# Evasive Active Hypothesis Testing

Meng-Che Chang and Matthieu R. Bloch, *Senior Member, IEEE*

***Abstract*—We consider a situation in which a decision maker takes sequential and adaptive sensing actions to collect measurements and estimate an unknown parameter taking finitely many values, in the presence of an adversary who also collects measurements whenever a sensing action is taken. This situation can be viewed as an abstraction in which to analyze the mitigation of information leakage inherent to control actions in systems with feedback, such as cyber-physical systems. Specifically, we formulate an *evasive* active hypothesis problem in which the objective is for the decision maker to control the risk of its test while minimizing the detection ability of the adversary, measured in terms of the asymptotic error exponent ratio between the adversary and the decision maker. We develop bounds on the exponent ratio that offer insight into optimal strategies that the decision maker can deploy to evade the adversary's detection. We illustrate the results with a numerical example corresponding to the detection of a wireless transmission.**

***Index Terms*—Active hypothesis testing, eavesdropper, physical layer security.**

## INTRODUCTION

MOST complex systems now rely on feedback mechanisms to ensure efficient operation, either to ensure end-to-end reliability in communication networks or stability in cyber-physical systems. Unfortunately, the presence of feedback signals also increases the attack surface of such systems, not only because the feedback signals can be intercepted or tampered with but also because the mere presence of a control mechanism might leak information about the operation of the underlying system, without even requiring the signal to be decoded. For instance, a recent study of IoT devices has shown that eavesdroppers can infer activity information, from interaction methods to functionality, even from encrypted traffic and without directly exposing information [2]. At a more abstract level, one of the security challenges faced in complex systems is that the *actions* taken by decision makers, such as the communicating parties in a communication network, or the controllers in a cyber-physical system, inherently contain, and therefore leak, information about the objective of the decision making process.

The objective of the present work is to take initial steps towards understanding the information-theoretic limits of information leakage induced by the actions of decision-makers in systems with feedback, as well as towards developing strategies that allow systems to operate efficiently while mitigating the information leakage to eavesdroppers. We adopt an active hypothesis testing problem in the presence of an eavesdropper as the abstraction in which to carry the analysis. Specifically, we consider a situation in which a decision maker takes sequential and adaptive sensing actions to collect measurements and estimate an unknown parameter taking finitely many values, in the presence of an adversary who also collects measurements whenever a sensing action is taken. Our objective is to develop optimal *evasive* active hypothesis testing strategies, in the sense that the strategies meet a risk-requirement for the decision maker while minimizing the detection ability of the adversary measured in terms of the adversary's asymptotic error exponent. This model is motivated in part by its analytical tractability but, most importantly, because sequential multiple-hypothesis testing has already found numerous engineering applications, ranging from target detection [3] to beam alignment [4]. In that regard the model captures the essence of the challenge, i.e., the leakage of information through actions, while remaining grounded in real engineering systems.

The growing concerns for data privacy and secrecy have already fostered the analysis of information leakage in decision making systems, as well as the design of mechanisms at the signal level to mitigate the information leakage in several research communities. For instance, there has been interest in the control community for using the imperfections of the physical-layer or the introduction of noise to secure state estimation [5], [6], [7]. More closely related to the present work, there have been several studies investigating hypothesis testing under information-theoretic security constraints. A first line of work consists of the studies of *stochastic encryption*, in which distributed sensors intentionally and locally corrupt their data to degrade (either by quantizing or introducing noise) the decision performance of an eavesdropper fusion center while maintaining an acceptable performance at a legitimate fusion center [8]. The use of stochastic encryption has been explored for various models, in which the legitimate parties exploit an advantage originating from an observation structure [9], [10] or secret keys [11], [12]. More recently, stochastic encryption has been extended to the sequential detection setting [13]. Another line of work consists of research efforts around distributed binary hypothesis testing against conditional independence and under secrecy constraints [14], [15]; therein, the objective is to control how public messages encoding blocks of data are designed to optimally trade off the rate of public communication, the exponent of the type II error, and the equivocation of an adversary.

The present work differs from previous studies by considering the framework of *active hypothesis testing* [16], also

Manuscript received October 15, 2020; revised March 17, 2021; accepted April 7, 2021. Date of publication April 20, 2021; date of current version June 21, 2021. This work was supported in part by NSF under Grant 1527074 and Grant 1955401. A preliminary version of these results was presented at the 2020 IEEE International Symposium on Information Theory [1]. *(Corresponding author: Meng-Che Chang.)*

The authors are with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA (e-mail: mchang301.gatech.edu; matthieu.bloch@ece.gatech.edu).

Digital Object Identifier 10.1109/JSAIT.2021.3074156

known as *controlled sensing* [17], in which the kernels governing noisy observations are dynamically adapted using past observations. While the foundations of this framework can be traced back to the pioneering work of Chernoff on sequential design of experiments [18], there has been a recent resurgence of interest driven in part by applications to machine learning. The rationale for our study is also slightly different from previous works. While previous studies of hypothesis testing under security constraints have been motivated by the risks posed by a *distributed* operation when an adversary intercepts messages, we are interested in understanding the risks and opportunities offered by *adaptivity* when an adversary indirectly benefits from the actions taken by decision makers.

The rest of the paper is organized as follows. We provide a brief overview of the notation used throughout the paper in Section I. We introduce the precise model under consideration, which we call *evasive active hypothesis testing*, and associated results in Section II. Therein, we also illustrate the results with a simple example motivated by beam alignment in 5G systems, in which legitimate parties attempt to steer a beam in a direction to quickly detect the presence of a transmission while slowing down the estimation of an eavesdropper. We provide proofs of the results in Section III and offer conclusions in Section IV.

## I. Notation

A length $n$ vector is denoted by $x^n \triangleq (x_1, \ldots, x_n)$, where $x_i$, $i \in [1, n]$, is the $i$th element of the vector. If $\mathcal{U}$ is an alphabet, we denote by $\mathcal{P}(\mathcal{U})$ the set of all distributions on $\mathcal{U}$. Similarly, $\mathcal{P}(\mathcal{U}, \mathcal{Y})$ is the set of all joint distributions on $\mathcal{U}$ and $\mathcal{Y}$. The type of a sequence $u^n \in \mathcal{U}^n$ of length $n$ is the empirical distribution in $\mathcal{P}(\mathcal{U})$ induced by $u^n$ and is denoted by $\hat{p}_{u^n}$. Similarly, if $y^n \triangleq (y_1, \ldots, y_n) \in \mathcal{Y}^n$ is another sequence then the joint type of $u^n$ and $y^n$ is the joint empirical distribution in $\mathcal{P}(\mathcal{U}, \mathcal{Y})$ induced by the sequences, denoted as $\hat{p}_{u^n, y^n}$. Formally, we have $\hat{p}_{u^n, y^n}(u, y) = \sum_{i=1}^n 1(u_{i+1} = u, y_i = y)/n$. $\mathcal{P}_n(\mathcal{U})$ denotes the set of all types generated by sequences with length smaller than $n$, and $\mathcal{P}_n(\mathcal{U}, \mathcal{Y})$ denotes the set of all joint types generated by pairs of sequences with length smaller than $n$. We further define $\hat{p}_{y^n|u}$ as the conditional type such that $\hat{p}_{y^n|u}(y) = \sum_{i=1}^n 1(u_i = u, y_i = y)/\sum_{i=1}^n 1(u_i = u)$. Given probability distributions $p_1$ and $p_2$ on some discrete alphabet $\mathcal{X}$, the relative entropy between $p_1$ and $p_2$ is defined as $D(p_1 \| p_2) \triangleq \sum_{x \in \mathcal{X}} p_1(x) \log \frac{p_1(x)}{p_2(x)}$. The Chernoff information between $p_1$ and $p_2$ is defined as $C(p_1 \| p_2) = \max_{s \in [0,1]} -\log(\sum_{x \in \mathcal{X}} p_1(x)^s p_2(x)^{1-s})$. If $\{p_1^u\}_{u \in \mathcal{U}}$ and $\{p_2^u\}_{u \in \mathcal{U}}$ are two sets of distributions on $\mathcal{X}$ parameterized by $u \in \mathcal{U}$ and if $q$ is a distribution on $\mathcal{U}$, we define the quantity $C(p_1 \| p_2; q) \triangleq \max_{s \in [0,1]} -\sum_u q(u) \log(\sum_{x \in \mathcal{X}} p_1^u(x)^s p_2^u(x)^{1-s})$.

## II. Model and Results

Consider the situation illustrated in Fig. 1, in which a decision maker and an eavesdropper engage in an active $M$-ary hypothesis testing problem to estimate an unknown parameter $\theta \in \Theta \triangleq \{0, \ldots, M-1\}$. It will be convenient to think of the problem as involving three terminals, Alice, Bob, and Eve, where Alice represents the controller part of the decision maker taking actions, Bob represents the sensor part of the decision maker getting observations, and Eve is the passive eavesdropper obtaining other observations. The split of the decision maker into two components is merely to simplify some of our discussions and, in many instances, Alice and Bob may be co-located so that the observations obtained by Bob cannot be eavesdropped when transmitted back to Alice. Alternatively, one can think of the communication between Bob and Alice as being encrypted so that no information leakage happens through the feedback link. The overall system then operates as follows. At each time step $k \geq 1$, Bob and Eve obtain observations $y_k \in \mathcal{Y}$ and $z_k \in \mathcal{Z}$, respectively, generated by kernels $p_\theta^{u_k} \in \{p_\theta^u\}_{u \in \mathcal{U}}$ and $q_\theta^{u_k} \in \{q_\theta^u\}_{u \in \mathcal{U}}$, respectively, where $u_k \in \mathcal{U}$ is controlled by Alice. In [1], we have analyzed the situation in which the distribution $p_\theta^{u_k}$ is conditionally independent of past observation $(y^{k-1}, z^{k-1}, u^{k-1})$ given the choice of action $u_k$. In this work, we extend to the slightly more general case in which the distribution $p_\theta^{u_k}(\cdot|y_{k-1})$ depends on the past observations $y_{k-1}$ but the distribution $q_\theta^{u_k}$ is still conditionally independent of past observations. This generalization is inspired by [19], which analyzes the sequential hypothesis testing with Markovian observations. The action $u_k$ at time $k$ is chosen according to a known closed-loop control policy $p(u_k|y^{k-1}, u^{k-1})$. The joint distribution of $(y^n, z^n, u^{n+1})$ under the hypothesis $\theta = i$ is therefore given by

$$p_i\Big(y^n, z^n, u^{n+1}\Big) \triangleq p(u_1)\left(\prod_{k=1}^n p_i^{u_k}(y_k|y_{k-1}) q_i^{u_k}(z_k) p\Big(u_{k+1}|y^k, u^k\Big)\right).$$

We are interested in sequential tests $\Gamma = (\phi, \tau, \delta)$ that consist of the following components: i) a *control policy* $\phi \triangleq \{p(u_k|y^{k-1}, u^{k-1})\}_{k \geq 1}$ that allows Alice to generate action $u_k$ at time $k$ according to the distribution $p(u^k|y^{k-1}, u^{k-1})$; ii) a *stopping rule* $\tau$ that allows Alice and Bob to stop the sequential estimation and defined as

$$\tau = \min_{i \in \Theta} \inf\{n : L_i(n) \geq \exp(b_i)\}, \tag{1}$$

where $L_i(n) \triangleq \frac{\prod_{k=1}^n p_i^{u_k}(y_k|y_{k-1})}{\max_{j \neq i} \prod_{k=1}^n p_j^{u_k}(y_k|y_{k-1})}$ and $\{b_i\}_{i=0}^{M-1}$ are thresholds having the form $b_i = \log(1/\bar{R}_i) + K$ for some constants $\bar{R}_i < 1$ and $K$; iii) a *decision rule* $\delta$ that allows Alice and Bob

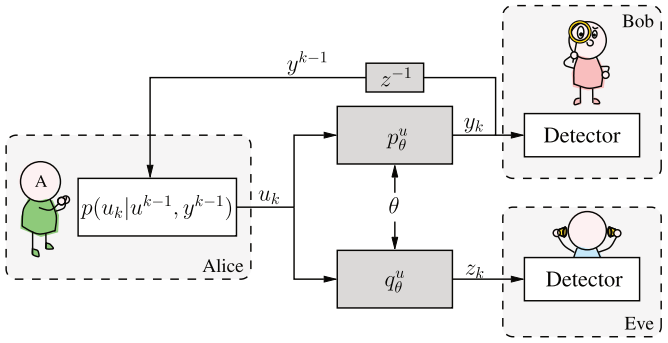


Fig. 1. Model of evasive active hypothesis testing.

to decide on a hypothesis and defined as

$$\delta(y^\tau) = i \quad \text{if} \quad L_i(\tau) = \max_{j\in\Theta} L_j(\tau). \tag{2}$$

The restriction to such tests is justified by their asymptotic optimality in the controlled sensing setting [17]. We also assume that i) the sets $\mathcal{Y}$, $\mathcal{Z}$, and $\mathcal{U}$ are finite; ii) there exists a prior $\{\pi_i\}_{i\in\Theta}$ on the parameter $\theta$ known by both Bob and Eve; iii) the kernel sets $\{p_\theta^u\}_{u\in\mathcal{U}}$ and $\{q_\theta^u\}_{u\in\mathcal{U}}$ are known to Alice, while Eve only knows $\{q_\theta^u\}_{u\in\mathcal{U}}$; iv) the control sequence $u^\tau$ and the sequential test $\Gamma$ are known to all parties; and v) $\forall i \neq j$, $\forall u \in \mathcal{U}$ and $\forall y \in \mathcal{Y}$, it holds that $0 < D(p_i^u(\cdot|y)\|p_j^u(\cdot|y)) < \infty$. Since the kernel set $\{p_\theta^u\}_{u\in\mathcal{U}}$ is not known to Eve, she cannot obtain any information about $\theta$ from the control sequence $u^\tau$. This assumption is not completely innocent and allows us to focus on the information leakage induced by the actions, without having to worry about the leakage from the action sequence itself. Alice and Bob's objective is to *evade* Eve by making Eve's decision as poor as possible while maintaining a desired accuracy for their own estimation; we call this problem *evasive active hypothesis testing*. Formally, for any $i \in \Theta$, Alice and Bob's probability of incorrectly deciding on $\delta(y^\tau) = i$ when $\theta \neq i$ should satisfy the risk constraints

$$\sum_{j\neq i} \pi_j \mathbb{P}_j\{\delta(y^\tau) = i\} < \bar{R}_i, \tag{3}$$

where $\mathbb{P}_i$ denotes the probability measure under hypothesis $i$ and the thresholds $\{\bar{R}_i\}_{i=0}^{M-1}$ are fixed and known. For simplicity, we assume in the following that all $\{\bar{R}_i\}_{i=0}^{M-1}$ are the same and equal to $\bar{R}$. Eve is assumed to apply a maximum-likelihood detector $\delta_{\mathrm{ML}}$ when Alice and Bob stop the test at time $\tau$, i.e.,

$$\delta_{\mathrm{ML}}(z^\tau) = \arg\max_i \prod_{k=1}^{\tau} q_i^{u_k}(z_k).$$

Under the test $\Gamma$ and the constraint $\bar{R}$, the ratio between the error exponent of Eve to that of Alice/Bob when the true hypothesis is $\theta = i$ is defined as

$$\gamma_i(\Gamma, \bar{R}) \triangleq \frac{-\log \mathbb{P}_i\{\delta_{\mathrm{ML}}(z^\tau) \neq i\}}{|\log \bar{R}|}. \tag{4}$$

The quantity $\gamma_i(\Gamma, \bar{R})$ captures the rate of exponential decay of Eve's probability of error when decreasing the value of $\bar{R}$. Alice and Bob's objective is to minimize the exponent ratio (4) subject to the constraints (3), i.e.,

$$\begin{aligned} \underset{\phi}{\text{minimize}} \quad & \gamma_i(\Gamma, \bar{R}) \\ \text{subject to} \quad & \sum_{k\neq j} \pi_k \mathbb{P}_k\{\delta(y^\tau) = j\} < \bar{R} \quad \text{for all } j \in \Theta. \end{aligned} \tag{5}$$

In the problem above, the minimization is taken over all control policies $\phi$ while fixing the stopping rule $\tau$ and the decision rule $\delta$ as in (1) and (2), respectively. Note that minimizing $\gamma_i(\Gamma, \bar{R})$ amounts to finding the specific tradeoff between Eve and Alice/Bob's error exponents that minimizes the ratio of the error exponents. One could extend the analysis to a complete tradeoff curve but this is outside the scope of the present work.

*Remark 1:* Eve's optimal test given her observations $z^\tau$, the sequence $u^\tau$, and her knowledge of the prior $\{\pi_i\}_{i\in\Theta}$ is a maximum a posteriori (MAP) detection. However, the MAP estimators of Alice/Bob and Eve have the form $\delta_{\mathrm{MAP}}(y^\tau) = \arg\max_{i\in\Theta} \pi_i \prod_{k=1}^{\tau} p_i^{u_k}(y_k|y_{k-1})$ and $\delta_{\mathrm{MAP}}(z^\tau) = \arg\max_{i\in\Theta} \pi_i \prod_{k=1}^{\tau} q_i^{u_k}(z_k)$. The likelihoods $\prod_{k=1}^{\tau} p_i^{u_k}(y_k|y_{k-1})$ and $\prod_{k=1}^{\tau} q_i^{u_k}(z_k)$ have dominant influences on the outcome of the corresponding MAP estimator when $\tau \to \infty$, which is the regime we want to analyze. Therefore, we assume an ML estimator is utilized by Alice/Bob and Eve to simplify the analysis. Furthermore, if Alice/Bob and Eve choose to use a MAP estimator, our characterization of $\gamma_i$ holds, because changing from an ML to a MAP estimator does not influence the error exponent $\lim_{\tau\to\infty} -\frac{1}{\tau}\log(\mathbb{P}_i(\delta_{\mathrm{ML}}(z^\tau) \neq i))$ and the relationship between the stopping time $\tau$ and $\bar{R}$ is only related to the stopping rule in (1) but not to Bob's estimator of $\theta$.

*Remark 2:* The control policies $\phi$ have to operate *without* the knowledge of the true value of the parameter $\theta$.

Upon denoting by $\gamma_i(\bar{R})$ the solution to the optimization problem (5), we define the asymptotic error exponent ratio as

$$\gamma_i \triangleq \lim_{\bar{R}\to 0} \gamma_i(\bar{R}).$$

Our results provide upper and lower bounds for the asymptotic error exponent ratio $\gamma_i$.

### A. Bounds on the Asymptotic Error Exponent Ratio

By [17], the constraint in (5) is automatically satisfied when the stopping rule is defined by (1) with $b_i = \log(1/\bar{R}) + K$ and $K \triangleq \log(M-1) + \max_{i\in\Theta}\log(\pi_i)$. Therefore, we focus on the characterization of the asymptotic error exponent ratio when $\bar{R} \to 0$, which we bound in the following theorems.

*Theorem 1:* No control policy $\phi$ can lower the asymptotic error exponent ratio $\gamma_i$ when $\theta = i \in \Theta$ below

$$\min_{\tilde{q}_{U,Y}} \frac{\tilde{C}}{\tilde{D}}\sqrt{\frac{\tilde{D}^2}{\tilde{D}^2 + 2\tilde{C}\tilde{d}^2}} + \frac{\tilde{D}}{2\tilde{d}^2}\left(\frac{2\left(\tilde{D}^2 + \tilde{C}\tilde{d}^2\right)}{\sqrt{\tilde{D}^2\left(\tilde{D}^2 + 2\tilde{C}\tilde{d}^2\right)}} - 2\right), \tag{6}$$

where $\tilde{C}$, $\tilde{D}$, and $\tilde{d}$ are defined as

$$\begin{aligned} \tilde{C} &\triangleq \min_{j\neq i} C(q_i\|q_j; \bar{q}_U), \\ \tilde{D} &\triangleq \min_{j\neq i} \sum_{u\in\mathcal{U}, y\in\mathcal{Y}} \bar{q}_{U,Y}(u,y) D\left(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\right), \\ \tilde{d} &\triangleq \max_{j\neq i} \max_{u,y,\tilde{y}} \left|\log\frac{p_i^u(y|\tilde{y})}{p_j^u(y|\tilde{y})} - D\left(p_i^u(\cdot|\tilde{y})\|p_j^u(\cdot|\tilde{y})\right)\right|. \end{aligned}$$

*Theorem 2:* There exists a control policy such that the asymptotic error exponent ratio $\gamma_i$ when $\theta = i \in \Theta$ is at most

$$\min_{\{q(u|y)\}_{y\in\mathcal{Y}}} \frac{\min_{j\neq i}\sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^q(y) q(u|y) C\left(q_i^u\|q_j^u\right)}{\min_{j\neq i}\sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^q(y) q(u|y) D\left(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\right)}, \tag{7}$$

where $u_i^q(y)$ is the steady state distribution of the Markov process characterized by the transition probability

$$p^q(y|\tilde{y}) = \sum_{u\in\mathcal{U}} q(u|\tilde{y}) p_i^u(y|\tilde{y}).$$

Although the bounds of Theorem 1 and Theorem 2 do not match in general, these bounds are quite tight when the ratio of the divergence of Bob's kernels to the Chernoff information of Eve's kernels is large. To be specific, the ratio $\sqrt{\frac{\tilde{D}^2}{\tilde{D}^2+2\tilde{C}\tilde{d}^2}}$ in (9) approaches 1 and the term $(\frac{2(\tilde{D}^2+\tilde{C}\tilde{d}^2)}{\sqrt{\tilde{D}^2(\tilde{D}^2+2\tilde{C}\tilde{d}^2)}}-2)$ approaches 0 when $\tilde{D} \gg \tilde{C}$, which is the situation that benefits Alice and Bob. Therefore, when $\tilde{D} \gg \tilde{C}$, the lower bound of $\gamma_i$ approaches $\min_{\bar{q}_{U,Y}\in\mathcal{P}(\mathcal{U},\mathcal{Y})} \frac{\tilde{C}}{\tilde{D}}$, which is equivalent to

$$\min_{\bar{q}_{U,Y}\in\mathcal{P}(\mathcal{U},\mathcal{Y})} \frac{\min_{j\neq i} C\big(q_i\|q_j;\bar{q}_U\big)}{\min_{j\neq i}\sum_{u\in\mathcal{U},y\in\mathcal{Y}}\bar{q}_{U,Y}(u,y)D\Big(p_i^u(\cdot|y)||p_j^u(\cdot|y)\Big)}. \tag{8}$$

The above quantity has a form similar to the upper bound in Theorem 2. The gap between the above equation and the upper bound in Theorem 2 has two causes. First, $C(q_i||q_j;\bar{q}_U)$ is smaller than $\sum_{u\in\mathcal{U}}\bar{q}_U(u)C(q_i^u||q_j^u)$ by definition. Secondly, (8) is minimized over all joint distribution $\bar{q}_{U,Y} \in \mathcal{P}(\mathcal{U},\mathcal{Y})$, while (7) is only minimized over conditional distributions $\{q(u|y)\}_{y\in\mathcal{Y}} \in \mathcal{P}(\mathcal{U})^{|\mathcal{Y}|}$. If we restrict ourselves to the special case in which the kernels of Bob are independent of past observations conditioned on each action and the minimization of (6) and (7) are achieved by a deterministic policy $q(u) = 1(u = u^*)$ for some $u^* \in \mathcal{U}$, then (8) becomes

$$\min_{u\in\mathcal{U}} \frac{\min_{j\neq i} C\Big(q_i^u||q_j^u\Big)}{\min_{j\neq i} D\Big(p_i^u||p_j^u\Big)}.$$

In this case, the lower bound is the same as the upper bound obtained in Theorem 2.

*Remark 3:* If we restrict ourselves to the special case in which the kernels of Bob are independent of past observations conditioned on each action and if the asymptotically optimal control policy of [17], which ignores Eve's presence, is chosen, then the asymptotic value of $\gamma_i(\Gamma,\bar{R})$ under this control policy is

$$\frac{\min_{j\neq i} C\Big(q_i^{u_i^\#}\|q_j^{u_i^\#}\Big)}{\min_{j\neq i} D\Big(p_i^{u_i^\#}\|p_j^{u_i^\#}\Big)}, \tag{9}$$

where

$$u_i^\# = \arg\max_{u\in\mathcal{U}} \min_{j\neq i} D\Big(p_i^u\|p_j^u\Big).$$

In general, the asymptotic ML exponent in (9) is higher than the one achieved in Theorem 2. Note that one can obtain the result of (9) by replacing the control policy in the proof of Theorem 2 with the one described in [17].

### B. Numerical Example

As an illustration, we apply our results to the detection of a base station in a millimeter wave environment, in which the base station (Alice) is equipped with $N = 8$ antennas while two terminals (Bob and Eve) are each equipped with a single antenna. Bob and Eve have to decide whether Alice is transmitting (hypothesis $H_0$) or not (hypothesis $H_1$). The channel gains $\mathbf{h}$ and $\mathbf{g}$ characterizing the channels from the base station to Bob and Eve, respectively, are assumed to correspond to a single path and given by

$$\mathbf{h} = \rho_{\text{Bob}}\mathbf{a}^H(\theta_{\text{Bob}}) \quad \mathbf{g} = \rho_{\text{Eve}}\mathbf{a}^H(\theta_{\text{Eve}}),$$

where $\rho_{\text{Bob}}$ and $\rho_{\text{Eve}}$ are static fading coefficients and $\theta_{\text{Bob}}$ and $\theta_{\text{Eve}}$ are the Angle of Departure (AoD) vectors from the base station. Assuming uniform linear arrays (ULA) are used for beamforming, the vector $\mathbf{a}(\theta)$ can be written as

$$\mathbf{a}(\theta) = \Big[1, e^{-j\frac{2\pi d}{\lambda}\sin(\theta)}, \ldots, e^{-j(N-1)\frac{2\pi d}{\lambda}\sin(\theta)}\Big]^T,$$

where we choose $d = \lambda/2$ to be the space between antennas. The actions of Alice consist in choosing a steering vector $\mathbf{u}$ in a codebook $\mathcal{U} = \{\mathbf{u}_k\}_{k=0}^5$, where we have chosen for our example

$$\mathbf{u}_k = \Big[1, e^{-j\pi\sin(\pi k/12)}, \ldots, e^{-j(N-1)\pi\sin(\pi k/12)}\Big]^T.$$

In other words, Alice's action consists in steering and aligning her beam with $\mathbf{a}(\theta)$, for pre-specified angles $\theta \in \Big\{0, \frac{\pi}{12}, \ldots, \frac{5\pi}{12}\Big\}$. For each action $\mathbf{u} \in \mathcal{U}$, Bob and Eve's received signals under hypotheses $H_0$ and $H_1$ are

$$H_0 : \begin{cases} \tilde{y} = \rho_{\text{Bob}}\mathbf{a}(\theta_{\text{Bob}})^H\mathbf{u} + n_1 \\ \tilde{z} = \rho_{\text{Eve}}\mathbf{a}(\theta_{\text{Eve}})^H\mathbf{u} + n_2 \end{cases}$$
$$H_1 : \begin{cases} \tilde{y} = n_1 \\ \tilde{z} = n_2 \end{cases}$$

where $n_1, n_2$ are zero-mean circularly symmetric Gaussian noises with variance $\sigma^2$. We finally assume both Bob and Eve test the hypothesis with hard-decoded signal

$$y \triangleq \big|\tilde{y} - \rho_{\text{Bob}}\mathbf{a}(\theta_{\text{Bob}})^H\mathbf{u}\big| \underset{1}{\overset{0}{\gtrless}} |\tilde{y}|$$
$$\text{and } z \triangleq \big|\tilde{z} - \rho_{\text{Eve}}\mathbf{a}(\theta_{\text{Eve}})^H\mathbf{u}\big| \underset{1}{\overset{0}{\gtrless}} |\tilde{z}|,$$

so that $\mathcal{Y} = \mathcal{Z} = \{0,1\}$. Consequently, Bob's kernels corresponding to $\mathbf{u} \in \mathcal{U}$ are given under hypotheses $H_0$ and $H_1$ as

$$H_0 : \begin{cases} p_0^u(0) = 1 - Q\left(\sqrt{\frac{|\rho_{\text{Bob}}\mathbf{a}(\theta_{\text{Bob}})^H\mathbf{u}|^2}{2\sigma^2}}\right) \\ p_0^u(1) = Q\left(\sqrt{\frac{|\rho_{\text{Bob}}\mathbf{a}(\theta_{\text{Bob}})^H\mathbf{u}|^2}{2\sigma^2}}\right) \end{cases}$$
$$H_1 : \begin{cases} p_1^u(0) = Q\left(\sqrt{\frac{|\rho_{\text{Bob}}\mathbf{a}(\theta_{\text{Bob}})^H\mathbf{u}|^2}{2\sigma^2}}\right) \\ p_1^u(1) = 1 - Q\left(\sqrt{\frac{|\rho_{\text{Bob}}\mathbf{a}(\theta_{\text{Bob}})^H\mathbf{u}|^2}{2\sigma^2}}\right) \end{cases},$$

where $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty \exp(-\frac{u^2}{2})du$. Eve's kernels $q_i^u(z)$, $i \in \{0,1\}$ are similarly defined using $\rho_{\text{Eve}}\mathbf{a}(\theta_{\text{Eve}})$ in place of $\rho_{\text{Bob}}\mathbf{a}(\theta_{\text{Bob}})$.

Fig. 2 illustrates the asymptotic exponent ratio $\gamma_1$ in the specific case where the azimuth angles are $\theta_{\text{Bob}} = \frac{2\pi}{9}$, $\theta_{\text{Eve}} = \frac{\pi}{3}$, the noise variance is $\sigma^2 = 0.1$, and Bob's path loss is $\rho_{\text{Bob}} = 1$. The bounds for the asymptotic exponent ratio given by Theorem 1 and Theorem 2 are shown as a function of

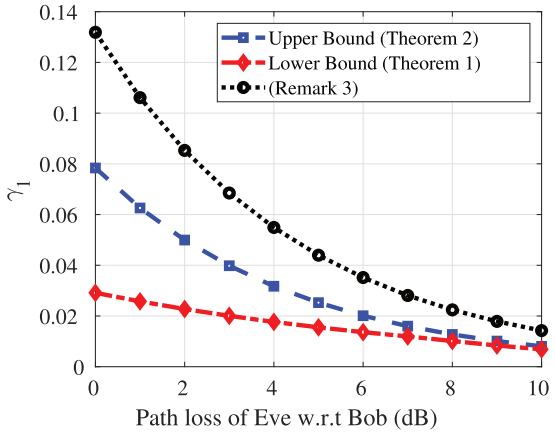


Fig. 2. Asymptotic exponent ratio $\gamma_1$ in the millimeter wave base station detecting problem.

Eve's path loss, defined as $10\log\frac{\rho_{\text{Bob}}}{\rho_{\text{Eve}}}$; the asymptotic exponent ratio from Remark 3, obtained when Bob chooses the control policy that only benefits himself and ignores Eve, is also shown as a reference. As expected, we observe that the gap between the two bounds becomes smaller when Eve's path loss increases because the ratio of Eve's Chernoff information to Bob's divergence dominates the right-hand side of (6).

## III. Proofs of Main Results

### A. Proof of Theorem 1 (Lower Bound)

Let $\bar{q}_{U,Y}$ be an arbitrary joint distribution on $\mathcal{U}$ and $\mathcal{Y}$, and $\bar{q}_U$ be the corresponding marginal distribution on $\mathcal{U}$. For all $\bar{q}_{U,Y}\in\mathcal{P}(\mathcal{U},\mathcal{Y})$, we first define $\tau_i(\bar{q}_{U,Y})$ as

$$\tau_i\big(\bar{q}_{U,Y}\big)\triangleq\frac{\big|\log\bar{R}\big|}{\min_{j\neq i}\sum_{u\in\mathcal{U},y\in\mathcal{Y}}\bar{q}_{U,Y}(u,y)D\Big(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\Big)}.$$

Without loss of generality, we assume $\tau_i(\bar{q}_{U,Y})$ is an integer in the proof below. To prove Theorem 1, we first need an upper bound on the error probability with a fixed number of actions. From [20, Problem 10.20], we know that for all $i\neq j$ and $n\in\mathbb{Z}$, if the sequence of actions $u^n$ has the type $\bar{q}_U$, we can upper bound the error probability $\mathbb{P}_i(\delta_{\text{ML}}(z^n)=j|\hat{p}_{u^n}=\bar{q}_U)$ by

$$\begin{aligned}&\mathbb{P}_i\big(\delta_{\text{ML}}\big(z^n\big)=j|\hat{p}_{u^n}=\bar{q}_U\big)\\&\leq\exp\left(-n\max_{s\in[0,1]}-\sum_u\bar{q}_U(u)\log\sum_{z\in\mathcal{Z}}q_i^u(z)^sq_j^u(z)^{1-s}\right)\\&=\exp\big(-nC(q_i\|q_j;\bar{q}_U)\big),\end{aligned}$$

where

$$C\big(q_i\|q_j;\bar{q}_U\big)=\max_{s\in[0,1]}-\sum_u\bar{q}_U(u)\log\left(\sum_{z\in\mathcal{Z}}q_i^u(z)^sq_j^u(z)^{1-s}\right).$$

Then, we have

$$\begin{aligned}&\mathbb{P}_i\big(\delta_{\text{ML}}\big(z^n\big)\neq i|\hat{p}_{u^n}=\bar{q}_U\big)\\&=\sum_{j\neq i}\mathbb{P}_i\big(\delta_{\text{ML}}\big(z^n\big)=j|\hat{p}_{u^n}=\bar{q}_U\big)\\&\leq(M-1)\max_{j\neq i}\mathbb{P}_i\big(\delta_{\text{ML}}\big(z^n\big)=j|\hat{p}_{u^n}=\bar{q}_U\big)\\&\leq(M-1)\exp\left(-n\min_{j\neq i}C\big(q_i\|q_j;\bar{q}_u\big)\right).\end{aligned}\tag{10}$$

Furthermore, the following lemma with proofs given in Appendix A gives an upper bound on the joint probability of $\tau\leq\tau_i(\bar{q}_{U,Y})(1-\epsilon)$ and $\hat{p}_{u^\tau,y^\tau}=\bar{q}_{U,Y}$ for any $0<\epsilon<1$.

*Lemma 1:* Let the stopping rule $\tau$ of the sequential test be defined in (1), and $0<\epsilon<1$. Then, for $\bar{R}$ small enough, the joint probability of $\tau\leq\tau_i(\bar{q}_{U,Y})(1-\epsilon)$ and $\hat{p}_{u^\tau,y^\tau}=\bar{q}_{U,Y}$ satisfies

$$\begin{aligned}&\mathbb{P}_i\big\{\tau\leq\tau_i\big(\bar{q}_{U,Y}\big)(1-\epsilon),\hat{p}_{u^\tau,y^\tau}=\bar{q}_{U,Y}\big\}\\&\leq C\exp\left\{\frac{-|\log\bar{R}|^2\big(\epsilon^2+o(1)\big)}{2\sum_{\ell=1}^{\tau_i(\bar{q}_{U,Y})(1-\epsilon)}d_i^2}\right\},\end{aligned}$$

for some constant $C$, where

$$d_i=\max_{j\neq i}\max_{u,y,\tilde{y}}\left|\log\frac{p_i^u(y|\tilde{y})}{p_j^u(y|\tilde{y})}-D\Big(p_i^u(\cdot|\tilde{y})\|p_j^u(\cdot|\tilde{y})\Big)\right|.$$

Let $N$ be some integer to be defined later; we write the probability $\mathbb{P}_i(\delta_{\text{ML}}(z^\tau)\neq i)$ as

$$\begin{aligned}&\mathbb{P}_i\big(\delta_{\text{ML}}(z^\tau)\neq i\big)\\&=\sum_{\bar{q}_{U,Y}\in\mathcal{P}_N(\mathcal{U},\mathcal{Y})}\mathbb{P}_i\big\{\delta_{\text{ML}}\big(z^\tau\big)\neq i,\hat{p}_{u^\tau,y^\tau}=\bar{q}_{U,Y}\big\}\\&\quad+\sum_{\bar{q}_{U,Y}\notin\mathcal{P}_N(\mathcal{U},\mathcal{Y})}\mathbb{P}_i\big\{\delta_{\text{ML}}\big(z^\tau\big)\neq i,\hat{p}_{u^\tau,y^\tau}=\bar{q}_{U,Y}\big\}\\&\leq|\mathcal{P}_N(\mathcal{U},\mathcal{Y})|\max_{\bar{q}_{U,Y}\in\mathcal{P}(\mathcal{U},\mathcal{Y})}\mathbb{P}_i\big\{\delta_{\text{ML}}\big(z^\tau\big)\neq i,\hat{p}_{u^\tau,y^\tau}=\bar{q}_{U,Y}\big\}\\&\quad+\mathbb{P}_i\big\{\hat{p}_{u^\tau,y^\tau}\notin\mathcal{P}_N(\mathcal{U},\mathcal{Y})\big\}.\end{aligned}\tag{11}$$

The term $\mathbb{P}_i\{\delta_{\text{ML}}(z^\tau)\neq i,\hat{p}_{u^\tau,y^\tau}=\bar{q}_{U,Y}\}$ can be represented as

$$\begin{aligned}&\mathbb{P}_i\big\{\delta_{\text{ML}}\big(z^\tau\big)\neq i,\hat{p}_{u^\tau,y^\tau}=\bar{q}_{U,Y}\big\}\\&=\sum_{k=1}^{\infty}\mathbb{P}_i\big(\tau=k,\hat{p}_{u^\tau,y^\tau}=\bar{q}_{U,Y}\big)\\&\quad\times\mathbb{P}_i\Big(\delta_{\text{ML}}\big(z^k\big)\neq i|\hat{p}_{u^\tau,y^\tau}=\bar{q}_{U,Y},\tau=k\Big)\\&\leq\sum_{k=1}^{\tau_i(\bar{q}_{U,Y})-1}\mathbb{P}_i\big(\tau\leq\tau_i\big(\bar{q}_{U,Y}\big)(1-\epsilon_k),\hat{p}_{u^\tau,y^\tau}=\bar{q}_{U,Y}\big)\\&\quad\times\mathbb{P}_i\Big(\delta_{\text{ML}}\big(z^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_k)}\big)\neq i|\hat{p}_{u^\tau,y^\tau}=\bar{q}_{U,Y},\tau=k\Big)\\&\quad+\sum_{k=\tau_i(\bar{q}_{U,Y})}^{\infty}\mathbb{P}_i\big(\tau=k,\hat{p}_{u^\tau,y^\tau}=\bar{q}_{U,Y}\big)\\&\quad\times\mathbb{P}_i\Big(\delta_{\text{ML}}\big(z^k\big)\neq i|\hat{p}_{u^\tau,y^\tau}=\bar{q}_{U,Y},\tau=k\Big)\\&\leq\sum_{k=1}^{\tau_i(\bar{q}_{U,Y})-1}\mathbb{P}_i\big(\tau\leq\tau_i\big(\bar{q}_{U,Y}\big)(1-\epsilon_k),\hat{p}_{u^\tau,y^\tau}=\bar{q}_{U,Y}\big)\\&\quad\times\mathbb{P}_i\Big(\delta_{\text{ML}}\big(z^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_k)}\big)\neq i|\hat{p}_{u^\tau,y^\tau}=\bar{q}_{U,Y},\tau=k\Big)\\&\quad+\mathbb{P}_i\Big(\delta_{\text{ML}}\big(z^{\tau_i(\bar{q}_{U,Y})}\big)\neq i|\hat{p}_{u^\tau,y^\tau}=\bar{q}_{U,Y},\tau=\tau_i\big(\bar{q}_{U,Y}\big)\Big),\end{aligned}\tag{12}$$

where $\epsilon_k$ are chosen such that $\tau_i(\bar{q}_{U,Y})(1-\epsilon_k) = k$. Given the stopping time $\tau = k$ and the type $\hat{p}_{u^\tau,y^\tau} = \bar{q}_{U,Y}$, the error probability $\mathbb{P}_i(\delta_{\mathrm{ML}}(z^k) \neq i | \hat{p}_{u^\tau,y^\tau} = \bar{q}_{U,Y}, \tau = k)$ can be represented as (10), which is a decreasing function of the number of observations $k$. Therefore, (12) follows from upper bounding $\mathbb{P}_i(\delta_{\mathrm{ML}}(z^k) \neq i | \hat{p}_{u^\tau,y^\tau} = \bar{q}_{U,Y}, \tau = k)$ by $\mathbb{P}_i(\delta_{\mathrm{ML}}(z^{\tau_i(\bar{q}_{U,Y})}) \neq i | \hat{p}_{u^\tau,y^\tau} = \bar{q}_{U,Y}, \tau = \tau_i(\bar{q}_{U,Y}))$ for all $k \geq \tau_i(\bar{q}_{U,Y})$ and from bounding the probability $\sum_{k=\tau_i(\bar{q}(u,y))}^{\infty} \mathbb{P}_i(\tau = k, \hat{p}_{u^\tau,y^\tau} = \bar{q}_{U,Y})$ by 1. By (10) and Lemma 1, when $\bar{R}$ is small enough, each term in the summation of (12) can be bounded as

$$\begin{aligned}
&\mathbb{P}_i\big\{\tau \leq \tau_i(\bar{q}_{U,Y})(1-\epsilon_k), \hat{p}_{u^\tau,y^\tau} = \bar{q}_{U,Y}\big\} \\
&\quad \times \mathbb{P}_i\Big\{\delta_{\mathrm{ML}}\Big(z^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_k)}\Big) \neq i | \hat{p}_{u^\tau,y^\tau} = \bar{q}_{U,Y}, \tau = k\Big\} \\
&\leq C' \exp\left\{\frac{-\big|\log \bar{R}\big|^2 \epsilon_k^2}{2\sum_{\ell=1}^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_k)} d_i^2}\right\} \\
&\quad \times \exp\left\{\frac{-(1-\epsilon_k)\big|\log \bar{R}\big| \min_{j\neq i} C\big(q_i \| q_j; \bar{q}_U\big)}{\min_{j\neq i}\sum_{u\in\mathcal{U},y\in\mathcal{Y}} \bar{q}_{U,Y}(u,y) D\Big(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\Big)}\right\} \\
&\leq C' \exp\big\{-\big|\log \bar{R}\big| \tilde{\gamma}_i\big(\bar{q}_{U,Y}, \epsilon_k\big)\big\}
\end{aligned}$$

for some constant $C'$, where

$$\begin{aligned}
&\tilde{\gamma}_i\big(\bar{q}_{U,Y}, \epsilon_k\big) \\
&\triangleq \frac{\big|\log \bar{R}\big|\epsilon_k^2}{2\sum_{\ell=1}^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_k)} d_i^2} \\
&\quad + \frac{\min_{j\neq i} C\big(q_i\|q_j;\bar{q}_U\big)}{\min_{j\neq i}\sum_{u\in\mathcal{U},y\in\mathcal{Y}} \bar{q}_{U,Y}(u,y) D\Big(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\Big)}(1-\epsilon_k) \\
&= \frac{\min_{j\neq i}\sum_{u\in\mathcal{U},y\in\mathcal{Y}} \bar{q}_{U,Y}(u,y) D\Big(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\Big)}{2d_i^2} \frac{\epsilon_k^2}{1-\epsilon_k} \\
&\quad + \frac{\min_{j\neq i} C\big(q_i\|q_j;\bar{q}_U\big)}{\min_{j\neq i}\sum_{u\in\mathcal{U},y\in\mathcal{Y}} \bar{q}_{U,Y}(u,y) D\Big(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\Big)}(1-\epsilon_k).
\end{aligned}$$

Also, the last term on the right hand side of (12) can be upper bounded by

$$\begin{aligned}
&\mathbb{P}_i\Big(\delta_{\mathrm{ML}}\Big(z^{\tau_i(\bar{q}_{U,Y})}\Big) \neq i | \hat{p}_{u^\tau,y^\tau} = \bar{q}_{U,Y}, \tau = \tau_i\big(\bar{q}_{U,Y}\big)\Big) \\
&\quad \leq (M-1)\exp\big\{-|\log \bar{R}| \tilde{\gamma}_i\big(\bar{q}_{U,Y}, 0\big)\big\}.
\end{aligned}$$

Minimizing $\tilde{\gamma}_i(\bar{q}_{U,Y}, \epsilon_k)$ over $\epsilon_k \in [0,1]$, we obtain the worst case exponent ratio

$$\begin{aligned}
\tilde{\gamma}_i^*\big(\bar{q}_{U,Y}\big) &\triangleq \min_{\epsilon_k\in[0,1]} \tilde{\gamma}_i\big(\bar{q}_{U,Y}, \epsilon_k\big) \\
&\geq \frac{\tilde{C}}{\tilde{D}}\sqrt{\frac{\tilde{D}^2}{\tilde{D}^2 + 2\tilde{C}\tilde{d}^2}} \\
&\quad + \frac{\tilde{D}}{2\tilde{d}^2}\left(\frac{2\Big(\tilde{D}^2 + \tilde{C}\tilde{d}^2\Big)}{\sqrt{\tilde{D}^2\Big(\tilde{D}^2 + 2\tilde{C}\tilde{d}^2\Big)}} - 2\right), \quad (13)
\end{aligned}$$

where we define

$$\begin{aligned}
\tilde{C} &\triangleq \min_{j\neq i} C\big(q_i\|q_j;\bar{q}_U\big), \\
\tilde{D} &\triangleq \min_{j\neq i} \sum_{u\in\mathcal{U},y\in\mathcal{Y}} \bar{q}_{U,Y}(u,y) D\Big(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\Big), \\
\tilde{d} &\triangleq d_i,
\end{aligned}$$

and the value of $\epsilon_k$ minimizing (13) is

$$\epsilon^* = 1 - \sqrt{\frac{\tilde{D}^2}{\tilde{D}^2 + 2\tilde{C}\tilde{d}^2}}.$$

Therefore,

$$\begin{aligned}
&\lim_{\bar{R}\to 0} \frac{-\log\big(\max_{\bar{q}_{U,Y}} \mathbb{P}_i\big\{\delta_{\mathrm{ML}}(z^\tau) \neq i, \hat{p}_{u^\tau,y^\tau} = \bar{q}_{U,Y}\big\}\big)}{\big|\log \bar{R}\big|} \\
&\quad \geq \min_{\bar{q}_{U,Y}} \frac{\tilde{C}}{\tilde{D}}\sqrt{\frac{\tilde{D}^2}{\tilde{D}^2 + 2\tilde{C}\tilde{d}^2}} + \frac{\tilde{D}}{2\tilde{d}^2}\left(\frac{2\Big(\tilde{D}^2 + \tilde{C}\tilde{d}^2\Big)}{\sqrt{\tilde{D}^2\Big(\tilde{D}^2 + 2\tilde{C}\tilde{d}^2\Big)}} - 2\right) \\
&\quad \triangleq \gamma_i^*.
\end{aligned}$$

Since $|\mathcal{P}_N(\mathcal{U},\mathcal{Y})|$ is a polynomial function of $N$, the scaling of $|\mathcal{P}_N(\mathcal{U},\mathcal{Y})|$ does not change the exponent. Therefore, from (11), if we can find some $\alpha$ such that when $N = |\log \bar{R}|\alpha$, the ratio $\lim_{\bar{R}\to 0} \frac{-\log \mathbb{P}_i\{\hat{p}_{u^\tau,y^\tau} \notin \mathcal{P}_N(\mathcal{U},\mathcal{Y})\}}{|\log \bar{R}|}$ is greater than $\gamma_i^*$, then

$$\lim_{\bar{R}\to 0} \frac{-\log(\mathbb{P}_i(\delta_{\mathrm{ML}}(z^\tau) \neq i))}{|\log \bar{R}|} \geq \gamma_i^*. \quad (14)$$

Let $N = \frac{|\log \bar{R}|\beta}{\min_{j'\neq i} \min_{q_{U,Y}} \sum_{u\in\mathcal{U},y\in\mathcal{Y}} q_{U,Y}(u,y) D(p_i^u(\cdot|y)\|p_{j'}^u(\cdot|y))}$ for some $\beta > 1$, then

$$\begin{aligned}
&\mathbb{P}_i\big\{\hat{p}_{u^\tau,y^\tau} \notin \mathcal{P}_N(\mathcal{U},\mathcal{Y})\big\} \\
&\quad \leq \mathbb{P}_i(\tau > N) \\
&\quad \leq \sum_{j\neq i} \mathbb{P}_i\left\{\log \frac{p_i(y^N)}{p_j(y^N)} < b_i\right\} \\
&\quad = \sum_{j\neq i} \mathbb{P}_i\Bigg\{\sum_{k=1}^N \log \frac{p_i^{u_k}(y_k|y_{k-1})}{p_j^{u_k}(y_k|y_{k-1})} \\
&\qquad\qquad - \sum_{k=1}^N D\Big(p_i^{u_k}(\cdot|y_{k-1})\|p_j^{u_k}(\cdot|y_{k-1})\Big) \\
&\qquad\qquad < b_i - \sum_{k=1}^N D\Big(p_i^{u_k}(\cdot|y_{k-1})\|p_j^{u_k}(\cdot|y_{k-1})\Big)\Bigg\} \\
&\quad \leq \sum_{j\neq i} \mathbb{P}_i\Bigg\{\sum_{k=1}^N \log \frac{p_i^{u_k}(y_k|y_{k-1})}{p_j^{u_k}(y_k|y_{k-1})} \\
&\qquad\qquad - \sum_{k=1}^N D\Big(p_i^{u_k}(\cdot|y_{k-1})\|p_j^{u_k}(\cdot|y_{k-1})\Big) \\
&\qquad\qquad < b_i - N \min_{j'\neq i} \min_{q(u,y)\in\mathcal{P}(\mathcal{U},\mathcal{Y})} \\
&\qquad\qquad \times \sum_{u\in\mathcal{U},y\in\mathcal{Y}} q(u,y) D\Big(p_i^u(\cdot|y)\|p_{j'}^u(\cdot|y)\Big)\Bigg\}
\end{aligned}$$

$$\le \sum_{j\neq i}\mathbb{P}_i\left\{\left|\sum_{k=1}^{N}\log\frac{p_i^{u_k}(y_k|y_{k-1})}{p_j^{u_k}(y_k|y_{k-1})} - \sum_{k=1}^{N}D\Big(p_i^{u_k}(\cdot|y_{k-1})\|p_j^{u_k}(\cdot|y_{k-1})\Big)\right| > N\min_{j'\neq i}\min_{q_{U,Y}\in\mathcal{P}(\mathcal{U},\mathcal{Y})} \times \sum_{u\in\mathcal{U},y\in\mathcal{Y}} q_{U,Y}(u,y)D\Big(p_i^u(\cdot|y)\|p_{j'}^u(\cdot|y)\Big) - b_i\right\}$$

$$\le 2(M-1)\exp\left\{-\frac{|\log\bar{R}|^2(\beta-1-o(1))^2}{2Nd_i^2}\right\}, \tag{15}$$

where (15) is from Azuma inequality. Therefore, the exponent

$$\lim_{\bar{R}\to 0}\frac{-\log\mathbb{P}\big(\hat{p}_{u^\tau,y^\tau}\notin\mathcal{P}_N(\mathcal{U},\mathcal{Y})\big)}{|\log\bar{R}|} > \frac{(\beta-1)^2}{2\beta} \times \frac{\min_{j'\neq i}\min_{q_{U,Y}\in\mathcal{P}(\mathcal{U},\mathcal{Y})}\sum_{u\in\mathcal{U},y\in\mathcal{Y}} q_{U,Y}(u,y)D\Big(p_i^u(\cdot|y)\|p_{j'}^u(\cdot|y)\Big)}{d_i^2}. \tag{16}$$

We can choose $\beta$ properly such that the right hand side of (16) is greater than $\gamma_i^*$, and hence, (14) holds.

### B. Proof of Theorem 2 (Upper Bound)

Let the action $u_k$ be generated from the distribution $q^*_{\hat{i}_{k-1}}$, where $\hat{i}_{k-1}$ is the ML estimation of the true hypothesis at time $k-1$, and for all $i\in\Theta$, $q_i^*$ is defined as

$$q_i^* = \arg\min_{q(\cdot|\cdot)} \times \frac{\min_{j\neq i}\sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^q(y)q(u|y)C\Big(q_i^u\|q_j^u\Big)}{\min_{j\neq i}\sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^q(y)q(u|y)D\Big(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\Big)}. \tag{17}$$

Define $\tilde{\tau}_i$ as

$$\tilde{\tau}_i \triangleq \frac{|\log\bar{R}|}{\min_{j\neq i}\sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q_i^*}(y)q_i^*(u|y)D\Big(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\Big)}. \tag{18}$$

Define $N$ as the smallest number such that the decision $\delta_{\mathrm{ML}}(y^{n'})$ is correct for all $n'\ge N$. Then, we have the following lemma, which states that the stopping time concentrates around $\tilde{\tau}_i$.

*Lemma 2:* Let the control policy $\phi$ defined by (17) and the stopping rule $\tau$ defined by (1), $\forall\epsilon>0$ and $1>\epsilon'>0$, we have

$$\lim_{\bar{R}\to 0}\mathbb{P}_i\{\tau\le\tilde{\tau}_i(1+\epsilon)|N\le n\} = 1, \tag{19}$$

when $n$ is chosen such that $\mathbb{P}(N>n)\le\epsilon'$ and $\tilde{\tau}_i$ is defined in (18).

For all $\epsilon>0, 1>\epsilon'>0$ and $n$ chosen as in Lemma 2, assume without loss of generality $\tilde{\tau}_i(1+\epsilon)$ is integer, we can lower bound $\mathbb{P}_i(\delta_{\mathrm{ML}}(z^\tau)\neq i)$ by

$$\begin{aligned}
&\mathbb{P}_i\big(\delta_{\mathrm{ML}}(z^\tau)\neq i\big)\\
&\ge \mathbb{P}(N\le n)\mathbb{P}_i\big(\delta_{\mathrm{ML}}(z^\tau)\neq i|N\le n\big)\\
&= \mathbb{P}(N\le n)\\
&\quad\times\sum_{k=1}^{\infty}\mathbb{P}_i(\tau=k|N\le n)\mathbb{P}_i\Big(\delta_{\mathrm{ML}}\Big(z^k\Big)\neq i|\tau=k,N\le n\Big)\\
&\ge \mathbb{P}(N\le n)\sum_{k=1}^{\tilde{\tau}_i(1+\epsilon)}\mathbb{P}_i(\tau=k|N\le n)\\
&\quad\times\mathbb{P}_i\Big(\delta_{\mathrm{ML}}\Big(z^{\tilde{\tau}_i(1+\epsilon)}\Big)\neq i|\tau=\tilde{\tau}_i(1+\epsilon),N\le n\Big)\\
&\ge \big(1-\epsilon'\big)\mathbb{P}_i\{\tau\le\tilde{\tau}_i(1+\epsilon)|N\le n\}\\
&\quad\times\mathbb{P}_i\Big(\delta_{\mathrm{ML}}\Big(z^{\tilde{\tau}_i(1+\epsilon)}\Big)\neq i|\tau=\tilde{\tau}_i(1+\epsilon),N\le n\Big).
\end{aligned}$$

By Lemma 2, $\forall\epsilon,\tilde{\delta}>0$, there exists $\bar{R}$ small enough such that $\mathbb{P}_i\{\tau\le\tilde{\tau}_i(1+\epsilon)|N\le n\}>1-\tilde{\delta}$. Therefore, $\forall\epsilon,\tilde{\delta}>0$, we have

$$\mathbb{P}_i\big(\delta_{\mathrm{ML}}(z^\tau)\neq i\big)\ge\big(1-\epsilon'\big)\Big(1-\tilde{\delta}\Big)\times\mathbb{P}_i\Big(\delta_{\mathrm{ML}}\Big(z^{\tilde{\tau}_i(1+\epsilon)}\Big)\neq i|\tau=\tilde{\tau}_i(1+\epsilon),N\le n\Big)$$

when $\bar{R}$ is small enough. Let $\tilde{\delta}_{ij}$ be the binary maximum likelihood decision between any pair of hypothesis $(i,j)$, $j\neq i$, then it must be true that

$$\begin{aligned}
&\mathbb{P}_i\Big(\delta_{\mathrm{ML}}\Big(z^{\tilde{\tau}_i(1+\epsilon)}\Big)\neq i|\tau=\tilde{\tau}_i(1+\epsilon),N\le n\Big)\\
&\quad\ge\mathbb{P}_i\Big(\tilde{\delta}_{ij}\Big(z^{\tilde{\tau}_i(1+\epsilon)}\Big)\neq i|\tau=\tilde{\tau}_i(1+\epsilon),N\le n\Big).
\end{aligned}\tag{20}$$

Then, for $\bar{R}$ small enough, we can further rewrite the probability $\mathbb{P}_i(\tilde{\delta}_{ij}(z^{\tilde{\tau}_i(1+\epsilon)})\neq i|\tau=\tilde{\tau}_i(1+\epsilon),N\le n)$ as

$$\begin{aligned}
&\mathbb{P}_i\Big(\tilde{\delta}_{ij}\Big(z^{\tilde{\tau}_i(1+\epsilon)}\Big)\neq i|\tau=\tilde{\tau}_i(1+\epsilon),N\le n\Big)\\
&=\mathbb{P}_i\Big(\tilde{\delta}_{ij}\Big(z^{\tilde{\tau}_i(1+\epsilon)}\Big)=j|\tau=\tilde{\tau}_i(1+\epsilon),N\le n\Big)\\
&=\mathbb{P}_i\left\{\sum_{k=1}^{\tilde{\tau}_i(1+\epsilon)}\log\frac{q_i^{u_k}(z_k)}{q_j^{u_k}(z_k)}<0\middle|\tau=\tilde{\tau}_i(1+\epsilon),N\le n\right\}\\
&=\mathbb{P}_i\left\{\sum_{k=n+1}^{\tilde{\tau}_i(1+\epsilon)}\log\frac{q_i^{u_k}(z_k)}{q_j^{u_k}(z_k)}<\sum_{k=1}^{n}\log\frac{q_j^{u_k}(z_k)}{q_i^{u_k}(z_k)}\middle|N\le n,\tau=\tilde{\tau}_i(1+\epsilon)\right\}.
\end{aligned}\tag{21}$$

Note that (21) can be viewed as the error probability of testing between hypotheses $i$ and $j$ with kernel distributions $\{q_i^{u_k}\}_{k=n+1}^{\tilde{\tau}_i(1+\epsilon)}$ and $\{q_j^{u_k}\}_{k=n+1}^{\tilde{\tau}_i(1+\epsilon)}$ by using the likelihood ratio test with the threshold $T=\sum_{k=1}^{n}\log\frac{q_j^{u_k}(z_k)}{q_i^{u_k}(z_k)}$. Furthermore, conditioned on the event $N\le n$, the actions $u_k$ are generated from $q_i^*$ for all $k>n$. We know that the likelihood ratio test

$$\sum_{k=n+1}^{\tilde{\tau}_i(1+\epsilon)} \log \frac{q_i^{u_k}(z_k)}{q_j^{u_k}(z_k)} > T$$

is equivalent to

$$\sum_{u\in\mathcal{U}} \hat{p}_{u_{n+1}^{\tilde{\tau}_i(1+\epsilon)}}(u)\left(D\left(\hat{p}_{z_{n+1}^{\tilde{\tau}_i(1+\epsilon)}|u}\|q_j^u\right) - D\left(\hat{p}_{z_{n+1}^{\tilde{\tau}_i(1+\epsilon)}|u}\|q_i^u\right)\right) > \frac{T}{\tilde{\tau}_i(1+\epsilon)-n},$$

where $\hat{p}_{u_{n+1}^{\tilde{\tau}_i(1+\epsilon)}}$ is the type of the action sequence $u_{n+1}^{\tilde{\tau}_i(1+\epsilon)} \triangleq (u_{n+1},\ldots,u_{\tilde{\tau}_i(1+\epsilon)})$, and $\hat{p}_{z_{n+1}^{\tilde{\tau}_i(1+\epsilon)}|u}$ is the conditional type of the sequence $z_{n+1}^{\tilde{\tau}_i(1+\epsilon)}$ given the action $u$. Notice that the threshold

$$\frac{T}{\tilde{\tau}_i(1+\epsilon)-n} \to 0$$

when $\tilde{\tau}_i \to \infty$. Then, from Appendix C and the fact that $u_k$ is generated from $q_i^*$ for all $k > n$, the error exponent $\alpha_{ij}$ can be described as

$$\alpha_{ij} \triangleq \lim_{\tilde{\tau}_i\to\infty} \frac{-1}{\tilde{\tau}_i(1+\epsilon)} \log \mathbb{P}_i\left(\tilde{\delta}_{ij}\left(z^{\tilde{\tau}_i(1+\epsilon)}\right)=j\right) \le \sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) C\left(q_i^u\|q_j^u\right). \tag{22}$$

Therefore,

$$\lim_{\bar{R}\to 0} \frac{-1}{|\log \bar{R}|} \log \mathbb{P}_i\left(\tilde{\delta}_{ij}\left(z^{\tilde{\tau}_i(1+\epsilon)}\right)=j\right) \le \frac{\sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) C\left(q_i^u\|q_j^u\right)(1+\epsilon)}{\min_{j\neq i}\sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) D\left(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\right)}.$$

From (20), under the control policy $\phi$ defined in (17), we have

$$\lim_{\bar{R}\to 0} \frac{-1}{|\log \bar{R}|} \log \mathbb{P}_i\left(\delta_{\mathrm{ML}}\left(z^{\tilde{\tau}_i(1+\epsilon)}\right)\neq i\right) \le \frac{\min_{j\neq i}\sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) C\left(q_i^u\|q_j^u\right)(1+\epsilon)}{\min_{j\neq i}\sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) D\left(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\right)}.$$

Since $\epsilon > 0$ can be arbitrary small, we have

$$\gamma_i \le \frac{\min_{j\neq i}\sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) C\left(q_i^u\|q_j^u\right)}{\min_{j\neq i}\sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) D\left(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\right)} = \min_{q(\cdot|\cdot)} \frac{\min_{j\neq i}\sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q}(y) q(u|y) C\left(q_i^u\|q_j^u\right)}{\min_{j\neq i}\sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q}(y) q(u|y) D\left(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\right)}.$$

## IV. Conclusion

While the information leakage resulting from actions taken by decision makers in a complex system might be unavoidable, our results suggest that, as long as there exists some margin in the system to meet performance objectives, the margin can be exploited to develop leakage-aware strategies that incur less leakage than the otherwise optimal strategies developed for performance alone. Specifically, in the context of the evasive active hypothesis testing studied here, we have shown that the error exponent of an eavesdropper who obtains observations whenever an action is taken can be near-optimally reduced with proper strategies. We emphasize that this ability stems from the interplay between i) the presence of a noisy observation structure, by which the eavesdropper obtains signal that are different from those of the decision maker; and ii) the inherent information asymmetry of the problem, which gives the decision maker an advantage because it controls the feedback mechanisms. Extension of these ideas to more complex situations in which the adversary might tamper with signals are natural but challenging avenues for future work.

## Appendix A
## Proof of Lemma 1

*Proof:* Recall that the test stops at time $n$ when

$$\log\left(\frac{p_{\tilde{i}}(y^n)}{\max_{j\neq\tilde{i}} p_j(y^n)}\right) \ge b_{\tilde{i}} \tag{23}$$

for some $\tilde{i}\in\Theta$. Then,

$$\mathbb{P}_i\left\{\tau \le \tau_i(\bar{q}_{U,Y})(1-\epsilon), \hat{p}_{u^\tau,y^\tau} = \bar{q}_{U,Y}\right\} \le \sum_{\tilde{i}\in\Theta} \mathbb{P}_i\left\{\exists n \le \tau_i(\bar{q}_{U,Y})(1-\epsilon) \text{ s.t } \log\left(\frac{p_{\tilde{i}}(y^n)}{\max_{j\neq\tilde{i}} p_j(y^n)}\right) \ge b_{\tilde{i}} \text{ and } \hat{p}_{u^n,y^n} = \bar{q}_{U,Y}\right\}.$$

We first focus on the case where (23) is satisfied with $\tilde{i} = i$. For all $n > 0$, we can write the generalized log likelihood ratio as

$$\begin{aligned}\log\left(\frac{p_i(y^n)}{\max_{j\neq i} p_j(y^n)}\right) &= \min_{j\neq i}\sum_{k=1}^n \log\left(\frac{p_i^{u_k}(y_k|y_{k-1})}{p_j^{u_k}(y_k|y_{k-1})}\right)\\ &= \min_{j\neq i}\left\{\sum_{k=1}^n\left[\log\left(\frac{p_i^{u_k}(y_k|y_{k-1})}{p_j^{u_k}(y_k|y_{k-1})}\right) - D\left(p_i^{u_k}(\cdot|y_{k-1})\|p_j^{u_k}(\cdot|y_{k-1})\right)\right] + \sum_{k=1}^n D\left(p_i^{u_k}(\cdot|y_{k-1})\|p_j^{u_k}(\cdot|y_{k-1})\right)\right\},\end{aligned}$$

where the term

$$\frac{1}{n}\sum_{k=1}^n\left[\log\left(\frac{p_i^{u_k}(y_k|y_{k-1})}{p_j^{u_k}(y_k|y_{k-1})}\right) - D\left(p_i^{u_k}(\cdot|y_{k-1})\|p_j^{u_k}(\cdot|y_{k-1})\right)\right]$$

converges to zero exponentially fast. To be specific, let

$$X_\ell \triangleq \sum_{k=1}^\ell\left[\log\left(\frac{p_i^{u_k}(y_k|y_{k-1})}{p_j^{u_k}(y_k|y_{k-1})}\right) - D\left(p_i^{u_k}(\cdot|y_{k-1})\|p_j^{u_k}(\cdot|y_{k-1})\right)\right]$$

be the zero-mean martingale sequence such that

$$\begin{aligned}|X_\ell - X_{\ell-1}| &= \left|\log\frac{p_i^{u_\ell}(y_\ell|y_{\ell-1})}{p_j^{u_\ell}(y_\ell|y_{\ell-1})} - D\Big(p_i^{u_\ell}(\cdot|y_{\ell-1})\|p_j^{u_\ell}(\cdot|y_{\ell-1})\Big)\right| \\ &\le \max_{u,y,\tilde{y}}\left|\log\frac{p_i^u(y|\tilde{y})}{p_j^u(y|\tilde{y})} - D\Big(p_i^u(\cdot|\tilde{y})\|p_j^u(\cdot|\tilde{y})\Big)\right| \\ &\triangleq d_{ij}.\end{aligned}$$

By Azuma's inequality, we have for all $j \neq i$ and $\forall\tilde{\epsilon} > 0$,

$$\mathbb{P}_i\{|X_n| \ge n\tilde{\epsilon}\} \le 2\exp\left(\frac{-n^2\tilde{\epsilon}^2}{2\sum_{\ell=1}^n d_{ij}^2}\right).$$

Define $j^* \triangleq \arg\min_{j\neq i}\sum_{u\in\mathcal{U},y\in\mathcal{Y}}\bar{q}(u,y)D(p_i^u(\cdot|y)\|p_j^u(\cdot|y))$. We have $\forall\tilde{\epsilon} > 0$,

$$\begin{aligned}&\mathbb{P}_i\left\{\log\left(\frac{p_i(y^n)}{\max_{j\neq i}p_j(y^n)}\right) > n\left(\frac{1}{n}\sum_{k=1}^n D\Big(p_i^{u_k}(\cdot|y_{k-1})\|p_{j^*}^{u_k}(\cdot|y_{k-1})\Big) + \tilde{\epsilon}\right)\right\} \\ &\le \mathbb{P}_i\left\{\log\left(\frac{p_i(y^n)}{p_{j^*}(y^n)}\right) > n\left(\frac{1}{n}\sum_{k=1}^n D\Big(p_i^{u_k}(\cdot|y_{k-1})\|p_{j^*}^{u_k}(\cdot|y_{k-1})\Big) + \tilde{\epsilon}\right)\right\} \\ &\le 2\exp\left(\frac{-n^2\tilde{\epsilon}^2}{2\sum_{\ell=1}^n d_i^2}\right), \qquad (24)\end{aligned}$$

where $d_i = \max_j d_{ij}$. Now, when $\tilde{i} = i$, we have

$$\begin{aligned}&\mathbb{P}_i\left\{\exists n \le \tau_i(\bar{q}_{U,Y})(1-\epsilon) \text{ s.t } \log\left(\frac{p_i(y^n)}{\max_{j\neq i}p_j(y^n)}\right) \ge b_i \text{ and } \hat{p}_{u^n,y^n} = \bar{q}_{U,Y}\right\} \\ &\le \sum_{\epsilon_n}\mathbb{P}_i\left\{\log\left(\frac{p_i\Big(y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}\Big)}{\max_{j\neq i}p_j\Big(y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}\Big)}\right) \ge b_i, \hat{p}_{u^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)},y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}} = \bar{q}_{U,Y}\right\}, \qquad (25)\end{aligned}$$

where for each $1 \le n \le \tau_i(\bar{q}_{U,Y})(1-\epsilon)$, $\epsilon_n > 0$ is chosen such that $n = \tau_i(\bar{q}_{U,Y})(1-\epsilon_n)$. Substituting the definition of $b_i$, when $\tau_i(\bar{q}_{U,Y})$ is large enough, each term in the summation of (25) can be written as

$$\begin{aligned}&\mathbb{P}_i\left\{\log\left(\frac{p_i\Big(y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}\Big)}{\max_{j\neq i}p_j\Big(y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}\Big)}\right) \ge |\log\bar{R}| + K, \hat{p}_{u^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)},y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}} = \bar{q}_{U,Y}\right\} \\ &\le \mathbb{P}_i\left\{\log\left(\frac{p_i\Big(y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}\Big)}{\max_{j\neq i}p_j\Big(y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}\Big)}\right) - \sum_{k=1}^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)} D\Big(p_i^{u_k}(\cdot|y_{k-1})\|p_{j^*}^{u_k}(\cdot|y_{k-1})\Big) \ge \epsilon_n'\right\}, \qquad (26)\end{aligned}$$

where

$$\begin{aligned}\epsilon_n' &= \big|\log\bar{R}\big| + K - \sum_{k=1}^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)} D\Big(p_i^{u_k}(\cdot|y_{k-1})\|p_{j^*}^{u_k}(\cdot|y_{k-1})\Big) \\ &= \tau_i(\bar{q}_{U,Y})\min_{j\neq i}\sum_{u\in\mathcal{U},y\in\mathcal{Y}}\bar{q}_{U,Y}(u,y)D\Big(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\Big) + K \\ &\quad -\tau_i(\bar{q}_{U,Y})(1-\epsilon_n) \\ &\quad \times \sum_{u\in\mathcal{U},y\in\mathcal{Y}}\hat{p}_{u^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)},y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}}(u,y) \\ &\quad \times D\Big(p_i^u(\cdot|y)\|p_{j^*}^u(\cdot|y)\Big), \qquad (27)\end{aligned}$$

where the joint type $\hat{p}_{u^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)},y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}} = \bar{q}_{U,Y}$ due to the second argument of the joint probability (26). Therefore, $\epsilon_n' = |\log\bar{R}|\epsilon_n + K > 0$. Then, from (24), we have

$$\begin{aligned}&\mathbb{P}_i\left\{\log\left(\frac{p_i\Big(y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}\Big)}{\max_{j\neq i}p_j\Big(y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}\Big)}\right) \ge |\log\bar{R}| + K, \hat{p}_{u^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)},y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}} = \bar{q}_{U,Y}\right\} \\ &\le 2\exp\left\{\frac{-|\log\bar{R}|^2\big({\epsilon_n}^2 + o(1)\big)}{2\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)d_i^2}\right\}\end{aligned}$$

Similarly, if (23) is satisfied with $\tilde{i} \neq i$, we can bound each corresponding term in the summation of (25) by

$$\begin{aligned}&\mathbb{P}_i\left\{\log\left(\frac{p_{\tilde{i}}\Big(y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}\Big)}{\max_{j\neq\tilde{i}}p_j\Big(y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}\Big)}\right) \ge |\log\bar{R}| + K, \hat{p}_{u^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)},y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}} = \bar{q}_{U,Y}\right\} \\ &\le \mathbb{P}_i\left\{\log\left(\frac{p_{\tilde{i}}\Big(y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}\Big)}{p_i\Big(y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}\Big)}\right) \ge |\log\bar{R}| + K, \hat{p}_{u^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)},y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}} = \bar{q}_{U,Y}\right\} \\ &\le \mathbb{P}_i\left\{\log\left(\frac{p_{\tilde{i}}\Big(y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}\Big)}{p_i\Big(y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}\Big)}\right) + \sum_{k=1}^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)} D\Big(p_i^{u_k}(\cdot|y_{k-1})\|p_{\tilde{i}}^{u_k}(\cdot|y_{k-1})\Big) \ge \epsilon_n''\right\},\end{aligned}$$

where

$$\begin{aligned}\epsilon_n'' &= \tau_i(\bar{q}_{U,Y}) \min_{j\neq i} \sum_{u\in\mathcal{U},y\in\mathcal{Y}} \bar{q}(u,y) D\Big(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\Big) + K \\ &\quad + \tau_i(\bar{q}_{U,Y})(1-\epsilon_n) \\ &\quad \times \sum_{u,y} \hat{p}_{u^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}, y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}}(u,y) \\ &\quad \times D\Big(p_i^u(\cdot|y)\|p_{\tilde{i}}^u(\cdot|y)\Big),\end{aligned}$$

which is larger than the one in (27) for all $\epsilon_n < 1$ by the definition of $j*$. Finally, as $\tau_i(\bar{q}_{U,Y})$ is large enough, we conclude that

$$\begin{aligned}&\mathbb{P}_i\big\{\tau \le \tau_i(\bar{q}_{U,Y})(1-\epsilon), \hat{p}_{u^\tau,y^\tau} = \bar{q}_{U,Y}\big\} \\ &\le \sum_{\epsilon_n} 2\exp\left\{\frac{-|\log\bar{R}|^2(\epsilon_n{}^2 + o(1))}{2\sum_{\ell=1}^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)} d_i^2}\right\} \\ &\quad + \sum_{\tilde{i}\neq i}\sum_{\epsilon_n} \mathbb{P}_i\left\{\log\left(\frac{p_{\tilde{i}}\Big(y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}\Big)}{\max_{j\neq\tilde{i}} p_j\Big(y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}\Big)}\right) \ge |\log\bar{R}| \right. \\ &\qquad \left. + K, \hat{p}_{u^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}, y^{\tau_i(\bar{q}_{U,Y})(1-\epsilon_n)}} = \bar{q}_{U,Y}\right\} \\ &\le C\exp\left\{\frac{-|\log\bar{R}|^2(\epsilon^2 + o(1))}{2\sum_{\ell=1}^{\tau_i(\bar{q}_{U,Y})(1-\epsilon)} d_i^2}\right\}, \qquad (28)\end{aligned}$$

for some constant $C > 0$, where (28) is from the fact that the addition of exponentially decreasing terms is dominated by the one with the smallest exponent. ∎

## Appendix B
## Proof of Lemma 2

*Proof:* From [17, eq. (63)], which states that $\mathbb{P}(N \ge n) = O(n^{-\Omega(1)})$, for all $1 > \epsilon' > 0$ we can choose $n$ large enough such that $\mathbb{P}_i(N > n) \le \epsilon'$. Note that for all $m \le n$,

$$\begin{aligned}\mathbb{P}N = m | N \le n &= \frac{\mathbb{P}N \le n | N = m \mathbb{P}N = m}{\mathbb{P}N \le n} \\ &\le \frac{\mathbb{P}N = m}{1-\epsilon'}.\end{aligned}$$

Then,

$$\begin{aligned}&\mathbb{P}(\tau > \tilde{\tau}_i(1+\epsilon) | N \le n) \\ &= \sum_{m=1}^{n} \mathbb{P}(\tau > \tilde{\tau}_i(1+\epsilon) | N = m, N \le n \mathbb{P}N = m | N \le n) \\ &= \sum_{m=1}^{n} \mathbb{P}(\tau > \tilde{\tau}_i(1+\epsilon) | N = m) \mathbb{P}(N = m | N \le n) \\ &\le \frac{1}{1-\epsilon'} \sum_{m=1}^{n} \mathbb{P}(\tau > \tilde{\tau}_i(1+\epsilon), N = m). \qquad (29)\end{aligned}$$

Each term in the summation of (29) can be represented as

$$\begin{aligned}&\mathbb{P}_i\{\tau > \tilde{\tau}_i(1+\epsilon), N = m\} \\ &\le \mathbb{P}_i\left\{\forall \tilde{i} \in \Theta \text{ s.t } \min_{j\neq\tilde{i}} \sum_{k=1}^{\tilde{\tau}_i(1+\epsilon)} \log\left(\frac{p_{\tilde{i}}^{u_k}(y_k|y_{k-1})}{p_j^{u_k}(y_k|y_{k-1})}\right) \right. \\ &\qquad \left. < |\log\bar{R}_{\tilde{i}}| + K, N = m\right\} \\ &\le \mathbb{P}_i\left\{\min_{j\neq i} \sum_{k=1}^{\tilde{\tau}_i(1+\epsilon)} \log\left(\frac{p_i^{u_k}(y_k|y_{k-1})}{p_j^{u_k}(y_k|y_{k-1})}\right) \right. \\ &\qquad \left. < |\log\bar{R}_i| + K, N = m\right\} \\ &= \mathbb{P}_i\left\{\sum_{k=1}^{\tilde{\tau}_i(1+\epsilon_m)} \log\left(\frac{p_i^{u_k+m}(y_{k+m}|y_{k+m-1})}{p_{\tilde{j}}^{u_k+m}(y_{k+m}|y_{k+m-1})}\right) \right. \\ &\qquad \left. < |\log\bar{R}| + K', N = m\right\},\end{aligned}$$

where $\epsilon_m$ is defined such that $\tilde{\tau}_i(1+\epsilon_m) = \tilde{\tau}_i(1+\epsilon) - m$, $K' = K + \sum_{k=1}^{m} \log(\frac{p_{\tilde{j}}^{u_k}(y_k|y_{k-1})}{p_i^{u_k}(y_k|y_{k-1})})$, and $\tilde{j} = \arg\min_{j\neq i} \sum_{k=1}^{\tilde{\tau}_i(1+\epsilon)} \log(\frac{p_i^{u_k}(y_k|y_{k-1})}{p_j^{u_k}(y_k|y_{k-1})})$.

We define $j^*$ as

$$j^* \triangleq \arg\min_{j\neq i} \sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) D\Big(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\Big),$$

and define $\mathcal{E}$ as the set of events such that

$$\begin{aligned}&\sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) D\Big(p_i^u(\cdot|y)\|p_{\tilde{j}}^u(\cdot|y)\Big) \\ &\quad = \sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) D\Big(p_i^u(\cdot|y)\|p_{j^*}^u(\cdot|y)\Big).\end{aligned}$$

Then, we have

$$\begin{aligned}&\mathbb{P}_i\left\{\sum_{k=1}^{\tilde{\tau}_i(1+\epsilon_m)} \log\left(\frac{p_i^{u_{k+m}}(y_{k+m})}{p_{\tilde{j}}^{u_{k+m}}(y_{k+m})}\right) < |\log\bar{R}| + K', N = m\right\} \\ &= \mathbb{P}_i\left\{\sum_{k=1}^{\tilde{\tau}_i(1+\epsilon_m)} \log\left(\frac{p_i^{u_{k+m}}(y_{k+m})}{p_{\tilde{j}}^{u_{k+m}}(y_{k+m})}\right) < |\log\bar{R}| + K', N = m, \mathcal{E}\right\} \\ &\quad + \mathbb{P}_i\left\{\sum_{k=1}^{\tilde{\tau}_i(1+\epsilon_m)} \log\left(\frac{p_i^{u_{k+m}}(y_{k+m})}{p_{\tilde{j}}^{u_{k+m}}(y_{k+m})}\right) \right. \\ &\qquad \left. < |\log\bar{R}| + K', N = m, \mathcal{E}^c\right\} \\ &\le \mathbb{P}_i\left\{N = m, \sum_{k=1}^{\tilde{\tau}_i(1+\epsilon_m)} \log\left(\frac{p_i^{u_{k+m}}(y_{k+m})}{p_{\tilde{j}}^{u_{k+m}}(y_{k+m})}\right) \right. \\ &\qquad - \sum_{k=1}^{\tilde{\tau}_i(1+\epsilon_m)} D\Big(p_i^{u_{k+m}}(\cdot|y_{k+m-1})\|p_{\tilde{j}}^{u_{k+m}}(\cdot|y_{k+m-1})\Big) \\ &\qquad \left. < \epsilon''\right\} \\ &\quad + \mathbb{P}_i\big\{N = m, \mathcal{E}^c\big\}, \qquad (30)\end{aligned}$$

where

$$\begin{aligned}\epsilon'' &= |\log \bar{R}| + K' \\ &\quad - \sum_{k=1}^{\tilde{\tau}_i(1+\epsilon_m)} D\Big(p_i^{u_{k+m}}(\cdot|y_{k+m-1}) \| p_{\tilde{j}}^{u_{k+m}}(\cdot|y_{k+m-1})\Big) \\ &= \tilde{\tau}_i \left( \min_{j\neq i} \sum_{y\in\mathcal{Y}, u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) D\Big(p_i^u(\cdot|y) \| p_j^u(\cdot|y)\Big)\right) \\ &\quad + K' - \sum_{k=1}^{\tilde{\tau}_i(1+\epsilon_m)} D\Big(p_i^{u_{k+m}}(\cdot|y_{k+m-1}) \| p_{\tilde{j}}^{u_{k+m}}(\cdot|y_{k+m-1})\Big)\end{aligned}$$

Notice that

$$\begin{aligned}&\lim_{\tilde{\tau}_i\to\infty} \frac{\sum_{k=1}^{\tilde{\tau}_i(1+\epsilon_m)} D\Big(p_i^{u_{k+m}}(\cdot|y_{k+m-1}) \| p_{\tilde{j}}^{u_{k+m}}(\cdot|y_{k+m-1})\Big)}{\tilde{\tau}_i(1+\epsilon_m)} \\ &= \sum_{y\in\mathcal{Y}, u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) D\Big(p_i^u(\cdot|y) \| p_{\tilde{j}}^u(\cdot|y)\Big) \qquad (31) \\ &= \min_{j\neq i} \sum_{y\in\mathcal{Y}, u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) D\Big(p_i^u(\cdot|y) \| p_j^u(\cdot|y)\Big), \qquad (32)\end{aligned}$$

where (31) is from the fact that $u_k$ is drawn from $q_i^*(u|y)$ for all $k > m$, and (32) is from the joint event $\sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) D(p_i^u(\cdot|y)\|p_{\tilde{j}}^u(\cdot|y)) = \sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q_i^*}(y)\ q_i^*(u|y)\ D(p_i^u(\cdot|y)\|p_{j^*}^u(\cdot|y))$. Therefore, we have for $\tilde{\tau}_i$ large enough

$$\epsilon'' = -\epsilon_m |\log \bar{R}|(1+o(1)).$$

Then, from Azuma's inequality, the first term on the right hand side of (30) goes to zero for all finite $m$ when $\tilde{\tau}_i \to \infty$. On the other hand, we define the set of indices

$$\begin{aligned}\mathcal{J} \triangleq \Bigg\{ j \in \Theta \,\&\, \Big| j \neq j^*, \sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) D\Big(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\Big) \\ \neq \sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) D\Big(p_i^u(\cdot|y)\|p_{j^*}^u(\cdot|y)\Big)\Bigg\},\end{aligned}$$

and bound the second term on the right hand side of (30) by

$$\begin{aligned}&\mathbb{P}_i\{N=m, \mathcal{E}^c\} \\ &= \mathbb{P}_i\{N=m, \tilde{j}\neq j^*, \mathcal{E}^c\} \\ &\leq \mathbb{P}_i\left\{ N=m, \exists j\in\mathcal{J} \text{ s.t } \sum_{k=1}^{\tilde{\tau}_i(1+\epsilon)} \log\left(\frac{p_{j^*}^{u_k}(y_k|y_{k-1})}{p_j^{u_k}(y_k|y_{k-1})}\right) < 0\right\} \qquad (33) \\ &\leq \sum_{j\in\mathcal{J}} \mathbb{P}_i\left\{ N=m, \sum_{k=1}^{\tilde{\tau}_i(1+\epsilon)} \log\left(\frac{p_{j^*}^{u_k}(y_k|y_{k-1})}{p_j^{u_k}(y_k|y_{k-1})}\right) \right. \\ &\qquad \left. - \sum_{k=1}^{\tilde{\tau}_i(1+\epsilon)} \mathbb{E}_i\left\{\log\frac{p_{j^*}^{u_k}(y_k|y_{k-1})}{p_j^{u_k}(y_k|y_{k-1})}\right\} < {\epsilon_j}'''\right\} \\ &\leq \sum_{j\in\mathcal{J}} \mathbb{P}_i\left\{ \sum_{k=1}^{\tilde{\tau}_i(1+\epsilon)} \log\left(\frac{p_{j^*}^{u_k}(y_k|y_{k-1})}{p_j^{u_k}(y_k|y_{k-1})}\right) \right. \\ &\quad \left. - \sum_{k=1}^{\tilde{\tau}_i(1+\epsilon)} \mathbb{E}_i\left\{\log\frac{p_{j^*}^{u_k}(y_k|y_{k-1})}{p_j^{u_k}(y_k|y_{k-1})}\right\} < {\epsilon_j}'''\right\},\end{aligned}$$

where (33) is from the definition of $\tilde{j}$, and

$$\begin{aligned}{\epsilon_j}''' &= \sum_{k=1}^{\tilde{\tau}_i(1+\epsilon)} \mathbb{E}_i\left\{\log\frac{p_j^{u_k}(y_k|y_{k-1})}{p_{j^*}^{u_k}(y_k|y_{k-1})}\right\} \\ &= \sum_{k=1}^{\tilde{\tau}_i(1+\epsilon)} \Big( D\Big(p_i^{u_k}(\cdot|y_{k-1})\|p_{j^*}^{u_k}(\cdot|y_{k-1})\Big) \\ &\qquad - D\Big(p_i^{u_k}(\cdot|y_{k-1})\|p_j^{u_k}(\cdot|y_{k-1})\Big)\Big) \\ &= \sum_{k=1}^{m} \Big( D\Big(p_i^{u_k}(\cdot|y_{k-1})\|p_{j^*}^{u_k}(\cdot|y_{k-1})\Big) \\ &\qquad - D\Big(p_i^{u_k}(\cdot|y_{k-1})\|p_j^{u_k}(\cdot|y_{k-1})\Big)\Big) \\ &\quad + \sum_{k=1}^{\tilde{\tau}_i(1+\epsilon_m)} \Big( D\Big(p_i^{u_{k+m}}(\cdot|y_{k+m-1})\|p_{j^*}^{u_{k+m}}(\cdot|y_{k+m-1})\Big) \\ &\qquad - D\Big(p_i^{u_{k+m}}(\cdot|y_{k+m-1})\|p_j^{u_{k+m}}(\cdot|y_{k+m-1})\Big)\Big).\end{aligned}$$

Notice that

$$\begin{aligned}&\lim_{\tilde{\tau}_i\to\infty} \frac{1}{\tilde{\tau}_i(1+\epsilon_m)} \sum_{k=1}^{\tilde{\tau}_i(1+\epsilon_m)} (D(p_i^{u_{k+m}}(\cdot|y_{k+m-1})\|p_{j^*}^{u_{k+m}}(\cdot|y_{k+m-1}) \\ &-D\Big(p_i^{u_{k+m}}(\cdot|y_{k+m-1})\|p_j^{u_{k+m}}(\cdot|y_{k+m-1})\Big)\Big) \\ &= \left( \sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) D\Big(p_i^u(\cdot|y)\|p_{j^*}^u(\cdot|y)\Big) \right. \\ &\qquad \left. - \sum_{y\in\mathcal{Y},u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) D\Big(p_i^u(\cdot|y)\|p_j^u(\cdot|y)\Big)\right) \\ &< 0\end{aligned}$$

from the definition of $j^*$, so ${\epsilon_j}'''$ approaches $-\infty$ when $\tilde{\tau}_i \to \infty$ for all $j \in \mathcal{J}$. Therefore, by Azuma's inequality, for all finite $m$, the first and the second term on the right hand side of (30) go to zero when $\tilde{\tau}_i \to \infty$. Then, we conclude that

$$\begin{aligned}&\lim_{\tilde{\tau}_i\to\infty} \mathbb{P}\tau > \tilde{\tau}_i(1+\epsilon) | N \leq n \\ &\leq \lim_{\tilde{\tau}_i\to\infty} \frac{1}{1-\epsilon'} \sum_{m=1}^{n} \mathbb{P}\tau > \tilde{\tau}_i(1+\epsilon), N=m \\ &= 0,\end{aligned}$$

and $\lim_{\tilde{\tau}_i\to\infty} \mathbb{P}_i\{\tau \leq \tilde{\tau}_i(1+\epsilon) | N \leq n\} = 1$. ∎

## Appendix C
## Proof of (22)

*Proof:* We first define the sets

$$\begin{aligned}K \triangleq \Bigg\{ z^{\tilde{\tau}_i(1+\epsilon)} \in \mathcal{Z}^{\tilde{\tau}_i(1+\epsilon)} : \sum_{u\in\mathcal{U}} \hat{p}_{u_{n+1}^{\tilde{\tau}_i(1+\epsilon)}}(u) \\ \left( D\Big(\hat{p}_{z_{n+1}^{\tilde{\tau}_i(1+\epsilon)}|u} \| q_j^u\Big) - D\Big(\hat{p}_{z_{n+1}^{\tilde{\tau}_i(1+\epsilon)}|u} \| q_i^u\Big)\right) < 0\Bigg\},\end{aligned}$$

and

$$K_u \triangleq \left\{ z^{\tilde{\tau}_i(1+\epsilon)} \in \mathcal{Z}^{\tilde{\tau}_i(1+\epsilon)} : D\left(\hat{p}_{z_{n+1}^{\tilde{\tau}_i(1+\epsilon)}|u} \| q_j^u\right) - D\left(\hat{p}_{z_{n+1}^{\tilde{\tau}_i(1+\epsilon)}|u} \| q_i^u\right) < 0 \right\},$$

It holds that $K \supseteq (\cap_{u\in\mathcal{U}} K_u)$. Then,

$$\begin{aligned}
&\lim_{\tilde{\tau}_i\to\infty} \frac{-1}{\tilde{\tau}_i(1+\epsilon)} \log \mathbb{P}_i\left\{\tilde{\delta}_{ij}\left(z^{\tilde{\tau}_i(1+\epsilon)}\right) = j\right\} \\
&= \lim_{\tilde{\tau}_i\to\infty} \frac{-1}{\tilde{\tau}_i(1+\epsilon)} \log \mathbb{P}_i\{K\} \\
&\le \lim_{\tilde{\tau}_i\to\infty} \frac{-1}{\tilde{\tau}_i(1+\epsilon)} \log \mathbb{P}_i\{\cap_{u\in\mathcal{U}} K_u\} \\
&= \lim_{\tilde{\tau}_i\to\infty} \frac{-1}{\tilde{\tau}_i(1+\epsilon)} \log \prod_{u\in\mathcal{U}} \mathbb{P}_i\{K_u\} \\
&= \lim_{\tilde{\tau}_i\to\infty} \sum_{u\in\mathcal{U}} \frac{-1}{\tilde{\tau}_i(1+\epsilon)} \log \mathbb{P}_i\{K_u\} \\
&= \lim_{\tilde{\tau}_i\to\infty} \sum_{u\in\mathcal{U}} \frac{N\left(u|u_{n+1}^{\tilde{\tau}_i(1+\epsilon)}\right)}{\tilde{\tau}_i(1+\epsilon)} \lim_{\tilde{\tau}_i\to\infty} \frac{-1}{N\left(u|u_{n+1}^{\tilde{\tau}_i(1+\epsilon)}\right)} \log \mathbb{P}_i\{K_u\},
\end{aligned}$$

where $N(u|u_{n+1}^{\tilde{\tau}_i(1+\epsilon)}) = \sum_{i=n+1}^{\tilde{\tau}_i(1+\epsilon)} 1(u_i = u)$. Notice that $\lim_{\tilde{\tau}_i\to\infty} \frac{-1}{N(u|u_{n+1}^{\tilde{\tau}_i(1+\epsilon)})} \log \mathbb{P}_i\{K_u\} = C(q_i^u \| q_j^u)$ from the definition of Chernoff information, and $\lim_{\tilde{\tau}_i\to\infty} \frac{N(u|u_{n+1}^{\tilde{\tau}_i(1+\epsilon)})}{\tilde{\tau}_i(1+\epsilon)} = \sum_{y\in\mathcal{Y}} u_i^{q_i^*}(y) q_i^*(u|y)$ because the actions are drawn from $q_i^*(u|y)$ for all time index greater than $n$. Then, we have

$$\begin{aligned}
&\lim_{\tilde{\tau}_i\to\infty} \frac{-1}{\tilde{\tau}_i(1+\epsilon)} \log \mathbb{P}_i\left\{\tilde{\delta}_{ij}\left(z^{\tilde{\tau}_i(1+\epsilon)}\right) = j\right\} \\
&\le \sum_{y\in\mathcal{Y}, u\in\mathcal{U}} u_i^{q_i^*}(y) q_i^*(u|y) C\left(q_i^u \| q_j^u\right).
\end{aligned}$$

■

## REFERENCES


[1] M.-C. Chang and M. R. Bloch, "Evasive active hypothesis testing," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2020, pp. 1248–1253.

[2] J. Ren, D. J. Dubois, D. Choffnes, A. M. Mandalari, R. Kolcun, and H. Haddadi, "Information exposure for consumer IoT devices: A multidimensional, network-informed measurement approach," in *Proc. Internet Meas. Conf. (IMC)*, 2019, pp. 1–9.

[3] M. Franceschetti, S. Marano, and V. Matta, "Chernoff test for strong-or-weak radar models," *IEEE Trans. Signal Process.*, vol. 65, no. 2, pp. 289–302, Jan. 2017.

[4] S. Chiu, N. Ronquillo, and T. Javidi, "Active learning and CSI acquisition for mmwave initial alignment," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 11, pp. 2474–2489, Nov. 2019.

[5] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.

[6] A. Tsiamis, K. Gatsis, and G. J. Pappas, "State estimation with secrecy against eavesdroppers," *IFAC PapersOnLine*, vol. 50, no. 1, pp. 8385–8392, 2017.

[7] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Trans. Autom. Control*, vol. 59, no. 2, pp. 341–354, Feb. 2014.

[8] B. Kailkhura, V. S. S. Nadendla, and P. K. Varshney, "Distributed inference in the presence of eavesdroppers: A survey," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 40–46, Jun. 2015.

[9] Z. Li and T. J. Oechtering, "Privacy-aware distributed Bayesian detection," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1345–1357, Oct. 2015.

[10] H. Jeon, J. Choi, S. W. McLaughlin, and J. Ha, "Channel aware encryption and decision fusion for wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 619–625, Apr. 2013.

[11] R. Soosahabi and M. Naraghi-Pour, "Scalable Phy-layer security for distributed detection in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1118–1126, Aug. 2012.

[12] R. Soosahabi, M. Naraghi-Pour, D. Perkins, and M. A. Bayoumi, "Optimal probabilistic encryption for secure detection in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 3, pp. 375–385, Mar. 2014.

[13] J. Zhang and X. Wang, "Asymptotically optimal stochastic encryption for quantized sequential detection in the presence of eavesdroppers," *IEEE Trans. Inf. Theory*, vol. 66, no. 3, pp. 1530–1548, Mar. 2020.

[14] M. Mhanna and P. Piantanida, "On secure distributed hypothesis testing," in *Proc. IEEE Int. Symp. Inf. Theory*, 2015, pp. 1605–1609.

[15] S. Sreekumar and D. Gündüz, "Testing against conditional independence under security constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, 2018, pp. 181–185.

[16] M. Naghshvar and T. Javidi, "Active sequential hypothesis testing," *Ann. Stat.*, vol. 41, no. 6, pp. 2703–2738, Dec. 2013.

[17] S. Nitinawarat, G. K. Atia, and V. V. Veeravalli, "Controlled sensing for multihypothesis testing," *IEEE Trans. Autom. Control*, vol. 58, no. 10, pp. 2451–2464, Oct. 2013.

[18] H. Chernoff, "Sequential design of experiments," *Ann. Math. Stat.*, vol. 30, no. 3, pp. 755–770, Sep. 1959.

[19] S. Nitinawarat and V. V. Veeravalli, "Controlled sensing for sequential multihypothesis testing with controlled Markovian observations and non-uniform control cost," *Seq. Anal.*, vol. 34, no. 1, pp. 1–24, 2015.

[20] I. Csiszar and J. Korner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York, NY, USA: Academic, 1982.



**Meng-Che Chang** received the B.Sc. degree in electrical engineering from National Chiao-Tung University in 2014, and the M.S. degree in communication engineering from National Chiao-Tung University in 2016. He is currently pursuing the Ph.D. degree with the School of Electrical and Computer Engineering, Georgia Institute of Technology.

**Matthieu R. Bloch** (Senior Member, IEEE) received the Engineering degree from Supélec, Gif-sur-Yvette, France, the M.S. degree in electrical engineering from the Georgia Institute of Technology, Atlanta, in 2003, the Ph.D. degree in engineering science from the Université de Franche-Comté, Besançon, France, in 2006, and the Ph.D. degree in electrical engineering from the Georgia Institute of Technology in 2008. From 2008 to 2009, he was a Postdoctoral Research Associate with the University of Notre Dame, South Bend, IN, USA. Since July 2009, he has been on the Faculty of the School of Electrical and Computer Engineering, the Georgia Institute of Technology. He is a coauthor of the textbook *Physical-Layer Security: From Information Theory to Security Engineering* (Cambridge University Press). His research interests are in the areas of information theory, error-control coding, wireless communications, and cryptography. He is a co-recipient of the IEEE Communications Society and IEEE Information Theory Society 2011 Joint Paper Award. He was the Chair of the Online Committee of the IEEE Information Theory Society from 2011 to 2014, an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY from 2016 to 2019, and a member of the Board of Governors of the IEEE Information Theory Society from 2016 to 2020. He currently serves as the second Vice-President of the IEEE Information Theory Society. He has been an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY since 2016.