ADLS: Attack Detection for Wireless Localization Using Least Squares

Yingying Chen, Wade Trappe, Richard P. Martin
{yingche,rmartin}@cs.rutgers.edu, trappe@winlab.rutgers.edu
Department of Computer Science and Wireless Information Network Laboratory
Rutgers University, 110 Frelinghuysen Rd, Piscataway, NJ 08854

Abstract— **Obtaining accurate positions of wireless devices is critical for location-dependent services. However, as more location-based services are deployed, the more tempting the localization service is as a target for malicious attacks. In this work, we propose an Attack Detection scheme using Least Squares (ADLS) for localization in wireless networks. ADLS is based on statistical significance testing. We provide both a theoretical formulation and analytic solution for our ADLS scheme. We further conducted a trace-driven evaluation by applying signal strength attacks to real data collected in an office building. Our experimental study provides strong evidence for the effectiveness of ADLS with high detection rates and low false positive rates.**

I. Introduction

As more location-dependent services are deployed, the localization system can become the target of malicious attacks. In particular, the localization infrastructure can be subjected to non-cryptographic attacks which cannot be addressed through traditional security services, for example, when signals are attenuated, amplified, or reflected by an adversary. It has been shown that localization performance can degrade significantly under these kinds of physical attacks, and that they are easy to implement with common materials [1].

Compromised localization results can lead to serious consequences because the location of wireless devices is a critical input to many upper-level network applications, which motivates us to provide the localization service with an attack detection capability. In this work we thus propose an Attack Detection scheme using Least Squares (ADLS) for wireless networks. Least Squares (LS) is a widely used multilateration algorithm, as is evidenced by its broad application as a step in many recent localization research works [2]–[5]. Our attack method could thus easily be incorporated as a step in LS algorithms, or could be used as a stand-alone detector if another localization algorithm is used. In addition, our analytic approach focuses on the linear least squares (LLS) because mathematical analysis of LLS is tractable, resulting in equations with closed-form solutions.

We use a combination of analytic and experimental analysis for our attack detection work. We propose a generalized mathematical model for attack detection which is the foundation of the ADLS scheme. We formulate attack detection as a statistical significance testing problem. Our approach is to apply linear regression to the LS localization process and then use the resulting residuals as the test statistic.

The statistical significance level is used to determine whether the localization result is being attacked by adversaries; if the observed statistic is different enough from the normal range, the ADLS claims there is an attack.

To evaluate our theoretical formulation and analytic solution, we experimented using an existing deployment of 802.11 wireless networks and the received signal strength (RSS) for ranging estimation. We applied a linear attenuation attack model to the RSS readings. We then quantified the effectiveness of ADLS by studying the detection rates and the false positive rates under attacks of different severities.

Our experimental results show that the ADLS scheme is effective in detecting location anomalies with high detection rates and low false positive rates. ADLS is easy to conduct and is suitable for both single hop and multi hop ranging methods because it is independent of the ranging modality used by the localization system.

II. Feasibility of Attacks

In our terminology, the wireless *node* or *device* is the object to be localized, and the *landmark* is a device or access point that knows its location. Localization is often built upon different ranging modalities from nodes to landmarks, such as Received Signal Strength (RSS), Time-of-Arrival (TOA) Angle-of-Arrival (AOA), and hop count. These all rely on the measurement of the physical properties of the wireless system. Adversaries can apply non-cryptographic attacks against the measurement processes, bypassing conventional security services, and as a result can affect the localization performance [5].

A. Signal Strength Attacks

In this work, we choose to use RSS as the ranging modality for LS localization. An adversary can attack the wireless node directly or compromise the landmarks involved in localization by attenuating or amplifying the signal strength readings. Based on our experimental attacks using real materials, we use the linear attack model [1] (i.e. a material causes a constant percentage power loss independent of distance) to describe the effect of an attack on the RSS readings at the wireless device or at the landmarks. We found that these attacks are easy to conduct with low cost materials. The linear relationship implies that it is easy for an adversary to control the effect

Proceedings of the Fifth Annual IEEE International Conference
on Pervasive Computing and Communications Workshops(PerComW'07)
0-7695-2788-4/07 $20.00 © 2007 IEEE

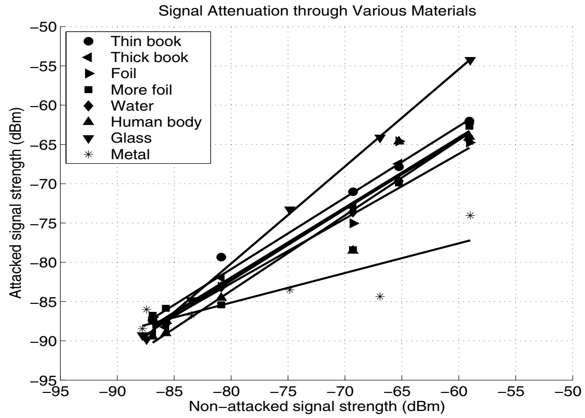

Fig. 1. Linear attack model based on signal strength going through different materials

of an attack on the observed signal strength by appropriately selecting different materials.

III. Localization Using Least Squares

To perform localization with LS requires 2 steps: ranging and lateration.

Ranging Step: There are many ways to perform ranging, such as RSS-to-distance, TOA-to-distance and hop-count. We note that ADLS can work with any ranging modality.

Lateration Step: From the estimated distances d_i and known positions (x_i, y_i) of the landmarks, the position (x, y) of the localizing node can be found by finding $(\hat{x}, \hat{y})$ satisfying:

$$(\hat{x}, \hat{y}) = arg\min_{x,y}\sum_{i=1}^{n}[\sqrt{(x_i-x)^2+(y_i-y)^2}-d_i]^2 \tag{1}$$

where n is the total number of landmarks. We call solving the above problem *Nonlinear Least Squares*, or NLS.

Solving the NLS problem requires significant complexity and is difficult to analyze. We can approximate the NLS solution and linearize the problem by solving the equation $\mathbf{Ax} = \mathbf{b}$ with [6]:

$$\mathbf{A} = \begin{pmatrix} x_1 - \frac{1}{n}\sum_{i=1}^{n} x_i & y_1 - \frac{1}{n}\sum_{i=1}^{n} y_i \\ \vdots & \vdots \\ x_n - \frac{1}{n}\sum_{i=1}^{n} x_i & y_n - \frac{1}{n}\sum_{i=1}^{n} y_i \end{pmatrix} \tag{2}$$

and

$$\mathbf{b} = \frac{1}{2}\begin{pmatrix} (x_1^2 - \frac{1}{n}\sum_{i=1}^{n} x_i^2) + (y_1^2 - \frac{1}{n}\sum_{i=1}^{n} y_i^2) \\ -(d_1^2 - \frac{1}{n}\sum_{i=1}^{n} d_i^2) \\ \vdots \\ (x_n^2 - \frac{1}{n}\sum_{i=1}^{n} x_i^2) + (y_n^2 - \frac{1}{n}\sum_{i=1}^{n} y_i^2) \\ -(d_n^2 - \frac{1}{n}\sum_{i=1}^{n} d_i^2) \end{pmatrix}. \tag{3}$$

Note that $\mathbf{A}$ is described by the coordinates of landmarks only, while $\mathbf{b}$ is represented by the distances to the landmarks together with the coordinates of landmarks. $\mathbf{x}$ is the position vector $(x, y)^T$. We call the above formulation of the problem *Linear Least Squares*, or LLS. The estimate of $\mathbf{x}$ is obtained via $\mathbf{x} = (\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{b}$.

IV. Attack Detection

A. Generalization of the Problem

The attack detection problem in localization can be formulated as statistical significance testing. We define the null hypothesis as $\mathbf{H_0}$: $normal(noattack)$. By choosing a test statistic $\mathbf{T}$ for significance testing, if an observed value of the test statistic $\mathbf{T^{obs}}$ differs enough from the hypothesized values, the null hypothesis will be rejected. In ADLS, rejecting $\mathbf{H_0}$ is equivalent to claiming that the localization result is under attack.

B. The Residuals

In practice, during the localization phase there are errors from the ranging estimation. The LLS formulation can be refined as $\mathbf{b} = \mathbf{Ax} + \mathbf{e}$ where $\mathbf{e}$ consists of estimation errors. The localization result is $\hat{\mathbf{x}} = (\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{b}$. Then the fitted values $\hat{\mathbf{b}}$ corresponding to the observed values $\mathbf{b}$ are given by

$$\hat{\mathbf{b}} = \mathbf{A}\hat{\mathbf{x}} = \mathbf{A}[(\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{b}] = \mathbf{A}(\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{b}. \tag{4}$$

Next, we define the vector of residuals $\hat{\mathrm{e}}$ as

$$\hat{\mathrm{e}} = \mathbf{b} - \hat{\mathbf{b}} = [1 - \mathbf{A}(\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T]\mathbf{b}. \tag{5}$$

We assume the errors are uncorrelated random variables following a Gaussian distribution. Then the residuals also follow the Gaussian distribution, $\mathbf{N}(\mu, \mathbf{\Sigma})$, since the residuals are a linear combination of the elements of $\mathbf{b}$ or of $\mathbf{e}$ [7]. Here, μ is the mean vector and $\mathbf{\Sigma}$ is the covariance matrix. We choose the residuals $\hat{\mathrm{e}}$ as the test statistic $\mathbf{T}$ for attack detection.

C. The Detection Scheme

For a node, after performing localization using LS, we have an observed residual $\hat{\mathrm{e}}^{\mathbf{obs}}$. The residuals are correlated Gaussian random variables and the multivariate Gaussian distribution of $\hat{\mathrm{e}}$ can be expressed as:

$$f(\hat{\mathrm{e}}) = \frac{1}{(\sqrt{2\pi})^n|\mathbf{\Sigma}|^{\frac{1}{2}}}e^{-\frac{1}{2}(\hat{\mathrm{e}}-\mu)^{\mathbf{T}}\mathbf{\Sigma^{-1}}(\hat{\mathrm{e}}-\mu)}. \tag{6}$$

In order to determine whether the location result is compromised by adversaries, we need to test the null hypothesis and calculate the probability

$$P = 1 - M \tag{7}$$

against the significance level α, where

$$M = \frac{1}{(\sqrt{2\pi})^n|\mathbf{\Sigma}|^{\frac{1}{2}}}\int ... \int_E e^{-\frac{1}{2}(\hat{\mathrm{e}}-\mu)^{\mathbf{T}}\mathbf{\Sigma^{-1}}(\hat{\mathrm{e}}-\mu)}d\hat{e}_1...d\hat{e}_n \tag{8}$$

and E is the integration region defined by $(\hat{\mathrm{e}}-\mu)^{\mathbf{T}}\mathbf{\Sigma^{-1}}(\hat{\mathrm{e}}-\mu) \leq X^2$ with

$$X^2 = (\hat{\mathrm{e}}^{\mathbf{obs}}-\mu)^{\mathbf{T}}\mathbf{\Sigma^{-1}}(\hat{\mathrm{e}}^{\mathbf{obs}}-\mu).$$

We can express the term

$$\begin{aligned}(\hat{\mathrm{e}}-\mu)^{\mathbf{T}}\mathbf{\Sigma^{-1}}(\hat{\mathrm{e}}-\mu) &= (\hat{\mathrm{e}}-\mu)^{\mathbf{T}}\mathbf{D^T D}(\hat{\mathrm{e}}-\mu) \\ &= (\mathbf{D}(\hat{\mathrm{e}}-\mu))^{\mathbf{T}}(\mathbf{D}(\hat{\mathrm{e}}-\mu)) \\ &= \mathbf{y^T y}. \end{aligned} \tag{9}$$

Substituting $\mathbf{y} = \mathbf{D}(\hat{\mathbf{e}} - \mu)$ into Equation (8), we get

$$M = \frac{1}{(\sqrt{2\pi})^n} \int \dots \int_{E'} e^{-\frac{1}{2}\mathbf{y}^{\mathbf{T}}\mathbf{y}} dy_1 \dots dy_n \qquad (10)$$

with E' defined by $\mathbf{y}^{\mathbf{T}}\mathbf{y} \leq X^2$. We further calculate the integral by changing to polar coordinates, we get

$$\begin{aligned} M &= \frac{1}{(\sqrt{2\pi})^n} \int_0^X \int_0^{2\pi} \int_0^{\pi} \dots \int_0^{\pi} [e^{-\frac{r^2}{2}} r^{n-1} dr d\phi_1 \\ &\quad sin\phi_2 d\phi_2 \dots sin^{n-2}\phi_{n-1} d\phi_{n-1}] \\ &= \frac{1}{(\sqrt{2\pi})^n} \int_0^X e^{-\frac{r^2}{2}} r^{n-1} dr \times \int_0^{2\pi} d\phi_1 \\ &\quad \times \prod_{i=2}^{n-1} \int_0^{\pi} sin^{i-1}\phi_i d\phi_i \\ &= \frac{2}{(\sqrt{\pi})^{n-2}} \times A_{r,n} \times \prod_{i=2}^{n-1} B_i \qquad (11) \end{aligned}$$

with

$$A_{r,n} = \frac{1}{(\sqrt{2})^n} \int_0^X e^{-\frac{r^2}{2}} r^{n-1} dr$$

and

$$B_i = \int_0^{\pi} sin^{i-1}\phi_i d\phi_i.$$

Using $v = r^2/2$, we have

$$A_{r,n} = \frac{1}{2} \int_0^{\frac{X^2}{2}} e^{-v} v^{\frac{n-2}{2}} dv = \frac{1}{2} \times \Gamma(\frac{n}{2}, \frac{X^2}{2}) \qquad (12)$$

where Γ is the incomplete gamma function. Since

$$B_i = \beta(\frac{i}{2}, \frac{1}{2}) = \frac{\Gamma(\frac{i}{2})}{\Gamma(\frac{i+1}{2})} \times \sqrt{\pi}. \qquad (13)$$

Through further simplification, we can get

$$\prod_{i=2}^{n-1} B_i = (\sqrt{\pi})^{n-2} \times \frac{1}{\Gamma(\frac{n}{2})}. \qquad (14)$$

Hence, substituting Equations (12) and (14) into (11), we obtain the probability mass

$$M = \frac{\Gamma(n/2, X^2/2)}{\Gamma(n/2)} \qquad (15)$$

where Γ is the incomplete gamma function. If the probability is sufficiently low, i.e., $P = 1 - M < \alpha$, then $\hat{\mathbf{e}}^{\mathbf{obs}}$ is statistically significant and we can conclude the location result is under attack. In our study, we have tested with $\alpha = 0.01$ and $\alpha = 0.05$.

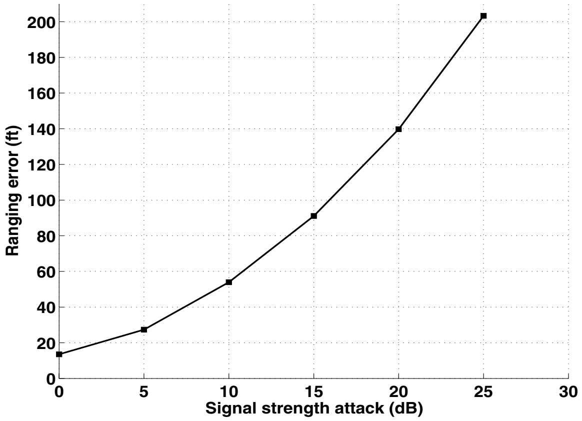

Fig. 2. Effects of RSS attacks to ranging estimation.

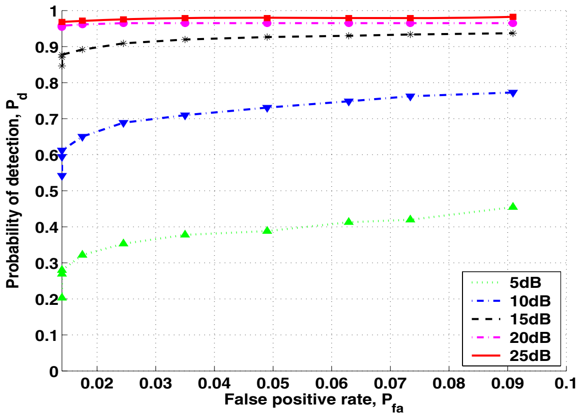

Fig. 3. ROC curves

V. Experimental Study

A. Methodolody

To evaluate the effectiveness of ADLS, we took a trace-driven approach by applying signal strength attenuation and amplification attacks, using a linear attack model obtained from our investigation as shown in Figure 1, to the RSS readings collected from a real office building. Our experimental study is performed utilizing the 802.11 wireless networks and 802.11 PCMCIA cards. We have collected RSS readings at 286 locations on a floor within the office building. The RSS reading at each location is averaged over 60 RSS samples with one sampling scan per second.

B. Metrics

In order to evaluate the performance of our attack detection methods, we will utilize the following metrics:

Detection Rate (DR): The Detection Rate is defined as the percentage of localization attempts that are determined to be under attack, i.e.:

$$DR = \frac{N_{attack}}{N_{total}} \qquad (16)$$

where N_{total} is the total number of localization attempts and N_{attack} is the number concluded under attack by detection. Note that when the signal is attacked, the detection rate corresponds to the probability of detection P_d, while under normal

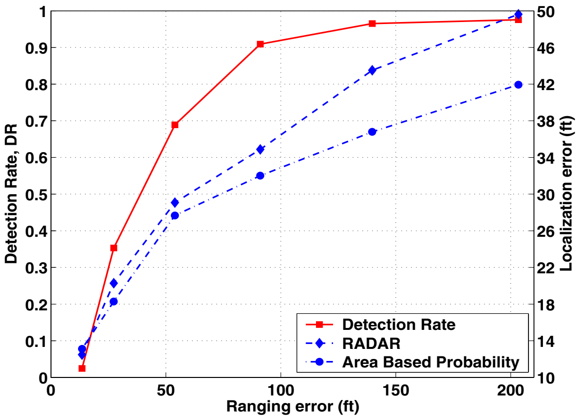

Fig. 4. Attack detection

(non-attack) conditions it corresponds to the probability of declaring a false positive P_{fa}. We will examine DR as a function of the attack strength.

Receiving Operating Characteristic (ROC) curve: To evaluate an attack detection scheme we want to study the false positive rate P_{fa} and probability of detection P_d together. The ROC curve is used to measure the tradeoff between false-positives and correct detections.

C. Discussion

We know that the relationship between the RSS error and the ranging error is multiplicative with distance [6]. Even small perturbation in RSS readings can cause large ranging errors due to this multiplicative factor. Figure 2 shows this effect that the ranging error increased faster as to the severity of signal strength attacks.

The ROC curves in Figure 3 show that for false positive rates less than 10%, the detection rates are above 90% and close to 99% when the attack strength increases to 20dB and 25dB. This shows that if the adversary wants to cause higher degree of localization error, it is almost certain that our attack detection mechanism will detect it. These results strongly indicate that using residuals in LS as a test statistic for attack detection is effective. For small attacks of less than 5dB, because the resulting impact on the final localization result would be small, the consequences of failing to detect such attacks would likely be small as well.

We further examine the relationship among attack detection, ranging error, and localization error. Figure 4 shows the Detection Rate when using residuals in LLS for attack detection, and the localization errors under the corresponding signal strength attacks with two representative localization algorithms: point-based algorithm, RADAR [8], and area-based algorithm, Area Based Probability [9]. The figure shows that detection rates are more than 90% for attack strength equal to or greater than 15dB, and at this attack strength the average localization error is about 35ft.

The above result is quite encouraging, as it shows that an attacker cannot cause gross localization errors without there being a very high probability of detection (>95%). In the case of using RSS, with mean errors of 10-15 ft [9], an attacker can not cause errors of about 2-3 times over the average error without a very high probability of detection.

In conclusion, we have proposed an Attack Detection scheme using Least Squares (ADLS) for wireless and sensor networks. Based on our theoretical formulation and analytic solution, our experimental study shows the promising results of using ADLS for attack detection in wireless localization. Our analysis shows that ADLS is independent of the ranging modality as well.

References

[1] Y. Chen, K. Kleisouris, X. Li, W. Trappe, and R. P. Martin, “The robustness of localization algorithms to signal strength attacks: a comparative study,” in *Proceedings of the International Conference on Distributed Computing in Sensor Systems (DCOSS)*, June 2006, pp. 546–563.

[2] P. Enge and P. Misra , *Global Positioning System: Signals, Measurements and Performance*. Ganga-Jamuna Pr, 2001.

[3] D. Niculescu and B. Nath, “Ad hoc positioning system (APS),” in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*, 2001, pp. 2926–2931.

[4] K. Langendoen and N. Reijers, “Distributed localization in wireless sensor networks: a quantitative comparison,” *Comput. Networks*, vol. 43, no. 4, pp. 499–518, 2003.

[5] Z. Li, W. Trappe, Y. Zhang, and B. Nath, “Robust statistical methods for securing wireless localization in sensor networks,” in *Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN)*, 2005, pp. 91–98.

[6] Y. Chen, J. Francisco, W. Trappe, and R. P. Martin, “A practical approach to landmark deployment for indoor localization,” in *Proceedings of the Third Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, September 2006.

[7] S. Weisberg, *Applied Linear Regression*. Wiley Series in Probability and Mathematical Statistics, 2005.

[8] P. Bahl and V. N. Padmanabhan, “Radar: An in-building rf-based user location and tracking system,” in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, March 2000, pp. 775–784.

[9] E. Elnahrawy, X. Li, and R. P. Martin, “The limits of localization using signal strength: A comparative study,” in *Proceedings of the First IEEE International Conference on Sensor and Ad hoc Communcations and Networks (SECON 2004)*, Oct. 2004, pp. 406–414.