Detecting Malicious Nodes in RSS-Based Localization

Manas Maheshwari*, Sai Ananthanarayanan P.R.**, Arijit Banerjee*, Neal Patwari**, Sneha K. Kasera*
*School of Computing
University of Utah
Salt Lake City, Utah-84112
{mmahesh,arijit,kasera@cs.utah.edu}
**Department of Electrical and Computer Engineering
University of Utah
Salt Lake City, Utah-84112
{saianantha21@gmail.com, npatwari@ece.utah.edu}

***Abstract*—Measurements of received signal strength (RSS) on wireless links provide position information in various localization systems, including multilateration-based and fingerprint-based positioning systems, and device-free localization systems. Existing localization schemes assume a fixed or known transmit power. Therefore, any variation in transmit power can result in error in location estimation. In this paper, we present a generic framework for detecting power attacks and identifying the source of such transmit power variation. Our results show that we can achieve close to zero missed detections and false alarms with RSS measurements of only 50 transmissions. We also present an analysis of trade-off between accuracy and latency of detection for our method.**

***Index Terms*—Localization, RSS, wireless security, sensor networks**

I. Introduction

Measurements of received signal strength (RSS) on wireless links have found application in various localization systems. RSS measurements have been used to estimate path lengths in multilateration positioning algorithms [16], to identify a device's location in fingerprint-based localization algorithms [3][13][21] and to monitor movement of a person or object through a static link in device-free localization algorithms [19][20].

The general method used by RSS based localization schemes in wireless sensor networks (WSNs) involve a number of sensor nodes deployed around the area of interest. These sensor nodes transmit radio signals and the RSS measurements obtained are used to model any perturbation in the wireless environment to provide localization information. More specifically, these RSS measurements (P_r), measured in dBm, are expressed as:

$$P_r = P_t - P_{loss} \tag{1}$$

where P_t is the transmit power in dBm and P_{loss} is the path loss in dB caused by the electromagnetic environment between the transmitter and the receiver antennas. Most of the existing localization schemes based on (1) assume a fixed transmit power. Therefore, any variation in transmit power can result in error in location estimation. Previous work has shown that change in transmit power by 15 dB can introduce up to 30 ft of localization error [5].

The transmit power can vary due to a number of reasons. These include

- *Faults* : Sensor nodes are prone to develop faults due to depleting battery levels [2] and physical damage. These faults may manifest as changes in transmit power.
- *Power control algorithms*: Most sensor network applications are strictly power constrained and use power control algorithms which vary transmit power in order to preserve battery life and to reduce interference with other nodes [1][15]. In such algorithms, where a node changes transmit power, the transmit power level must be communicated to the receiver nodes in the network. However, data corruption (due to packet errors, etc.) or software bugs can introduce cases where a node's transmit power changes without the receiver nodes in the network finding out about the change.
- *Adversarial circumstances*: Sensor nodes are often deployed in unattended and potentially hostile environments where they are susceptible to node capturing attacks by adversaries [6][14]. An adversary can manage to capture a few nodes in the network and then reprogram them with malicious code to change their transmit power.

Even if the existing localization schemes require the transmit power to be communicated to the receiver, in the case of faulty and adversarial node, there is no guarantee that the right transmit power gets communicated. We use the term *power attack* to denote a change in transmit power, not communicated to the receiver nodes, that can cause significant error in the estimated location, regardless of the reason of its occurrence.

In this paper, we show that RSS measurements can be used to detect power attacks reliably in real-time. We present a generic framework for detecting power attacks and identifying the source of such transmit power variation. We conduct

experiments and evaluate our method for indoor settings. Our results show that we can achieve close to zero missed detections and false alarms with RSS measurements of only 50 transmissions. We also present an analysis of trade-off between accuracy and latency of detection for our method. The algorithm developed is of low complexity and hence can be implemented on nodes with few resources.

The remainder of this paper is organized as follows. In Section II, we discuss some previous approaches to secure WSNs and argue why these would not work for RSS based localization methods. In Section III, we list our assumptions and describe our adversary model. Section IV presents our method to detect changes in RSS caused by a change in transmit power. In Section V and VI, we present our experiments and results respectively. In Section VII, we conclude the paper and indicate directions for future work.

II. Related work

In this section, first we briefly describe the existing work on securing WSNs. Then, we present a qualitative evaluation of these works and discuss their limitations with reference to RSS based localization.

- *Key based authentication and encryption methods*: Significant work has involved securing WSNs using traditional key based authentication and encryption protocols [7][8]. These methods, although resource intensive, do provide admission control and some level of security as long as the adversary is assumed not to gain physical control over the sensor nodes. However, if the adversary has physical control over the nodes, it can obtain security keys and passwords and maliciously insert cloned nodes in the network. The adversary can even reprogram a node to make it behave maliciously while still using the original security keys and passwords.
- *Tamper proof memory* [6]: This provides a method to secure a node from being reprogrammed by an adversary and when combined with security passwords and keys, can serve to protect a malicious node from affecting the system. However, use of tamper proof memory would result in an increase in the implementation cost of the system.
- *Using Device signatures* [12]: Device signatures can be used as alternative to traditional key based encryption methods. These signatures can protect the system from maliciously inserted cloned nodes. However, most device signatures depend on hardware characteristics and would not change with the software installed on the nodes. Hence, this method is not robust against malicious reprogramming.

Other works on secure localization include SPINE [4], ROPE [11], SeRLoc [9] and HirLoc [10]. These works assume the availability of some reference points, special locator nodes or key-based secure communication between anchor nodes to prevent against a variety of attacks in WSNs. Hence, these methods are vulnerable to capture of critical nodes by the adversary.

In comparison to the existing works, the method developed in this paper is completely passive, uses only RSS measurements, and aims to reliably detect power attacks.

III. Assumptions and Adversary model

We assume that faulty or malicious nodes are never present in majority in the network and all nodes have equal probability of developing fault or being targeted by an adversary. We also assume that the malicious nodes do not collude with each other. We ignore the possibility of an adversary reporting false readings of RSS values it receives from other transmitters. Since faulty nodes are just a weaker form of the adversary being considered, all further discussions apply to both malicious and faulty nodes.

We define two parameters related to an adversary's action which we would then use in our method. As discussed in Section I, an adversary can affect a RSS based localization system by changing the transmit power of a node. We parameterize this action by considering how fast and by how much the change occurs. To this effect, we define the following parameters of malicious activity:

- *Minimum attack window size* (w_{min}): Defined as the smallest set of contiguous transmissions which would always contain at least one power change. We do not assume any particular profile for power changes and w_{min} can have more than one power change. In real scenarios, w_{min} is not expected to be known beforehand, however an educated guess of w_{min} can be made based on the expected movement activity and noise in WSNs. A detection window can then be chosen from the collected data, of size greater than w_{min}, to detect attack reliably with desired probabilities of detection and false alarm as discussed in section IV-E.
- *Minimum attack amplitude* (a_{min}): Defined as the minimum power change required to perform an attack with significant changes in the estimated location. Power attack with an amplitude less than a_{min} are not considered to be significantly harmful to the application, and thus are not important to detect. The value of a_{min} is thus set by the application.

IV. Method

A. Network

We assume a WSNs with N transceiver nodes. Define, for a transmitter k, a neighbor set given by $\mathcal{H}_k = \{n_0, n_1, ...n_{M-1}\}$ consisting of M receivers capable of communicating with k. We make RSS measurements on each link between node pair (k, n_l) where $n_l \in \mathcal{H}_k$. A fully connected network is not required for our detection method, however, the neighbour set for each transmitter is assumed to be known at all nodes and remain constant. Detection in networks where $\mathcal{H}_k$ can change with time will be considered in future works.

B. Model

Let $r_{k,j}(i)$ be the RSS measured at receiver j for transmission from node k at time i where $k \in \{1, ..., N\}$ and $j \in \mathcal{H}_k$. We define RSS vector as:

$$\mathbf{r}_k(i) = [r_{k,n_0}(i), ..., r_{k,n_{M-1}}(i)]^\mathsf{T} \tag{2}$$

and mean of RSS vector over a window of time T as:

$$\bar{\mathbf{r}}_k(i) = \frac{1}{T}\sum_{t=1}^{T} \mathbf{r}_k(i-t) \tag{3}$$

Using (2) and (3), we can define the change in RSS for a transmission of node k at time i as

$$\Delta\mathbf{r}_k(i) = \mathbf{r}_k(i) - \bar{\mathbf{r}}_k(i) \tag{4}$$

Next, we consider two cases for $\Delta\mathbf{r}_k(i)$:

1) *No attack*: When a power attack is not present, changes in RSS can be caused by many reasons. However, these changes are equally likely to increase or decrease the RSS measurement. For example, noise and quantization error are likely to be zero mean. If the sensor moves, it is likely to move towards some nodes and away from others, and therefore changes should be modeled as zero mean. Movement of people and objects in the environment will similarly tend to increase RSS on some links and decrease RSS on others [17]. Thus for generality, we model $\Delta\mathbf{r}_k(i)$ as

$$\Delta\mathbf{r}_k(i) = \boldsymbol{\epsilon} \tag{5}$$

where $\boldsymbol{\epsilon}$ is a vector of zero mean random variables. We do not make any assumptions about the distribution or the correlation between elements of $\boldsymbol{\epsilon}$.

2) Attack: When there is a power attack from k, $\Delta\mathbf{r}_k(i)$ can no longer be modelled as a vector of zero mean random variables. For this case, we model $\Delta\mathbf{r}_k(i)$ as

$$\Delta\mathbf{r}_k(i) = a_k\mathbf{1} + \boldsymbol{\epsilon} \tag{6}$$

where a_k is the transmit power variation by k and $\mathbf{1} = [1, ..., 1]^T$.

We consider deciding between the following two hypotheses:

- H_0: No power attack from transmitter k is present.
- H_1: A power attack from transmitter k is present.

C. Estimating a_k

The main difficulty of the detection problem considered is that, under H_1, we do not know the amplitude, a_k, of the power attack *a priori*. In order to judge the likelihood that H_1 is occurring, we first need to estimate a_k.

Since we are estimating a_k given H_1, we know that the amplitude of our estimate must be greater than a_{min}, which is the minimum attack amplitude parameter.

We first define $\bar{a}$ as

$$\bar{a} = \frac{1}{M}\sum_{j=0}^{M-1} \Delta\mathbf{r}_{k,n_j}(i) \tag{7}$$

where M is the size of $\mathcal{H}_k$ and $\Delta\mathbf{r}_{k,n_j}(i)$ represent the j^{th} element of $\Delta\mathbf{r}_k(i)$.

Then, the maximum likelihood estimate $\hat{a}_k$ can be defined as

$$\hat{a}_k = \begin{cases} \max\ (\ \bar{a},\ +a_{min}\ ), & \bar{a} > 0 \\ \min\ (\ \bar{a},\ -a_{min}\ ), & \bar{a} \leq 0 \end{cases} \tag{8}$$

D. Detecting power attack

Next, we consider the problem of detecting a power attack. Define a time window, $Q_k(i)$, of p transmissions for transmitter k ending at time i as

$$Q_k(i) = [\Delta\mathbf{r}_k(i-p-1),\ \Delta\mathbf{r}_k(i-p-2),\ ...,\ \Delta\mathbf{r}_k(i)\ ]^\mathsf{T} \tag{9}$$

Also define a line in space $\mathbb{R}^{|\mathcal{H}_k|}$, with slope 1, as:

$$\mathcal{L}:\ \Delta\mathbf{r}_{k,n_0} = \Delta\mathbf{r}_{k,n_1} = \cdots\ = \Delta\mathbf{r}_{k,n_{M-1}} = \hat{a}_k \tag{10}$$

To choose between H_0 and H_1 for the window $Q_k(i)$, we use the distance of $\Delta\mathbf{r}_k(i-j)$ from $\mathcal{L}$, $\forall\ j \in [0, p)$ and decide with the hypothesis test

$$\min_{j\in[0,p)} (d_k(i-j)) \underset{H_1}{\overset{H_0}{\gtrless}} \gamma_i \tag{11}$$

where γ_i is an appropriately chosen threshold for the window $Q_k(i)$ (as discussed later in Section IV-E).

The distance $d_k(i)$ is calculated using the estimated parameter $\hat{a}_k$ as

$$d_k(i) = ||\Delta\mathbf{r}_k(i) - \hat{a}_k\mathbf{1}||^2 \tag{12}$$

If there is a power attack at time j such that $\Delta\mathbf{r}_k(j) \in Q_k(i)$, we can model $\Delta\mathbf{r}_k(j)$ as (6). This lies in a region of constant diameter around $\mathcal{L}$ and hence, $d_k(j)$ is smaller than the threshold value γ_i. Thus, we choose H_1 for $Q_k(i)$.

When there is no attack in $Q_k(i)$, $\Delta\mathbf{r}_k(j)$ can lie randomly at any point in space. In this case, $d_k(j)$ is greater than $\gamma_i\ \forall\ j$ such that $\Delta\mathbf{r}_k(j) \in Q_k(i)$ and hence, we can choose H_0 for $Q_k(i)$.

Figure 1 illustrates attack detection in $\mathbb{R}^3$ where $\mathcal{H}_k = \{n_0, n_1, n_2\}$. The cylinder around $\mathcal{L}$ is the detection region. Note that as the number of receivers and thus the number of dimensions increase, the region of constant diameter around $\mathcal{L}$ occupies increasingly smaller percentage of total volume in space and the probability of a normal transmission lying in detection region decreases. Hence, the number of false alarms decrease as the total number of receivers increases.

E. Choosing γ_i

To successfully detect a power attack, we need to set the threshold appropriately. The value of γ_i would vary with the environment noise. In this section, we describe the method we use to find the optimal γ_i automatically.

For a transmitter k, $Q_k(i)$ represents data from a time window of $\Delta\mathbf{r}_k(i)$ of size p. Using (12), we get p distances from $\mathcal{L}$ for a transmitter from this data. Let $\mathbf{d}_{min}$ denote

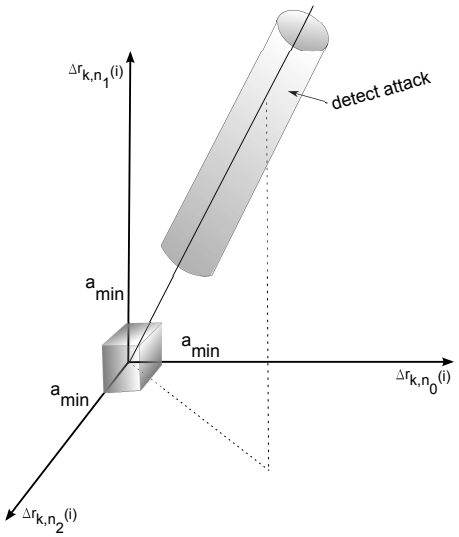

Figure 1. Attack detection in $\mathbb{R}^3$ space

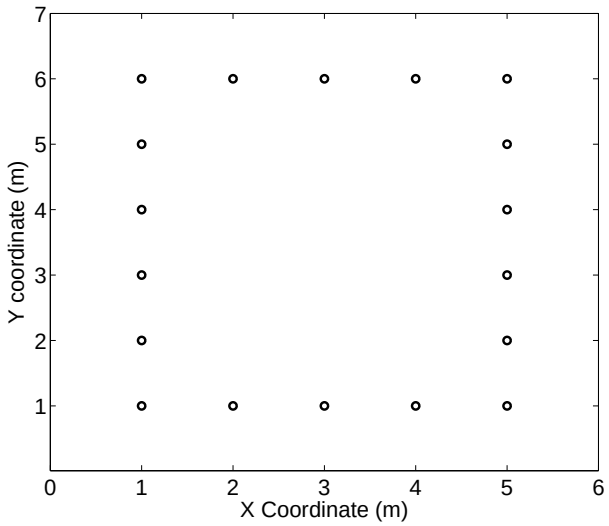

Figure 2. The layout of a 18-node wireless network deployment for attack detection

the vector giving minimum distance points recorded for each transmitter in $Q_k(i)$ such that

$$\mathbf{d}_{min}[k] = \min_{l \in [0,p-1]} (d_k(i-l)) \tag{13}$$

where $\mathbf{d}_{min}[k]$ is the k^{th} element of $\mathbf{d}_{min}$. Let's also define the mean of $\mathbf{d}_{min}$ as

$$m_d = \frac{1}{M} \sum_{k=0}^{M-1} d_{min}[k] \tag{14}$$

and the standard deviation of $\mathbf{d}_{min}$ as

$$s_d = \sqrt{\frac{1}{M} \sum_{k=0}^{M-1} (d_{min}[k] - m_d)^2} \tag{15}$$

Then we chose γ as:

$$\gamma = m_d - 2s_d \tag{16}$$

If there is no malicious transmitter, $d_{min}[k]$ is dependent on the environment noise only. For this case, all elements of $\mathbf{d}_{min}$ would lie close to each other and hence the calculated γ_i lies well below $d_{min}[k]$. If k is malicious, $d_{min}[k]$ would be small and since majority of nodes are assumed to be normal, the calculated γ_i would lie above $d_{min}[k]$.

If malicious nodes were colluding, there is a possibility that the calculated γ_i would always let a few malicious node pass the detection test. However, we leave colluding adversaries for future work. Window size p is chosen such that it is greater than the estimated parameter w_{min}.

F. Evaluation

We evaluate our detection algorithm based on probability of false alarm and probability of missed detections defined as below:

- False alarm (P_{FA}): power attack detected for a normal node.
- Missed detection (P_M): failure to detect power attack by a malicious node.

V. Experiments

This section describes the experiments we perform for testing our proposed detection algorithm. We deploy a network of eighteen TelosB wireless sensors nodes, in an indoor lab, for the experiments presented in this paper. The nodes operate in the 2.4 GHz frequency band. A token-passing protocol called Spin [18] is used to schedule transmission of nodes in a manner which prevents packet collisions while still maintaining high data collection rate. When one node transmits, all other nodes receive the packet and make the RSS measurements. These RSS measurements are transmitted to a base station along with the node's unique ID. The base station collects all RSS measurements and forwards the data to a laptop for storage and later processing.

We define *spin cycle* as one round of the token passing scheduling protocol used. Each spin cycle consist of RSS dataset with exactly one transmission from every transmitter node. The data collected consist of more than 2000 spin cycles for each experiment performed.

We perform two experiments. The experimental setup is shown in Figure 2.

1) *No-attack*
   During this experiment, there is no attack in the network. The subject walks in a random pattern in the network for a 8 minute period. The nodes transmit at their normal power at 4 transmissions per second.
2) *Attack*
   To simulate a power attack, we program node 0 at location (0,0) with malicious code, modified to vary transmit power, at least once every 16 transmissions,

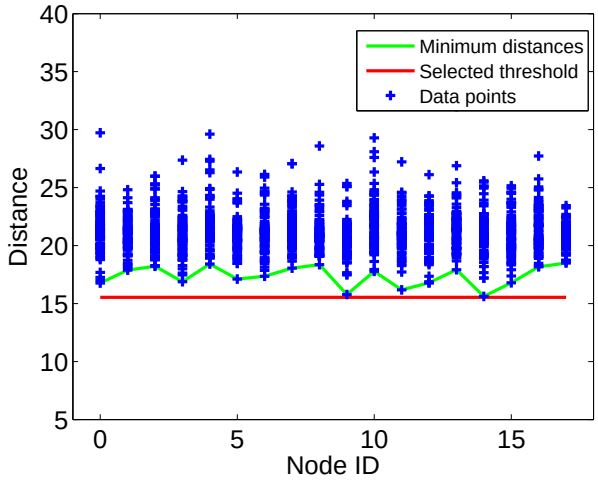

Figure 3. Distances from slope 1 line $\mathcal{L}$ with normal nodes

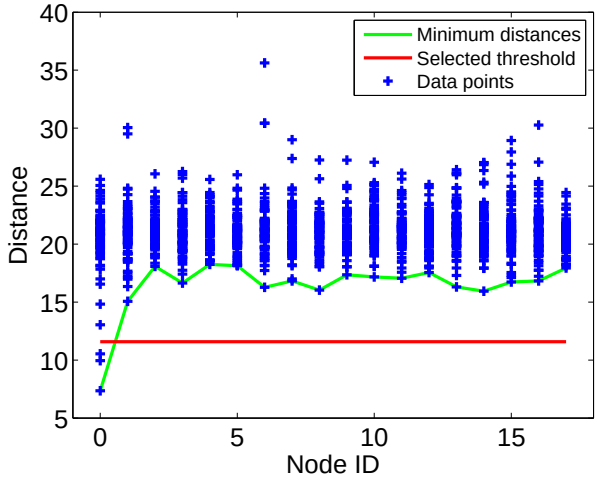

Figure 4. Distance from slope 1 line $\mathcal{L}$ with node 0 malicious

randomly. All nodes still transmit at 4 transmissions per second. The subject performs same motion, as in *No-attack* experiment, in the monitored area. No one else is present in the area during both the experiments.

VI. Results

This section presents the results for the two experiments described in Section V and an analysis of the trade-off between accuracy and latency of detection for our method.

First, we present results for the *No-attack* experiment. We validate our model with a sample data set of 50 consecutive spin cycles. Each spin cycle gives us one data point in $\mathbb{R}^{|\mathcal{H}_k|}$ space for each node. The distance, $d_k(i)$, from $\mathcal{L}$ are calculated for all k and plotted in Figure 3. From the distances plotted, we pick the minimum distance for each node and use the minimums to calculate the threshold distance γ_i as discussed in Section IV-E.

From Figure 3, we observe that the minimums of all nodes

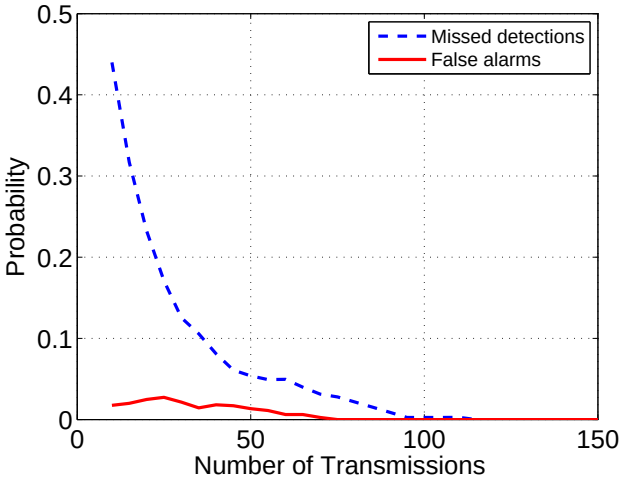

Figure 5. Detector performance with 5 dB variations

lie above the threshold γ_i. Hence we detect no malicious activity which is consistent with our *No-attack* experiment.

Then, we present the results for the *Attack* experiment. This experiment simulates the scenario with one malicious node in the network. We program node 0 to act maliciously by varying its transmit power once every 16 transmissions. Figure 4 plots the distances for every node from $\mathcal{L}$. From the figure, we observe that some of the data points from node 0 are below the threshold γ_i. These data points correspond to the malicious transmissions from node 0. Hence, using (11), we can accurately detect malicious activity with RSS data from 50 consecutive spin cycles and also identify the malicious node in the network.

Next, we use the data from *Attack* experiment to evaluate the trade-off between accuracy and latency of detection. We analyse the characteristics of P_{FA} and P_M with number of transmissions for this data.

We choose a window of p consecutive transmissions where $p \in (16, 300]$ and calculate P_{FD} and P_M by sampling over a large data set. Since we are choosing a window size greater than 16, every window will have at least one malicious transmission from node 0. We detect a hit if at least one of the data point for node 0 lie below the calculated threshold. If all the points for node 0 are above the threshold, it is a missed detection. Similarly, for a normal node, we get a false alarm if any one of its data point lie below the threshold. False alarm for one or more normal nodes is considered as a false alarm for the method.

We plot probability of false alarm and probability of missed detection, when p consecutive transmissions are used for detection, for actual transmit power variation, a_k, of 5 dB and 10 dB in 5 and 6 respectively. From the plots, we observe that higher detection accuracy can be obtained with more number of transmissions which implies higher latency in detection. P_{FD} and P_M are almost zero after 100 transmissions for the 5 dB case and 50 transmissions for the 10 dB case.

Using the above plots, we can get an estimate of time

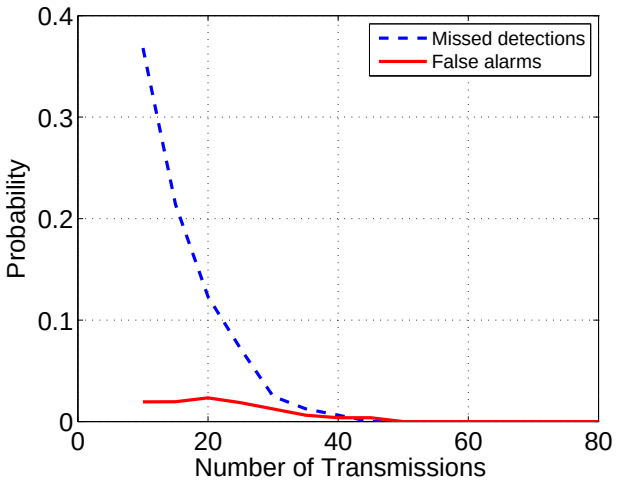

Figure 6. Detector performance with 10 dB variations

required to detect a malicious transmission in real time. For this experiment, the mean interval between two successive transmissions by a node was around 250 ms. Hence, we can detect malicious activity with 100% accuracy (0 missed detection, 0 false alarms) in 25 seconds for 5 dB variations and in 12.5 seconds for 10 dB variations.

VII. Conclusion

In this paper, we explore a security problem with RSS-based localization techniques in which unreported changes in transmit power can result in inaccurate location estimates. These changes in transmit power can be caused by a faulty node or a malicious node. We develop a method to detect such changes in transmit power using the RSS measurements only and present detection performance of our detector in indoor environment.

Several avenues for future research remain:

- *Smarter colluding adversaries*: We assumed that the malicious node do not collude with each other to perform more sophisticated power attack by varying their power in a coordinated manner. Dealing with such attacks is definitely an interesting research problem.
- *Faking RSS values:* So far we only considered a malicious node capable of varying its transmit power. A malicious node can also report false RSS values received from other transmitters in order to create similar effects. Our preliminary experiments indicate that such action are less significant than varying transmit power. However, an adversary can combine both type of effects to perform advanced attacks.

References

[1] B. Zurita Ares, P. G. Park, C. Fischione, A. Speranzon, and K. H. Johansson. On power control for wireless sensor networks: System model, middleware component and experimental evaluation. In *European Control Conference*, 2007.

[2] S. Blom, C. Bellettini, A. Sinigalliesi, L. Stabellini, M. Rossi, and G. Mazzini. Transmission power measurements for wireless sensor nodes and their relationship to the battery level. In *2nd International Symposium on Wireless Communication Systems, 2005*, pages 342–345, Siena, Italy, 2005. IEEE.

[3] M. Brunato and R. Battiti. Statistical learning theory for location fingerprinting in wireless LANs. *Computer Networks*, 47(6):825–845, 2005.

[4] S. Capkun and J.P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, volume 3, pages 1917–1928. IEEE, 2005.

[5] Y. Chen, K. Kleisouris, X. Li, W. Trappe, and R. Martin. The robustness of localization algorithms to signal strength attacks: a comparative study. *Distributed Computing in Sensor Systems*, pages 546–563, 2006.

[6] C. Hartung, J. Balasalle, and R. Han. Node compromise in sensor networks: The need for secure systems. Technical report, 2005.

[7] K. Jamshaid and L. Schwiebert. Seken (secure and efficient key exchange for sensor networks). In *IEEE International Conference on Performance, Computing, and Communications*, pages 415–422, 2004.

[8] A. Khalili, J. Katz, and W.A. Arbaugh. Toward secure key distribution in truly ad-hoc networks. In *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on*, pages 342 – 346, 2003.

[9] L. Lazos and R. Poovendran. SeRLoc: Secure range-independent localization for wireless sensor networks. In *Proceedings of the 3rd ACM workshop on Wireless security*, pages 21–30. ACM, 2004.

[10] L. Lazos and R. Poovendran. HiRLoc: High-resolution robust localization for wireless sensor networks. *IEEE Journal on Selected Areas in Communications*, 24(2):233–246, 2006.

[11] L. Lazos, R. Poovendran, and S. Čapkun. ROPE: robust position estimation in wireless sensor networks. In *Proceedings of the 4th international symposium on Information processing in sensor networks*, page 43. IEEE Press, 2005.

[12] K. Rasmussen and S. Capkun. Implications of radio fingerprinting on the security of sensor networks. In *Proceedings of IEEE SECURECOMM*, 2007.

[13] T. Roos, P. Myllymaki, and H. Tirri. A statistical modeling approach to location estimation. *IEEE Transactions on Mobile Computing*, pages 59–69, 2002.

[14] P. Tague and R. Poovendran. Modeling adaptive node capture attacks in multi-hop wireless networks. *Ad Hoc Netw.*, 5:801–814, August 2007.

[15] H.X. Tan and W. Seah. Dynamic topology control to reduce interference in MANETs. In *Proc. of the 2nd International Conference on Mobile Computing and Ubiquitous Networking*, pages 117039–1. Citeseer, 2005.

[16] X. Wang, O. Bischoff, R. Laur, and S. Paul. Localization in Wireless Ad-hoc Sensor Networks using Multilateration with RSSI for Logistic Applications. *Procedia Chemistry*, 1(1):461–464, 2009.

[17] A.J. Wilson. *Device-free localization with received signal strength measurements in wireless networks*. PhD thesis, The University of Utah, 2010.

[18] J. Wilson and N. Patwari. Spin: A token ring protocol for rss collection, "http://span.ece.utah.edu/spin".

[19] J. Wilson and N. Patwari. Radio tomographic imaging with wireless networks. *IEEE Transactions on Mobile Computing*, 9(5):621–632, 2010.

[20] J. Wilson and N. Patwari. See Through Walls: Motion Tracking Using Variance-Based Radio Tomography Networks. *IEEE Transactions on Mobile Computing*, 2010.

[21] M.A. Youssef, A. Agrawala, and A. Udaya Shankar. Wlan location determination via clustering and probability distributions. In *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003. (PerCom 2003)*, pages 143 – 150, 2003.