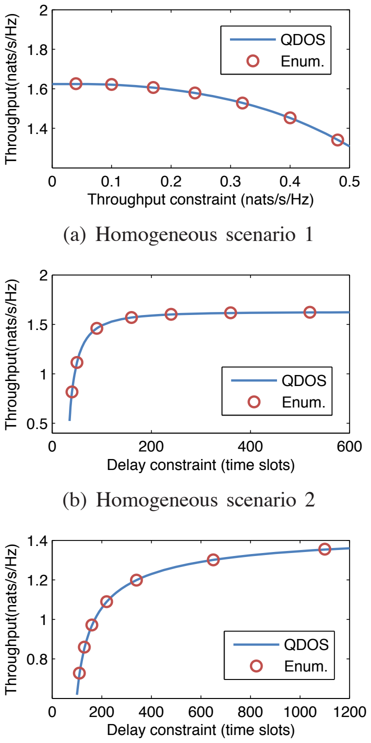
The proposed scheme can effectively guarantee that the delay on the set of potential-worst links is less than a specified value γ. Considering that there are n_p links in this set, if these links have comparable performance given the threshold pair derived from above equations, the delay of each link is approximately equal to $n_p\gamma$. Since the worst link belongs to the set of potential-worst links, the delay of all other secure links outside the set is not longer than $n_p\gamma$. In this case, the delay performance of each secure link is guaranteed to be not worse than a specific level (i.e., $n_p\gamma$) by our scheme.

If potential-worst links do not have comparable performance given the derived thresholds, the delay of the worst link can be longer than $n_p\gamma$. In this case, the proposed scheme cannot guarantee that each link meets the delay performance of a specific level. However, by setting constraints on the whole set of potential-worst links, the scheme is still beneficial to avoid the severe starvation of low-quality secure links in heterogeneous scenarios.

Another possible solution for heterogeneous scenarios is to separate the worst links from the secure links, treat them as an individual type, and derive a special threshold for them. This scheme can achieve better performance than the one proposed in this section, since there are more degree of freedoms to select thresholds for various links. However, it also increases

TABLE I
NORMALIZED SNR FOR SECURE LINKS AND REGULAR LINKS OF DIFFERENT NODES

		Node 1	Node 2	Node 3	Node 4	Node 5
Homo	Secure	1	1	1	1	1
	Regular	5	5	5	5	5
Hetero	Secure	0.4	0.4	1	1	1
	Regular	2	2	5	5	5



(a) Homogeneous scenario 1

(b) Homogeneous scenario 2

(c) Heterogeneous scenario

Fig. 5. Optimal throughput under various QoS constraints.

the number of link types in our scheme. Moreover, after separating the worst links, there may be still heterogeneity among secure links, and the further separation is needed. As a result, much more types of links need to be considered, which significantly increases the complexity of the scheme as discussed in Section VII-A and may not be practical in many cases.

VI. Performance Evaluation

In this section, the new scheduling scheme is evaluated by several experiments. In our simulation, we consider a network consisting of five nodes[4], and each of them maintains its own regular link and secure link to other nodes. The transmission rate on a link is assumed to be equal to the channel capacity given by

$$R = \log(1 + \rho|H|^2) \text{ nats/s/Hz},$$

where H denotes the random channel gain that follows a complex Gaussian distribution with the variance equal to 1, and ρ is the normalized SNR for the link. In the simulations for homogeneous scenarios, all links belonging to the same type are set with identical normalized SNR as given in Table I, while in heterogeneous cases, the links of Node 1 and Node 2 have evidently worse link quality as shown by Table I. In addition, the transmission duration for regular links is equal to 30 time slots, while that for secure links varies in different experiments and its default value is 30 time slots. Moreover, to reflect traffic load of the network, channel occupancy ratio is introduced and defined as

$$P = 1 - \prod_m (1 - p_{s,m} - p_{r,m}).$$

Without being explicitly specified, $p_{s,m}$ and $p_{r,m}$ for any node m are equal to 0.1 in our experiments. In this case, the channel occupancy ratio is 0.672.

Based on above parameters, our scheme is evaluated with Matlab programs. Given a specific setting (including thresholds for different types of links, channel access probabilities for nodes, transmission duration, etc.), our network simulation program runs for 10^7 time slots and performance results, such as overall throughput, throughput on secure links, and delay of secure links, are recorded. Note that the performance variation introduced by channel condition/medium access randomness is negligible with the specified running time (i.e., 10^7 time slots).

TABLE II
THROUGHPUT AND DELAY WITH DOUBLE CONSTRAINTS UNDER HOMOGENEOUS SCENARIOS.

P	0.15	0.30	0.45	0.60	0.75	0.90
θ_{total} (nats/s/Hz)	0.836	1.224	1.338	1.385	1.385	1.272
θ_s (nats/s/Hz)	0.401	0.399	0.418	0.432	0.429	0.401
σ_s (slot times)	68.70	75.07	75.12	74.88	75.19	75.05

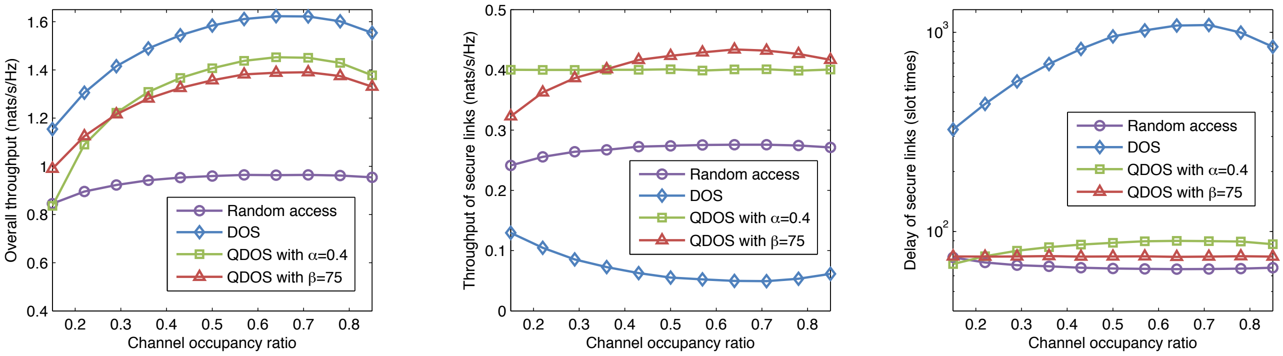
A. Homogeneous Scenarios

To verify the optimality of threshold pairs derived in Section IV, we compare the throughput performance of our scheme (denoted by QDOS) with the optimal throughput obtained by the enumeration method (denoted by Enum.) under various QoS constraints. In the enumeration method, we search over all possible threshold combinations (ϕ_s, ϕ_r), and our network simulation program runs for each combination. Based on simulation results, threshold combinations that do not guarantee the QoS constraints are removed. Among remaining ones the combination leading to the maximum overall throughput is selected and the corresponding maximum value is recorded.

The comparison results between QDOS and Enum. under various QoS constraints are shown in Fig. 5(a) and Fig. 5(b). It can be observed that the throughput of QDOS is always equal to the optimal value obtained through enumerating all possible threshold pairs. These results demonstrate the optimality of our scheme.

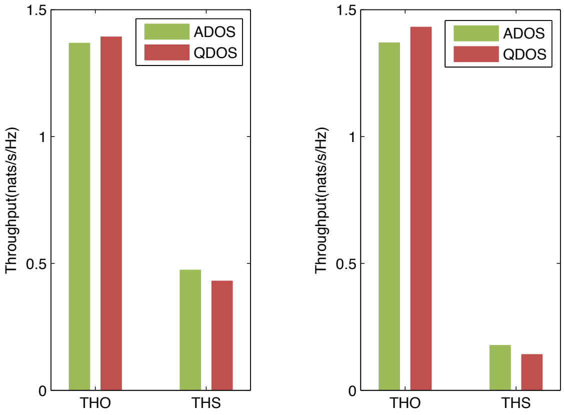
Performance results of our scheduling scheme with different QoS constraints are shown in Fig. 6. For comparison, performance of another two access schemes is provided: 1) the pure random access scheme, namely the scheme with both ϕ_s and ϕ_r equal to zero; 2) the distributed opportunistic

[4] Since our method is insensitive to the number of nodes in the network, a simulation with five nodes is enough to demonstrate the network performance.



(a) Overall throughput (b) Throughput of secure links (c) Delay of secure links

Fig. 6. Throughput and delay with different schemes under homogeneous scenarios.



(a) Case 1 (b) Case 2

Fig. 7. Performance comparison between QDOS and ADOS under homogeneous scenarios.

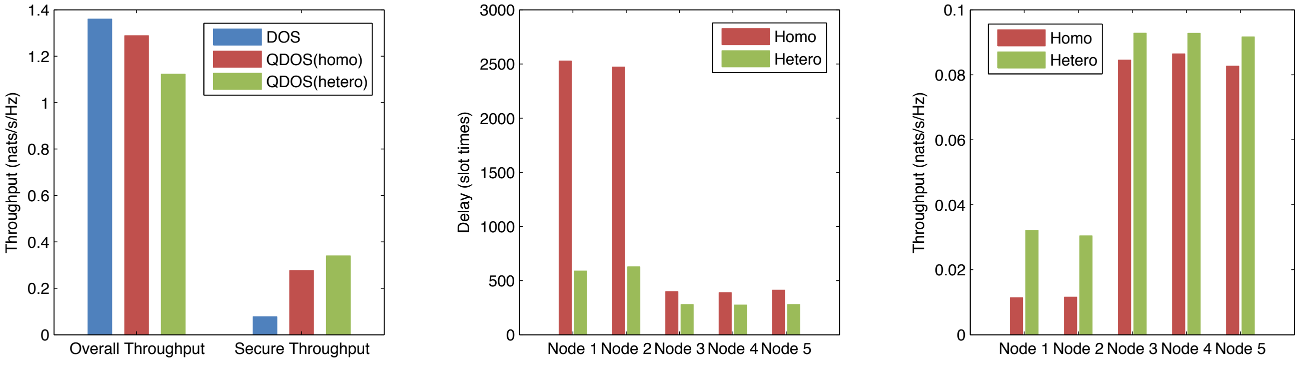
scheme (DOS) proposed in [16]. From Fig. 6(a), we know that the overall throughput of our scheme is significantly higher than that of the random access scheme. Also, when the channel occupancy ratio is greater than 0.2, the throughput performance loss of our scheme as compared to DOS scheme is within 14%. This result indicates that the overall throughput of our scheme is not significantly compromised. Fig. 6(b) and Fig. 6(c) show the QoS of secure links under different schemes. The results indicate that there is no QoS guarantee on secure links in DOS scheme. In contrast, our scheme with the throughput constraint can effectively guarantee the throughput performance of secure links, while our scheme with the delay constraint successfully controls the delay on secure links to an acceptable level. Moreover, note that the throughput requirement $\alpha = 0.4$ is not satisfied in the low channel occupancy ratio range when only the delay constraint is imposed on our scheme. Also, the delay requirement $\beta = 75$ is violated in the high channel occupancy range if our scheme only sets the throughput constraint. Therefore, if both throughput QoS and delay QoS are required, our scheduling scheme with double constraints needs to be applied. In Table II, the overall throughput (θ_{total}) and QoS of secure links for our scheme with double constraints are summarized. The results show that both delay (σ_s) and throughput (θ_s) requirements of secure links are satisfied at any channel occupancy ratio (P). This confirms the effectiveness of our scheme.

In addition, our scheme is compared to the approach proposed in [19] (ADOS) in two cases. In the first case, the transmission duration for secure links is equal to that for regular ones, i.e., $D_s = 30$. In this case, the delay QoS requirement for secure links is set to 75 time slots as before. In the second case, the transmission duration for secure links is equal to 5 time slots. This case is also a typical one: in many scenarios, messages requiring high-level security (e.g., bank/game account information) usually have much smaller sizes than regular ones (e.g., P2P streams) [32]. In the second case, the delay QoS requirement for secure links is set to 25 time slots. In addition, since ADOS scheme cannot directly guarantee a specific QoS requirement for secure links as discussed in Section II, we impose a weight coefficient for secure links in the objective function of [19], and keep tuning this coefficient until the delay QoS constraint is satisfied.

The performance results under two schemes, including the overall throughout (marked as THO) and the throughput of secure links (marked as THS), are shown in Fig. 7. In the first case, the performance gain of QDOS over ADOS is about 2%. In the second case where D_r/D_s becomes larger, the gain increases to 5%. This can be explained as follows. According to Eq. (12) in [19], when D_r/D_s increases, ADOS scheme provides more channel access opportunities to secure links to guarantee the fairness. The more preference on secure links has a negative impact on the overall throughput and leads to larger performance gap as compared to QDOS.

B. Heterogeneous Scenarios

The scheme derived for heterogeneous scenarios are evaluated in this section. A set of links with different normalized SNRs are used in the evaluations, and their SNR values are given in Table I. Based on these SNRs, the CDFs of transmission rates on these links are determined according to Eq. (**??**). Following the definition of potential-worst links in Section **??**, we identify these links (i.e., Link 1 and Link 2) in our evaluation setting, and impose QoS constraints on them.

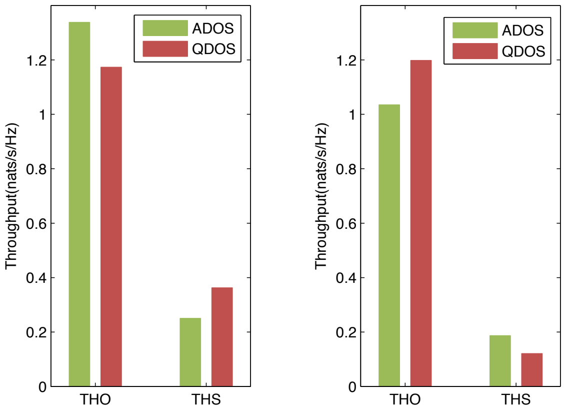


(a) Overall throughput

(b) Delay of secure links

(c) Throughput of secure links

Fig. 8. Throughput and delay with different schemes in the heterogeneous scenario.



(a) Case 1

(b) Case 2

Fig. 9. Performance comparison between QDOS and ADOS under heterogeneous scenarios.

To verify the optimality of QDOS scheme derived for heterogeneous scenarios, we compare QDOS with Enum. as discussed in Section VI-A. In this experiment, the delay constraint for potential-worst links varies from 100 time slots to 1200 time slots. The comparison results are shown in Fig. 5(c). It can be observed that the throughput of QDOS under various delay QoS requirements is always equal to the optimal throughput obtained from the enumeration method. This confirms that the derived threshold pairs for heterogeneous scenarios are optimal.

To study the performance of QDOS for heterogeneous scenarios, we compare it with various schemes. First, we evaluate the performance difference between homogeneous and heterogeneous QDOS. In this case, we require that the delay QoS of each secure link is controlled to the level of 600 time slots or less. If QDOS designed for homogeneous cases is applied, all secure links are equally treated, and the previous QoS requirement on each individual secure link leads to a delay constraint equal to 120 on the whole set of secure links (there are five secure links in total). With QDOS designed for heterogeneous scenarios, the delay constraint is only imposed on potential-worst secure links, and the previous QoS requirement converts to a delay constraint equal to 300 on the potential-worst link set (there are two secure links in this set).

The simulation results under two QDOS schemes (QDOS for homogeneous scenarios and QDOS for heterogeneous scenarios) are given in Fig. 8. For comparison, the performance of DOS proposed by [16] is also provided. The overall throughput and the throughput of secure links are plotted in Fig. 8(a). It can be found that the overall throughput under QDOS for heterogeneous scenarios degrades 17.8% and 13.1% as compared to that under DOS and that under QDOS for homogeneous scenario respectively. The drop in the overall throughput is due to the fact that more transmission opportunities are provided to secure links (especially potential-worst ones) in QDOS for heterogeneous scenarios, which is reflected by the throughput of secure links under three schemes as shown in Fig. 8(a). QoS performance for each secure link under two QDOS schemes is shown in Fig. 8(b) and Fig. 8(c). With QDOS designed for homogeneous scenarios, the delay QoS of potential-worst secure links (secure links of Node 1 and Node 2) severely violates the requirement set previously and the throughput performance of these links indicates severe starvation. With QDOS designed for heterogeneous scenarios, both delay and throughput performance of potential-worst secure links are significantly improved, and the delay QoS of each secure link meets the performance requirement, which demonstrates the necessity and effectiveness of considering heterogeneous scenarios in QDOS.

The QDOS scheme for heterogeneous scenarios is also compared to ADOS in two cases. In the first case, the transmission duration for secure links (D_s) is 30 time slots, which is equal to that for regular links (D_r). In this case, the delay requirement is given by 300 time slots. In the second case, D_r remains as 30 time slots, while D_s is set to 5 time slots. This setting is common in real communication scenarios: secure links are usually used to transmit the most critical messages such as control frames, which is shorter than regular data frames. In this case, the delay constraint is set to 50 time slots. Similar to the experiment in homogeneous scenarios, the objective function in [19] is modified by adding a weight coefficient for secure links, and the coefficient is tuned until that the delay QoS requirement is satisfied.

The comparison results are shown in Fig. 9. In the first case, the overall throughput of QDOS is 12% lower than that of ADOS, while in the second case, our scheme outperforms ADOS by 16%. The results indicate that when the radio between D_r and D_s varies, the relative performance gain of QDOS over ADOS also changes. This can be explained by considering two factors. On the one hand, for the sake of fairness, ADOS provides more channel access opportunities to low-quality links under heterogeneous scenarios, which causes the degradation of the overall throughput. On the other hand, in ADOS scheme each node has individual thresholds for determining whether to take transmission opportunities. Compared to unified thresholds for all nodes, this scheme is beneficial to improve the overall throughput under heterogeneous scenarios. When the first factor dominates as in the second case (larger D_r/D_s), our scheme is better than ADOS. If the second factor dominates as in the first case (smaller D_r/D_s), our scheme does not outperform ADOS. In addition, the comparison results indicate that our scheme for heterogeneous scenarios can be further improved if each node has individual thresholds as ADOS. This is subject to the future research.

VII. Discussion

A. Beyond Two Types of Links

In previous sections, two types of links, i.e., secure links and regular links, are considered. Actually, our scheme can be extended to support multiple types of links with various QoS requirements. The scheme supporting multiple types of links follows the same framework as developed in Section IV, and the key steps for deriving optimal thresholds for different types of links are summarized as follows:

1) Convert the objective function (i.e., the overall throughput) based on the optimal stopping theory [22] and the method of Lagrange multipliers [29] as Eq. (3) in Section IV-A. Let $\{\lambda_i\}$ $(i \in [1, n])$ denote the Lagrange multipliers for QoS constraints, where n is the total number of these constraints.
2) Define the profit function according to QoS requirements as Appendix B. The expectation of the defined profit must have the same expression as the converted objective function.
3) Derive the optimal thresholds with respect to $\{\lambda_i\}$ and x^* and the maximum expected profit equation following the same strategies as those in Appendix B and Appendix F.
4) Determine $\{\lambda_i\}$ and x^* based on KKT conditions (n equations) and the maximum expected profit equation. Finally, the optimal thresholds can be calculated.

As the number of link types grows, the number of QoS constraints on various types of links linearly increases. To derive and calculate the optimal thresholds (i.e., the third step and the fourth step) with n QoS constraints, 2^n cases need to be considered since each constraint could be active or not. Thus, the complexity of determining optimal thresholds exponentially increases as the number of link types. Such growing complexity limits the number of link types that can be considered in our scheme. The scheme proposed in Section V is a remedy to this issue. With this scheme, we can provide QoS to a group of links even if there are heterogeneous rate distributions among the group, which can be considered as the union of several link sets with homogeneous link distributions. In this way, we decrease the number of link types considered in the scheduling scheme, which reduces complexity of the scheme.

B. Information Exchange for QDOS

In our scheme, each node needs rate distributions and channel access probabilities of other nodes to calculate the optimal threshold. As mentioned previously, we assume that these parameters are known by each node, as previous work [19][21]. However, in reality, rate distribution and channel access probability of each node are collected by the node itself, and need to be exchanged among different nodes. For this purpose, a startup phase can be introduced. In this phase, nodes exchange their channel access probabilities and rate distribution information with others. After this phase, each node can calculate the optimal thresholds and initiate data transmissions following the scheduling scheme proposed in the paper. If a node detects the variation of its parameters after the startup phase, it notifies the change to other nodes by piggybacking the new parameters in its data transmission.

Other nodes keep overhearing data transmissions in the medium, extract the new parameters, and update the optimal threshold. Generally, when these parameters vary slowly (i.e. large channel coherence time), the performance penalty introduced by the above information exchange scheme is minimal, since the overhead is negligible as compared to a large amount of data transmissions. However, if these parameters vary quickly (i.e. small coherence time), it is difficult to catch up the variation of these parameters through information exchange. How to make a scheduling scheme (including our scheme and the related ones [19][21]) perform well under such scenarios is an interesting but challenging problem, which demands future research.

VIII. Conclusions

Opportunistic scheduling considering QoS constraints for hybrid links of a wireless network was studied in this paper. Given different scenarios of rate distributions, two QoS scheduling schemes were derived based on the optimal stopping theory. These schemes balance throughput and QoS guarantee of hybrid wireless links. Performance results showed that QoS of a specific link type could be guaranteed without significantly compromising the overall throughput of hybrid links. Although this paper takes secure links and regular links as an example of hybrid links, the QoS-oriented opportunistic scheduling schemes derived in this paper are completely applicable to other scenarios of hybrid links.

As indicated by simulation results, adopting individual threshold for each link of a node is beneficial to improve the overall throughput in heterogeneous scenarios. How to extend this paper to support individual threshold for each node is subject to future research.

Appendix A
Constraint Qualification

To check whether the constraint qualification holds for our optimization problems, we first define

$$g_1 = E[R_N^s D_s] \quad \text{and} \quad g_2 = E[T_s].$$

The values of g_1 and g_2 are determined by the decision rule for keeping or dropping the transmission opportunities. In our paper, this rule is characterized by two thresholds ϕ_s (for secure links) and ϕ_r (for regular links). If the current transmission rate supported by the link that captures the channel is higher than the corresponding threshold, the transmission opportunity is taken. Otherwise, the opportunity is dropped. Thus, we have

$$\nabla g_1 = \begin{pmatrix} \frac{\partial g_1}{\partial \phi_s} \\ \frac{\partial g_1}{\partial \phi_r} \end{pmatrix} \quad \text{and} \quad \nabla g_2 = \begin{pmatrix} \frac{\partial g_2}{\partial \phi_s} \\ \frac{\partial g_2}{\partial \phi_r} \end{pmatrix}.$$

According to Eq. (6), it can be shown that

$$\begin{aligned} \frac{\partial g_1}{\partial \phi_s} &= \frac{f_s(\phi_s)\int_{\phi_s}^{\infty} r\mathrm{d}F_s(r) - \phi_s f_s(\phi_s)(1-F_s(\phi_s))}{(1-F_s(\phi_s))^2} \\ &> \frac{f_s(\phi_s)\int_{\phi_s}^{\infty} \phi_s\mathrm{d}F_s(r) - \phi_s f_s(\phi_s)(1-F_s(\phi_s))}{(1-F_s(\phi_s))^2} = 0 \end{aligned}$$

Also, we have $\frac{\partial g_1}{\partial \phi_r} = 0$.. Similarly, we can derive that

$$\frac{\partial g_2}{\partial \phi_s} = \frac{(t + P_r(1-F_r(\phi_r))D_r)f_s(\phi_s)}{P_s(1-F_s(\phi_s))^2},$$

and

$$\frac{\partial g_2}{\partial \phi_r} = \frac{-P_r f_r(\phi_r) D_r}{P_s(1-F_s(\phi_s))}.$$

It can be observed that $\frac{\partial g_2}{\partial \phi_s}$ is always greater than zero, while $\frac{\partial g_2}{\partial \phi_r}$ is always less than zero. Furthermore, the constraints in our problem can be expressed as

$$G_1 = E[R_N^s D_s] - \alpha E[T_s] = g_1 - \alpha g_2,$$

and

$$G_2 = E[T_s] - \beta = g_2 - \beta.$$

Thus, the gradients of $G1$ and $G2$ are given by

$$\nabla G_1 = \nabla g_1 - \alpha \nabla g_2, \quad \text{and} \quad \nabla G_2 = \nabla g_2.$$

To verify linear independence constraint qualification, we need to investigate whether the gradients of active constraints are linearly independent. If only the constraint G_2 is active (in the optimization problems in Section IV-B or Section IV-C), we only need to verify that $\nabla G_2 \neq \mathbf{0}$. Note that $\nabla G_2 = \nabla g_2$ and $\frac{\partial g_2}{\partial \phi_r}$ is always less than zero. Hence, ∇G_2 is not equal to $\mathbf{0}$ for any (ϕ_s, ϕ_r).

If only the constraint G_1 is active (in the optimization problems in Section IV-A or Section IV-C), we only need to verify that $\nabla G_1 \neq \mathbf{0}$. Since $\frac{\partial g_1}{\partial \phi_r} = 0$ and $\nabla G_1 = \nabla g_1 - \alpha \nabla g_2$, we can derive that $\frac{\partial G_1}{\partial \phi_r} = -\alpha \frac{\partial g_2}{\partial \phi_r}$. Because throughput requirement α is greater than zero and $\frac{\partial g_2}{\partial \phi_r}$ is always less than zero, $\frac{\partial G_1}{\partial \phi_r}$ is always greater than zero. Hence, ∇G_1 is not equal to $\mathbf{0}$ for any (ϕ_s, ϕ_r).

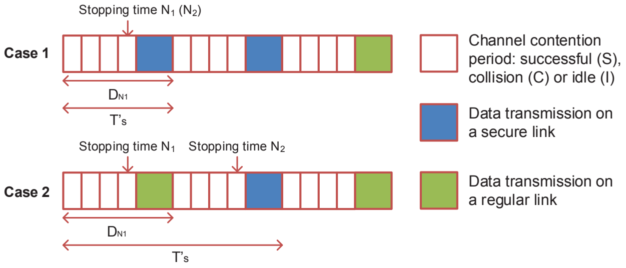

Stopping time N$_1$ (N$_2$)
Case 1
D$_{N1}$
T'$_s$
Stopping time N$_1$
Stopping time N$_2$
Case 2
D$_{N1}$
T'$_s$
Channel contention period: successful (S), collision (C) or idle (I)
Data transmission on a secure link
Data transmission on a regular link

Fig. 10. Two cases for stopping rule N_1: 1) a secure link wins the channel; 2) a regular link wins the channel.

When both G_1 and G_2 are active (in the optimization problem in Section IV-C), assume that there exists a pair (ϕ_s, ϕ_r) such that ∇G_1 and ∇G_2 are linearly dependent. Then we have $\nabla G_1 = c\nabla G_2$, where c is a constant. Following that, it can be shown that $\nabla g_1 - \alpha \nabla g_2 = c\nabla g_2$. If so, we have $\nabla g_1 = (\alpha + c)\nabla g_2$. Since $\frac{\partial g_1}{\partial \phi_r} = 0$ while $\frac{\partial g_2}{\partial \phi_r} < 0$, we can conclude that $(\alpha + c)$ is equal to zero, which further leads to $\nabla g_1 = 0$. However, we have shown that $\frac{\partial g_1}{\partial \phi_s}$ is always greater than 0. This is a contradiction. Hence for any pair (ϕ_s, ϕ_r), ∇G_1 and ∇G_2 are linearly independent.The above derivation shows that for our optimization problems in Section IV-A, Section IV-B, and Section IV-C, the linear independence constraint qualification holds with respect to any threshold pair (ϕ_s, ϕ_r).

Appendix B
Proof of Proposition 4.1

For the sake of clarity, we define the profit for stopping rule N_1 (i.e., a node successfully contends the channel at time N_1 and then starts the transmission) as

$$R_{N_1} D_{N_1} + \lambda R_{N_2}^s D_s - x^* T_{N_1} - \lambda \alpha T_s^{'},$$

where N_2 is the first stopping time for secure links after N_1 (including N_1). Thus, if the link that wins the channel contention at N_1 is a secure one, N_2 is equal to N_1. Also, $T_s^{'}$ denotes the time from the beginning of the contention period for stopping rule N_1 to the end of the transmission for stopping rule N_2, as shown in Fig. 10. Also, according to the memoryless characteristic of our system model, we have

$$E[T_s^{'}] = E[T_s].$$

Thus, the maximum expected profit for stopping rules, denoted by L^*, can be expressed as

$$\max_{N \in \zeta} E[R_N D_N] - x^* E[T_N] - \lambda(\alpha E[T_s] - E[R_N^s D_s]).$$

According to Theorem 6.1 in [22] and KKT conditions, the value of L^* is zero. Moreover, it can be observed that the above expression is identical with the optimization formulation presented in Section IV-A. Therefore solving the optimization problem in Section IV-A is equivalent to finding the optimal stopping rule that maximizes its expected profit. To maximize this expectation, the opportunistic scheduling allows the packet transmission only when the system meets the most favorable opportunity: given a node that successfully contents the channel, if the profit for transmitting immediately is greater than the maximum expected profit with skipping the opportunity and waiting for the next stopping time, the node starts the transmission; otherwise the opportunity is dropped.

Consider a node successfully contends the channel for its secure link. If the node takes this transmission opportunity, the profit can be quantified as

$$R_sD_s + \lambda R_sD_s - x^*D_s - \lambda\alpha D_s - (x^* + \lambda\alpha)T_{cont},$$

where T_{cont} is the contention period before this successful channel contention. However, if the node skips this opportunity, based on the time-invariant characteristic of the system, the maximum expected profit is given by $L^* - (x^* + \lambda\alpha)T_{cont}$. Hence, if

$$(1 + \lambda)R_sD_s - x^*D_s - \lambda\alpha D_s \geq L^*,$$

the profit for taking the transmission opportunity is greater than that with skipping the opportunity and waiting for the next stopping time. In this case, the packet on this secure link is transmitted. However, if $(1 + \lambda)R_sD_s - x^*D_s - \lambda\alpha D_s < L^*$, transmitting immediately is less favorable than waiting for better opportunity. In this case, the node drops the transmission and the channel contention restarts. Therefore, the stopping threshold for secure links is given by $R_s \geq \frac{x^*+\lambda\alpha}{1+\lambda} = \phi_s$. Similarly, if a regular link succeeds in channel contention, the maximum expected profit with skipping the transmission opportunity is $L^* - (x^* + \lambda\alpha)T_{cont}$, while the expected profit from taking the transmission opportunity is given by

$$R_rD_r + \lambda E[R_N^sD_s] - x^*D_r - \lambda\alpha(D_r + E[T_s]) - (x^* + \lambda\alpha)T_{cont}.$$

Note that after the end of current transmission, the expected waiting time for the next transmission on secure links is equal to $E[T_s]$ according to the memoryless characteristic of our system model. In addition, based on KKT conditions [29], we have $\lambda(E[R_N^sD_s] - \alpha E[T_s]) = 0$. Thus, the profit expression can be simplified as $R_rD_r - x^*D_r - \lambda\alpha D_r - (x^* + \lambda\alpha)T_{cont}$. Therefore, when $R_rD_r - x^*D_r - \lambda\alpha D_r \geq L^*$, the regular packet is transmitted. Otherwise the transmission opportunity is skipped. Hence, the transmission threshold for regular links is given by $\phi_r = x^* + \lambda\alpha$. The proposition is proved. Also, the derivation for the optimal stopping rules with the delay constraint and double constraints follows the similar framework as presented above.

Appendix C
Derivation on the delay expression

To derive the expression of the average delay for the secure link of node m, i.e. $E[T_{s,m}]$, we define p_1 as the probability that, given a time slot, the secure link successfully contents the channel and takes the transmission opportunity following the stopping rule. Thus, p_1 can be expressed as

$$p_1 = P_{s,m}(1 - F_{s,m}(\phi_s)).$$

Also, p_2 is defined as the probability that other secure links or regular links win the channel contention in a given time slot and take the transmission opportunity following the stopping rule. Hence, it can be shown that

$$p_2 = \sum_{i \neq m} P_{s,i}(1 - F_{s,i}(\phi_s)) + \sum_i P_{r,i}(1 - F_{r,i}(\phi_r)).$$

For convenience, we use $p_{2,s}$ and $p_{2,r}$ to denote the first term and the second term in the right hand side of the above equation, respectively. Furthermore, the probability p_3, defined as the probability that no transmission will start at the end of a given time slot, can be expressed as

$$p_3 = 1 - p_1 - p_2.$$

Considering the first time slot after a transmission on the secure link of node m, if this link wins the channel contention again and the current transmission rate exceeds the threshold for secure links, another transmission will start on this link. In this case, the delay is given by

$$T_{s,m} = t + D_s,$$

If a transmission starts on other links at the end of the slot (we use C_2 to denote this case), according to the memoryless characteristic of our system model, the expected delay of the secure link of node m under this case can be denoted as

$$E[T_{s,m}|C_2] = t + D_0 + E[T_{s,m}],$$

where D_0 denotes the expected transmission time after the end of the given time slot under C_2, and can be expressed as

$$D_0 = \frac{p_{2,s}}{p_2}D_s + \frac{p_{2,r}}{p_2}D_r.$$

If no transmission starts at the end of the slot (we use C_3 to denote this case), the expected delay is given by

$$E[T_{s,m}|C_3] = t + E[T_{s,m}].$$

Therefore, it can be shown that

$$E[T_{s,m}] = p_1(t+D_s) + p_2(t+D_0+E[T_{s,m}]) + p_3(t+E[T_{s,m}]).$$

Hence, we have

$$E[T_{s,m}] = \frac{t + p_1D_s + p_2D_0}{p_1} = \frac{\Delta}{P_{s,m}(1 - F_{s,m}(\phi_s))},$$

where

$$\Delta = t + \sum_i P_{s,i}(1 - F_{s,i}(\phi_s))D_s + \sum_i P_{r,i}(1 - F_{r,i}(\phi_r))D_r.$$

The average delay on the set of secure links can be derived in a similar way.

Appendix D
Proof of Proposition 4.2

The overall throughput of secure links is the summation of throughput of each secure link. Hence, we have

$$\theta_s = \sum_{m=1}^{M} \theta_{s,m} = \sum_{m=1}^{M} \frac{E[R_{s,m}D_s]}{E[T_{s,m}]},$$

where $\theta_{s,m}$ denotes the throughput on the secure link of node m, $R_{s,m}$ stands for the rate for the transmission on this link, and $T_{s,m}$ indicates the time between two successive transmissions on the link. Furthermore, it can be shown that

$$\theta_s = \sum_{m=1}^{M} \frac{\frac{\int_{\phi_s}^{\infty} r\mathrm{d}F_{s,m}(r)}{1-F_{s,m}(\phi_s)} D_s}{\frac{t+\sum_i P_{s,i}(1-F_{s,i}(\phi_s))D_s+\sum_i P_{r,i}(1-F_{r,i}(\phi_r))D_r}{P_{s,m}(1-F_{s,m}(\phi_s))}}.$$

The previous equation can be simplified as

$$\theta_s = \frac{P_s D_s \int_{\phi_s}^{\infty} r\mathrm{d}F_s(r)}{t + P_s D_s(1 - F_s(\phi_s)) + P_r D_r(1 - F_r(\phi_r))}. \quad (10)$$

For the lower bound, if the throughput requirement α is less than θ_s^L, namely

$$\alpha < \frac{P_s D_s \int_{\phi^*}^{\infty} r\mathrm{d}F_s(r)}{t + P_s D_s(1 - F_s(\phi^*)) + P_r D_r(1 - F_r(\phi^*))},$$

the optimal threshold pair (ϕ^*, ϕ^*) for the unconstrained case is located in the feasible domain, which indicates that this pair is also the optimal solution for the constrained problem. In this case, the throughput constraint is inactive.

For the upper bound, let θ_s^U denote the maximum possible throughput on secure links. Apparently, the throughput requirement α cannot be greater than θ_s^U. To determine θ_s^U, we set ϕ_r to approach ∞ and derive the optimal threshold for secure links that maximizes the system overall throughput following similar framework presented in Appendix B. It can be shown that ϕ_s is equal to the maximum overall throughput x^*. Also, since the threshold for regular links approaches infinity, there is no throughput on regular links and the overall throughput is equal to the throughput of secure links. Thus, we have

$$\theta_s^U = x^* = \phi_s.$$

Therefore, based on Eq. (10), the maximum throughput of secure links can be determined by

$$\theta_s^U = \frac{P_s \int_{\theta_s^U}^{\infty} r\mathrm{d}F_s(r)}{\frac{t}{D_s} + P_s(1 - F_s(\theta_s^U))}.$$

The proposition is proved.

Appendix E
Proof of Proposition 4.4

The average delay for secure links is given by

$$\beta = E[T_s] = \frac{t + P_r(1 - F_r(\phi_r))D_r}{P_s(1 - F_s(\phi_s))} + D_s.$$

Thus, we have the following inequalities

$$\frac{t}{P_s(1 - F_s(\phi_s))} + D_s \le \beta \le \frac{t + P_r D_r}{P_s(1 - F_s(\phi_s))} + D_s.$$

It follows that

$$\frac{t}{P_s(\beta - D_s)} \le (1 - F_s(\phi_s)) \le \frac{t + P_r D_r}{P_s(\beta - D_s)}.$$

Since $F_s(\cdot)$ is a rate distribution function, its value increases with ϕ_s. Thus, it can be shown that

$$F_s^{-1}(1 - \frac{t + P_r D_r}{P_s(\beta - D_s)}) \le \phi_s \le F_s^{-1}(1 - \frac{t}{P_s(\beta - D_s)}).$$

For convenience, the lower bound and the upper bound in above inequalities are denoted by ϕ_s^L and ϕ_s^H, respectively. Furthermore, we consider $E[R_N^s D_s]$, which is given by

$$E[R_N^s D_s] = \frac{\int_{\phi_s}^{\infty} r\mathrm{d}F_s(r)}{(1 - F_s(\phi_s))} D_s.$$

Since $E[R_N^s D_s]$ is a function increasing with ϕ_s, it can be shown that

$$\frac{\int_{\phi_s^L}^{\infty} r\mathrm{d}F_s(r)}{(1 - F_s(\phi_s^L))} D_s \le E[R_N^s D_s] \le \frac{\int_{\phi_s^H}^{\infty} r\mathrm{d}F_s(r)}{(1 - F_s(\phi_s^H))} D_s.$$

Moreover, based on $E[R_N^s D_s] - \alpha E[T_s] = 0$ and $E[T_s] = \beta$, we have

$$E[R_N^s D_s] = \alpha\beta.$$

Hence, it can be shown that

$$\frac{\int_{\phi_s^L}^{\infty} r\mathrm{d}F_s(r)}{\beta(1 - F_s(\phi_s^L))} D_s \le \alpha \le \frac{\int_{\phi_s^H}^{\infty} r\mathrm{d}F_s(r)}{\beta(1 - F_s(\phi_s^H))} D_s.$$

This proves Proposition 4.4.

Appendix F
Proof of Proposition 5.1

We can define the profit of stopping rule N as

$$R_N D_N - x^* T_N - \omega T_{pw}^{'} + \gamma\omega,$$

where $T_{pw}^{'}$ denotes the time from the beginning of contention period for stopping rule N to the end of the next transmission on potential-worst links. Furthermore, L^* is defined as the maximum expected profit for stopping rules and has the identical expression as the optimization formulation presented in Section V-B. Similar with Appendix B, to solve the optimization problem in Section V-B, we only need to find the optimal stopping rule that maximizes the expected stopping profit. In addition, note that L^* is equal to zero.

If a link from the set ξ takes the channel successfully, the profit for transmitting a packet on this link can be expressed as

$$R_{s,pw} D_s - x^* D_s - \omega D_s + \gamma\omega - (x^* + \omega)T_{cont}, \quad (11)$$

where $R_{s,pw}$ is the transmission rate on this link and follows the distribution

$$F_{s,pw}(r) = \frac{1}{\sum_{m\in\xi} P_{s,m}} \sum_{m\in\xi} P_{s,m} F_{s,m}(r).$$

If a secure link which is not a potential-worst one wins the channel contention, the profit for transmitting immediately is

$$R_{s,nw} D_s - x^* D_s - \omega D_s - \omega E[T_{pw}] + \gamma\omega - (x^* + \omega)T_{cont}$$

where $R_{s,nw}$ denotes the transmission rate on the link that successfully takes the channel and follows the distribution

$$F_{s,nw}(r) = \frac{1}{\sum_{m\notin\xi} P_{s,m}} \sum_{m\notin\xi} P_{s,m} F_{s,m}(r).$$

According to the KKT conditions [29], $\omega\left(E[T_{pw}] - \gamma\right) = 0$. The above profit expression can be simplified as

$$R_{s,nw} D_s - x^* D_s - \omega D_s - (x^* + \omega)T_{cont}.$$

As a result, the average profit for transmitting immediately on the secure link that wins the channel contention can be denoted as

$$\begin{aligned}&R_sD_s-\tfrac{\sum_{i\in\xi}P_{s,i}}{P_s}\left[x^*D_s{+}\omega D_s{-}\gamma\omega{+}(x^*{+}\omega)T_{cont}\right]\\&-\tfrac{P_s-\sum_{i\in\xi}P_{s,i}}{P_s}\left[x^*D_s{+}\omega D_s{+}(x^*{+}\omega)T_{cont}\right]\\&=R_sD_s-x^*D_s-\omega D_s+\tfrac{\sum_{i\in\xi}P_{s,i}}{P_s}\gamma\omega-(x^*+\omega)T_{cont},\end{aligned}$$

where R_s follows the distribution

$$\frac{\sum_{i\in\xi}P_{s,i}}{P_s}F_{s,pw}(r)+\frac{P_s-\sum_{i\in\xi}P_{s,i}}{P_s}F_{s,nw}(r)=F_s(r).$$

Thus, if this profit is greater than the maximum expected profit with skipping this transmission and waiting for the next stopping time, namely

$$R_sD_s-x^*D_s-\omega D_s+\frac{\sum_{i\in\xi}P_{s,i}}{P_s}\gamma\omega\geq L^*,$$

then the packet is transmitted. Hence, the threshold for secure links is given by

$$\phi_s=x^*+\omega-\frac{\sum_{i\in\xi}P_{s,i}}{P_s}\frac{\gamma\omega}{D_s}.$$

The regular case can be derived similarly as that in Appendix B. If

$$R_rD_r-x^*D_r-\omega D_r-\omega E[T_{pw}]+\gamma\omega\geq L^*,$$

namely, $R_r\geq x^*+\omega$, the regular packet is transmitted on the link that wins the channel contention. In summary, the optimal threshold pair is given by

$$\begin{cases}\phi_s=x^*+\omega-\frac{\sum_{i\in\xi}P_{s,i}}{P_s}\frac{\gamma\omega}{D_s},\\ \phi_r=x^*+\omega.\end{cases}\tag{12}$$

To calculate the optimal threshold pair, the maximum expected profit equation is derived as follows. Considering the first successful channel contention, if a potential-worst secure link wins the channel contention, it starts its transmission only when $R_{s,pw}\geq\phi_s$. In this case, the profit is given by

$$R_{s,pw}D_s-x^*D_s-\omega D_s+\gamma\omega-(x^*+\omega)kt,$$

where k is the number of time slots before the first successful channel contention. Note that the above equation is identical with Eq. (11) when T_{cont} is equal to kt. On the other hand, if $R_{s,pw}<\phi_s$, the transmission opportunity is skipped and then maximum expected profit is $L^*-(x^*+\omega)kt$. Combining previous two cases, if a potential-worst link wins the channel contention, the maximum profit following the optimal stopping rule can be expressed as

$$(R_{s,pw}-\phi_s)^+D_s+\gamma\omega\frac{\sum_{i\notin\xi}P_{s,i}}{P_s}\mathrm{u}(R_{s,pw}-\phi_s)-(x^*+\omega)kt,$$

where $(\cdot)^+$ denotes $\max\{\cdot,0\}$ and $u(\cdot)$ is the step function. Similarly, if a secure link which is not potential-worst wins the contention, the maximum profit is given by

$$(R_{s,nw}-\phi_s)^+D_s-\gamma\omega\frac{\sum_{i\in\xi}P_{s,i}}{P_s}\mathrm{u}(R_{s,nw}-\phi_s)-(x^*+\omega)kt.$$

If a regular link contends the channel successfully, the maximum profit can be derived as $(R_r-\phi_r)^+D_r-(x^*+\omega)kt$. Therefore, we have

$$\begin{aligned}L^*=\;&(\textstyle\sum_{i\in\xi}P_{s,i})E[(R_{s,pw}-\phi_s)^+D_s\\&+\gamma\omega\tfrac{P_s-\sum_{i\in\xi}P_{s,i}}{P_s}\mathrm{u}(R_{s,pw}-\phi_s)-(x^*+\omega)kt]\\&+(P_s-\textstyle\sum_{i\in\xi}P_{s,i})E[(R_{s,nw}-\phi_s)^+D_s\\&-\gamma\omega\tfrac{\sum_{i\in\xi}P_{s,i}}{P_s}\mathrm{u}(R_{s,nw}-\phi_s)-(x^*+\omega)kt]\\&+P_rE[(R_r-\phi_r)^+D_r-(x^*+\omega)kt].\end{aligned}$$

Rearranging the above equation, we get

$$\begin{aligned}&(x^*+\omega)t{=}P_sD_sE[(R_s{-}\phi_s)^+]{+}P_rD_rE[(R_r{-}\phi_r)^+]\\&+\tfrac{(P_s-\sum_{i\in\xi}P_{s,i})(\sum_{i\in\xi}P_{s,i})\gamma\omega}{P_s}(F_{s,nw}(\phi_s){-}F_{s,pw}(\phi_s)).\end{aligned}\tag{13}$$

In addition, based on the KKT conditions, we have

$$\omega\left(E[T_{pw}]-\gamma\right)=0,\tag{14}$$

where T_{pw} can be expressed as

$$T_{pw}=\frac{t+P_r(1-F_r(\phi_r))D_r+P_s(1-F_s(\phi_s))D_s}{(\sum_{i\in\xi}P_{s,i})(1-F_{s,pw}(\phi_s))}.$$

Combining Eqs. (12), (13), and (14), (x^*,ω) can be solved with LMA [30]. Following that, the optimal threshold pair can be calculated according to Eq. (12).

References

[1] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 6, pp. 2180–2189, 2008.

[2] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *Signal Processing, IEEE Transactions on*, vol. 58, no. 3, pp. 1875–1888, 2010.

[3] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *INFOCOM, 2011 Proceedings IEEE*. IEEE, 2011, pp. 1125–1133.

[4] E.-K. Lee, M. Gerla, and S. Y. Oh, "Physical layer security in wireless smart grid," *Communications Magazine, IEEE*, vol. 50, no. 8, pp. 46–52, 2012.

[5] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on*. IEEE, 2008, pp. 1–8.

[6] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 24, no. 3, pp. 339–348, 1978.

[7] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1334–1387, 1975.

[8] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda, "Performance anomaly of 802.11b," in *INFOCOM. 2003 Proceedings IEEE*, vol. 2. IEEE, 2003, pp. 836–843.

[9] X. Liu, E. K. P. Chong, and N. B. Shroff, "Opportunistic transmission scheduling with resource-sharing constraints in wireless networks," *Selected Areas in Communications, IEEE Journal on*, vol. 19, no. 10, pp. 2053–2064, 2001.

[10] P. Viswanath, D. N. C. Tse, and R. Laroia, "Opportunistic beamforming using dumb antennas," *Information Theory, IEEE Transactions on*, vol. 48, no. 6, pp. 1277–1294, 2002.

[11] A. Lera, A. Molinaro, and S. Pizzi, "Channel-aware scheduling for QoS and fairness provisioning in IEEE 802.16/wimax broadband wireless access systems," *Network, IEEE*, vol. 21, no. 5, pp. 34–41, 2007.

[12] J. Kampeas, A. Cohen, and O. Gurewitz, "Capacity of distributed opportunistic scheduling in nonhomogeneous networks," *Information Theory, IEEE Transactions on*, vol. 60, no. 11, pp. 7231–7247, 2014.

[13] X. Qin and R. Berry, "Exploiting multiuser diversity for medium access control in wireless networks," in *INFOCOM. 2003 Proceedings IEEE*, vol. 2. IEEE, 2003, pp. 1084–1094.

[14] Y. Xue and T. Kaiser, “Pursuing multiuser diversity in an OFDM system with decentralized channel state information,” in *Communications, 2004 IEEE International Conference on*, vol. 6. IEEE, 2004, pp. 3299–3303.

[15] Y. Yu and G. B. Giannakis, “Opportunistic medium access for wireless networking adapted to decentralized CSI,” *Wireless Communications, IEEE Transactions on*, vol. 5, no. 6, pp. 1445–1455, 2006.

[16] D. Zheng, W. Ge, and J. Zhang, “Distributed opportunistic scheduling for ad hoc networks with random access: an optimal stopping approach,” *Information Theory, IEEE Transactions on*, vol. 55, no. 1, pp. 205–222, 2009.

[17] H. Chen and J. S. Baras, “Distributed opportunistic scheduling for wireless ad-hoc networks with block-fading model,” *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 11, pp. 2324–2337, 2013.

[18] A. Banchs, A. Garcia-Saavedra, P. Serrano, and J. Widmer, “A game-theoretic approach to distributed opportunistic scheduling,” *Networking, IEEE/ACM Transactions on*, 2011.

[19] A. Garcia-Saavedra, A. Banchs, P. Serrano, and J. Widmer, “Distributed opportunistic scheduling: A control theoretic approach,” in *INFOCOM, 2012 Proceedings IEEE*. IEEE, 2012, pp. 540–548.

[20] A. Garcia-Saavedra, A. Banchs, P. Serrano, and J. Widmer, “Adaptive mechanism for distributed opportunistic scheduling,” *Wireless Communications, IEEE Transactions on*, 2014.

[21] S.-S. Tan, D. Zheng, J. Zhang, and J. Zeidler, “Distributed opportunistic scheduling for ad-hoc communications under delay constraints,” in *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010.

[22] T. S. Ferguson. Optimal stopping and applications. [Online]. Available: http://www.math.ucla.edu/ tom/Stopping/contents.html

[23] W. Mao, S. Wu, and X. Wang, “QoS-oriented distributed opportunistic scheduling for wireless networks with hybrid links,” in *Proceedings of GLOBECOM*. IEEE, 2013.

[24] K. Römer and F. Mattern, “The design space of wireless sensor networks,” *Wireless Communications, IEEE*, vol. 11, no. 6, pp. 54–61, 2004.

[25] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, “A survey on wireless body area networks,” *Wireless Networks*, vol. 17, no. 1, pp. 1–18, 2011.

[26] R. L. Cruz and A. V. Santhanam, “Optimal routing, link scheduling and power control in multihop wireless networks,” in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 1. IEEE, 2003, pp. 702–711.

[27] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[28] M. S. Bazaraa, H. D. Sherali, and C. M. Shetty, *Nonlinear programming: theory and algorithms*. John Wiley & Sons, 2006.

[29] J. Arora, *Introduction to optimum design*. Elsevier Academic Press, 2004.

[30] J. E. Dennis Jr and R. B. Schnabel, *Numerical methods for unconstrained optimization and nonlinear equations*. Siam, 1996, vol. 16.

[31] MathWorks, Inc. [Online]. Available: http://www.math.ucla.edu/ tom/Stopping/contents.html

[32] Y.-D. Lin, C.-N. Lu, Y.-C. Lai, W.-H. Peng, and P.-C. Lin, “Application classification using packet size distribution and port association,” *Journal of Network and Computer Applications*, vol. 32, no. 5, pp. 1023–1030, 2009.