Proactive Eavesdropping via Jamming over HARQ-Based Communications

Jie Xu*, Kai Li†, Lingjie Duan†, and Rui Zhang‡
*School of Information Engineering, Guangdong University of Technology
†Engineering Systems and Design Pillar, Singapore University of Technology and Design
‡Department of Electrical & Computer Engineering, National University of Singapore
Email: jiexu@gdut.edu.cn, kai_li@sutd.edu.sg, lingjie_duan@sutd.edu.sg, elezhang@nus.edu.sg

***Abstract*—This paper studies the wireless surveillance of a hybrid automatic repeat request (HARQ) based suspicious communication link over Rayleigh fading channels. We propose a proactive eavesdropping approach, where a half-duplex monitor can opportunistically jam the suspicious link to exploit its potential retransmissions for overhearing more efficiently. In particular, we consider that the suspicious link uses at most two HARQ rounds for transmitting the same data packet, and we focus on two cases without and with HARQ combining at the monitor receiver. In both cases, we aim to maximize the successful eavesdropping probability at the monitor, by adaptively allocating the jamming power in the first HARQ round according to fading channel conditions, subject to an average jamming power constraint. For both cases, we show that the optimal jamming power allocation follows a threshold-based policy, and the monitor jams with constant power when the eavesdropping channel gain is less than the threshold. Numerical results show that the proposed proactive eavesdropping scheme achieves higher successful eavesdropping probability than the conventional passive eavesdropping, and HARQ combining can help further improve the eavesdropping performance.**

I. Introduction

Recent advances in user-controlled wireless networks and devices such as ad hoc networks and drones have posed new threats to public security, since they can be misused to facilitate or commit crimes and terror attacks. In order to prevent or defend against such misuse, there is a growing need for authorized parties to legitimately monitor and eavesdrop suspicious communication links. In this case, different from conventional wireless security that assumes communication links are rightful and aims to maximize the secrecy rate against illegal eavesdropping [1], we consider a new wireless surveillance paradigm that focuses on legitimately eavesdropping suspicious wireless communication links [2]–[8].

Passive eavesdropping is a commonly adopted wireless surveillance approach, which, however, is unable to overhear the suspicious communications clearly once the legitimate monitors (eavesdroppers) are far away from suspicious transmitters (STs), due to the severe path-loss and channel fading of the eavesdropping link. To cope with this issue, proactive eavesdropping via jamming has been proposed in [3]–[5], where a full-duplex monitor sends jamming signals to interfere with the suspicious receiver (SR) to moderate the suspicious link transmission parameters (such as power and/or rate), for facilitating the simultaneous eavesdropping. By exploiting the channel fluctuations over time, the monitor can adaptively adjust its jamming power based on instantaneous channel conditions, for improving the eavesdropping performance [3]. It is worth noting that the above works largely focus on maximizing the eavesdropping capacity of the monitor assisted with jamming, in which the same packet is transmitted once in the suspicious communication link. In practice, however, most wireless communication systems are operated based on hybrid automatic repeat request (HARQ) protocols to ensure reliable communications, where the transmitter may retransmit the same packet if the receiver fails to decode [9], [10]. Furthermore, the existing works assume full-duplex monitors with simultaneous jamming and eavesdropping, but the performance is practically limited by the self-interference from the jamming to the eavesdropping antennas at the monitor [11].

To overcome these limitations, this paper studies the wireless surveillance of an HARQ-based suspicious communication link via a practical half-duplex legitimate monitor over Rayleigh fading channels. We consider that the suspicious communication link implements the HARQ protocol as follows. Initially, the ST transmits a coded packet to the SR; depending on whether the SR decodes it successfully or not, it replies an acknowledgement (ACK) or negative acknowledgement (NACK); upon receiving a NACK, the ST retransmits the same coded packet again. This operation is repeated until either an ACK is received or the number of retransmissions exceeds a maximum threshold. Under this setup, we propose a proactive eavesdropping approach, where the monitor opportunistically jams the suspicious link to exploit its potential retransmissions for overhearing more efficiently.

In particular, we assume the number of HARQ rounds for the suspicious communication to be two with at most one retransmission for the same packet.[1] In this case, the monitor must work in the eavesdropping mode without any jamming in the second HARQ round, since the half-duplex monitor cannot jam and eavesdrop the suspicious link at the same time, and there will be no more retransmissions of the same packet that can be eavesdropped. We focus on two cases without and with HARQ combining at the monitor receiver, which decodes each retransmitted packet independently, or combines all previously

[1]If more than one retransmissions are allowed, our eavesdropping performance is expected to be further improved, as there will be more chances for the monitor to jam and eavesdrop the suspicious link retransmissions.

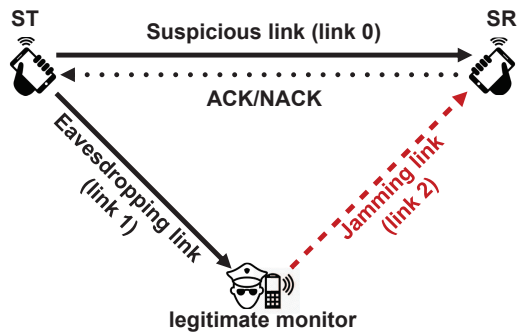

Fig. 1. Wireless surveillance of an HARQ-based suspicious communication link, where the legitimate monitor opportunistically jams the suspicious link to increase the chance of its retransmission for proactive eavesdropping.

received copies of the same packet to decode with maximum ratio combining (MRC), respectively.[2] In both cases, we aim to maximize the successful eavesdropping probability at the monitor, by adaptively allocating the jamming power in the first HARQ round based on fading channel conditions, subject to an average jamming power constraint. For both cases, we show that the optimal jamming power allocation follows a threshold-based policy, in which the monitor jams with constant power when the eavesdropping channel gain is less than a threshold; otherwise, the jamming power is zero and the monitor eavesdrops in the first round. Specifically, we find that with HARQ combining, the threshold is generally smaller than the case without HARQ combining; therefore, in this case the monitor prefers jamming only when the eavesdropping channel gain is even weaker. Finally, numerical results show that the proposed proactive eavesdropping schemes achieve higher successful eavesdropping probability than the conventional passive eavesdropping, and HARQ combining can help further improve the eavesdropping performance.

II. System Model

As shown in Fig. 1, a half-duplex legitimate monitor aims to overhear a suspicious communication link from an ST to an SR, which employs the HARQ protocol with two transmission rounds at most for the same packet. In this case, the monitor must work in the eavesdropping mode without any jamming in the second HARQ round, and can jam or eavesdrop (but not at the same time) in the first round. Intuitively, jamming the SR in the first round can increase the probability of packet retransmission in the second round of the suspicious link, but lose the chance of eavesdropping it in the first round.

We consider a quasi-static channel model, where wireless channels remain unchanged at each transmission round of one packet, but can change independently over different rounds and for different packets. Let g_i^t denote the channel power gain of link i at the t-th transmission round for one packet, where $i = 0$, 1, and 2 represent the suspicious link, the eavesdropping link, and the jamming link, respectively. Here, $t = \mathrm{I}$ and $t = \mathrm{II}$ denote the initial transmission and the retransmission rounds of the same packet, respectively. Rayleigh fading is considered, where for any $t \in \{\mathrm{I}, \mathrm{II}\}$, g_i^t follows an exponential distribution with the rate parameter λ_i (or the mean value $1/\lambda_i$), $i \in \{0, 1, 2\}$. We consider that at each transmission round t, the channel state information (CSI) g_0^t of the suspicious link is only available at the SR. Therefore, the ST adopts a fixed transmit power P_0 and a fixed data rate R (in bps/Hz) to deliver different packets over time. It is also assumed that at the beginning of round $t = \mathrm{I}$, the monitor perfectly knows the CSI g_1^{I} of the eavesdropping link via efficient channel estimation based on the received pilot signal from the ST, and it also knows the channel distribution information (CDI) of all the three links (i.e., the values of λ_i's) based on long-term observation.

Based on the CSI g_1^{I} of the eavesdropping link, in round $t = \mathrm{I}$ the monitor can adaptively adjust its power for jamming or just eavesdrop without jamming to maximize the surveillance performance over the HARQ-based suspicious communication. Let $Q(g_1^{\mathrm{I}}) \geq 0$ denote the jamming power in round $t = \mathrm{I}$ based on the exactly known g_1^{I}, where $Q(g_1^{\mathrm{I}}) = 0$ tells that the monitor eavesdrops without jamming in the first round. Our objective is to optimize the jamming power $Q(g_1^{\mathrm{I}})$'s according to the eavesdropping channel condition g_1^{I}'s over time to maximize the successful eavesdropping probability (to be defined later), subject to an average jamming power budget. We address this problem in the following by considering two cases without and with HARQ combining at the monitor receiver, respectively.

III. Optimal Jamming without HARQ Combining

In this section, we consider that if the monitor fails to decode the packet in the initial transmission round $t = \mathrm{I}$, it will discard the packet in this round; then in any retransmission round $t = \mathrm{II}$, it will only use the retransmitted packet for decoding, for ease of implementation. In the following, we first derive the successful eavesdropping probability under given jamming power $Q(g_1^{\mathrm{I}})$ for any given g_1^{I}. Then, we decide the jamming power allocation to maximize the successful eavesdropping probability by considering all possible values of g_1^{I}'s over time given the average jamming power budget.

A. Successful Eavesdropping Probability Under Given g_1^I and $Q(g_1^I)$

In this subsection, we obtain the successful eavesdropping probability under any given g_1^{I} and $Q(g_1^{\mathrm{I}})$, denoted as $\mathcal{P}_{\text{eav}}(g_1^{\mathrm{I}}, Q(g_1^{\mathrm{I}}))$. In particular, we have either $Q(g_1^{\mathrm{I}}) > 0$ (in jamming mode) or $Q(g_1^{\mathrm{I}}) = 0$ (in eavesdropping mode) in round $t = \mathrm{I}$.

1) Jamming with $Q(g_1^I) > 0$: In this case, the monitor can only overhear the retransmission in round $t = \mathrm{II}$, provided that the suspicious transmission in round $t = \mathrm{I}$ fails. First, we obtain the probability of suspicious retransmission, which is

[2]With the same packet retransmitted, the considered HARQ protocol with MRC is referred to as "chase combining (CC)" in practice [10]. There is another HARQ protocol with combining, namely "incremental redundancy (IR)", where if a NACK is received, the ST transmits additional coded bits, instead of retransmitting the same packet. Our results in this paper can also be extended to the case of IR, which is left for future work.

equivalent to the outage probability at the SR after the initial transmission of the ST in round $t = \text{I}$. In this round, the received signal-to-interference-and-noise ratio (SINR) at the SR is

$$\gamma_0^{\text{I}}(Q(g_1^{\text{I}})) = \frac{g_0^{\text{I}} P_0}{g_2^{\text{I}} Q(g_1^{\text{I}}) + \sigma^2}, \tag{1}$$

where σ^2 denotes the noise power at the receiver. Note that g_0^{I} and g_2^{I} are independent exponentially distributed variables with rate parameters λ_0 and λ_2, respectively. By letting

$$\bar{\gamma} = 2^R - 1 \tag{2}$$

denote the minimum received signal-to-noise ratio (SNR) or SINR requirement for successfully decoding the packet by assuming the optimal Gaussian signalling employed, we have the probability of suspicious retransmission as [4]

$$\begin{aligned} p_0^{\text{I-out}}(Q(g_1^{\text{I}})) &= \mathbb{P}(\gamma_0^{\text{I}}(Q(g_1^{\text{I}})) < \bar{\gamma}) \\ &= 1 - \frac{\lambda_2/(\bar{\gamma} Q(g_1^{\text{I}}))}{\lambda_0/P_0 + \lambda_2/(\bar{\gamma} Q(g_1^{\text{I}}))} e^{-\lambda_0 \sigma^2 \bar{\gamma}/P_0}. \end{aligned} \tag{3}$$

Next, we obtain the conditional successful eavesdropping probability of the monitor in round $t = \text{II}$, denoted by $p_1^{\text{II-suc}}$. In this round, the received SNR at the monitor is given as $\gamma_1^{\text{II}} = g_1^{\text{II}} P_0/\sigma^2$. As g_1^{II} is exponentially distributed with the rate parameter λ_1, we have

$$p_1^{\text{II-suc}} = \mathbb{P}(\gamma_1^{\text{II}} \geq \bar{\gamma}) = e^{-\lambda_1 \sigma^2 \bar{\gamma}/P_0}. \tag{4}$$

By combining the probability $p_0^{\text{I-out}}(Q(g_1^{\text{I}}))$ of suspicious retransmission in (3) and the conditional successful eavesdropping probability $p_1^{\text{II-suc}}$ in (4), we have the successful eavesdropping probability under given g_1^{I} and $Q(g_1^{\text{I}}) > 0$ as

$$\begin{aligned} &\mathcal{P}_{\text{eav}}(g_1^{\text{I}}, Q(g_1^{\text{I}})) = p_1^{\text{II-suc}} p_0^{\text{I-out}}(Q(g_1^{\text{I}})) \\ &= e^{-\lambda_1 \sigma^2 \bar{\gamma}/P_0} - \frac{\lambda_2 P_0}{\lambda_0 \bar{\gamma} Q(g_1^{\text{I}}) + \lambda_2 P_0} e^{-(\lambda_0+\lambda_1)\sigma^2 \bar{\gamma}/P_0} \\ &\triangleq \Phi(Q(g_1^{\text{I}})). \end{aligned} \tag{5}$$

Note that the function $\Phi(Q(g_1^{\text{I}}))$ is independent of g_1^{I}, and is monotonically increasing and concave with respect to the jamming power $Q(g_1^{\text{I}}) \geq 0$.

2) Eavesdropping with $Q(g_1^{I}) = 0$: In this case, the received SNR at the monitor is $\gamma_1^{\text{I}} = g_1^{\text{I}} P_0/\sigma^2$. If γ_1^{I} is no smaller than the minimum SNR requirement $\bar{\gamma}$ in (2) (i.e, $\gamma_1^{\text{I}} \geq \bar{\gamma}$), or equivalently $g_1^{\text{I}} \geq \bar{g} \triangleq \bar{\gamma}\sigma^2/P_0$, the monitor can successfully decode the ST's transmitted packet in this round, no matter whether the retransmission of the suspicious link occurs or not. Here, we have the successful eavesdropping probability under given $g_1^{\text{I}} \geq \bar{g}$ and $Q(g_1^{\text{I}}) = 0$ as

$$\mathcal{P}_{\text{eav}}(g_1^{\text{I}}, Q(g_1^{\text{I}})) = 1. \tag{6}$$

On the other hand, if $\gamma_1^{\text{I}} < \bar{\gamma}$ or equivalently $g_1^{\text{I}} < \bar{g}$, the monitor cannot decode the packet in round $t = \text{I}$. Therefore, it can only overhear the retransmission in round $t = \text{II}$, under the condition that the suspicious transmission in round $t = \text{I}$ fails. The successful eavesdropping probability in this case can be similarly obtained as that in (5). By replacing $Q(g_1^{\text{I}}) > 0$ in (5) as $Q(g_1^{\text{I}}) = 0$, we have the successful eavesdropping probability under given $g_1^{\text{I}} < \bar{g}$ and $Q(g_1^{\text{I}}) = 0$ as

$$\mathcal{P}_{\text{eav}}(g_1^{\text{I}}, Q(g_1^{\text{I}})) = \Phi(0), \tag{7}$$

where $\Phi(\cdot)$ is given in (5).

By combining $\mathcal{P}_{\text{eav}}(g_1^{\text{I}}, Q(g_1^{\text{I}}))$ in (5), (6), and (7), it follows that the successful eavesdropping probability under any given g_1^{I} and $Q(g_1^{\text{I}})$ is obtained as

$$\mathcal{P}_{\text{eav}}(g_1^{\text{I}}, Q(g_1^{\text{I}})) = \begin{cases} \Phi(Q(g_1^{\text{I}})), & \text{if } Q(g_1^{\text{I}}) > 0, \\ 1, & \text{if } Q(g_1^{\text{I}}) = 0 \text{ and } g_1^{\text{I}} \geq \bar{g}, \\ \Phi(0), & \text{if } Q(g_1^{\text{I}}) = 0 \text{ and } g_1^{\text{I}} < \bar{g}. \end{cases} \tag{8}$$

B. Successful Eavesdropping Probability Maximization

Our objective is to maximize the successful eavesdropping probability over all possible g_1^{I}'s, subject to the average jamming power budget at the monitor, denoted by $Q_{\text{ave}} > 0$. Towards this end, we adaptively allocate the jamming power $Q(g_1^{\text{I}})$'s based on the exact CSI observation of g_1^{I}'s for different packets. The optimization problem for the monitor is formulated as

$$\begin{aligned} \text{(P1)}: \max_{\{Q(g_1^{\text{I}}) \geq 0\}} \quad & \mathbb{E}_{g_1^{\text{I}}} \left(\mathcal{P}_{\text{eav}}(g_1^{\text{I}}, Q(g_1^{\text{I}})) \right) \\ \text{s.t.} \quad & \mathbb{E}_{g_1^{\text{I}}} \left(Q(g_1^{\text{I}}) \right) \leq Q_{\text{ave}}, \end{aligned} \tag{9}$$

where $\mathbb{E}_{g_1^{\text{I}}}(\cdot)$ denotes the expectation operation over g_1^{I}. We have the following proposition.

Proposition 3.1: The optimal jamming power solution to problem (P1) is given as

$$Q^*(g_1^{\text{I}}) = \begin{cases} 0, & \forall g_1^{\text{I}} \geq \bar{g} \\ \frac{Q_{\text{ave}}}{1 - e^{-\lambda_1 \sigma^2 \bar{\gamma}/P_0}}, & \forall g_1^{\text{I}} < \bar{g} \end{cases}. \tag{10}$$

Proof: Under any packet transmission with $g_1^{\text{I}} \geq \bar{g}$, it is evident that setting the jamming power as $Q(g_1^{\text{I}}) = 0$ achieves $\mathcal{P}_{\text{eav}}(g_1^{\text{I}}, Q(g_1^{\text{I}})) = 1$ in (6), while setting $Q(g_1^{\text{I}}) > 0$ achieves $\mathcal{P}_{\text{eav}}(g_1^{\text{I}}, Q(g_1^{\text{I}})) < 1$ in (5). Therefore, we have $Q^*(g_1^{\text{I}}) = 0$ for any $g_1^{\text{I}} \geq \bar{g}$.

Next, consider another packet transmission with $g_1^{\text{I}} < \bar{g}$. In this case, by combining (5) and (7), it is evident that $\mathcal{P}_{\text{eav}}(g_1^{\text{I}}, Q(g_1^{\text{I}}))$ is a monotonically increasing and concave function with respect to the jamming power $Q(g_1^{\text{I}}) \geq 0$, but irrespective of g_1^{I}. Based on the Jensen's inequality, it is optimal to set the jamming power to be identical, i.e., $Q^*(g_1^{\text{I}}) = Q^*, \forall g_1^{\text{I}} < \bar{g}$. Furthermore, note that the optimality of (P1) is achieved when the average jamming power constraint is met with strict equality. Notice that $\mathbb{P}(g_1^{\text{I}} < \bar{g}) = 1 - e^{-\lambda_1 \sigma^2 \bar{\gamma}/P_0}$. Then it follows that $(1 - e^{-\lambda_1 \sigma^2 \bar{\gamma}/P_0}) \cdot Q^* = Q_{\text{ave}}$. Therefore, we have $Q^*(g_1^{\text{I}}) = Q^* = \frac{Q_{\text{ave}}}{1 - e^{-\lambda_1 \sigma^2 \bar{\gamma}/P_0}}$ for any $g_1^{\text{I}} < \bar{g}$.

By combining the above two scenarios, this proposition is verified. ■

From Proposition 3.1, it is observed that the optimal jamming power allocation follows a threshold-based policy. When the eavesdropping channel gain g_1^{I} is larger than or equal to the threshold $\bar{g}$, the monitor does not jam as it can successfully eavesdrop; otherwise, when g_1^{I} is smaller than $\bar{g}$, it is optimal for the monitor to employ constant-power jamming to maximize the probability of retransmission and hence the successful eavesdropping probability.

IV. Optimal Jamming with HARQ Combining

In this section, we consider that if the SR or the monitor fails to decode the packet eavesdropped in the initial transmission

($t = \mathrm{I}$), it will use it to combine with the retransmitted packet in the second round ($t = \mathrm{II}$) via the MRC technique.

A. Successful Eavesdropping Probability Under Given g_1^I and $Q(g_1^I)$

In the following, we obtain the successful eavesdropping probability under any given g_1^{I} and $Q(g_1^{\mathrm{I}})$, denoted as $\hat{\mathcal{P}}_{\text{eav}}(g_1^{\mathrm{I}}, Q(g_1^{\mathrm{I}}))$.

1) Jamming with $Q(g_1^I) > 0$: In this case, eavesdropping is not feasible at the monitor in round $t = \mathrm{I}$, and hence, no MRC is implementable. Therefore, the successful eavesdropping probability under given g_1^{I} and $Q(g_1^{\mathrm{I}}) > 0$ is same as that in (5) without HARQ combining, i.e., $\hat{\mathcal{P}}_{\text{eav}}(g_1^{\mathrm{I}}, Q(g_1^{\mathrm{I}})) = \Phi(Q(g_1^{\mathrm{I}}))$.

2) Eavesdropping with $Q(g_1^I) = 0$: When $g_1^{\mathrm{I}} \geq \bar{g}$, the eavesdropping is always successful in round $t = \mathrm{I}$. Therefore, we have the successful eavesdropping probability under given $g_1^{\mathrm{I}} \geq \bar{g}$ and $Q(g_1^{\mathrm{I}}) = 0$ as $\hat{\mathcal{P}}_{\text{eav}}(g_1^{\mathrm{I}}, Q(g_1^{\mathrm{I}})) = 1$.

When $g_1^{\mathrm{I}} < \bar{g}$, the eavesdropping is not successful at round $t = \mathrm{I}$. Nevertheless, if retransmission occurs, the monitor can implement MRC to combine the two copies of the same packet that are received in the two rounds, respectively. First, note that the probability of retransmission can be similarly obtained as that in (3) by calculating the outage probability of suspicious transmission. As no jamming is employed here, we have the probability of retransmission as

$$p_0^{\text{I-out}}(0) = 1 - e^{-\lambda_0 \sigma^2 \bar{\gamma}/P_0}, \tag{11}$$

with $p_0^{\text{I-out}}(Q(g_1^{\mathrm{I}}))$ given in (3).

Next, we derive the conditional successful eavesdropping probability under given g_1^{I} when retransmission occurs, denoted as $\hat{p}_1^{\text{I+II-suc}}(g_1^{\mathrm{I}})$. With MRC, the received SNR at the monitor is given as

$$\gamma_1^{\mathrm{I}} + \gamma_1^{\mathrm{II}} = \frac{(g_1^{\mathrm{I}} + g_1^{\mathrm{II}})P_0}{\sigma^2}. \tag{12}$$

As g_1^{II} is exponentially distributed with rate parameter λ_1, we have

$$\begin{aligned}\hat{p}_1^{\text{I+II-suc}}(g_1^{\mathrm{I}}) &= \mathbb{P}\left(\gamma_1^{\mathrm{I}} + \gamma_1^{\mathrm{II}} \geq \bar{\gamma}\right) = \mathbb{P}\left(g_1^{\mathrm{II}} \geq \frac{\sigma^2 \bar{\gamma}}{P_0} - g_1^{\mathrm{I}}\right) \\ &= e^{-\frac{\bar{\gamma}\lambda_1 \sigma^2}{P_0} + g_1^{\mathrm{I}} \lambda_1}. \end{aligned} \tag{13}$$

Then, by taking into account the probability of retransmission $p_0^{\text{I-out}}(0)$ in (11), we have the successful eavesdropping probability under given $g_1^{\mathrm{I}} < \bar{g}$ and $Q(g_1^{\mathrm{I}}) = 0$ as

$$\begin{aligned}&\hat{\mathcal{P}}_{\text{eav}}(g_1^{\mathrm{I}}, Q(g_1^{\mathrm{I}})) = \hat{p}_1^{\text{I+II-suc}}(g_1^{\mathrm{I}}) \cdot p_0^{\text{I-out}}(0) \\ &= e^{-\bar{\gamma}\lambda_1 \sigma_1^2/P_0 + g_1^{\mathrm{I}}\lambda_1}(1 - e^{-\lambda_0 \sigma^2 \bar{\gamma}/P_0}) = e^{g_1^{\mathrm{I}}\lambda_1}\Phi(0). \end{aligned} \tag{14}$$

By combining the above cases, it follows that with HARQ combining, the successful eavesdropping probability under any given g_1^{I} and $Q(g_1^{\mathrm{I}})$ is

$$\hat{\mathcal{P}}_{\text{eav}}(g_1^{\mathrm{I}}, Q(g_1^{\mathrm{I}})) = \begin{cases} \Phi(Q(g_1^{\mathrm{I}})), & \text{if } Q(g_1^{\mathrm{I}}) > 0, \\ 1, & \text{if } Q(g_1^{\mathrm{I}}) = 0 \text{ and } g_1^{\mathrm{I}} \geq \bar{g}, \\ e^{g_1^{\mathrm{I}}\lambda_1}\Phi(0), & \text{if } Q(g_1^{\mathrm{I}}) = 0 \text{ and } g_1^{\mathrm{I}} < \bar{g}. \end{cases} \tag{15}$$

By comparing (15) with (8), it is evident that their only difference lies in the case when the monitor chooses to overhear in round $t = \mathrm{I}$ (i.e., $Q(g_1^{\mathrm{I}}) = 0$) but the eavesdropping in round $t = \mathrm{I}$ is not successful (i.e., $g_1^{\mathrm{I}} < \bar{g}$). Thanks to the MRC, the successful eavesdropping probability increases by a factor of $e^{g_1^{\mathrm{I}}\lambda_1} > 1$ in (15).

B. Successful Eavesdropping Probability Maximization

With HARQ combining, the successful eavesdropping probability maximization problem is formulated as

$$\begin{aligned}(\mathrm{P2}): \max_{\{Q(g_1^{\mathrm{I}}) \geq 0\}} \ & \mathbb{E}_{g_1^{\mathrm{I}}}\left(\hat{\mathcal{P}}_{\text{eav}}(g_1^{\mathrm{I}}, Q(g_1^{\mathrm{I}}))\right) \\ \text{s.t. } & \mathbb{E}_{g_1^{\mathrm{I}}}\left(Q(g_1^{\mathrm{I}})\right) \leq Q_{\text{ave}}. \end{aligned} \tag{16}$$

Note that problem (P2) is more challenging to solve than (P1). This is due to the fact that under any given $g_1^{\mathrm{I}} < \bar{g}$, the function $\hat{\mathcal{P}}_{\text{eav}}(g_1^{\mathrm{I}}, Q(g_1^{\mathrm{I}}))$ is non-convex as it is discontinuous for $Q(g_1^{\mathrm{I}}) = 0$. Despite this fact, we have the following proposition.

Proposition 4.1: The optimal jamming power allocation $\{Q^\star(g_1^{\mathrm{I}})\}$ to problem (P2) follows a threshold-based policy, given by

$$Q^\star(g_1^{\mathrm{I}}) = \begin{cases} \sqrt{\frac{\lambda_2 P_0}{\lambda_0 \bar{\gamma} \mu^\star} e^{-(\lambda_0 \sigma_0^2 + \lambda_1 \sigma_1^2)\bar{\gamma}/P_0}} - \frac{\lambda_2 P_0}{\lambda_0 \bar{\gamma}}, & \forall g_1^{\mathrm{I}} \leq \bar{g}^\star \\ 0, & \forall g_1^{\mathrm{I}} > \bar{g}^\star, \end{cases} \tag{17}$$

with the threshold $\bar{g}^\star$ given as

$$\bar{g}^\star = \min\left(\bar{g}, \frac{1}{\lambda_1} \ln\left(1 + \frac{\left(\sqrt{\frac{\mu^\star \lambda_2 P_0}{\lambda_0 \bar{\gamma}}} - \sqrt{e^{-\frac{(\lambda_0 \sigma^2 + \lambda_1 \sigma^2)\bar{\gamma}}{P_0}}}\right)^2}{e^{-\frac{\lambda_1 \sigma^2 \bar{\gamma}}{P_0}} - e^{-\frac{(\lambda_0 + \lambda_1)\sigma^2 \bar{\gamma}}{P_0}}}\right)\right). \tag{18}$$

Here, $\mu^\star$ satisfying

$$0 \leq \mu^\star \leq \frac{\lambda_0 \bar{\gamma}}{\lambda_2 P_0} e^{-(\lambda_0 \sigma_0^2 + \lambda_1 \sigma_1^2)\bar{\gamma}/P_0} \tag{19}$$

corresponds to a parameter such that $\mathbb{E}(Q^\star(g_1^{\mathrm{I}})) = Q_{\text{ave}}$.

Proof: See Appendix A. ∎

By comparing Proposition 4.1 with Proposition 3.1, it is observed from (18) that the threshold $\bar{g}^\star$ for (P2) is smaller than $\bar{g}$ for (P1). This shows that with the HARQ combining, the monitor may not jam even when it cannot successfully eavesdrop in the initial round. For illustration, we provide a numerical example in Fig. 2 to show the thresholds for (P1) and (P2), for which the parameters are set as in Section V later. It is observed that with the jamming power Q_{ave} increasing, the threshold $\bar{g}^\star$ for the case with HARQ combining increases monotonically. This indicates that with more jamming power, the monitor should distribute its jamming power over more packets when eavesdropping fails in the initial round.

V. Numerical Results

In this section, we provide numerical results to evaluate the performance of our proposed proactive eavesdropping schemes as compared to the conventional passive eavesdropping without jamming, i.e., $Q(g_1^{\mathrm{I}}) = 0, \forall g_1^{\mathrm{I}}$. In the simulation, we normalize the noise powers at the SR and the monitor as $\sigma^2 = 1$, set the average channel power gain of the Rayleigh fading suspicious, eavesdropping, and jamming links as $1/\lambda_0 = 1, 1/\lambda_1 = 0.2$, and $1/\lambda_2 = 0.2$, respectively. Furthermore, we fix the transmit power by the ST as $P_0 = 10$ dB.

Fig. 3 shows the successful eavesdropping probability at the monitor versus the average jamming power Q_{ave}, where

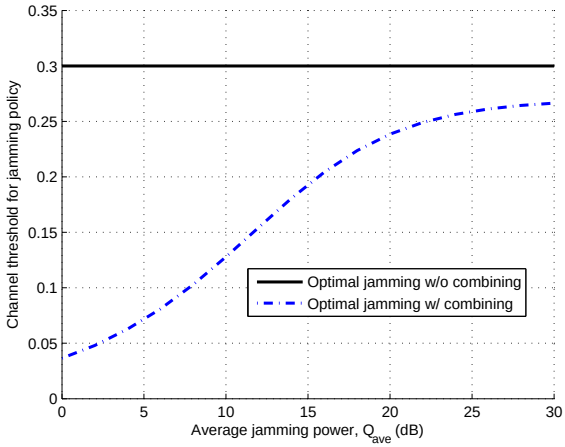

Fig. 2. The thresholds for jamming policy in the two HARQ cases without versus with combining.

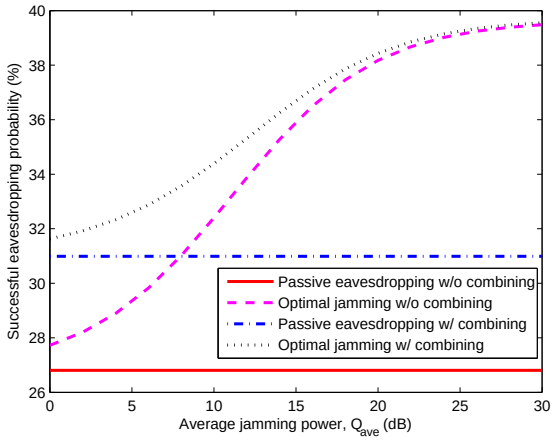

Fig. 3. The successful eavesdropping probability versus the average jamming power Q_{ave}, where $R = 2$ bps/Hz.

the communication rate at the suspicious link is $R = 2$ bps/Hz. It is observed that no matter without or with HARQ jamming, the proposed proactive eavesdropping achieves much higher successful eavesdropping probability than the respective passive eavesdropping case. It is also observed that for both passive and proactive eavesdropping, HARQ combining generally helps further improve the eavesdropping performance. Nevertheless, when Q_{ave} becomes large, the proactive eavesdropping with HARQ combining is observed to achieve a similar eavesdropping performance as that without HARQ combining. This can be explained based on Fig. 2, where as Q_{ave} becomes large, the threshold $\bar{g}^{\star}$ with HARQ combining increases towards $\bar{g}$, the threshold for the case without combing. In this case, the monitor needs to jam over more packets when the eavesdropping fails in the initial round, over which the HARQ combining is not applicable, thus making the two schemes perform similar.

Fig. 4 shows the successful eavesdropping probability versus the suspicious communication rate R, where the average jamming power is $Q_{\text{ave}} = 20$ dB. It is observed that at small R values, passive (proactive) eavesdropping with HARQ combining achieves similar eavesdropping performance as that without HARQ combining. This is due to the fact that with small R, the eavesdropping is likely to be successful in the initial round, and thus no HARQ combining is required. By contrast, at large R values, eavesdropping with HARQ combining is observed to perform better than that without HARQ combining, as retransmission occurs with a higher probability.

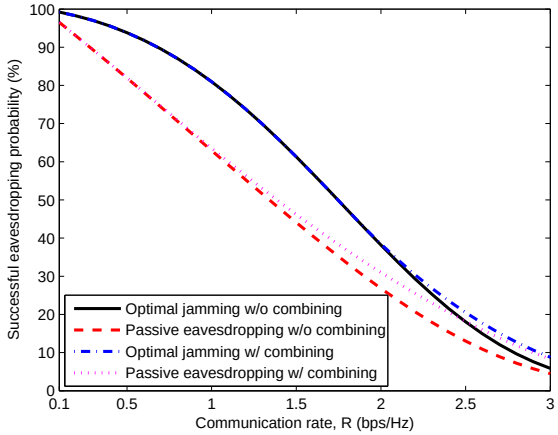

Fig. 4. The successful eavesdropping probability versus the communication rate R at the suspicious communication, where $Q_{\text{ave}} = 20$dB.

VI. Conclusion

This paper presented a new wireless surveillance scenario over an HARQ-based suspicious communication link via a half-duplex monitor. We proposed a proactive eavesdropping via jamming based approach, where the monitor jams opportunistically to improve the surveillance performance via exploiting the potential retransmission in the suspicious link. In both cases without and with HARQ combining at the monitor receiver, we showed that the optimal jamming power allocation follows a threshold-based policy, where the monitor jams with a constant power in the initial round when the eavesdropping channel gain is less than a threshold. It is hoped that this paper can provide new insights on exploiting the retransmission in practical HARQ protocols to improve the performance of wireless surveillance.

Appendix

A. Proof of Proposition 4.1

Though problem (P2) is non-convex in general, it satisfies the so-called time-sharing condition in [12]. Therefore, strong duality or zero duality gap holds between problem (P2) and its dual problem. Therefore, we use the Lagrange duality method to obtain the optimal solution.

Let $\mu \geq 0$ denote the dual variable associated with the average jamming power constraint. Then the partial Lagrangian of (P2) is denoted as

$$\mathcal{L}(\{Q(g_1^{\mathrm{I}})\},\mu) = \mathbb{E}_{g_1^{\mathrm{I}}}\left(\hat{\mathcal{P}}_{\text{eav}}(g_1^{\mathrm{I}},Q(g_1^{\mathrm{I}}))\right) - \mu\left(\mathbb{E}_{g_1^{\mathrm{I}}}\left(Q(g_1^{\mathrm{I}})\right) - Q_{\text{ave}}\right). \quad (20)$$

The dual function is given as

$$\psi(\mu) = \max_{\{Q(g_1^{\mathrm{I}})\geq 0\}} \mathcal{L}(\{Q(g_1^{\mathrm{I}})\},\mu). \quad (21)$$

The dual problem is

$$\text{(D2)}: \min_{\mu\geq 0} \psi(\mu). \quad (22)$$

Due to the strong duality between (P2) and (D2), we solve (P2) by first solving problem (21) to obtain the dual function $\psi(\mu)$ under any given $\mu \geq 0$, and then solving (D2) via searching over $\{Q(g_1^{\mathrm{I}})\}$ to minimize $g(\mu)$.

1) Solving Problem (21) Under Given $\mu \geq 0$: Problem (21) can be decomposed into various subproblems each for one g_1^{I}.

$$\max_{Q(g_1^{\mathrm{I}})\geq 0} \hat{\mathcal{P}}_{\text{eav}}(Q(g_1^{\mathrm{I}})) - \mu Q(g_1^{\mathrm{I}}). \quad (23)$$

We solve problem (23) by considering $g_1^{\mathrm{I}} \geq \bar{g}$ and $g_1^{\mathrm{I}} < \bar{g}$, respectively. First, for any $g_1^{\mathrm{I}} \geq \bar{g}$, it is evident that the optimal solution to problem (23) is given as

$$\tilde{Q}(g_1^{\mathrm{I}}) = 0, \forall g_1^{\mathrm{I}} \geq \bar{g}, \quad (24)$$

with the achieved optimal value being 1.

Next, consider problem (23) for any given $g_1^{\mathrm{I}} < \bar{g}$. In this case, problem (23) can be solved by considering two regimes with $Q(g_1^{\mathrm{I}}) = 0$ and $Q(g_1^{\mathrm{I}}) > 0$, respectively.

In the regime with $Q(g_1^{\mathrm{I}}) = 0$, the achieved objective value for problem (23) is a constant $v_0(g_1^{\mathrm{I}}) = e^{g_1^{\mathrm{I}}\lambda_1}\Phi(0)$.

In the other regime with $Q(g_1^{\mathrm{I}}) > 0$, problem (23) becomes

$$\max_{Q(g_1^{\mathrm{I}})>0} \Phi(Q(g_1^{\mathrm{I}})) - \mu Q(g_1^{\mathrm{I}}). \quad (25)$$

As $\Phi(Q(g_1^{\mathrm{I}}))$ is concave over $Q(g_1^{\mathrm{I}}) \geq 0$, this problem is convex. By checking the first-order derivative of the objective function, the optimal solution to problem (25) is derived as $\bar{Q}_\mu$ (irrespective of g_1^{I}). If $\mu \leq \frac{\lambda_0\bar{\gamma}}{\lambda_2 P_0} e^{-(\lambda_0\sigma_0^2+\lambda_1\sigma_1^2)\bar{\gamma}/P_0}$, we have

$$\bar{Q}_\mu = \sqrt{\frac{\lambda_2 P_0}{\lambda_0\bar{\gamma}\mu} e^{-(\lambda_0+\lambda_1)\sigma^2\bar{\gamma}/P_0}} - \frac{\lambda_2 P_0}{\lambda_0\bar{\gamma}}, \quad (26)$$

with the achieved objective value given as

$$v_\mu = \left(\sqrt{\frac{\mu\lambda_2 P_0}{\lambda_0\bar{\gamma}}} - \sqrt{e^{-(\lambda_0\sigma_0^2+\lambda_1\sigma_1^2)\bar{\gamma}/P_0}}\right)^2 + \Phi(0). \quad (27)$$

Otherwise, if $\mu > \frac{\lambda_0\bar{\gamma}}{\lambda_2 P_0} e^{-(\lambda_0\sigma_0^2+\lambda_1\sigma_1^2)\bar{\gamma}/P_0}$, we have $\bar{Q}_\mu = 0$ and $v_\mu = \Phi(0)$.

By comparing $v_0(g_1^{\mathrm{I}})$ versus v_μ for the two regimes, the optimal solution to problem (23) under $g_1^{\mathrm{I}} < \bar{g}_1$ is given as

$$\tilde{Q}(g_1^{\mathrm{I}}) = \begin{cases} \bar{Q}_\mu, & \text{if } v_\mu > v_0(g_1^{\mathrm{I}}) \\ 0, & \text{if } v_\mu < v_0(g_1^{\mathrm{I}}), \end{cases}, \forall g_1^{\mathrm{I}} < \bar{g}. \quad (28)$$

2) Finding Optimal $\mu \geq 0$ to Solve (D2): Next, we solve (D2) to find the optima μ, denoted by $\mu^\star$. It is easy to show that at the optimality of (P2), the average jamming power constraint must be tight. Therefore, the optimal $\mu^\star$ can be found by using the equation $\mathbb{E}_{g_1^{\mathrm{I}}}(\tilde{Q}(g_1^{\mathrm{I}})) = Q_{\text{ave}}$, with $\tilde{Q}(g_1^{\mathrm{I}})$ given in (24) and (28).

Under $\mu^\star$, the corresponding $\tilde{Q}(g_1^{\mathrm{I}})$'s in (28) become the optimal jamming power allocation $Q^\star(g_1^{\mathrm{I}})$'s for (P2). After some simple manipulation, we can further show that (19) must hold in order for the jamming power constraint to be tight. With (19), we can obtain (17) based on (28). Hence, this proposition is proved.

REFERENCES

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[2] J. Xu, L. Duan, and R. Zhang, "Surveillance and intervention of infrastructure-free mobile communications: A new wireless security paradigm," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 152–159, Aug. 2017.

[3] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 2790–2806, May 2017.

[4] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over rayleigh fading channels," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 80–83, Feb. 2016.

[5] Y. Zeng, and R. Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1449–1461, Dec. 2016.

[6] G. Ma, J. Xu, L. Duan, and R. Zhang, "Wireless surveillance of two-hop communications," in *Proc. IEEE SPAWC*, 2017, pp. 1–5.

[7] H. Tran and H. Zepernick, "Proactive attack: A strategy for legitimate eavesdropping," in *Proc. IEEE ICCE*, 2016, pp. 457–461.

[8] C. Zhong, X. Jiang, F. Qu, and Z. Zhang, "Multi-antenna wireless legitimate surveillance systems: Design and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4585–4599, Jul. 2017.

[9] A. Larmo, M. Lindström, M. Meyer, G. Pelletier, J. Torsner, and H. Wiemann, "The LTE link-layer design," *IEEE Commun. Mag.*, vol. 47, no. 4, pp. 52–59, Apr. 2009.

[10] J.-F. Cheng, "Coding performance of hybrid ARQ schemes," *IEEE Trans. Commun.*, vol. 54, no. 6, pp. 1017–1029, Jun. 2006.

[11] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.

[12] W. Yu, and R. Lui, "Dual methods for nonconvex spectrum optimization of multicarrier systems," *IEEE Trans. Commun.*, vol. 54, no. 7, pp. 1310–1322, Jul. 2006.