

Location Spoofing Detection for VANETs by a Single Base Station in Rician Fading Channels

Shihao Yan¹, Robert Malaney¹

¹School of Electrical Engineering & Telecommunications,
The University of New South Wales,
Sydney, NSW 2052, Australia

Emails: shihao.yan@unsw.edu.au; r.malaney@unsw.edu.au

Ido Nevat², Gareth W. Peters³

²Institute for Infocomm Research, A*STAR, Singapore.

³Department of Statistical Science,

University College London, London, UK

Emails: ido-nevat@i2r.a-star.edu.sg; gareth.peters@ucl.ac.uk

Abstract—In this work we examine the performance of a Location Spoofing Detection System (LSDS) for vehicular networks in the realistic setting of Rician fading channels. In the LSDS, an authorized Base Station (BS) equipped with multiple antennas utilizes channel observations to identify a malicious vehicle, also equipped with multiple antennas, that is spoofing its location. After deriving the optimal transmit power and the optimal directional beamformer of a potentially malicious vehicle, robust theoretical analysis and detailed simulations are conducted in order to determine the impact of key system parameters on the LSDS performance. Our analysis shows how LSDS performance increases as the Rician K -factor of the channel between the BS and legitimate vehicles increases, or as the number of antennas at the BS or legitimate vehicle increases. We also obtain the counter-intuitive result that the malicious vehicle's optimal number of antennas conditioned on its optimal directional beamformer is equal to the legitimate vehicle's number of antennas. The results we provide here are important for the verification of location information reported in IEEE 1609.2 safety messages.

I. INTRODUCTION

In wireless networks the integrity of location information is of growing importance. As such, the authentication (or verification) of location information has attracted considerable research interest in recent years [1–7]. In many circumstances the device (client) itself obtains its location information directly (e.g., via GPS), and the wider network can only achieve the client's location information through requests to the client. In such a context, the client can easily spoof or falsify its claimed location in order to disrupt some network functionality (e.g., geographic routing protocols [8], or directional access control protocols [9]). The adverse effects of location spoofing can be more severe in Vehicular Ad Hoc Networks (VANETs) due to the possibility of life-threatening accidents. Less critically, a malicious vehicle could spoof its location in order to seriously disrupt other vehicles [10] or to selfishly enhance its own functionality within the network [11]. The integrity of claimed location in VANETs is therefore important, and motivates the introduction of an LSDS to that scenario. Within IEEE 1609.2 revocation of certificates belonging to malicious vehicles will occur [12] - an LSDS will form part of the revocation logic.

Recently, many location spoofing detection protocols for VANETs have been proposed (e.g., [13–15]). In [13], the authors proposed an autonomous and cooperative scheme for

detecting and mitigating false claimed locations by exploiting specific properties of VANETs, such as high node density and mobility. The authors of [14] developed a location spoofing detection algorithm by comparing the claimed location with a neighbor table consisting of other vehicles' identifications and locations. To overcome the non line-of-sight (LOS) problem in location verification systems, a cooperative algorithm was proposed in [15]. Some generic location spoofing detection algorithms (not dedicated to VANETs), were also proposed in recent years (e.g., [3–6]). These algorithms utilize some observations such as Received Signal Strength (RSS), Time of Arrival (TOA), and Angle of Arrival (AOA), and performance analysis of these algorithms were provided under specific observation models.

However, the following question has not been explored in the literature. *How does the performance of an LSDS depend on the proportion of the channel which is LOS?* In the VANET environment it is highly likely that a vehicle possesses some LOS component towards a BS for the majority of its travel time. As such, answering the above question in the context of VANETs is important, and forms the thrust of the work presented here. In order to investigate the above question, we consider Rician fading channels in which the Rician K -factor is defined as the ratio between the power of the LOS component and the power of other scattered components. We utilize the complex signals measured by an authorized multiple-antenna BS to verify a claimed location of a vehicle that is equipped with multiple antennas, and infer whether the vehicle is *legitimate* (reporting its true location) or *malicious* (spoofing its claimed location). Adopting a practical threat model, in which the on-road malicious vehicle keeps some minimum distance away from its claimed location, we analyze the performance of our LSDS. In order to guarantee fairness, we also determine the optimal transmit power and the optimal directional beamformer for the malicious vehicle to minimize the detection rate. Our analysis demonstrates that our LSDS works well even when the Rician K -factor is low (e.g., -3dB), and that detection performance increases as the Rician K -factor of the channel between the legitimate vehicle and the BS increases. We also obtain a counter-intuitive observation, that the malicious vehicle can minimize the detection rate by setting its number of antennas equal to the legitimate vehicle's

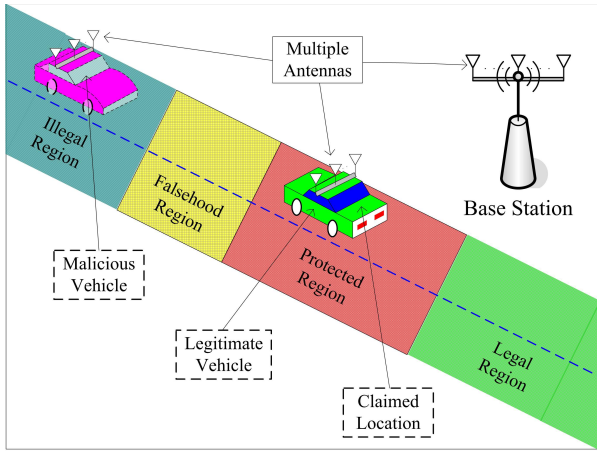


Fig. 1. Illustration of the VANETs application scenario of interest.

number of antennas when it adopts the optimal directional beamformer. This is counter-intuitive since *a priori* one would have thought it would be optimal to set the number of antennas as large as possible.

II. SYSTEM MODEL

A. System Assumptions

The VANETs application scenario of interest is illustrated in Fig. 1, where the BS, the legitimate vehicle, and the malicious vehicle are each equipped with a uniform linear array (ULA) with N_B , N_L , and N_M elements, respectively. In this figure, the “Protected Region” is the area where a vehicle (legitimate or malicious) claims to be. The BS is to verify whether the vehicle is indeed at his claimed location or not based on wireless channel observations. If the vehicle passes such a verification, a specific action will follow in the “Legal Region” (e.g., a traffic light turns green). The “Falsehood Region” indicates the minimum distance between the claimed location and the malicious vehicle’s location. The malicious vehicle is inside the “Illegal Region” while it claims that it is inside the “Protected Region” in order to bring some selfish benefits (e.g., it keeps the traffic light green in advance for itself). We adopt the polar coordinate system as shown in Fig. 2, where the location of the BS is selected as the origin, the legitimate vehicle’s location is denoted as $\mathbf{x}_L = (d_L, \theta_L)$, and the malicious vehicle’s location is denoted as $\mathbf{x}_M = (d_M, \theta_M)$. We assume that the claimed location is the same as the legitimate vehicle’s location (i.e., \mathbf{x}_L is also the claimed location of the legitimate or malicious vehicle). We adopt a practical threat model, in which the distance between \mathbf{x}_M and the malicious vehicle’s claimed location \mathbf{x}_L is larger than a predetermined threshold r_m , i.e., $|\mathbf{x}_M - \mathbf{x}_L| \geq r_m$. The orientation of the BS ULA is aligned with the x -axis, which is publicly known. The orientations of the ULAs of the legitimate and malicious vehicles are under the control of the legitimate and malicious vehicles, respectively, i.e., the angles ψ_L and ψ_M as shown in Fig. 2 are under the control of the legitimate and malicious vehicles, respectively.

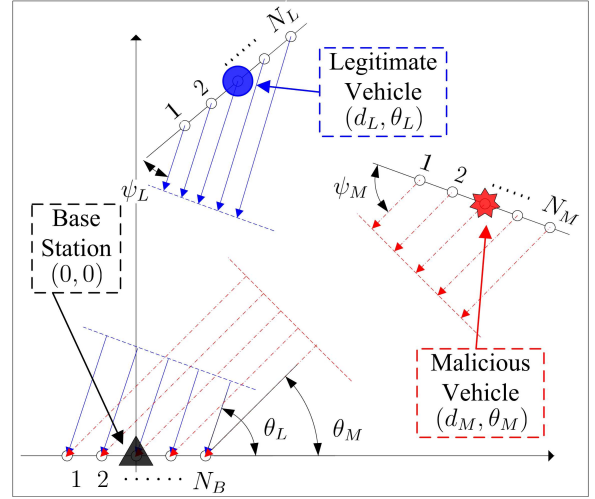


Fig. 2. Illustration of the orientations of the three ULA antennas and the geometry of the BS, legitimate vehicle, and malicious vehicle.

B. Channel Model

With no loss of generality, we assume the legitimate channel (legitimate vehicle-to-BS) and the malicious channel (malicious vehicle-to-BS) are subject to Rician fading. Then, the $N_B \times N_L$ legitimate channel matrix is given by

$$\mathbf{H} = \sqrt{\frac{K_L}{1 + K_L}} \mathbf{H}_o + \sqrt{\frac{1}{1 + K_L}} \mathbf{H}_r, \quad (1)$$

where K_L is the Rician K -factor of the legitimate channel, \mathbf{H}_o is the LOS component of the matrix, and \mathbf{H}_r is the scattered component of the matrix. The entries of \mathbf{H}_r are independent and identically distributed (i.i.d) circularly-symmetric complex Gaussian random variables with zero mean and unit variance. Denoting ρ_B as the space between two antenna elements of the ULA at the BS, \mathbf{H}_o is given by $\mathbf{H}_o = \mathbf{r}_L^T \mathbf{t}_L$, where \mathbf{r}_L and \mathbf{t}_L are defined as

$$\mathbf{r}_L = [1, \dots, \exp(j(N_B - 1)\tau_B \cos \theta_L)], \quad (2)$$

$$\mathbf{t}_L = [1, \dots, \exp(j(N_L - 1)\tau_L \cos \psi_L)], \quad (3)$$

and T denotes the transpose operation. In (2) and (3), we have $\tau_B = 2\pi f_0 \rho_B / c$ and $\tau_L = 2\pi f_0 \rho_L / c$, where f_0 is the carrier frequency, c is the speed of propagation of the plane wave, and ρ_L is the space between two antenna elements of the ULA at the legitimate vehicle.

The $N_B \times N_M$ malicious channel matrix is given by

$$\mathbf{G} = \sqrt{\frac{K_M}{1 + K_M}} \mathbf{G}_o + \sqrt{\frac{1}{1 + K_M}} \mathbf{G}_r, \quad (4)$$

where K_M is the Rician K -factor of the malicious channel, \mathbf{G}_o is the LOS component of the matrix. \mathbf{G}_r is the scattered component of the matrix and is a matrix with i.i.d circularly-symmetric complex Gaussian random variables with zero mean and unit variance. \mathbf{G}_o can be written as $\mathbf{G}_o = \mathbf{r}_M^T \mathbf{t}_M$, where \mathbf{r}_M and \mathbf{t}_M are given by

$$\mathbf{r}_M = [1, \dots, \exp(j(N_B - 1)\tau_B \cos \theta_M)], \quad (5)$$

$$\mathbf{t}_M = [1, \dots, \exp(j(N_M - 1)\tau_M \cos \psi_M)], \quad (6)$$

In (6), we have $\tau_M = 2\pi f_0 \rho_M / c$, where ρ_M is the space between two antenna elements of the ULA at the malicious vehicle.

C. Observation Model

Throughout this work we denote the null hypothesis where the vehicle is legitimate as \mathcal{H}_0 and denote the alternative hypothesis where the vehicle is malicious as \mathcal{H}_1 . The $N_B \times 1$ complex observation vector received from the legitimate vehicle (under \mathcal{H}_0) is given by

$$\mathbf{y} = \sqrt{P_L g(d_L)} \mathbf{H} \mathbf{b} s + \mathbf{n}_L, \quad (7)$$

where P_L is the transmit power of the legitimate vehicle, $g(d_L)$ is the path loss gain given by $g(d_L) = (c/4\pi f_0 d_0)^2 (d_0/d_L)^\eta$, d_0 is a reference distance, η is the path loss exponent, \mathbf{b} is the beamformer adopted by the legitimate vehicle which satisfies $\|\mathbf{b}\| = 1$, s is the publicly known pilot symbol (without loss of generality we assume $s = 1$), and \mathbf{n}_L is the additive white Gaussian noise vector, of which the entries are i.i.d circularly-symmetric complex Gaussian random variables with zero mean and variance σ_L^2 . We note that \mathbf{b} and P_L are under the control of the legitimate vehicle. We assume that the legitimate vehicle cooperates with the BS to facilitate the verification procedure. To this end, the legitimate vehicle sets $\mathbf{b} = \mathbf{t}_L^\dagger / \|\mathbf{t}_L\|$ to maximize $|\mathbf{t}_L \mathbf{b}|$, where † denotes the conjugate transpose operation. In addition, the legitimate vehicle sets its transmit power to that required by the BS (we assume P_L is publicly known). As per (7), the likelihood function of \mathbf{y} conditioned on a known s under \mathcal{H}_0 is

$$f(\mathbf{y}|\mathcal{H}_0) = \frac{1}{\pi^{N_B} \det(\mathbf{R}_0)} \exp [-(\mathbf{y} - \mathbf{m}_0)^\dagger \mathbf{R}_0^{-1} (\mathbf{y} - \mathbf{m}_0)], \quad (8)$$

where \mathbf{m}_0 and \mathbf{R}_0 are the mean vector and covariance matrix of \mathbf{y} under \mathcal{H}_0 , respectively, which are given by

$$\mathbf{m}_0 = \sqrt{\frac{P_L g(d_L) K_L N_B}{1 + K_L}} \mathbf{r}_L^T, \quad (9)$$

$$\mathbf{R}_0 = \left(\frac{P_L g(d_L)}{K_L + 1} + \sigma_L^2 \right) \mathbf{I}_{N_B}. \quad (10)$$

Likewise, the complex observation vector received from the malicious vehicle (under \mathcal{H}_1) is given by

$$\mathbf{y} = \sqrt{P_M g(d_M)} \mathbf{G} \mathbf{p} s + \mathbf{n}_M, \quad (11)$$

where P_M is the transmit power of the malicious vehicle, $g(d_M)$ is the path loss gain given by $g(d_M) = (c/4\pi f_0 d_0)^2 (d_0/d_M)^\eta$, \mathbf{p} is the beamformer adopted by the malicious vehicle which satisfies $\|\mathbf{p}\| = 1$, and \mathbf{n}_M is the additive white Gaussian noise vector, of which the entries are i.i.d circularly-symmetric complex Gaussian random variables with zero mean and variance σ_M^2 . As per (11), the likelihood function of \mathbf{y} under \mathcal{H}_1 for given \mathbf{x}_M , P_M , and \mathbf{p} is

$$f(\mathbf{y}|\mathbf{x}_M, P_M, \mathbf{p}, \mathcal{H}_1) = \frac{1}{\pi^{N_B} \det(\mathbf{R}_1)} \exp [-(\mathbf{y} - \mathbf{m}_1)^\dagger \mathbf{R}_1^{-1} (\mathbf{y} - \mathbf{m}_1)], \quad (12)$$

where \mathbf{m}_1 and \mathbf{R}_1 are the mean vector and covariance matrix of \mathbf{y} under \mathcal{H}_1 , respectively, which are given by

$$\mathbf{m}_1 = \sqrt{\frac{P_M g(d_M) K_M}{1 + K_M}} \mathbf{G}_o \mathbf{p}, \quad (13)$$

$$\mathbf{R}_1 = \left(\frac{P_M g(d_M)}{K_M + 1} + \sigma_M^2 \right) \mathbf{I}_{N_B}. \quad (14)$$

We note that \mathbf{x}_M , P_M , and \mathbf{p} are under the control of the malicious vehicle. We will discuss in the next section how the malicious vehicle sets these parameters so as to minimize the detection rate.

III. LOCATION SPOOFING DETECTION SYSTEM

In this section, we first present the decision rule adopted in our LSDS. We then discuss the attack strategy of the malicious vehicle (e.g., how to set \mathbf{x}_M , P_M , and \mathbf{p}) in order to minimize the detection rate. Finally, we analyze the detection performance of our LSDS based on the malicious vehicle's attack strategy.

A. Decision Rule of the LSDS

We adopt the Likelihood Ratio Test (LRT) as the decision rule of our LSDS. This is due to the fact that the LRT achieves the highest detection rate (the probability to detect a malicious vehicle) for any given false positive rate (the probability to detect a legitimate vehicle as malicious) [16]. The LRT decision rule is given by

$$\Lambda(\mathbf{y}) \triangleq \frac{f(\mathbf{y}|\mathbf{x}_M, P_M, \mathbf{p}, \mathcal{H}_1)}{f(\mathbf{y}|\mathcal{H}_0)} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\geq}} \lambda, \quad (15)$$

where $\Lambda(\mathbf{y})$ is the likelihood ratio of \mathbf{y} , λ is the threshold corresponding to $\Lambda(\mathbf{y})$, and \mathcal{D}_0 and \mathcal{D}_1 are the binary decisions that infer whether the vehicle is legitimate or malicious, respectively. Given the decision rule in (15), the false positive and detection rates of an LSDS are functions of λ . The specific value of λ can be set through predetermining a false positive rate, minimizing the Bayesian average cost, or maximizing the mutual information between the system input and output [5]. In this work, we adopt the false positive rate, $\Pr(\Lambda(\mathbf{y}) > \lambda | \mathcal{H}_0)$, and detection rate, $\Pr(\Lambda(\mathbf{y}) > \lambda | \mathcal{H}_1)$, as the core performance metrics for our LSDS. In addition, we adopt the minimum total error as the unique performance metric in order to investigate the impact of key system parameters on the performance of our LSDS.

B. Attack Strategy of the Malicious Vehicle

We assume the malicious vehicle knows all the information known by the BS or the legitimate vehicle. We first discuss how does the malicious vehicle set its true location \mathbf{x}_M . Since there is only one BS in our LSDS, the difference between d_L and d_M can be eliminated by the malicious vehicle through adjusting its transmit power P_M . This is the reason why a single BS cannot detect location spoofing attacks based on the RSS of a channel. As such, we assume the malicious vehicle sets \mathbf{x}_M by minimizing the difference between θ_M and θ_L

under the constraint $|\mathbf{x}_M - \mathbf{x}_L| \geq r_m$. Then, the adopted value of \mathbf{x}_M can be obtained through

$$\mathbf{x}_M^* \triangleq (d_M^*, \theta_M^*) = \underset{|\mathbf{x}_M - \mathbf{x}_L| \geq r_m}{\operatorname{argmin}} |\theta_M - \theta_L|. \quad (16)$$

Given the application scenario of interest as shown in Fig. 1, we assume that \mathbf{x}_M^* is known to the BS. The average signal-to-noise ratio (SNR) of a channel can be readily estimated. As such, we assume that the malicious vehicle adjusts its transmit power to make sure that the average SNR of the malicious channel is the same as that of the legitimate channel, i.e., $\bar{\gamma}_M = \bar{\gamma}_L$, where $\bar{\gamma}_L = P_L g(d_L)/\sigma_L^2$ and $\bar{\gamma}_M = P_M g(d_M)/\sigma_M^2$. Therefore, the transmit power of the malicious vehicle conditioned on \mathbf{x}_M is given by

$$P_M^*(\mathbf{x}_M) = \frac{P_L g(d_L) \sigma_M^2}{g(d_M) \sigma_L^2}. \quad (17)$$

We next discuss how does the malicious vehicle sets its beamformer \mathbf{p} , which is the key vector controlled by the malicious vehicle. The Kullback-Leibler (KL) divergence from $f(\mathbf{y}|\mathbf{x}_M, P_M, \mathbf{p}, \mathcal{H}_1)$ to $f(\mathbf{y}|\mathcal{H}_0)$ is defined as

$$D_{KL}(f(\mathbf{y}|\mathbf{x}_M, P_M, \mathbf{p}, \mathcal{H}_1) || f(\mathbf{y}|\mathcal{H}_0)) = \int \ln \Lambda(\mathbf{y}) f(\mathbf{y}|\mathbf{x}_M, P_M, \mathbf{p}, \mathcal{H}_1) d\mathbf{y}. \quad (18)$$

As per (18), we know that the KL divergence is also the expected log likelihood ratio when the alternative hypothesis is true. Based on (15), we also know that the larger the KL divergence, the more evidence we have for the alternative hypothesis [17]. As such, the malicious vehicle is to minimize the KL divergence presented in (18) in order to minimize the detection rate. Substituting (8) and (12) into (18), we have

$$D_{KL}(f(\mathbf{y}|\mathbf{x}_M, P_M, \mathbf{p}, \mathcal{H}_1) || f(\mathbf{y}|\mathcal{H}_0)) = \operatorname{tr}(\mathbf{R}_0^{-1} \mathbf{R}_1) - N_B - \ln \left(\frac{\det \mathbf{R}_1}{\det \mathbf{R}_0} \right) + \underbrace{(\mathbf{m}_0 - \mathbf{m}_1)^\dagger \mathbf{R}_0^{-1} (\mathbf{m}_0 - \mathbf{m}_1)}_{f_D(\mathbf{p})}. \quad (19)$$

As per (19), we know that only the term $f_D(\mathbf{p})$ is a function of \mathbf{p} . As such, the optimal \mathbf{p} is the one that minimizes $f_D(\mathbf{p})$. Given the format of \mathbf{R}_0 presented in (10), we can see that $f_D(\mathbf{p})$ is minimized when $\|\mathbf{m}_0 - \mathbf{m}_1\|$ is minimized. A constraint on our solution is that we assume the malicious vehicle adopts a directional beamformer, the direction of which is chosen (see below) so as to minimize detection. The rationale for this assumption is that it allows the attacker to optimize his solution based on only one parameter (allowing rapid in-the-field decision making), and allows for a clarity of exposition. The format of our directional beamformer \mathbf{p} is given by

$$\mathbf{p} = \frac{1}{\sqrt{N_M}} [1, \dots, \exp(j(N_M - 1)\tau_M \cos \varphi)]^T, \quad (20)$$

where φ is the beamforming direction. Then, the optimal beamforming direction φ (the value of φ that minimizes the

detection rate) conditioned on \mathbf{x}_M and P_M can be obtained through

$$\varphi^*(\mathbf{x}_M, P_M) = \underset{\varphi \in [0, \pi]}{\operatorname{argmin}} \|\mathbf{m}_0 - \mathbf{K}\mathbf{p}\|, \quad (21)$$

where $\mathbf{K} = \sqrt{P_M g(d_M) K_M / (1 + K_M)} \mathbf{G}_o$. Substituting $\varphi^*(\mathbf{x}_M, P_M)$ into (20), we obtain the optimal directional beamformer of the malicious vehicle, denoted as $\mathbf{p}^*(\mathbf{x}_M, P_M)$. We note that $\mathbf{p}^*(\mathbf{x}_M, P_M)$ may not be the globally optimal beamformer (only near-optimal) for the malicious vehicle due to the imposition of the one-parameter solution (φ) of (20) in obtaining $\mathbf{p}^*(\mathbf{x}_M, P_M)$.

C. Detection Performance of the LSDS

Without loss of generality, we first analyze the detection performance of our LSDS for a general \mathbf{x}_M . Obviously, the malicious vehicle will optimize its transmit power P_M and its beamformer \mathbf{p} for a given \mathbf{x}_M . As such, the following analysis is for $P_M = P_M^*(\mathbf{x}_M)$, and $\mathbf{p} = \mathbf{p}^*[\mathbf{x}_M, P_M^*(\mathbf{x}_M)]$. In order to derive the false positive and detection rates in closed-form expressions, we further assume $\sigma_L^2 = \sigma_M^2$ and $K_L = K_M$ such that $\mathbf{R}_0 = \mathbf{R}_1$. We would like to highlight that these assumptions are practical since the malicious vehicle will not be very far from its claimed location in order to keep a low detection rate. Also, as we show later the detection rate is minimized when $K_L = K_M$, i.e., $K_L = K_M$ is the best case for the malicious vehicle. We will also assume the system knows K_L , through a predetermined measurement campaign in the vicinity of the BS. In principle, knowledge of K_L could be replaced by a pdf which is then encapsulated within the LSDS decision framework. Substituting (8) and (12) into (15), the LRT decision rule can be rewritten as

$$\mathbb{T}(\mathbf{y}) \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\geq}} \Gamma, \quad (22)$$

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

$$\mathbb{T}(\mathbf{y}) = 2\operatorname{Re}\{[\mathbf{m}_1^*(\mathbf{x}_M) - \mathbf{m}_0]^\dagger \mathbf{R}_0^{-1} \mathbf{y}\}, \quad (23)$$

Γ is the threshold for $\mathbb{T}(\mathbf{y})$ given by

$$\Gamma = \ln \lambda + \operatorname{Re}\{[\mathbf{m}_1^*(\mathbf{x}_M) - \mathbf{m}_0]^\dagger \mathbf{R}_0^{-1} [\mathbf{m}_1^*(\mathbf{x}_M) + \mathbf{m}_0]\}, \quad (24)$$

$\mathbf{m}_1^*(\mathbf{x}_M)$ is given by

$$\mathbf{m}_1^*(\mathbf{x}_M) = \sqrt{\frac{P_L g(d_L) K_L}{1 + K_L}} \mathbf{G}_o \mathbf{p}^*[\mathbf{x}_M, P_M^*(\mathbf{x}_M)], \quad (25)$$

and $\operatorname{Re}\{\}$ denotes the real part of a complex number. Then, we derive the false positive rate, $\alpha(\lambda, \mathbf{x}_M)$, and the detection rate, $\beta(\lambda, \mathbf{x}_M)$, of the LSDS in the following theorem.

Theorem 1: The false positive and detection rates of the LSDS for a given \mathbf{x}_M are given by

$$\alpha(\lambda, \mathbf{x}_M) = \mathcal{Q} \left\{ \frac{\ln \lambda + [\mathbf{m}_1^*(\mathbf{x}_M) - \mathbf{m}_0]^\dagger \mathbf{R}_0^{-1} [\mathbf{m}_1^*(\mathbf{x}_M) - \mathbf{m}_0]}{\sqrt{2[\mathbf{m}_1^*(\mathbf{x}_M) - \mathbf{m}_0]^\dagger \mathbf{R}_0^{-1} [\mathbf{m}_1^*(\mathbf{x}_M) - \mathbf{m}_0]}} \right\}, \quad (26)$$

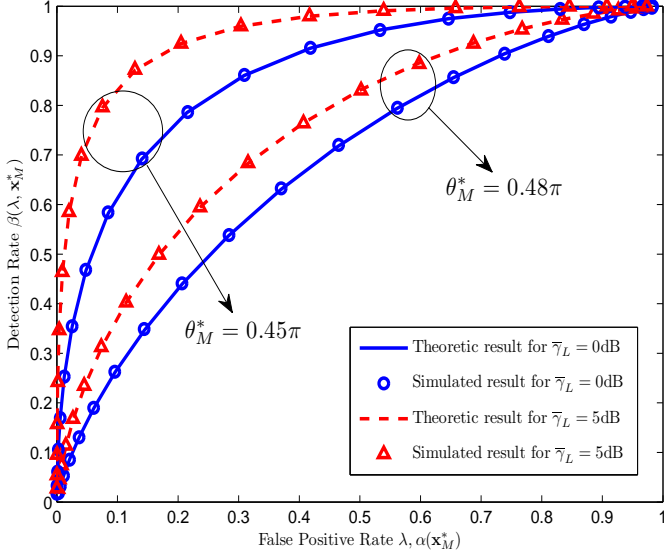


Fig. 3. ROC curves of our LSDS for $N_B = 4$, $N_L = 3$, $N_M = 3$, $\theta_L = \pi/2$, $K_L = K_M = 1\text{dB}$, $\sigma_L^2 = \sigma_M^2 = 0\text{dB}$, $P_M = P_M^*(\mathbf{x}_M^*)$, and $\mathbf{p} = \mathbf{p}^*(\mathbf{x}_M^*, P_M^*(\mathbf{x}_M^*))$.

$$\beta(\lambda, \mathbf{x}_M) = \mathcal{Q} \left\{ \frac{\ln \lambda - [\mathbf{m}_1^*(\mathbf{x}_M) - \mathbf{m}_0]^\dagger \mathbf{R}_0^{-1} [\mathbf{m}_1^*(\mathbf{x}_M) - \mathbf{m}_0]}{\sqrt{2[\mathbf{m}_1^*(\mathbf{x}_M) - \mathbf{m}_0]^\dagger \mathbf{R}_0^{-1} [\mathbf{m}_1^*(\mathbf{x}_M) - \mathbf{m}_0]}} \right\} \quad (27)$$

where $\mathcal{Q}(x) = \frac{1}{2\pi} \int_x^\infty \exp\left(-\frac{t^2}{2}\right) dt$.

Proof: As per (23), we derive the distributions of the test statistic $\mathbb{T}(\mathbf{y})$ under \mathcal{H}_0 and \mathcal{H}_1 as follows

$$\mathbb{T}(\mathbf{y})|\mathcal{H}_0 \sim \mathcal{N} \left(2\text{Re}\{[\mathbf{m}_1(\mathbf{x}_M) - \mathbf{m}_0]^\dagger \mathbf{R}_0^{-1} \mathbf{m}_0\}, \right. \\ \left. 2[\mathbf{m}_1^*(\mathbf{x}_M) - \mathbf{m}_0]^\dagger \mathbf{R}_0^{-1} [\mathbf{m}_1^*(\mathbf{x}_M) - \mathbf{m}_0] \right), \quad (28)$$

$$\mathbb{T}(\mathbf{y})|\mathcal{H}_1 \sim \mathcal{N} \left(2\text{Re}\{[\mathbf{m}_1(\mathbf{x}_M) - \mathbf{m}_0]^\dagger \mathbf{R}_0^{-1} \mathbf{m}_1(\mathbf{x}_M)\}, \right. \\ \left. 2[\mathbf{m}_1^*(\mathbf{x}_M) - \mathbf{m}_0]^\dagger \mathbf{R}_0^{-1} [\mathbf{m}_1^*(\mathbf{x}_M) - \mathbf{m}_0] \right). \quad (29)$$

As per the decision rule in (22) and the definitions of the false positive and detection rates, we obtain the desirable results in (26) and (27) after some algebraic manipulations. ■

The minimum total error conditioned on a \mathbf{x}_M can be expressed as [19]

$$\epsilon(\mathbf{x}_M) = 1 - \beta(\lambda, \mathbf{x}_M) + \alpha(\lambda, \mathbf{x}_M). \quad (30)$$

We note that the detection performance of the LSDS based on \mathbf{x}_M^* can be obtained by substituting \mathbf{x}_M^* into our derived performance metrics. We also note that a decision similar to (22) can be obtained for the case where $\mathbf{R}_0 \neq \mathbf{R}_1$. Under this case, the false positive and detection rates cannot be obtained in closed-form expressions since the distribution of the corresponding test statistic is intractable. However, we can utilize a similar methodology presented in [20] to approximate

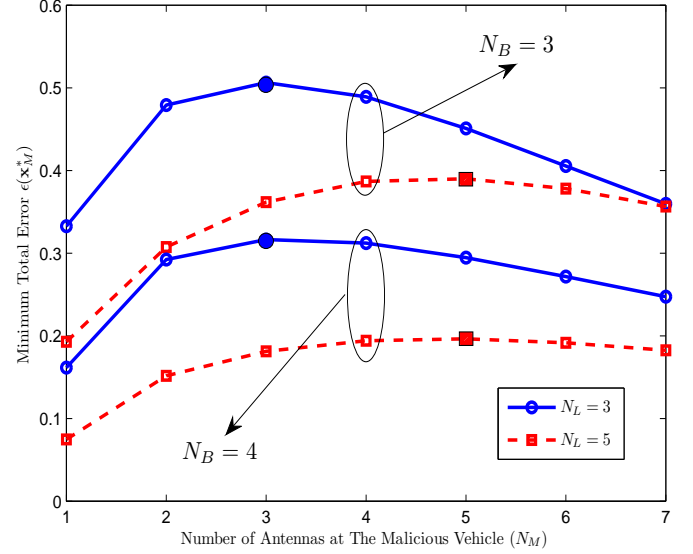


Fig. 4. Minimum total error versus N_M of our LSDS for $\theta_L = \pi/3$, $\theta_M^* = \pi/4$, $K_L = K_M = 1\text{dB}$, $\sigma_L^2 = \sigma_M^2 = 0\text{dB}$, $\bar{\gamma}_L = 0\text{dB}$, $P_M = P_M^*(\mathbf{x}_M^*)$, and $\mathbf{p} = \mathbf{p}^*(\mathbf{x}_M^*, P_M^*(\mathbf{x}_M^*))$.

the distributions of the test statistics in order to obtain the approximations of the false positive and detection rates. Due to the limited space, we left such analysis for further work and we investigate the detection performance of the LSDS for $\mathbf{R}_0 \neq \mathbf{R}_1$ through numerical simulations in the following section.

IV. NUMERICAL RESULTS

In this section, we first present numerical simulations to verify the accuracy of our provided analysis. We also provide some useful insights on the impact of the SNR of the legitimate channel, the location of the malicious vehicle, number of antennas (i.e., N_B , N_L , N_M), and Rician K -factors (i.e., K_L , K_M) on the detection performance of our LSDS.

In Fig. 3, we present the Receiver Operating Characteristic (ROC) curve of our LSDS. In this figure, we first observe that the Monte Carlo simulations precisely match the theoretic results, which confirms our analysis provided in Theorem 1. We also observe that the ROC curves for $\bar{\gamma}_L = 5\text{dB}$ dominate the ROC curves for $\bar{\gamma}_L = 0\text{dB}$. This observation demonstrates that the detection performance of the LSDS increases as the legitimate vehicle's transmit power increases. This is due to the fact that the impact of the channel noise will be relatively suppressed by increasing the transmit power. As expected, we further observe that the ROC curve shifts towards the left-upper corner as $|\theta_M^* - \theta_L|$ increases. This demonstrates the necessity to guarantee a minimum distance between the malicious vehicle's claimed location and its true location.

In Fig. 4, we present the minimum total error versus the number of antennas at the malicious vehicle (N_M) of our LSDS. As expected, we first observe that the minimum total error decreases as N_B or N_L increases. This is due to the fact that the more antennas the legitimate or the BS is equipped

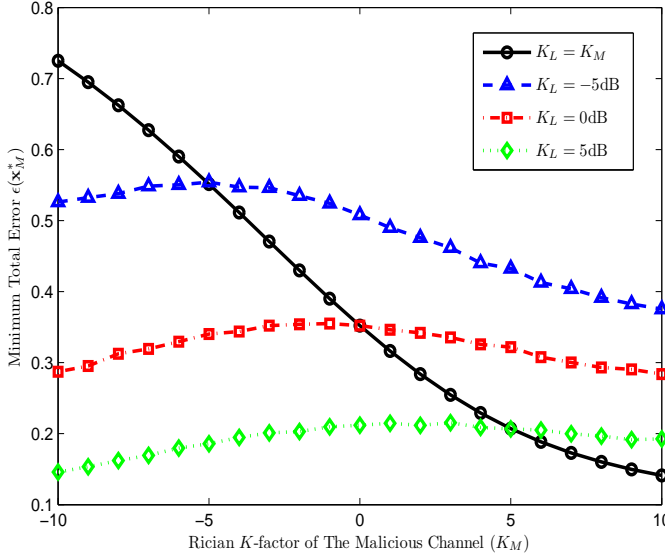


Fig. 5. Minimum total error versus K_M of our LSDS for $N_B = 4$, $N_L = 3$, $N_M = 3$, $\theta_L = \pi/3$, $\theta_M^* = \pi/4$, $\sigma_L^2 = \sigma_M^2 = 0\text{dB}$, $\overline{\gamma}_L = 0\text{dB}$, $P_M = P_M^*(\mathbf{x}_M^*)$, and $\mathbf{p} = \mathbf{p}^*(\mathbf{x}_M^*, P_M^*(\mathbf{x}_M^*))$.

with, the more beamforming gain we can achieve for the legitimate channel. In addition, it is interesting to observe that the minimum total error is maximized when $N_M = N_L$ for arbitrary N_B . This shows that the optimal number of antennas utilized by the malicious vehicle to minimize the detection rate is the same as the number of antennas at the legitimate vehicle. This indicates that if the malicious vehicle is equipped with more antennas than the legitimate vehicle, its attack strategy is to use the same number of antennas as the legitimate vehicle, not to use all of its antennas. In practice, we do not know the number of antennas equipped at the malicious vehicle, but this observation suggests that we can assume $N_M = N_L$ for the attack strategy of the malicious vehicle.

In Fig. 5, we present the simulated minimum total error versus the Rician K -factor of the malicious channel (K_M) of our LSDS. As expected, we first confirm that for $K_L = K_M$ the minimum total error decreases as K_M (or K_L) increases. In addition, it is interesting to observe that the minimum total error is maximized when $K_M = K_L$ for arbitrary K_L . This indicates that the malicious vehicle's attack strategy is to select a true location that is in an environment similar to that of its claimed location (so that K_M is close to K_L) to launch location spoofing attacks.

V. CONCLUSION

In this work, we investigated the detection performance of an LSDS for VANETs with a single BS in Rician fading channels. We first determined the malicious vehicle's true location based on a given VANETs scenario and then determined the optimal transmit power and the optimal directional beamformer for the malicious vehicle to minimize the detection rate. Our analysis first shows that the LSDS performance increases as the Rician K -factor of the legitimate

channel, the number of antennas at the BS, or the number of antennas at the legitimate vehicle increases. We also obtained a counter-intuitive observation that the malicious vehicle's optimal number of antennas is equal to the legitimate vehicle's number of antennas. Finally, we showed that the Rician K -factor of the malicious channel that minimizes the detection rate is identical to the Rician K -factor of the legitimate channel.

ACKNOWLEDGMENTS

This work was funded by The University of New South Wales and Australian Research Council Grant DP120102607.

REFERENCES

- [1] R. A. Malaney, "A location enabled wireless security system," in *Proc. IEEE GlobeCOM*, Nov. 2004, pp. 2196–2200.
- [2] A. Vora, M. Nesterenko, "Secure location verification using radio broadcast," *IEEE Trans. on Dependable and Secure Computing*, vol. 3, no. 4, pp. 377–385, Oct. 2006.
- [3] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2418–2434, Jun. 2010.
- [4] 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.
- [5] 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.
- [6] S. Yan, R. Malaney, I. Nevat, and G. Peters, "Signal strength based location verification under spatially correlated shadowing," in *Proc. IEEE ICC*, Jun. 2014, pp. 2617–2623.
- [7] S. Yan and R. Malaney, "Location Verification Systems in Emerging Wireless Networks," ZTE Communications, No.3, (arXiv:1307.3348) 2013.
- [8] T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfer, "Influence of falsified position data on geographic ad-hoc routing," in *Proceedings of the second European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS)*, Jul. 2005, pp. 102–112.
- [9] S. Capkun, M. Cagalj, G. Karame, and N.O. Tippenhauer, "Integrity regions: authentication through presence in wireless networks," *IEEE Trans. Mob. Comput.*, vol. 9, no. 11, pp. 1608–1621, Nov. 2010.
- [10] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, Jan. 2007.
- [11] B. Yu, C. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs," *J. Parallel Distrib. Comput.*, vol. 73, no. 6, pp. 746–756, Jun. 2013.
- [12] T. Zhang and L. Delgrossi, "Vehicle Safety Communications: Protocols, Security, and Privacy," Wiley, 2012.
- [13] T. Leinmüller, E. Schoch, and F. Kargl, "Position verification approaches for vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 16–21, Oct. 2006.
- [14] G. Yan, S. Olariu, and M. Weigle, "Providing location security in vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 16, no. 6, pp. 48–55, Dec. 2009.
- [15] O. Abumansoor, A. Boukerche, "A secure cooperative approach for nonlinear-of-sight location verification in VANET," *IEEE Trans. Veh. Technol.*, vol. 61, pp. 275–285, Jan. 2012.
- [16] J. Neyman and E. Pearson, "On the problem of the most efficient tests of statistical hypotheses," *Phil. Trans. R. Soc. A*, vol. 231, pp. 289–337, Jan. 1933.
- [17] S. Eguchi and J. Copas, "Interpreting Kullback-Leibler divergence with the Neyman-Pearson lemma," *J. Multivar. Anal.*, vol. 97, no. 9, pp. 2034–2040, Oct. 2006.
- [18] G. E. Forsythe and G. H. Golub, "On the stationary values of a seconddegree polynomial on the unit sphere," *J. Soc. Ind. Appl. Math.*, vol. 13, no. 4, pp. 1050–1068, 1965.
- [19] M. Barkat, *Signal Detection and Estimation*. Boston, MA: Artech House, 2005.
- [20] I. Nevat, G. W. Peters, and I. B. Collings, "Distributed detection in sensor networks over fading channels with multiple antennas at the fusion centre," *IEEE Trans. Signal Process.*, vol. 62, pp. 671–683, Feb. 2014.