Location Verification Systems Based on Received Signal Strength with Unknown Transmit Power

Shihao Yan, *Member, IEEE,* Gareth W. Peters, Ido Nevat, *Member, IEEE,* and Robert Malaney, *Member, IEEE*

***Abstract*—In the context of location verification systems (LVSs), this work proves that knowledge of a legitimate user's transmit power has no effect on the optimal performance of an RSS-based LVS. Specifically, we prove that the detection performance of a generalized likelihood ratio test (GLRT), where the unknown transmit power is estimated, is identical to that of a differential likelihood ratio test (D-LRT). Our analysis also proves the asymptotic optimality of D-LRT for an RSS-based LVS with unknown transmit power. These results are important for real-world deployments of LVSs, since D-LRT incurs a significantly lower implementation cost relative to GLRT.**

***Index Terms*—Physical layer security, location verification, generalized likelihood ratio test, received signal strength.**

I. Introduction

Location-based technologies and services (e.g., geographic routing protocols, location-based access control protocols, and location-based key generation) are becoming widely used in emerging wireless networks [1–5]. Meanwhile, current mainstream positioning systems, such as the now ubiquitous WiFi positioning systems and GPS, are highly vulnerable to location-spoofing attacks due to their openness and wide public availability. Against this background, the deployment of a location verification system (LVS), which provides methods to guarantee the reliability of the location information (e.g., [6–10]), is of growing importance. The main purpose of an LVS is to verify (based on signal observations) whether the claimed location of a user is consistent with his true position.

The LVS based on received signal strength (RSS) is of particular interest due to the simplicity in acquiring RSS observations [11]. However, a challenging issue to address in an RSS-based LVS is that the transmit power of a legitimate user (who reports his true location) may be unknown for a range of reasons - automatic power-saving functionality at battery exhaustion being one example [12]. In addition, from the perspective of designing an RSS-based LVS, whether we should set the legitimate user's actual transmit power to be a known (i.e. public) or unknown variable is another challenging issue. This is due to the fact that if the transmit power is an unknown variable, a malicious user (who spoofs his claimed location) will not have to meet any specific signal value at the receiving base station (BS). This, in turn, begs the question as to whether, in such a case, there remains any benefit to an RSS-based LVS. These two issues, which are the focus of this work, turn out to have a rather surprising answer - the known or unknown legitimate user's transmit power does not matter.

Considering the case in which the legitimate user's power is unknown, both the null and alternative hypothesis are composite. That is, the likelihood functions depend on the unknown transmit powers of the legitimate and malicious users. In this first case, the location verification is a composite binary detection problem with unknown transmit powers at all elements of the observation vector, for which the generalized likelihood ratio test (GLRT) is known to be asymptotically optimal (e.g., [13]). In the GLRT, the transmit powers have to be estimated first, which means that the complexity of the GLRT is high (from a signal processing perspective) [14]. However, we note that the above composite binary detection problem can also be solved by the likelihood ratio test (LRT) based on differential observations (D-LRT). In the D-LRT, the transmit powers are removed by differencing, and thus D-LRT is of lower complexity relative to the GLRT. In the second case, where the legitimate user's power is publicly known, the likelihood functions are completely determined in both the null hypothesis and alternative hypothesis. This is due to the fact that the malicious user will optimize his transmit power accordingly (otherwise he becomes easier to be detected as shown in [9]) and this optimized transmit power can be determined by the BS as well. For the second case, the binary detection problem can be solved by LRT, which is the uniformly most powerful test.

The main contribution of this work is to formally prove that the D-LRT is exactly equivalent (exactly the same detection performance) to the GLRT, a conclusion that is independent of localization error on the true location of the legitimate or malicious user. It is well known that GLRT is asymptotically optimal (e.g., [13]) for the composite binary detection problem. As such, our proof indirectly demonstrates the asymptotic optimality of D-LRT. This rather counter-intuitive result provides useful guidelines for real world RSS-based LVSs, due to the lower complexity of the D-LRT solution. With the aid of [9], this work also proves that the detection performance of RSS-based LVSs is independent of whether the legitimate user's transmit power is unknown or publicly known.

II. System Model

We now outline the system model and state the assumptions adopted in this work. We denote the null hypothesis (i.e., the user is legitimate) and the alternative hypothesis (i.e., the user is malicious) by $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. The composite log-

S. Yan is with the Research School of Engineering, The Australian National University, Canberra, ACT, Australia (email: shihao.yan@anu.edu.au). G. W. Peters is with the Department of Statistical Science, University College London, London, United Kingdom (email: gareth.peters@ucl.ac.uk). I. Nevat is with TUM CREATE, Singapore (email: ido.nevat@tum-create.edu.sg). R. Malaney is with the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, Australia (email: r.malaney@unsw.edu.au). This work was supported by the Australian Research Council's Discovery Projects (DP150103905).

normal RSS observation model is given by [11, 15]

$$\begin{cases} \mathcal{H}_0: \ \mathbf{y} = \theta_0 \mathbf{1}_N + \mathbf{u} + \mathbf{w}, \\ \mathcal{H}_1: \ \mathbf{y} = \theta_1 \mathbf{1}_N + \mathbf{v} + \mathbf{w}, \end{cases} \tag{1}$$

where $\mathbf{y}$ is the $N \times 1$ original RSS observation vector, θ_0 presents the unknown transmit power of the legitimate user, θ_1 presents the unknown transmit power of the malicious user, and $\mathbf{1}_N$ is the $N \times 1$ vector with all elements set to unity. In (1), each element of $\mathbf{u}$ is given by $u_i = p - 10\gamma \log_{10}\left(\frac{d_i^c}{d}\right), i = 1, 2, \ldots, N$, where p is a reference received power corresponding to a reference distance d, γ is the path loss exponent, d_i^c is the Euclidean distance from the i-th BS to the legitimate user's claimed location (also his true location). Each element of $\mathbf{v}$ is given by $v_i = p - 10\gamma \log_{10}\left(\frac{d_i^t}{d}\right)$, where d_i^t is the Euclidean distance from the i-th BS to the malicious user's true location. We first note that in practice the malicious user's true location cannot be known, which in turn means that the vector $\mathbf{v}$ is also unknown. However, following the methodology adopted in [9], we also note that the optimal location (in terms of leading to the minimum detection errors) for the malicious user to launch location spoofing attacks can be determined under some practical constraints (e.g., the malicious user should be on a specific road section). In this work we consider the worst-case scenario, where the malicious user is actually at the optimal location. Such a circumstance leads to the vector $\mathbf{v}$ being known due to the fact that the BS can determine this optimal location. In the log-normal RSS observation model, the measurement is in dB and the noise $\mathbf{w}$ in (1) is widely assumed to be a normal random variable with zero mean and covariance matrix $\mathbf{R}$ [11, 15]. As such, $\mathbf{y}$ under $\mathcal{H}_0$ conditional on θ_0 follows a multivariate normal distribution, which is

$$f\left(\mathbf{y}|\theta_0, \mathcal{H}_0\right) = \mathcal{N}(\theta_0 \mathbf{1}_N + \mathbf{u}, \mathbf{R}). \tag{2}$$

In addition, $\mathbf{y}$ under $\mathcal{H}_1$ also follows a multivariate normal distribution, i.e., $f\left(\mathbf{y}|\theta_1, \mathcal{H}_1\right) = \mathcal{N}(\theta_1 \mathbf{1}_N + \mathbf{v}, \mathbf{R})$.

III. Generalized Likelihood Ratio Test (GLRT) Based on Original RSS Observations

When the transmit powers in the observation model are unknown, the binary detection problem in the RSS-based LVS becomes a composite hypothesis test, for which the GLRT is asymptotically optimal [13]. As such, in this section we first consider the GLRT.

The binary decision rule embedded in the GLRT based on the original observations obtained from (1) is given by

$$\Lambda\left(\mathbf{y}\right) \triangleq \frac{f\left(\mathbf{y}|\hat{\theta}_1, \mathcal{H}_1\right)}{f\left(\mathbf{y}|\hat{\theta}_0, \mathcal{H}_0\right)} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \lambda_R, \tag{3}$$

where $\Lambda\left(\mathbf{y}\right)$ is the likelihood ratio of $\mathbf{y}$, λ_R is the threshold corresponding to $\Lambda\left(\mathbf{y}\right)$, $\hat{\theta}_0$ and $\hat{\theta}_1$ are the maximum-likelihood estimations of θ_0 and θ_1, respectively, and $\mathcal{D}_0$ and $\mathcal{D}_1$ are the binary decisions that infer whether $\mathbf{y}$ is from $\mathcal{H}_0$ or $\mathcal{H}_1$, respectively. We note that the specific value of λ_R can be set by using different strategies or optimization frameworks, e.g., through predetermining a false positive rate [13], to minimize the Bayesian average cost (e.g., the total error rate that is the sum of the false positive rate and miss detection rate) [13], or to maximize the mutual information between the system input and output [16]. Following (3), we present the variant of the decision rule embedded in the GLRT based on $\mathbf{y}$ in Lemma 1.

Lemma 1: The binary decision rule of the GLRT based on $\mathbf{y}$ is given by

$$\mathbb{T}(\mathbf{y}) \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \Gamma_R, \tag{4}$$

where $\mathbb{T}(\mathbf{y})$ is the test statistic given by

$$\mathbb{T}(\mathbf{y}) \triangleq \mathbf{c}^T \mathbf{R}^{-1} \left(\mathbf{y} - \frac{\mathbf{y}^T \mathbf{R}^{-1} \mathbf{1}_N}{\mathbf{1}_N^T \mathbf{R}^{-1} \mathbf{1}_N} \mathbf{1}_N\right), \tag{5}$$

Γ_R is the threshold corresponding to $\mathbb{T}(\mathbf{y})$ given by

$$\Gamma_R \triangleq \ln \lambda_R + \frac{1}{2} \mathbf{c}^T \mathbf{R}^{-1} \mathbf{e}, \tag{6}$$

and the definitions of $\mathbf{c}$ and $\mathbf{e}$ are given by

$$\mathbf{c} = \left(\mathbf{v} - \mathbf{u} - \frac{(\mathbf{v} - \mathbf{u})^T \mathbf{R}^{-1} \mathbf{1}_N}{\mathbf{1}_N^T \mathbf{R}^{-1} \mathbf{1}_N} \mathbf{1}_N\right), \tag{7}$$

$$\mathbf{e} = \left(\mathbf{v} + \mathbf{u} - \frac{(\mathbf{v} + \mathbf{u})^T \mathbf{R}^{-1} \mathbf{1}_N}{\mathbf{1}_N^T \mathbf{R}^{-1} \mathbf{1}_N} \mathbf{1}_N\right). \tag{8}$$

Proof: We first derive the closed-form expressions for $\hat{\theta}_0$ and $\hat{\theta}_1$. Based on (2), the log likelihood function of $\mathbf{y}$ conditioned on θ_0 under $\mathcal{H}_0$ is

$$\begin{aligned} \ln f\left(\mathbf{y}|\theta_0, \mathcal{H}_0\right) = &-\frac{1}{2} \ln |\mathbf{R}| - \frac{N}{2} \ln(2\pi) \\ &- \frac{1}{2} (\mathbf{y} - \theta_0 \mathbf{1}_N - \mathbf{u})^T \mathbf{R}^{-1} (\mathbf{y} - \theta_0 \mathbf{1}_N - \mathbf{u}). \end{aligned}$$

Then, the first derivative of $\ln f\left(\mathbf{y}|\theta_0, \mathcal{H}_0\right)$ with respect to θ_0 can be derived as

$$\begin{aligned} \frac{\partial \ln f\left(\mathbf{y}|\theta_0, \mathcal{H}_0\right)}{\partial \theta_0} &= \frac{\partial \ln f\left(\mathbf{y}|\theta_0, \mathcal{H}_0\right)}{\partial \left(\theta_0 \mathbf{1}_N\right)} \frac{\partial \left(\theta_0 \mathbf{1}_N\right)}{\partial \theta_0} \\ &= -\theta_0 \mathbf{1}_N^T \mathbf{R}^{-1} \mathbf{1}_N + (\mathbf{y} - \mathbf{u})^T \mathbf{R}^{-1} \mathbf{1}_N. \end{aligned} \tag{9}$$

The second derivative of $\ln f\left(\mathbf{y}|\theta_0, \mathcal{H}_0\right)$ with respect to θ_0 is derived as $-\mathbf{1}_N^T \mathbf{R}^{-1} \mathbf{1}_N$, which is less than zero due to the fact that $\mathbf{R}$ is a positive-definite symmetric matrix. As such, $\hat{\theta}_0$ is derived in a closed-form expression, which is given by

$$\hat{\theta}_0 = \frac{(\mathbf{y} - \mathbf{u})^T \mathbf{R}^{-1} \mathbf{1}_N}{\mathbf{1}_N^T \mathbf{R}^{-1} \mathbf{1}_N}. \tag{10}$$

Following a similar procedure, we also derive $\hat{\theta}_1$ as

$$\hat{\theta}_1 = \frac{(\mathbf{y} - \mathbf{v})^T \mathbf{R}^{-1} \mathbf{1}_N}{\mathbf{1}_N^T \mathbf{R}^{-1} \mathbf{1}_N}. \tag{11}$$

We then obtain the likelihood ratio conditioned on $\hat{\theta}_0$ and $\hat{\theta}_1$ in the log domain as

$$\begin{aligned} \ln \Lambda\left(\mathbf{y}\right) = &\left((\hat{\theta}_1 - \hat{\theta}_0) \mathbf{1}_N + \mathbf{v} - \mathbf{u}\right)^T \mathbf{R}^{-1} \mathbf{y} \\ &- \frac{1}{2} \left((\hat{\theta}_1 - \hat{\theta}_0) \mathbf{1}_N + \mathbf{v} - \mathbf{u}\right)^T \mathbf{R}^{-1} \left((\hat{\theta}_1 + \hat{\theta}_0) \mathbf{1}_N + \mathbf{v} + \mathbf{u}\right). \end{aligned} \tag{12}$$

Substituting (10) and (11) into (12), we obtain

$$\ln\Lambda\left(\mathbf{y}\right)=\mathbf{c}^T\mathbf{R}^{-1}\left(\mathbf{y}-\frac{\mathbf{y}^T\mathbf{R}^{-1}\mathbf{1}_N}{\mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N}\mathbf{1}_N\right)-\frac{1}{2}\mathbf{c}^T\mathbf{R}^{-1}\mathbf{e}. \quad (13)$$

Following (13), we obtain the desired result in Lemma 1 after some algebraic manipulations. ■

***Theorem** 1:* The false positive and detection rates of GLRT based on $\mathbf{y}$ are given by

$$\alpha_R = \mathcal{Q}\left(\frac{\ln\lambda_R + \frac{1}{2}\mathbf{c}^T\mathbf{R}^{-1}\mathbf{c}}{\sqrt{\mathbf{c}^T\mathbf{R}^{-1}\mathbf{c}}}\right), \quad (14)$$

$$\beta_R = \mathcal{Q}\left(\frac{\ln\lambda_R - \frac{1}{2}\mathbf{c}^T\mathbf{R}^{-1}\mathbf{c}}{\sqrt{\mathbf{c}^T\mathbf{R}^{-1}\mathbf{c}}}\right), \quad (15)$$

where $\mathcal{Q}[x] = \frac{1}{\sqrt{2\pi}}\int_x^{\infty}\exp(-t^2/2)dt$.

Proof: In order to obtain the false positive and detection rates, we have to derive the distributions of the test statistic $\mathbb{T}(\mathbf{y})$ under both $\mathcal{H}_0$ and $\mathcal{H}_1$. We first derive the covariance matrix of $\mathbb{T}(\mathbf{y})$, which is the same for $\mathcal{H}_0$ and $\mathcal{H}_1$ due to the fact that the covariance matrix of $\mathbf{y}$ under $\mathcal{H}_0$ and $\mathcal{H}_1$ is the same. To this end, we first define z as

$$z = \frac{\mathbf{y}^T\mathbf{R}^{-1}\mathbf{1}_N}{\mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N}. \quad (16)$$

The variance of z is derived as

$$\sigma_z^2 = \frac{\mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N}{(\mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N)^2} = \frac{1}{\mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N}. \quad (17)$$

Denoting the covariance of $(\mathbf{y}-z\mathbf{1}_N)$ as $\mathbf{G}$, the (i,j)-th $(i,j = 1,2,\ldots,N)$ element of $\mathbf{G}$ is given by

$$G_{ij} = \sigma_z^2 + R_{ij} - \mathrm{Cov}(y_i,z) - \mathrm{Cov}(y_j,z), \quad (18)$$

where R_{ij} is the (i,j)-th element of $\mathbf{R}$. In (18), $\mathrm{Cov}(y_k,z)$ is the covariance of y_k and z, which is derived as $(k=i,j)$

$$\mathrm{Cov}(y_k,z) = \frac{\mathbf{1}_N^T(\mathbf{R}^{-1})^T\mathbf{R}(:,k)}{\sqrt{R_{kk}\sigma_z^2}}, \quad (19)$$

where $\mathbf{R}(:,k)$ denotes the k-th column of $\mathbf{R}$. Since $\mathbf{R}$ is a positive-definite symmetric matrix, we have $(\mathbf{R}^{-1})^T\mathbf{R} = \mathbf{R}^{-1}\mathbf{R} = \mathbf{I}_N$ ($\mathbf{I}_N$ is the $N\times N$ identity matrix), which results in $\mathbf{1}_N^T(\mathbf{R}^{-1})^T\mathbf{R}(:,k) = 1$. As such, defining $R_{kk} = \sigma_R^2$, we have $\mathrm{Cov}(y_k,z) = 1/\sigma_R\sigma_z$, which is not dependent on k. Therefore, we obtain $\mathbf{G} = \mathbf{R} + \xi\mathbf{1}_{N\times N}$, where ξ is

$$\xi = \frac{1}{\mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N} - \frac{2\sqrt{\mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N}}{\sigma_R}, \quad (20)$$

and $\mathbf{1}_{N\times N}$ is the $N\times N$ matrix with all elements set to unity. With the definition z, following (5) the test statistic can be rewritten as $\mathbb{T}(\mathbf{y}) = \mathbf{c}^T\mathbf{R}^{-1}(\mathbf{y} - z\mathbf{1}_N)$, and therefore the covariance matrix of $\mathbb{T}(\mathbf{y})$ is given by

$$\begin{aligned}&\mathbf{c}^T\mathbf{R}^{-1}\mathbf{G}\left(\mathbf{c}^T\mathbf{R}^{-1}\right)^T\\ &\quad = \mathbf{c}^T\mathbf{R}^{-1}\mathbf{c} + \xi\mathbf{c}^T\mathbf{R}^{-1}\mathbf{1}_{N\times N}\left(\mathbf{c}^T\mathbf{R}^{-1}\right)^T. \quad (21)\end{aligned}$$

As per the definition of $\mathbf{c}$ given in (7), we have

$$\mathbf{c}^T\mathbf{R}^{-1}\mathbf{1}_N = \left((\mathbf{v}-\mathbf{u})^T - \frac{(\mathbf{v}-\mathbf{u})^T\mathbf{R}^{-1}\mathbf{1}_N}{\mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N}\mathbf{1}_N^T\right)\mathbf{R}^{-1}\mathbf{1}_N = 0.$$

As such, with regard to the second term in (21) we have

$$\begin{aligned}\xi\mathbf{c}^T\mathbf{R}^{-1}\mathbf{1}_{N\times N}\left(\mathbf{c}^T\mathbf{R}^{-1}\right)^T &= \xi\left(\mathbf{c}^T\mathbf{R}^{-1}\mathbf{1}_N\right)\mathbf{1}_N^T\left(\mathbf{c}^T\mathbf{R}^{-1}\right)^T\\ &= \mathbf{0}_{N\times N}, \quad (22)\end{aligned}$$

where $\mathbf{0}_{N\times N}$ is the $N\times N$ matrix with all elements equal zero. Substituting (22) into (21), we obtain the final covariance matrix of the test statistic $\mathbb{T}(\mathbf{y})$ as

$$\mathbf{c}^T\mathbf{R}^{-1}\mathbf{G}\left(\mathbf{c}^T\mathbf{R}^{-1}\right)^T = \mathbf{c}^T\mathbf{R}^{-1}\mathbf{c}. \quad (23)$$

The means of $\mathbf{y}$ under $\mathcal{H}_0$ and $\mathcal{H}_1$ are $(\hat{\theta}_0\mathbf{1}_N + \mathbf{u})$ and $(\hat{\theta}_1\mathbf{1}_N + \mathbf{v})$, respectively. As such, the distributions of $\mathbb{T}(\mathbf{y})$ under $\mathcal{H}_0$ and $\mathcal{H}_1$ are given by

$$\mathbb{T}(\mathbf{y})|\mathcal{H}_0 \sim \mathcal{N}\left(\mathbf{c}^T\mathbf{R}^{-1}\left(\mathbf{u}-\frac{\mathbf{u}^T\mathbf{R}^{-1}\mathbf{1}_N}{\mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N}\mathbf{1}_N\right), \mathbf{c}^T\mathbf{R}^{-1}\mathbf{c}\right), \quad (24)$$

$$\mathbb{T}(\mathbf{y})|\mathcal{H}_1 \sim \mathcal{N}\left(\mathbf{c}^T\mathbf{R}^{-1}\left(\mathbf{v}-\frac{\mathbf{v}^T\mathbf{R}^{-1}\mathbf{1}_N}{\mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N}\mathbf{1}_N\right), \mathbf{c}^T\mathbf{R}^{-1}\mathbf{c}\right). \quad (25)$$

As per the decision rule in (4) and the definitions of the false positive and detection rates, we obtain the results in (14) and (15) after some algebraic manipulations. ■

IV. Comparison between GLRT and D-LRT in RSS-based LVSs

For the specific observation model given in (1), the composite binary detection problem in the RSS-based LVS can also be solved by the D-LRT [9], where the unknown transmit powers, θ_0 and θ_1, are removed by differencing. For convenience, we represent the detection performance of the D-LRT in the following lemma, which is Theorem 2 in [9].

***Lemma** 2:* The false positive and detection rates of D-LRT are given by

$$\alpha_D = \mathcal{Q}\left(\frac{\ln\lambda_D + \frac{1}{2}\left(\mathbf{\Delta v}-\mathbf{\Delta u}\right)^T\mathbf{D}^{-1}\left(\mathbf{\Delta v}-\mathbf{\Delta u}\right)}{\sqrt{\left(\mathbf{\Delta v}-\mathbf{\Delta u}\right)^T\mathbf{D}^{-1}\left(\mathbf{\Delta v}-\mathbf{\Delta u}\right)}}\right), \quad (26)$$

$$\beta_D = \mathcal{Q}\left(\frac{\ln\lambda_D - \frac{1}{2}\left(\mathbf{\Delta v}-\mathbf{\Delta u}\right)^T\mathbf{D}^{-1}\left(\mathbf{\Delta v}-\mathbf{\Delta u}\right)}{\sqrt{\left(\mathbf{\Delta v}-\mathbf{\Delta u}\right)^T\mathbf{D}^{-1}\left(\mathbf{\Delta v}-\mathbf{\Delta u}\right)}}\right), \quad (27)$$

where λ_D is the threshold corresponding to the likelihood ratio of $\mathbf{\Delta y}$, $\Delta u_m = u_m - u_N$, $\Delta v_m = v_m - v_N$, $D_{mn} = R_{NN} + R_{mn} - R_{mN} - R_{nN}$, $m = 1,\ldots,N-1$, and $n = 1,\ldots,N-1$.

***Proposition** 1:* We have $\alpha_R = \alpha_D$ and $\beta_R = \beta_D$ for $\lambda_R = \lambda_D$. That is, the performance of the D-LRT is equivalent to the performance of the GLRT based on $\mathbf{y}$.

Proof: From (14), (15), (26), and (27), we can see that α_R, β_R, α_D, and β_D are all in the form of the $\mathcal{Q}$ function. We denote $\alpha_R = \mathcal{Q}(\zeta_R)$, $\beta_R = \mathcal{Q}(\eta_R)$, $\alpha_D = \mathcal{Q}(\zeta_D)$, and $\beta_D = \mathcal{Q}(\eta_D)$. In order to prove $\alpha_R = \alpha_D$ and $\beta_R = \beta_D$ for $\lambda_R = \lambda_D$, we only need to prove $\zeta_R - \eta_R = \zeta_D - \eta_D$. As per (14), (15), (26), and (27), in order to prove $\zeta_R - \eta_R = \zeta_D - \eta_D$, it suffices to prove the following equation

$$\mathbf{c}^T\mathbf{R}^{-1}\mathbf{c} = \left(\mathbf{\Delta v}-\mathbf{\Delta u}\right)^T\mathbf{D}^{-1}\left(\mathbf{\Delta v}-\mathbf{\Delta u}\right). \quad (28)$$

This equation is the same as (55) in [9], which has been proved in [9], and thus the proof of Proposition 1 follows. ■

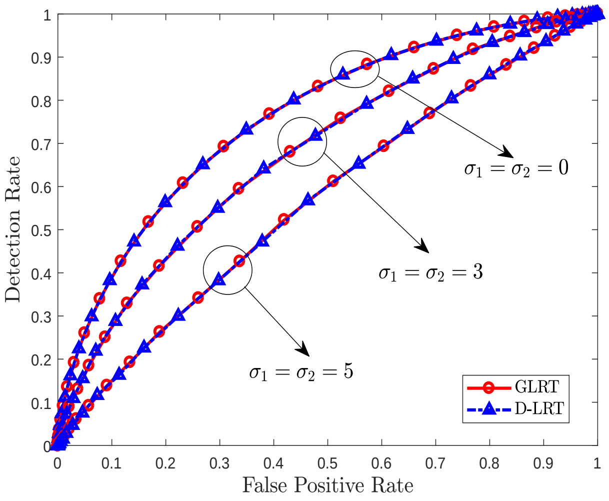

Fig. 1. The receiver operating characteristic (ROC) curves of the GLRT and D-LRT with localization errors on the true location of the legitimate user, where $N = 4$, $\mathbf{R} = \sigma_{dB}^2\mathbf{I}_N$, $\sigma_{dB} = 3$, $\mathbf{\Sigma} = \mathrm{diag}\{\sigma_1^2, \sigma_2^2\}$, the reported location is $[0, 0]$, the best location to attack for the malicious user is $[5, 10]$, and the locations of the N BSs are $[22.3, 45.5]$, $[37.9, -33.4]$, $[54.1, 77.5]$, and $[-13.8, 93.1]$.

Based on Proposition 1, the composite hypothesis testing problem in the RSS-based LVS can be solved through the more efficient D-LRT, in which the detection performance is equivalent to that of the more complex GLRT. This indicates that in RSS-based LVSs, estimating the unknown transmit power or removing it by differencing does not affect the detection performance. The latter strategy (i.e., D-LRT) is of lower complexity and therefore more desirable in practice. That is, with unknown transmit powers RSS-based LVSs should be designed based on the D-LRT since this strategy incurs a lower implementation cost.

In Fig. 1, we verify our Proposition 1 and also examine the impact of localization error on the performance of the GLRT and D-LRT. Specifically, we consider the localization error on the true location of the legitimate user, where the legitimate user's true location follows a normal distribution with the reported location as the mean and $\mathbf{\Sigma}$ as the covariance matrix. In Fig. 1, we observe that the performances of the GLRT and D-LRT are identical regardless of the size of the localization errors. This can be explained by the fact that Proposition 1 is valid for arbitrary vectors $\mathbf{u}$ and $\mathbf{v}$ (such as arbitrary vectors $\mathbf{\Delta u}$ and $\mathbf{\Delta v}$), while the size of the localization errors only affects the vector $\mathbf{u}$ and $\mathbf{\Delta u}$. Therefore, our analysis indicates the identical performance of the GLRT and D-LRT a result that is independent of localization errors on the true location of the legitimate or malicious user. This observation also confirms the asymptotic optimality of the D-LRT even with localization errors. In this figure, we also observe that the detection performance of both the GLRT and D-LRT decreases as the localization error increases.

***Proposition** 2:* The detection performance of the RSS-based LVSs using the GLRT and D-LRT is the same for the following two scenarios.

Scenario 1: The legitimate user's transmit power is publicly known and the malicious user optimizes his transmit power.

Scenario 2: The legitimate user's transmit power is unknown to BSs or the malicious user.

Proof: The proof follows from our Theorem 1, Lemma 2 and the Theorem 1 in [9]. ■

The intuitive explanation of Proposition 2 is that the benefits of knowing the legitimate user's transmit power by the BS are counteracted by the malicious user through optimizing his transmit power accordingly. As such, we can conclude that setting the legitimate user's transmit power to be known or unknown has no effect the RSS-based LVSs.

V. Conclusion

In this work, we first proved that the unknown transmit power in an RSS-based LVS, which can be estimated or removed by differencing, has no effect on the detection performance of the LVS. In addition, we analytically showed that setting the legitimate user's transmit power to be known or unknown has no effect on the detection performance of the RSS-based LVS.

References

[1] M. Z. Win, A. Conti, S. Mazuelas, Y. Shen, W. M. Gifford, D. Dardari, and M. Chiani, "Network localization and navigation via cooperation," *IEEE Commun. Mag.*, vol. 49, no. 5, pp. 56–62, May 2011.

[2] W. Dai, Y. Shen, and M. Z. Win, "Distributed power allocation for cooperative wireless network localization," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 1, pp. 28–40, Jan. 2015.

[3] C. Liu, N. Yang, J. Yuan, and R. Malaney, "Location-based secure transmission for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 7, pp. 1458–1470, Jul. 2015.

[4] S. Yan and R. Malaney,"Location-based beamforming for enhancing secrecy in Rician wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2780–2791, Apr. 2016.

[5] J. Lim, H. Yu, K. Kim, M. Kim, and S. Lee, "Preserving Location Privacy of Connected Vehicles With Highly Accurate Location Updates," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 540–543, Mar. 2017.

[6] J. T. Chiang, J. J. Haas, J. Choi, and Y. Hu, "Secure location verification using simultaneous multilateration," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 584–591, Feb. 2012.

[7] Y. Wei and Y. Guan, "Lightweight location verification algorithms for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 5, pp. 938–950, May 2013.

[8] M. E. P. Monteiro, J. L. Rebelatto, and R. D. Souza, "Information-theoretic location verification system with directional antennas for vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 1, pp. 93–103, Jan. 2016.

[9] S. Yan, I. Nevat, G. Peters, and R. Malaney, "Location verification systems under spatially correlated shadowing," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4132–4144, Jun. 2016.

[10] J. Y. Koh, I. Nevat, D. Leong, and W. C. Wong, "Geo-spatial location spoofing detection for internet of things," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 971–978, Dec. 2016.

[11] S. Tomic, M. Beko, R. Dinis, and P. Montezuma, "A closed-form solution for RSS/AoA target localization by spherical coordinates conversion," *IEEE Wireless Commun. Lett.*, vol. 5, no. 6, pp. 680–683, Dec. 2016.

[12] S. Tomic, M. Beko, and R. Dinis, "Distributed RSS-AoA based localization with unknown transmit powers," *IEEE Wireless Commun. Lett.*, vol. 5, no. 4, pp. 392–395, Aug. 2016.

[13] Bernard C. Levy, *Principles of Signal Detection and Parameter Estimation*, Springer, New York, 2008.

[14] J. K. Tugnait, "Using artificial noise to improve detection performance for wireless user authentication in time-variant channels," *IEEE Wireless Commun. Lett.*, vol. 3, no. 4, pp. 377–380, Aug. 2014.

[15] G. Wang, H. Chen, Y. Li, and M. Jin, "On received-signal-strength based localization with unknown transmit power and path loss exponent," *IEEE Wireless Commun. Lett.*, vol. 1, no. 5, pp. 536–539, Oct. 2012.

[16] S. Yan, R. Malaney, I. Nevat, and G. Peters, "Optimal information-theoretic wireless location verification," *IEEE Trans. Veh. Technol.*, vol. 63, no. 7, pp. 3410–3422, Sep. 2014.