International Global Navigation Satellite Systems Association
IGNSS Symposium 2018

Colombo Theatres, Kensington Campus, UNSW Australia
7 – 9 February 2018

Location Verification Performance in the Presence of Verifier Location Error

Ullah Ihsan
Electrical Engineering & Telecommunications, UNSW Australia
ihsanullah@ieee.org

Ziqing Wang
Electrical Engineering & Telecommunications, UNSW Australia
ziqing.wang1@student.unsw.edu.au

Robert Malaney
Electrical Engineering & Telecommunications, UNSW Australia
r.malaney@unsw.edu.au

Andrew Dempster
Electrical Engineering & Telecommunications, UNSW Australia
a.dempster@unsw.edu.au

Shihao Yan
College of Engineering & Computer Science, ANU Australia
shihao.yan@mq.edu.au

ABSTRACT

In this paper, we study the impact on the performance of a Differential Received Signal Strength (DRSS) based Location Verification System (LVS) caused by location errors in the reported positions of verifiers. In this system, the verifiers (trusted) and a non-verified user (initially untrusted) report their locations using the Global Positioning System (GPS). The user's reported position is verified by consistency checks with DRSS measurements made by verifiers. We illustrate how the anticipated location errors on verifier GPS positions can have a significant impact on the location verification performance. The results reported here are important for real-world implementations of an LVS in the context of emerging vehicular networks, in which the verifiers are other nearby vehicles.

KEYWORDS: Vehicle Ad-hoc Network (VANET), Location Verification System (LVS), Intelligent Transportation System (ITS), Differential Received Signal Strength (DRSS)

1. INTRODUCTION

The number of vehicles on our roads is growing at a faster pace than road infrastructure development. This imbalance has resulted in increased traffic congestion and increased road accidents. Engineers in recent times have worked to address these growing problems by introducing an Intelligent Transportation System (ITS). Amongst other outcomes, an ITS aims at efficiently addressing traffic routing, congestion, accidents, smart-roadside tolling, and distribution of traffic loads (e.g. Dimitrakopoulos et al. 2010; Weiland et al. 2000). Such a system greatly relies on the accurate locations of vehicles to achieve its aimed functionalities. However, a user can cheat an ITS by spoofing their location (reporting a claimed GPS position far from their actual position). If such malicious behaviour goes unnoticed this can lead to serious repercussions, e.g., vehicle collisions, injuries and even loss of human life.

A Vehicular Ad-hoc Network (VANET) is an example of an ITS. A VANET enables real time communication in both, vehicle-to-vehicle and vehicle-to-infrastructure. Location verification within the context of VANETs has received considerable attention in recent years (e.g. Malaney 2004, Yan, et al. 2012; Wei, et al. 2013; Yan, et al. 2014). Beyond GPS (or more generally any satellite based positioning system) several positioning schemes such as mobile positioning (e.g. Zhao, 2000) and hybrid positioning systems (e.g. De Angelis, et al. 2013) are in use to help with the location information requirements before the VANET can be allowed to make critical decisions. All such positioning schemes are prone to errors (e.g. Warner, et al. 2003; Tippenhauer et al. 2009; Zandbergen, 2009). While it is possible for a user in these systems to fake his reported location, there is always an error, to some degree, in the reported user's position even if he doesn't intend to spoof his true position. A user, if able to spoof his location, or if the error in his location exceeds system limitations (depending on system parameters), can produce in serious security risks.

In a recent work (Yan et al. 2016) the performance of a DRSS based LVS spatially correlated shadowing was investigated. This work assumed a certain number of verifying static base stations with known (zero error) true locations, and derived the anticipated performance of LVS under such channel conditions. Here, we extend the work of Yan et al. 2016 by studying the performance of a DRSS based LVS when positions of the verifiers possess realistic location errors that arise from GPS positioning. This study mimics the scenario where the verifiers are no longer static base stations, but rather other nearby (trusted) vehicles.

The remainder of this paper is composed as follows. Section 2 describes the system model, Section 3 highlights the attack model, Section 4 provides the numerical results and section 5 concludes the paper.

2. SYSTEM MODEL

The LVS system model is outlined below.

1. System consists of N number of verifiers with known true position $\mathbf{X}_\mathrm{i} = [x_i\,, y_i]$ where $i = 1,2,\ldots,N$.
2. The known true positions $\mathbf{X}_\mathrm{i}$ of all verifiers are subjected to $\mathbf{K}$; the GPS error in units of distance (meters). $\mathbf{K}$ is obtained in simulation via the setting of a standard deviation σ_e in an assumed Gaussian error distribution $f(\sigma_e)$.
3. The claimed position for a genuine or malicious user is referred to as $\mathbf{X_c} = [x_c\,, y_c]$.
4. The malicious and genuine user's true positions are denoted by $\mathbf{X_t} = [x_t\,, y_t]$.
5. Under the 'independent hypothesis' $\mathbf{H_o}$, the system assumes the user to be genuine, that is $\mathbf{X_c} = \mathbf{X_t}$.
6. Under the 'dependent hypothesis' $\mathbf{H_1}$, the system considers the user to be malicious, that is $\mathbf{X_c} \neq \mathbf{X_t}$. For a fake user $||\mathbf{X_c} - \mathbf{X_t}|| \geq r$ where r is the minimum distance between the true and the claimed location of the malicious user. r is a-priori information and is assumed to be known.

Under $\mathbf{H_o}$, the RSS value received from the genuine user by the *i-th* verifier is given by,

$$y_i = u_i + \omega_i\,, \qquad i = 1,2,\ldots,N\,,$$

where $\boldsymbol{\omega_i}$ is a zero-mean normal random variable with variance $\sigma^2_{\boldsymbol{dB}}$ and

$$u_i = p - 10\,\gamma\, log_{10}\left(\frac{d_i^c}{d}\right).$$

Here γ is the pathloss exponent, d_i^c is the Euclidean distance between the true location of the genuine user and the *i-th* verifier and is given by,

$$d_i^c = \sqrt{(x_c - x_i)^2 + (y_c - y_i)^2},$$

and p is calculated as,

$$p = p_t G_t G_r \frac{\lambda^2}{(4\pi d)^2}\,.$$

Here p_t is the transmit power, G_t and G_r are dimensionless quantities and represent transmit and receive antenna gains respectively, λ is the wavelength, and d is the reference distance. Under spatially correlated shadowing conditions ω_i is corelated to ω_j forming a covariance matrix **R** of size N x N. The element R_{ij} of the covariance matrix **R** is given by,

$$R_{ij} = \sigma^2_{\boldsymbol{dB}} \exp\left(-\frac{d_{ij}}{\mathrm{D_c}} \ln 2\right) \qquad i = 1,2,\dots,N \;\text{ and }\; j = 1,2,\dots,N\,,$$

where d_{ij} is the Euclidean distance between the *i-th* and *j-th* verifier, and $\mathrm{D_c}$ is a constant.

Under $\mathbf{H_1}$, the RSS value received by the *i-th* verifier from the malicious user is given by,

$$y_i = p_x + v_i + \omega_i\,, \qquad i = 1,2,\dots,N,$$

where p_x is the extra boosted transmit power set by the malicious user (its value will impact the overall value of p and would be measured the same at all verifiers), and

$$v_i = p - 10\,\gamma\, log_{10}\left(\frac{d_i^t}{d}\right),$$

where d_i^t is the Euclidean distance between fake user and *i-th* verifier.

3. ATTACK MODEL

The malicious user doesn't need to adjust his power but adjusts his location to minimize his chances of detection under DRSS based LVS. We derive the optimal attack location $\mathbf{X}_\mathrm{t}^*$ for the malicious user by calculating the minimum KL divergence from $f(\mathbf{H_1})$ to $f(\mathbf{H_o})$ as below,

$$\mathbf{X}_\mathrm{t}^* = \underset{\|\boldsymbol{X_t} - \boldsymbol{X_c}\| \geq \boldsymbol{r}}{\operatorname{argmin}} \boldsymbol{\varphi}(\mathbf{X_t})\,,$$

where,

$$\boldsymbol{\varphi}(\mathbf{X_t}) = \boldsymbol{D_{KL}}[f(\mathbf{H_1})||f(\mathbf{H_o})].$$
$$= \int_{-\infty}^{\infty} \ln\frac{f(\mathbf{H_1})}{f(\mathbf{H_o})}\, f(\boldsymbol{H_o})\, d\Delta\mathbf{y}.$$

$$= \frac{1}{2}(\Delta\mathbf{v} - \Delta\mathbf{u})^{\mathrm{T}}\,\mathbf{D}^{-1}\,(\Delta\mathbf{v} - \Delta\mathbf{u}).$$

Under $\mathbf{H_o}$ **,** $\Delta\mathbf{y}$ is the (N-1) dimensional DRSS vector given below,

$$\Delta\mathbf{y} = [\Delta y_1\,, \Delta y_2\,, \ldots, \Delta y_{N-1}]^{\mathrm{T}}.$$

whose m-th element is,

$$\Delta y_m = \Delta u_m + \Delta\omega_m\,, \qquad m = 1\,, 2\,, \ldots, N-1.$$

$\Delta\mathbf{u} = [\Delta u_1\,, \Delta u_2\,, \ldots, \Delta u_{N-1}]^{\mathrm{T}}$ is the mean vector with m-*th* element $\Delta u_m = u_m - u_N$. $\Delta\omega_m$ is Gaussian with mean zero and variance given by $2(\sigma^2_{\boldsymbol{dB}} - R_{mN})$. The m-*th* element of $\Delta\omega_m$ is $\Delta\omega_m = \omega_m - \omega_N$. The $(N-1)$ x $(N-1)$ covariance matrix for the $(N-1)$ dimensional DRSS vector $\Delta\mathbf{y}$ is denoted by **D**. The (m, n)-th element $(n = 1\,, 2\,, \ldots, N-1)$ of **D** is given by,

$$D_{mn} = R_{NN} + R_{mn} - R_{mN} - R_{nN}\,.$$

Under $\mathbf{H_1}$ **, t**he m-th value for the DRSS vector $\Delta\mathbf{y}$ is given by,

$$\Delta y_m = \Delta v_m + \Delta\omega_m.$$

$\Delta\mathbf{v} = [\Delta v_1\,, \Delta v_2\,, \ldots, \Delta v_{N-1}\,]^{\mathrm{T}}$ and m-th value of $\Delta\mathbf{v}$ is $\Delta v_m = v_m - v_N$.

4. NUMERICAL RESULTS

4.1 Performance Evaluation Metric

We define a simplified Bayes average cost function to quantify the performance of the LVS in terms of total error. In this function, equal unit costs are assigned to all the decisions. This is set as

$$\varepsilon = P(D_1|\mathbf{H_o})P(\mathbf{H_o}) + P(D_0|\mathbf{H_1})P(\mathbf{H_1}).$$

where $P(\mathbf{H_o})$ and $P(\mathbf{H_1})$ are the a priori probabilities of the occurrences of $\mathbf{H_o}$ (genuine user) and $\mathbf{H_1}$ (malicious user). The a priori probabilities are all set to 0.5. Also, we denote $\alpha = P(D_1|\mathbf{H_o})$ as the false positive rate and $\beta = P(D_1|\mathbf{H_1})$ as the detection rate. In this case, the total error function can be further simplified to

$$\varepsilon = 0.5 \times \alpha + 0.5 \times (1 - \beta).$$

4.2 Results

We now present our numerical results to show the influence of different factors on the performance of DRSS-based LVS system. To be specific the impact of changes in positioning error, the number of verifiers and minimal distance '*r*', on the DRSS based LVS is investigated. In our simulation, *N trusted* verifiers and a claimant (a not yet trusted vehicle) are deployed with randomly generated positions within a 150m x 150m square area. All the verifiers are subjected to different positioning errors in x and y, which are drawn from a zero-mean Gaussian distribution with a fixed standard deviation. The claimant vehicle overhears the communication between verifier vehicles (thus acquires the location of all the vehicles),

and if malicious, can calculate the optimal attacking position given his knowledge of verifier positions and his claimed location. We assume the malicious vehicle's knowledge of the verifier locations is also subject to the positioning errors (i.e. we assume it has no means to acquire the true locations of verifiers). For the physical channel characteristics, the path loss exponent is set to $\gamma = 3$, the transmitted power is set to 30dBm, the reference distance is set to be d = 1m, and the standard deviation of spatially-correlated log-normal shadowing is set to be 5dB. We again note the constraint 'r' that is imposed on the malicious vehicle. That is, its optimal attack position cannot be too close to the claimed location (if at the claimed location there is a higher chance for the malicious vehicle to get caught). We have set the standard deviation of the GPS positioning error from 0m to 50m. To average out the fluctuations caused by the limited simulation runs, a polynomial fitting with an order of 6 is utilised.

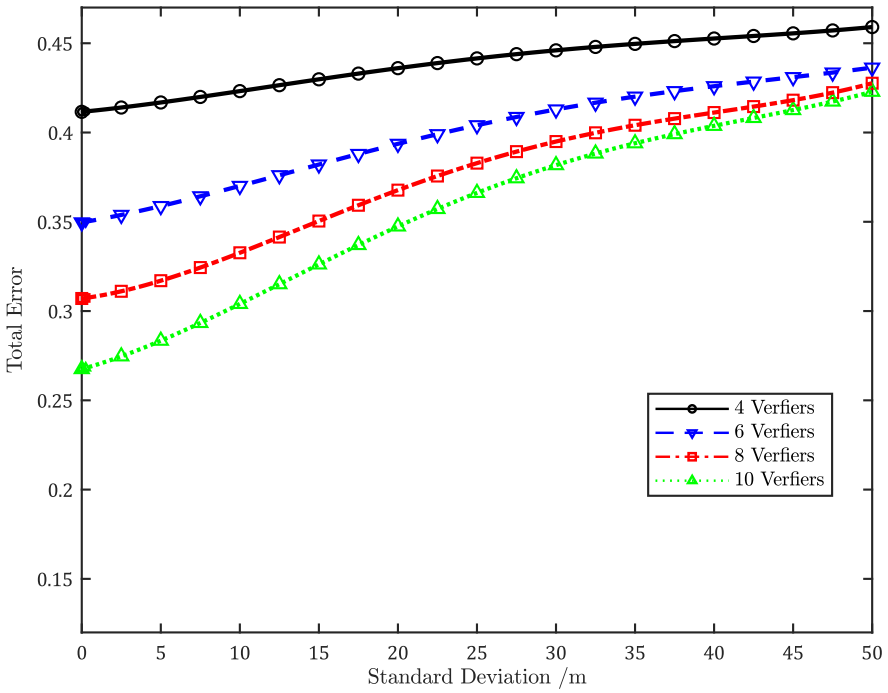

Fig 1: Total error curves of the DRSS-based LVS for $\sigma_{dB} = 5,\ D_c = 400m, r = 50m,\ \boldsymbol{X_t} = \boldsymbol{X_t^*}$ and $N = 4, 6, 8, 10$.

In Fig. 1, we present the total error curves of the DRSS-based LVS with different numbers of verifiers. From each curve, we can see that the performance of the DRSS-based LVS is significantly degraded with the increase in positioning error. We can also see that LVS performance improves with an increase in the number of verifiers. However, this improvement is comparatively significant at lower error deviation values and with a smaller number of verifiers. To be specific, increasing the number of verifiers from 4 to 6 will offer 13% of performance boost at the standard deviation of 5m, 12% of performance boost at the standard deviation of 10m, 8% at 20m, 7% at 30m, 6% at 40m and 4% at 50m. However, increasing the number of verifiers from 6 to 8 can only provide 10% of performance boot at 10m, 6% at 20m, 4% at 30m, 2% at 40m and below 1% at 50m.

Fig.2 shows similar results bit for higher 'r' – quantifying how the larger values of 'r' make for better system performance.

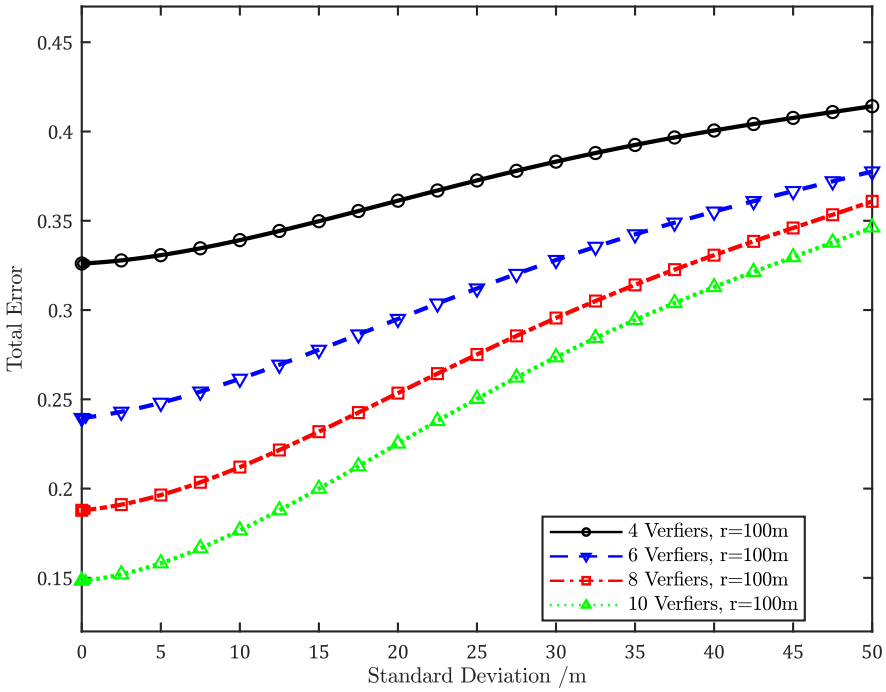

Fig. 2: Total error curves of the DRSS-based LVS for $\sigma_{dB} = 5,\ D_c = 400m, r = 100m,\ \boldsymbol{X_t} = \boldsymbol{X_t^*}$ and $N = 4, 6, 8, 10$.

Finally, in Fig. 3 we plot the impact of uniformly setting the location error of the x and y values of the verifier positions (previous results assumed independent error applied to both components of $\mathbf{X}_\mathrm{i} = [x_i\ , y_i]$).

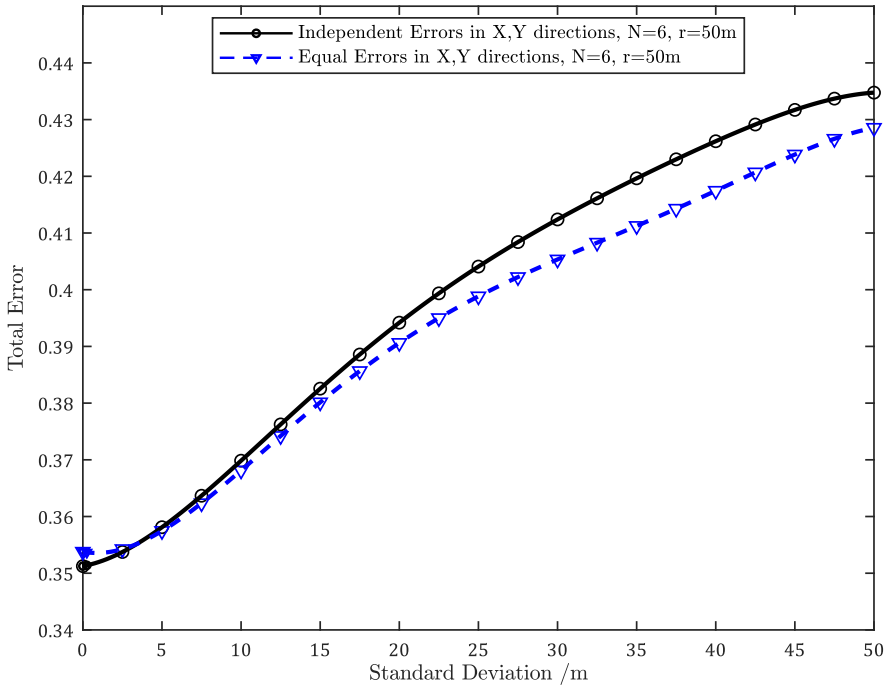

Fig. 3: Total error curves of the DRSS-based LVS with independent/uniform error standard deviations in X and Y directions for $\sigma_{dB} = 5,\ D_c = 400m, r = 50m,\ \boldsymbol{X_t} = \boldsymbol{X_t^*}$ and $N = 6$.

From the figure we can see that the independent errors will further degrade the system performance compared to the uniform error situation, mainly in the high standard deviation region.

5. CONCLUSIONS

In this work, we have analysed the performance of a DRSS based LVS system subject to correlated spatial shadowing and with verifiers under the influence of GPS error. We observe that increasing GPS error directly relates to the degradation in system's performance; that is the ability of the LVS system to detect a fake user decreases. Further, the performance of the DRSS based LVS enhances with an increase in the number of verifiers. As expected it also improves with increasing distance between the claimed location and optimal attack location. The quantitative results presented here are useful to our understanding of location authentication algorithms under real-world conditions in which location information on verifier position is contaminated with realistic GPS errors.

7. REFERENCES

(De Angelis, et al. 2013), G. Angelis, G. Baruffa and S. Cacopardi, "GNSS/cellular hybrid positioning system for mobile users in urban scenarios", IEEE Transactions on intelligent transportation systems 14(1): 313-321.

(Dimitrakopoulos, et al. 2010), G. Dimitrakopoulos and P. Demestichas, "Intelligent transportation systems", IEEE Vehicular Technology Magazine 5(1): 77-84.

(Weiland, et al. 2000), R. Weiland and L. Purser, "Intelligent transportation systems", Transportation in the new millennium.

(Malaney, 2004), R. Malaney, "A location enabled wireless security system", Global Telecommunications Conference, GLOBECOM '04, IEEE.

(Yan, et al. 2012), S. Yan, R. Malaney, I. Nevat and G. Peters, "An information theoretic location verification system for wireless networks", Global Telecommunications Conference, GLOBECOM '12, IEEE.

(Wei, et al. 2013), Y. Wei and Y. Guan, "Lightweight location verification algorithms for wireless sensor networks", IEEE transactions on parallel and distributed systems 24(5): 938-950.

(Yan, et al. 2014), S. Yan, R. Malaney, I. Nevat and G. Peters, "Optimal information-theoretic wireless location verification", IEEE Transactions on Vehicular Technology 63(7): 3410-3422.

(Zhao, 2000), Y. Zhao, "Mobile phone location determination and its impact on intelligent transportation systems", IEEE Transactions on intelligent transportation systems 1(1): 55-64.

(Warner, et al. 2003), J. Warner and R. Johnston, “GPS spoofing countermeasures”, Homeland Security Journal 25(2): 19-27.

(Tippenhauer, et al. 2009), N. Tippenhauer, K. Rasmussen and C. Pöpper, “Attacks on public WLAN-based positioning systems”, Proceedings of the 7th international conference on Mobile systems, applications, and services, ACM.

(Yan, et al. 2016), S. Yan, I. Nevat, G. Peters and R. Malaney, “Location verification systems under spatially correlated shadowing”, IEEE Transactions on Wireless Communications 15(6): 4132-4144.

(Zandbergen 2009), P. Zandbergen, “Accuracy of iPhone locations: A comparison of assisted GPS, WiFi and cellular positioning”, Transactions in GIS 13(s1): 5-25.