FCC SAS Workshop 2014
GN Docket No. 12-354
Focus Area C: SAS Monitoring and Management of Spectrum Use (C1, C2, C3)

LOCATION VERIFICATION USING DIFFERENTIAL RECEIVED SIGNAL STRENGTH

Tamoghna Roy, A. A. (Louis) Beex, and Jeffrey H. Reed
Wireless@VT, ECE, Virginia Tech, Blacksburg, VA 24061

ABSTRACT

An efficient enforcement mechanism is one of the pre-requisites for a spectrum sharing system. The enforcement system should be able to verify conformance and take prompt action to ensure compliance. Thus verification is the first step of any enforcement system. Verification should be prompt to ensure that licensed users can use the spectrum access system with a minimum of delay. In addition the verification system should be sensitive and able to ascertain with high probability whether the location information provided by a user is valid or not.

A basic verification approach is outlined here, based on some anchor nodes and a trusted transmitter (which may itself be one of the anchor nodes). The locations of the anchor nodes and the transmitter are known. To begin, the received signal strength of the known transmitter is recorded at the different anchor points and then all pairwise differences are computed. From these pairwise values, the corresponding differential quantity obtained from the log-distance relationships are subtracted, resulting in residuals. These residuals – which are modeling errors in the DRSS (differential received signal strength) localization criterion – account for the stochastic characteristics (e.g. shadowing) of the environment under consideration and act as a point of reference. When an untrusted transmitter announces its location the above process is used to compute a second set of residuals and the two sets of residuals are compared using appropriate statistical tests in order to arrive at the conclusion that they are, or are not, drawn from the same distribution.

While extensive simulation and refinement of the DRSS residual approach is in progress, our initial simulation results show that this approach can detect differences between the announced and actual location of an untrusted transmitter down to as low as 100 m. It is relevant to further note that evaluation of the modeling residuals is based on known locations, does not require any optimization, and is therefore a quick process.

1. INTRODUCTION

Enforcement of spectrum sharing in a (database-driven) dynamic SAS requires verification of conformance to transmit requests that are deemed acceptable (this includes characteristics such as transmit power, modulation format, etc.). The acceptability of one or more of the latter characteristics may be location dependent, thereby requiring that a user report its location so that it can be verified and the transmit request can be declared valid or conforming. A user - with otherwise conforming equipment and transmit requests - could be spoofing its location in order to get more advantageous transmit

capability. Location verification works to quickly avoid/mitigate such behavior that is detrimental to network performance, by declaring location-spoofed transmit requests invalid. If there is a reach-back capability built into the SAS then a user that is non-conforming (NCU) due to faulty equipment can be turned off remotely and quick enforcement is possible. However, if there is an NCU and there is no reach-back possible, then the location verification step will need to be followed or replaced with a much more complex localization step in order to facilitate enforcement by more time-consuming means.

In this work we give a method for location verification using Differential Received Signal Strength (DRSS) information. Signal Strength information is readily available and the proposed method is computationally efficient, which makes it fast. Section 2 gives an overview of the notations and equations used and then proceeds to explain the proposed location verification method. Section 3 presents initial simulation results with a brief discussion. The conclusion and directions for future work are provided in Section 4.

2. OVERVIEW OF THE METHOD

2.1 Background

The signal from an emitter suffers attenuation due to path loss, a phenomenon that is modeled by a log-distance relationship [1]. The RSS value recorded at the *k*-th anchor node is given by:

$$P(d_k) = P(d_0) - 10\alpha \log_{10}\left({d_k}/{d_0} \right) \tag{1}$$

where α is the path loss constant ranging from 2 (ideal Line of Sight (LOS) conditions) to 6. $P(d_0)$ is the power at a known distance d_0 and d_k is the Euclidean distance between the *k*-th anchor node and the emitter:

$$d_k = \sqrt{(x_k - x)^2 + (y_k - y)^2} \tag{2}$$

The expression in (1) accounts for the path loss. Other stochastic components of the environment can be lumped into a single random variable, resulting in the RSS model:

$$L(d_k) = P(d_0) - 10\alpha \log_{10}\left({d_k}/{d_0} \right) + x_k \tag{3}$$

where x_k represents the random component. Depending on the environment we want to model, x_k can assume a particular form. In this work we are simulating an environment which has spatially correlated shadowing. So in this case x_k follows a normal distribution:

$$X_k \sim N\left(0, \sigma_s^2\right) \tag{4}$$

where σ_s^2 is the shadowing variance. The two random variables X_i and X_j are correlated and the correlation matrix is given by:

$$R(i,j) = \sigma_s^2 \exp\left(-\frac{d_{ij}}{d_c}\ln 2\right) \tag{5}$$

where d_{ij} is the distance between the *i*-th and the *j*-th anchor nodes and d_c is the so-called correlation distance – corresponding to a correlation coefficient of 0.5.

The RSS expression in (3) depends on a constant term $P(d_0)$ which needs to be calibrated and that makes for an expensive proposition. One way to bypass that parameter is to take the pairwise difference between the RSS values recorded at different anchor nodes [2]. Thus, the log-distance relationship for DRSS (differential received signal strength) is modified to:

$$\begin{aligned} L(d_i, d_j) &= L(d_i) - L(d_j) \\ &= 10\alpha \log_{10}\left(d_j / d_i\right) + \Delta x_{ij} \end{aligned} \tag{6}$$

The term Δx_{ij} is the difference between two correlated Gaussian variables X_i and X_j:

$$\Delta X_{ij} \sim N\left(0, 2\left(1-\rho_{ij}\right)\sigma_s^2\right) \tag{7}$$

and ρ_{ij} is the corresponding correlation coefficient.

2.2 Verification Approach

In a practical situation we will have the RSS values and hence can calculate the quantity $L(d_i, d_j)$. Given an estimate of the path loss component α we can calculate the term $10\alpha \log_{10}\left(d_j / d_i\right)$ since the positions of the reference nodes are known. We rewrite (6) in the following way:

$$\xi_{ij} = L(d_i, d_j) - 10\alpha \log_{10}\left(d_j / d_i\right) \tag{8}$$

where ξ_{ij} is the DRSS residual obtained for the *i*-th and *j*-th anchor nodes for a transmitter at (x, y).

In the proposed verification scheme we use a reference transmitter, i.e. a transmitter for which we know the position. This reference transmitter can be seen as a trustworthy user. In fact we can take one of the anchor nodes to be a reference node and use a beacon signal to evaluate the (ground-truth) residuals.

When an unknown transmitter announces its location we assume it to be true, calculate the residuals, and compare with the residuals obtained from the reference case. Based on an appropriate comparison method we then conclude if the announced location of the transmitter is true or not.

We illustrate the point with an example. Figure 1 shows the location of the anchor nodes (N = 16) and the reference transmitter, as well as the announced and the actual location of the unknown transmitter in a 1000 m by 1000 m area. The

distance between the actual location and the announced location of the unknown transmitter – which will be called the "spoof distance" – is 100 m.

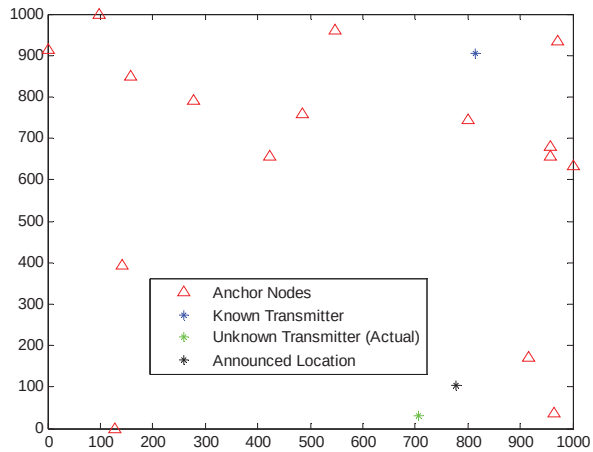

Figure 1: Configuration of the Anchor Nodes, Reference Transmitter, and Unknown Transmitter with Spoof Distance = 100 m.

Figure 2 indicates the distribution of residuals in the form of boxplots (the median in red, the blue box indicating the 25th and 75th percentile, and the whiskers indicating $\pm 3\sigma$) as obtained for the position of the reference transmitter, the announced location of the unknown transmitter, and the actual location of the transmitter.

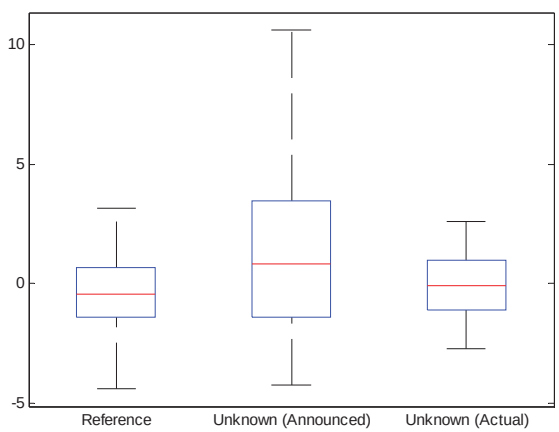

Figure 2: Boxplot of Residuals for the Reference and Unknown Transmitter with Spoof Distance = 100 m.

While in reality the actual location of the unknown transmitter will not be known to us, that particular case is shown here for illustrative purposes; noting that Figure 2 shows that the distribution of residuals obtained using the location of the reference transmitter and the distribution of residuals obtained using the actual location of the unknown transmitter have comparable spread. On the other hand, for a spoof distance of 100 m the spread of the distribution of residuals is markedly different.

To illustrate this point further, we look at a second case, with a spoof distance of 10 m. Figure 3 shows the configuration of the anchor nodes and the transmitters and Figure 4 shows the boxplots of the various residuals. From Figure 4 we see that the spread of all three distributions is comparable, unlike in the previous case.

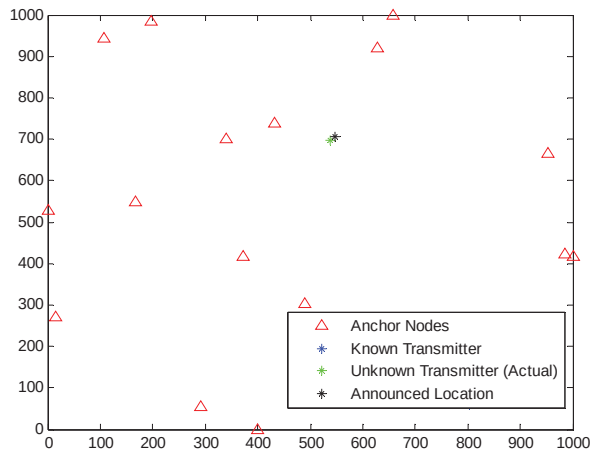

Figure 3: Configuration of the Anchor Nodes, Reference Transmitter, and Unknown Transmitter with Spoof Distance = 10 m.

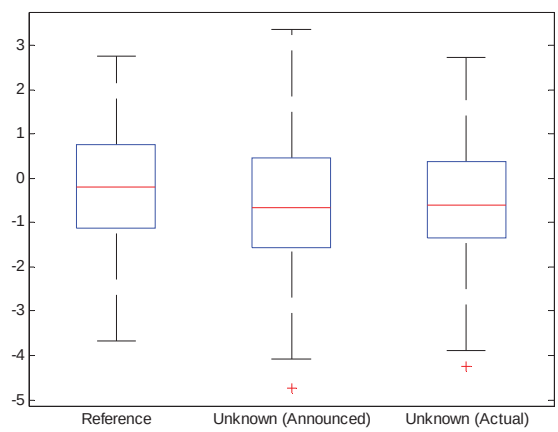

Figure 4: Boxplot of Residuals for the Reference and Unknown Transmitter with Spoof Distance = 10 m.

The two examples above indicate that the spread of the distribution of the residuals gives an idea about the spoof distance. While the boxplots shown in Figures 2 and 4 provide a qualitative comparison between the spread of the two distributions, it is desirable to have a quantitative measure to compare the spread of two distributions. For such a quantitative measure we define the 'Contrast Index' (CI) as follows:

$$CI = \frac{M\left(\xi_{ij}^{announced}\right)}{M\left(\xi_{ij}^{reference}\right)} \tag{9}$$

where $M(.)$ represents an appropriate measure of dispersion, $\xi_{ij}^{announced}$ are the residuals obtained using the announced location of the unknown transmitter, and $\xi_{ij}^{reference}$ are the residuals computed using the location of the reference transmitter.

The next task is to choose a measure of dispersion. Variance is by far the most common measure of dispersion, with variants available that are robust against outliers. However, for our purpose it is desired to highlight the contrast. Hence we chose Range, i.e. the difference between the maximum and the minimum value of the residuals, as the measure of dispersion.

3. RESULTS AND DISCUSSION

3.1 Simulation Results

For simulation purposes we define an environment which has dimension of 1000 m by 1000 m. For each realization, within that box we randomly distribute the anchor nodes, the reference, and the unknown transmitter. A particular spoof distance is set and used to generate an announced location for the unknown transmitter.

As mentioned earlier, we are simulating an environment with spatially correlated shadowing. Table 1 shows the relevant simulation parameters:

Table 1: Simulation Parameters

Parameters	Value
Path Loss Component (α)	4
Standard Deviation of Shadowing (σ_s)	1 dB
Correlation Distance (d_c)	500 m
Reference Power $(P[d_0])$	-2.85 dBm
Ensemble Size	10,000

Figure 5 shows the histogram of the Contrast Index for a Spoof Distance of 0 m, i.e. the histogram for ground truth behavior, when using *N*=16 anchor nodes.

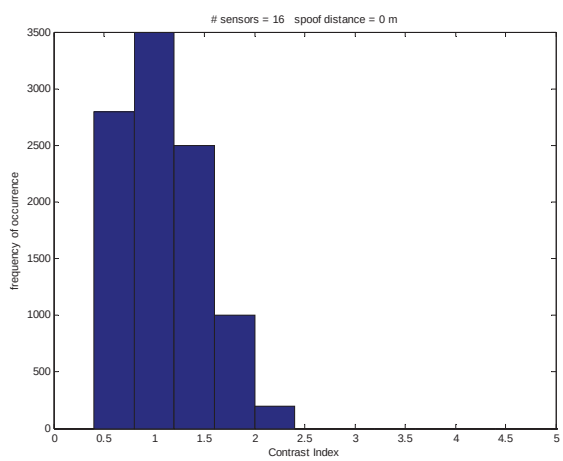

Figure 5: Contrast Index for Spoof Distance of 0 m, 16 anchor nodes.

Figure 6 shows the histogram of the Contrast Index for a Spoof Distance of 100 m, when using *N*=16 anchor nodes.

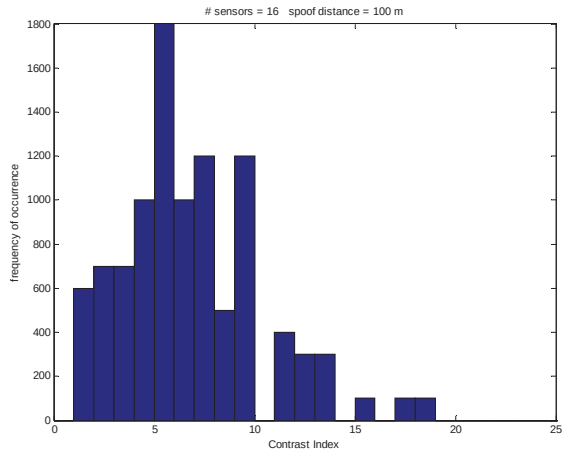

Figure 6: Contrast Index for Spoof Distance of 100 m, 16 anchor nodes.

3.2 Discussion

Figure 5 shows that the range of the residuals is generally distributed around the value of 1 when the spoof distance is 0 m, which is expressed in Fig. 2 by the similarity in the box plots for the reference and actual location. As expected, the contrast index increases as the Spoof Distance increases; this is observed in Fig. 6. As a result, the contrast index can be used for location verification. Figures 5 and 6 suggest that a threshold can be determined to decide between the hypotheses "Announced Location is True" and "Announced Location is False" in a trade-off between the probabilities of false alarm and missed alarm. Fig. 7 shows the sample CDFs (cumulative distribution functions) based on the raw data that produced the histograms in Figs. 5 and 6. The ground truth is actually shown as 1-CDF, in order to make an equal-error comparison easier.

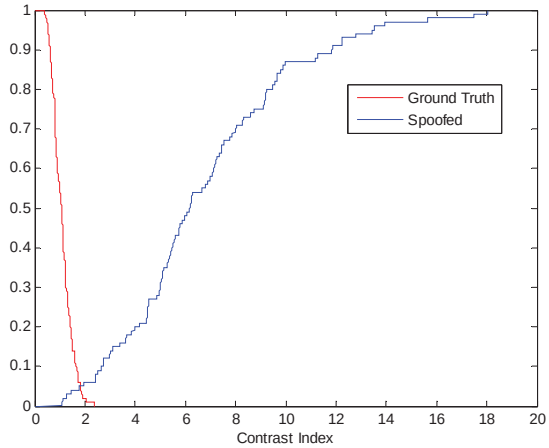

Figure 7: Sample CDFs, spoof distance 100 m, 16 anchor nodes.

The illustrative example arising from Fig. 7 occurs at the (equal-error) intersection of the two graphs: for a CI threshold of 1.8 there is a 5% probability of missing a spoofed distance of 100 m, while there is also a 5% probability of false alarm. Note that 94% (or more) of spoof distances of 100 m (or more) will be detected with the CI threshold set to 2.4. While the 5% false alarm rate in this example may be high, using for example a different Contrast Index or more anchor nodes could

reduce the false alarm probability. Note also that for the example above, using a CI of 2.4 reduces the false alarm probability to zero, while still detecting 94% of spoof distances of 100 m or more. While spoofing of location may provide benefit to an individual user, allowing location spoofing to happen takes away capacity from the network, i.e. it would be at the expense of other users, and therefore cannot be tolerated. Fortunately, the approach outlined here could be an effective mechanism of enforcement that could be quite inexpensive to implement as well. The latter is due to being computationally fast, not involving optimization, and being based on RSS measurements.

This work is being extended in the direction of finding better measures of dispersion, automating the process of choosing a suitable threshold, and determining the effect of the number of anchors used.

4. CONCLUSION

A framework for location verification was presented which has low latency and yet is effective in detecting spoof distances greater than 100 m. The approach is based on readily available received signal strength measurements and the behavior of the residuals in a model that incorporates correlated shadowing.

ACKNOWLEDGMENT

This work is supported by the National Science Foundation under Grant 1247928. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

[1] T. S. Rappapport, Wireless Communications: Principles and Practice, 2nd ed. New Jersey: Prentice-Hall, 2002.

[2] Jeong Heon Lee and R.M. Buehrer, "Location Estimation Using Differential RSS with Spatially Correlated Shadowing," IEEE Global Telecommunications Conference (GLOBECOM) 2009, pp. 1-6, Nov. 30 - Dec. 4, 2009.