Device-Free Passive Localization

Matthew Mah

Abstract

This report describes a Device-Free Passive Localization System (DfP). The system provides a software solution over nominal WiFi equipment to detect the presence and track intruders in an area of interest. The system is based on measuring the changes in the received RSSI at a fixed receiver form a fixed transmitter. Using RSSI values for multiple transmitters and monitoring points, we show a system is able to detect intruders with a high probability and very low false positive rate. Moreover, the system is able to track the intruder with an accuracy of a few feet.

1 Background

In the recent years, 802.11[1] wireless LANs (WLAN) installations have become increasing common, providing communication capabilities in the office, at home, and public places. In an office environment WLANs usually employ infrastructure mode in which a number of Access Points (APs) are carefully positioned to provide access from any location in the office. While the wireless communication is the primary reason for deploying WLANs, the deployed infrastructure can also be used for other purposes. For example, the RF signals have been used for determining the location of a receiver [1-7, 9]. In one such technology developed at the University of Maryland, Horus, the position of a wireless card can be tracked using the received signal strength in a pure software solution, to an accuracy of a few feet. Based on the user location, many context-aware applications can be implemented in a WLAN environment such as location-sensitive information retrieval and direction finding inside a building. All extensions on the use of WLANs require an active participation of a device with a NIC (Network Interface Card) in it. In contrast, a DfP system operates without requiring any active participation of the person being monitored or tracked.

The DfP technology is based on both the knowledge that RF signals are affected by the presence of people in the environment and preliminary measurements indicating the RF signal changes are significant. The extent of the impact depends on the location of the person relative to the NIC. The DfP system infers the presence or movement of people from changes in received signal strength. Using the signal strength:

1. By monitoring the RSSI at one or more locations in an area/building in which WiFi is deployed, we can reliably detect the presence of people.

2. As we can detect the presence of people, we can quantify such detection. For example, we can determine the number of people and their location. We need to determine the accuracies that can be achieved in this process.

The DfP system primarily uses the standard access point and wireless card components of any Wi-Fi installation.

2 System Architecture

The basic architecture of a DfP system is shown in Figure 1. It consists of the Access Points (APs) and Monitoring Points (MPs) along with a DfP server. The APs of any WLAN deployment double as DfP APs. MPs monitor the RSSI of AP beacons and report thee values to the DfP Server. As we expect the location of MPs to be fixed, any stationary desktop computers which are normally used by the users can be used as MPs. The DfP server is a PC which performs computations on the RSSI streams and initiates actions as necessary.

The DfP System is envisioned to support three modes of operation:

Monitoring Mode In this mode, DfP System expects no movement of people anywhere in its protected area and raises alarms on detecting any movements. This mode may be appropriate for providing night time protection. In this mode MPs recognize the change of RSSI values and inform the DfP Server accordingly. The NS then takes the appropriate security steps reflecting the specific configurations.

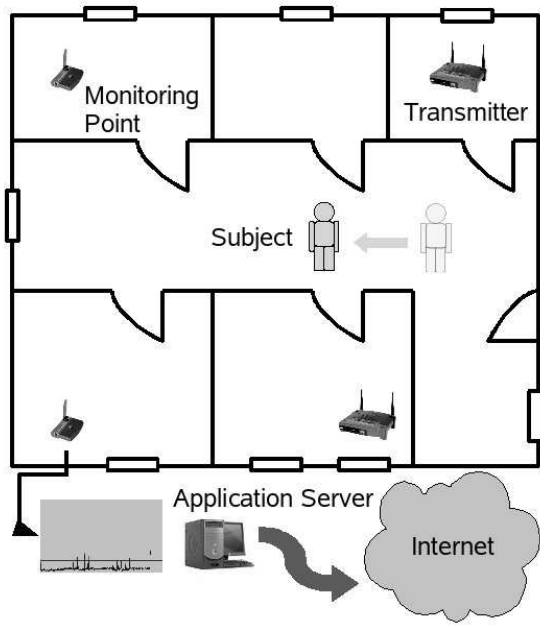


Figure 1: DfP System Diagram

Tracking Mode The DfP System uses its tracking capability to not only detect the presence of an intruder, but also provides the location and the path taken by the intruder in the protected area. In the tracking mode, the DfP System tracks one intruder at a time. This mode is suitable for supporting the protection at night. An MP records changes in the RSSI value and sends it to the DfP Server. NS detects that multiple monitoring points have recorded change in the RSSI values and uses this information to determine the location. Over time the pattern of the intruder's movement is computed, analyzed and used for taking the appropriate security actions by the DfP Server.

DfP Mode DfP System tracks multiple people and keeps track of each separately in this mode. This is suitable for daytime monitoring and tracking the movement of each person in the protected area.

3 The DfP System

3.1 Mathematical Model

Consider a set of n access points and m MPs. Let s denote the signal strength received at MP_i from AP_j as $s_{i,j}$. For a quiescent RF environment, the signal strength received at MP_i from AP_j is a constant value. When a person enters the area of interest, the value of $s_{i,j}$ changes and the presence of the intruder is detected. Since this change is a function of the location (x, y) at which the person is standing, the signal strength received at MP_i from AP_j when a person is at location (x, y), denoted by $s_{i,j}(x, y)$, can be inverted and the intruder can be tracked.

If people are standing at N locations in the area of interest denoted by $(x_1, y_1), \ldots, (x_N, y_N)$, the DfP system uses the value of $s_{i,j}(x_k, y_k)$ for all i, j, and k to detect the number of persons in the area and track them.

Since the locations of intruders is not known to the monitoring system, we will denote the signal strength measurements available to the system as a function of time as $s_{i,j}(t) = s_{i,j}\big(x(t), y(t)\big)$. In our experiments with known intruder movement, we can parameterize the position x, y as functions of t.

3.2 Detection of an Intruder

We assume that the RSSI data series are streams. Each monitoring point is observing RSSI in real-time, and wishes to detect intrusions as soon as possible. A detection occurs when a single monitoring point suspects an intrusion based on RSSI from a single access point. We combine alerts from different monitoring points to give the overall system alert.

The overall system alert can be based on detections for multiple distinct pairs of monitoring point and access point pairs. These detections should be simultaneous or near simultaneous, within a time buffer of b seconds. Simultaneous detections are required when $b = 0$. For an alert at time t with N detections required with time buffer b

1. At least one monitoring point i detects exactly at time t for the signal $s_{i,j}(t)$.

2. In the time interval $[t - b, t]$ there are $N - 1$ detections by other distinct pairs of monitoring points and access points.

The parameters N and b are variable to adjust system sensitivity.

We used two separate statistical techniques to detect intrusion events (a change in the environment). Each technique uses statistics for short ($\leq$ 30 sec) time windows to determine detections. The first technique is based on moving averages and the second is based on the variance. We start by detecting intruders based on the moving average.

3.2.1 Moving Average Based Detection

In this technique, detections are determined by comparing two moving averages of received signal strength indicators with possibly different window sizes. Let q_i be a series of measurements over time for a single monitor listening to a single access point. The averages $\alpha_{1,k}$ and $\alpha_{2,k}$ are defined as follows for time index k:

$$\alpha_{1,k} = \frac{1}{w_l} \cdot \sum_{i=k}^{k+w_l-1} q_i \quad (1)$$

$$\alpha_{2,k} = \frac{1}{w_s} \cdot \sum_{i=k+w_l}^{k+w_l+w_s-1} q_i \quad (2)$$

w_l and w_s are the window lengths for the two averages $\alpha_{1,k}$ and $\alpha_{2,k}$ respectively.

When the relative difference between the two averages exceeds a parameter τ,

$$\left| \frac{\alpha_{1,k} - \alpha_{2,k}}{\alpha_{1,k}} \right| > \tau \quad (3)$$

we declare an event detection for the time corresponding to $t = k + w_s$. The AS recomputes $\alpha_{1,k}$ and $\alpha_{1,k}$ periodically to check for event detection.

The intuition is that the w_l window represents history of a static situation, and the w_s window represents an estimate of the current state. When the current state differs noticeably from the history, we suspect an intrusion. The AS computes $\alpha_{1,k}$ and $\alpha_{1,k}$ for each time index k in the time period of interest to check for detections.

The system alerts when a tunable number of monitor and access point pairs give near simultaneous detections. Detections at times t_1 and t_2 are considered near simultaneous if $|t_1 - t_2| \leq T$, for the time buffer parameter b. For simultaneous events, $b = 0$.

3.2.2 Moving Variance Based Detection

The second detection technique examines the variance in a moving window of the raw data and compares it to the variance during a silence/static period. Let w be the size of our window. We compute the variance, v_t, as:

$$\bar{q_t} = \frac{1}{w} \cdot \sum_{i=k}^{k+w-1} q_i \quad (4)$$

$$v_t = \frac{1}{w-1} \cdot \sum_{i=k}^{k+w-1} (q_i - \bar{q_t})^2 \quad (5)$$

The detection criterion for any series q_i is based on the variance of a training period with no movement. For a training period $[t_{start}, t_{end}]$, we compute the average of the variances $\bar{v_t}$ and the standard deviation of the variance σ_v for the w-sized windows within it.

$$\bar{v_t} = \frac{1}{t_{end} - t_{start} + 1} \cdot \sum_{t=t_{start}}^{t_{end}} v_t \quad (6)$$

$$\sigma_v = \sqrt{\frac{1}{w} \cdot \sum_{t=t_{start}}^{t_{end}} (v_t - \bar{v_t})^2} \quad (7)$$

The moving variance detection technique of the AS detects an event at time $t + w$ for a single raw stream when $v_t > \bar{v_t} + r \cdot \sigma_v$ for an appropriate value of the parameter r. For a normally distributed variance measurements v_t, values above the threshold will be r standard deviations above the mean. Each data stream has its own σ_v value.

The moving variance detection system alerts when a tunable number of monitor and access point pairs give simultaneous or near simultaneous detections, using the same criterion as the moving average technique. Detections at times t_1 and t_2 are considered near simultaneous if $|t_1 - t_2| \leq b$, for the time buffer parameter b.

4 Tracking of an Intruder

In order to perform tracking, we construct a radio map of the area of interest either by collecting samples or using a propagation model. We use machine learning techniques to compare the received signal strength when a person is present to signal strengths stored in the radio map for the different monitoring points. We use Bayesian inference to detect the location of an intruder.

More formally, given a signal strength vector (s) for the signal strength readings at different MPs, we want to find the location l in the radio map that maximizes $P(l/s)$. This can be written as:

$$\begin{aligned} \arg\max_l P(l/\overline{s}) &= \arg\max_l P(s/l) \cdot \frac{P(l)}{P(s)} \\ &= \arg\max_l P(s/l) \cdot P(l) \end{aligned} \quad (8)$$

Assuming that all locations are uniform, the term $P(l)$ can be factored out form the maximization process in Equation 8. This leads to

$$\arg\max_l P(l/s) = \arg\max_l P(s/l) \quad (9)$$

where $P(s/l)$ can be obtained from the constructed radio map.

Using the super position law, the same principle is conjectured to be generalizable to cover the tracking of multiple intruders.

5 Experimental Evaluation

This section presents the experiments performed to evaluate the performance of the DfP system.

5.1 Evaluation Metrics

We use two metrics to quantify the performance of the detection capability of the DfP system:

1. Probability of detection (PD): which is the probability that the system will correctly identify events (changes in the environment).

2. False positives (FP): the number of times the system incorrectly identifies a period with no movement as an event. Since the number of possible false positives is undefined, we report this as a raw, unscaled number.

5.2 Experimental Testbed

We performed four experiments to test the performance of the DfP in a controlled environment chosen to minimize outside interference. Each experiment used a unique layout of two access points and two monitoring points. Each monitoring point recorded the received signal strength indicator from each access point beacon, which broadcasted every 100 milliseconds. Both access points ran on the same channel.

In each experiment the monitoring points recorded for approximately 1800 sec. While the monitoring stations were recording, a person walked through a series of four positions, pausing for 60 seconds at each position. Each position was three feet from the previous position. After pausing at the fourth position, the person left the room. Movement through the four positions was repeated a second time for each experiment layout to test repeatability. The periods of activity accounted for roughly 8 of 30 minutes in each experiment.

The layouts for the four experiments are shown in Figures 5.2 to 5.2. The four movement locations are shown in the center. Times for movements in each experimental layout are shown in table 1.

For each of the experiments described above, there are four separate RSSI streams, one for each pair of access point and monitoring point. Smoothed RSSI

	Experiment Number			
Position	1	2	3	4
1	480	360	560	430
2	540	420	610	490
3	600	480	670	550
4	660	540	730	610
Empty	720	600	790	670
1	1060	1120	1310	1190
2	1120	1180	1370	1250
3	1180	1240	1430	1310
4	1240	1300	1490	1370
Empty	1300	1360	1550	1430

Table 1: Experiment Movement Times (seconds)

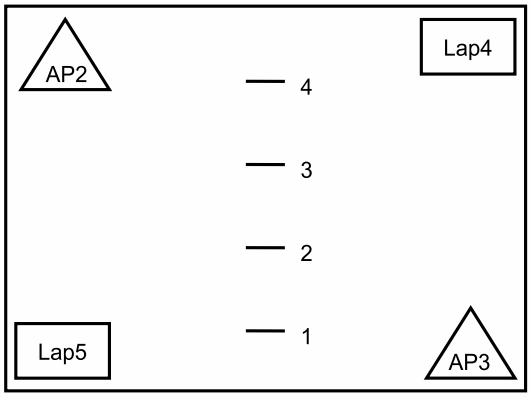


Figure 2: Experiment 1 Layout

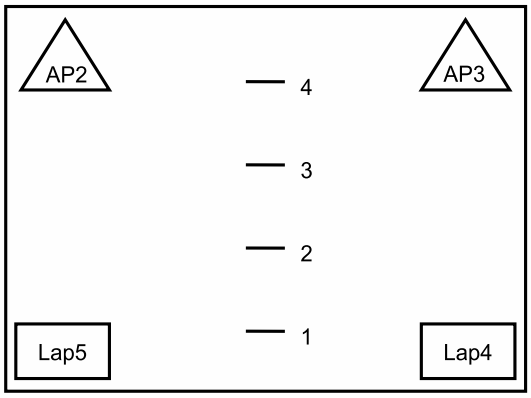


Figure 3: Experiment 2 Layout

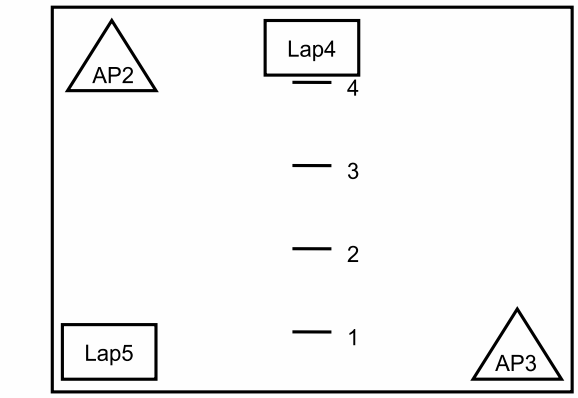


Figure 4: Experiment 3 Layout

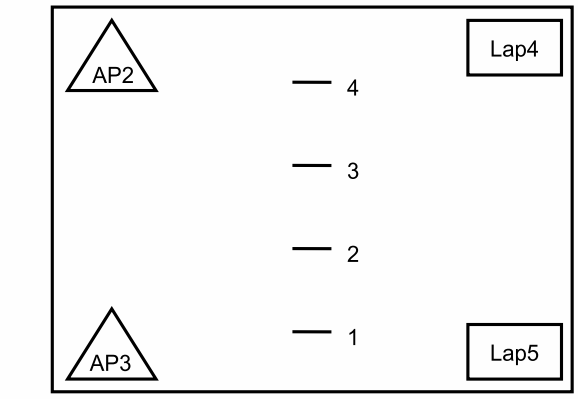


Figure 5: Experiment 4 Layout

measurements for each experiment are shown in Figures 6 to 9. The times for event movements are shown with vertical lines.

Figures 10 and 11 show variance for moving windows of size $w = 40$, with the σ_v value derived from the time interval $[10, 340]$. The y-axis values for these plots are normalized to σ_v. There are two separate plots to aid distinguishing the variance of each pair of monitoring point and access point.

In the RSSI figures, clear discontinuities occur at the times corresponding to the movement events. In the variance plots, there are clear spikes in the variance for the movement events.

5.3 Analysis

Table 2 shows the parameter values used for analysis of the moving average techniques and Table 3 shows those for the moving variance technique. Each column shows the values for one parameter. All combinations of parameter values were used for analysis. There were a total of $4*5*4*4*3 = 960$ combinations of parameters for the moving average technique, and $3 * 5 * 4 * 4 = 240$ combinations of parameters for the moving variance technique. Each combination of parameters was used to analyze each of the four experimental layouts.

w_l	w_s	τ	N	b
20	3	0.02	1	0.0
50	5	0.03	2	0.5
100	10	0.04	3	1.0
200	15	0.05	4	
	20			

Table 2: Moving Average Parameter Values

w	r	N	b
20	2	1	0.0
40	3	2	0.2
80	4	3	0.5
	5	4	1.0
	6		

Table 3: Moving Variance Parameter Values

We begin by evaluating our metrics while varying a single parameter. The metrics are combined over all other parameters and over the four experimental layouts. For false positives (FP) we examine the sum over all parameter combinations, and for probability of detection (PD) we examine the average, which preserves $0 \leq PD \leq 1$.

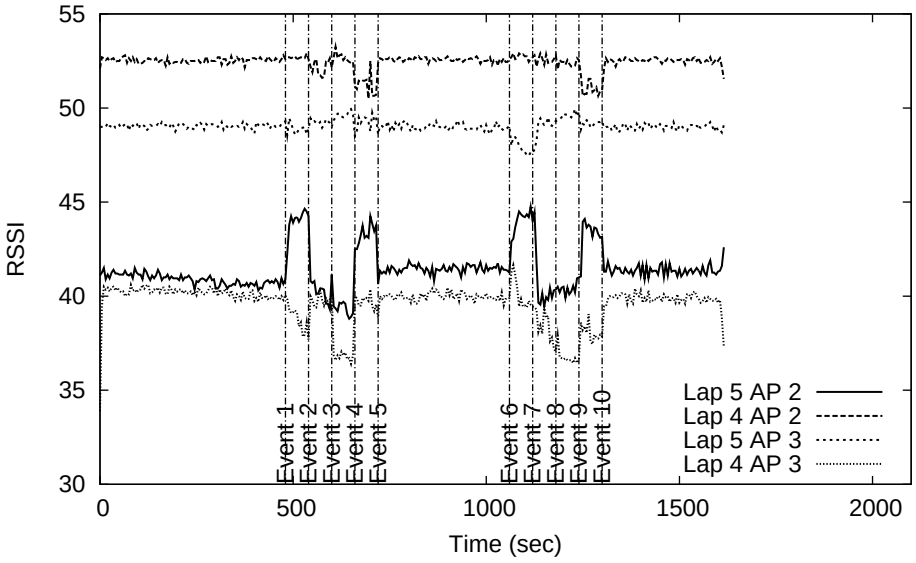


Figure 6: Experiment 1 RSSI

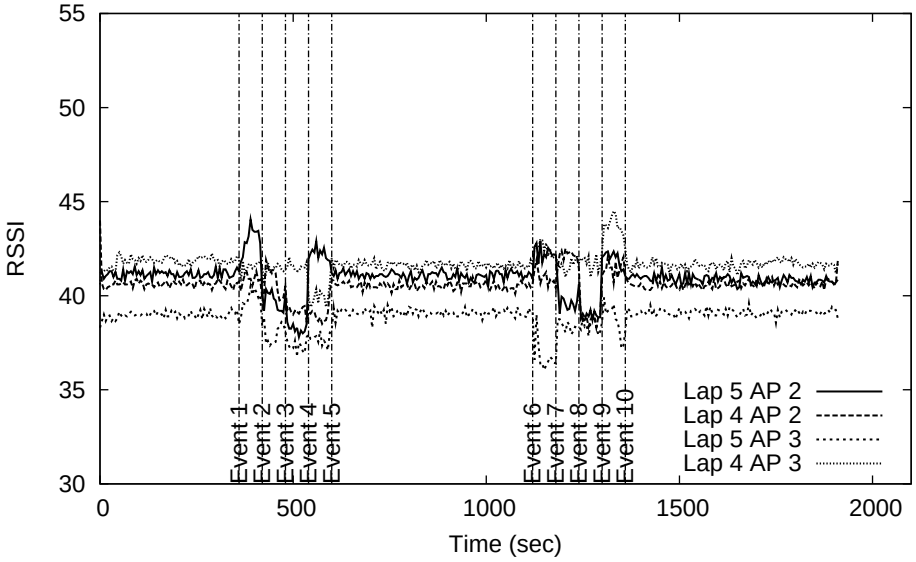


Figure 7: Experiment 2 RSSI

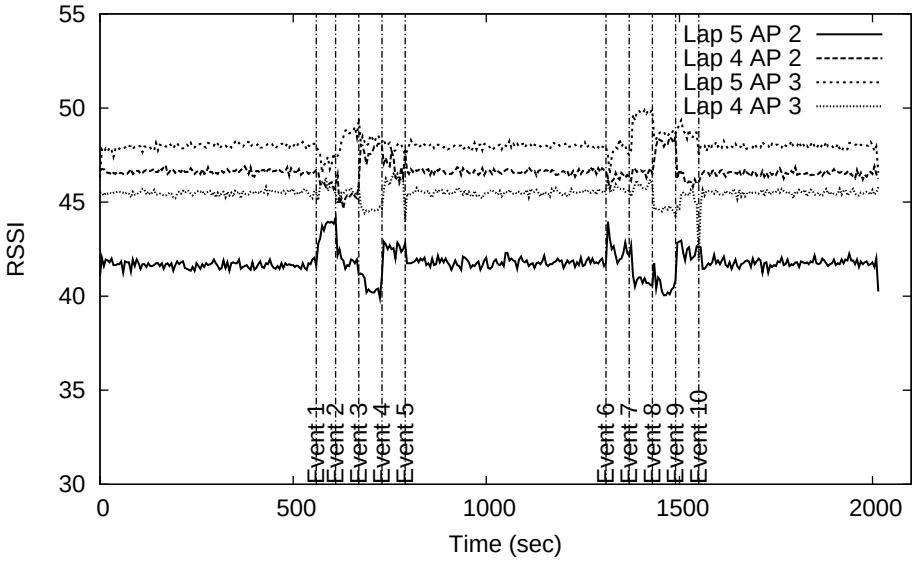


Figure 8: Experiment 3 RSSI

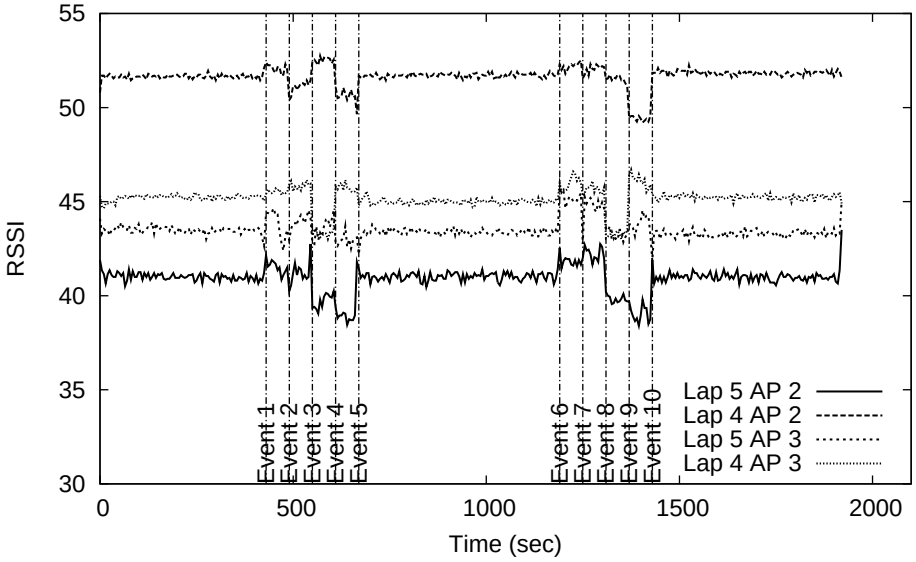


Figure 9: Experiment 4 RSSI

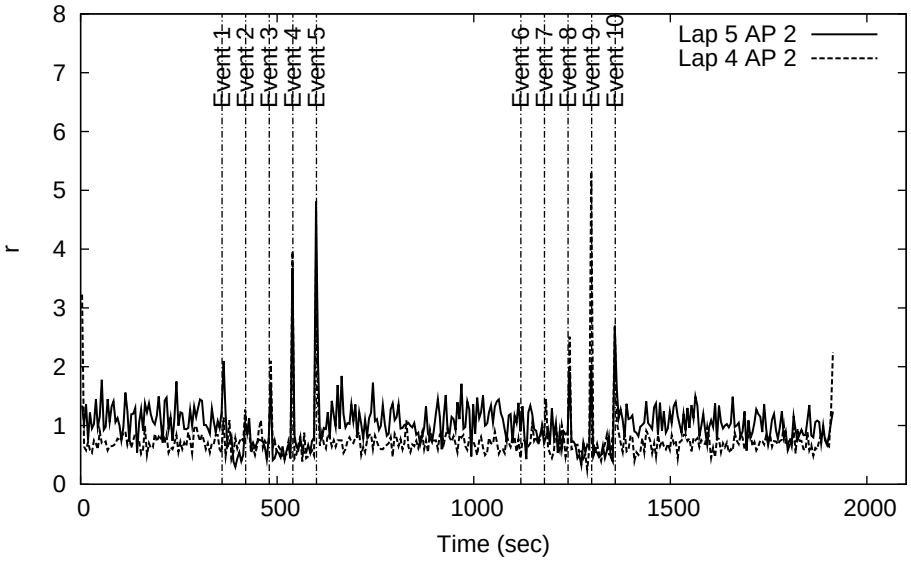


Figure 10: Experiment 2 Moving Variance $w = 40$: Series 1,2 of 4

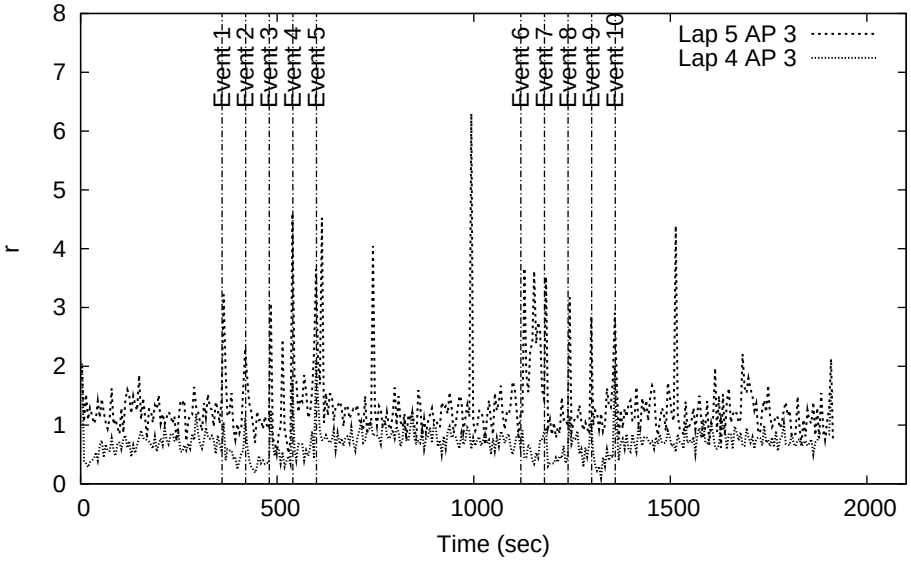


Figure 11: Experiment 2 Moving Variance $w = 40$: Series 3,4 of 4

In the ideal case for determining optimal parameter values, changing a parameter will both increase probability of detecting movement events and reduce the false positive rate. Most parameters, however, affect overall system sensitivity. To increase probablility of detection, they also increase the false positive rate. Finding parameters to maximize the probability of detection and minimize false positives is an optimization problem.

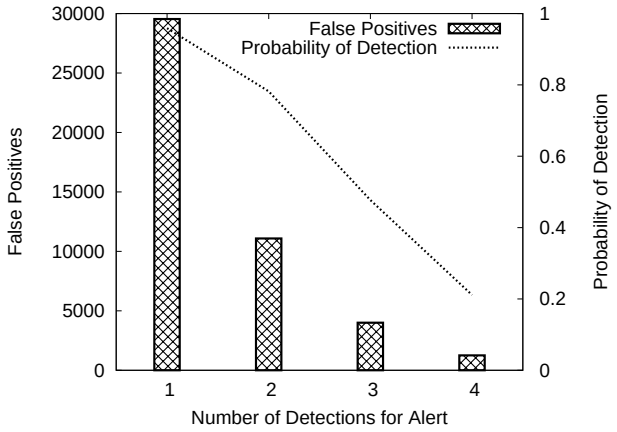
Requiring multiple pairs of access points and monitoring point detections for alerts reduces the system sensitivity, for both the moving average and moving variance detection methods. For the moving average technique (Figure 12(a)), FP is reduced from 29544 for single-detection alerts to 1252 for four-detection alerts. The PD also reduces dramatically from 95.9% to 21.1%. For the moving variance technique (Figure 13(a)), FP is reduced from 11244 for single-detection alerts to 22 for four-detection alerts. The PD decreases from 99.8% to 51.2%.

The time buffer parameter has a lesser effect on FP and PD. For the moving average technique (Figure 12(b)), increasing the time buffer from 0 seconds to 1 second increases FP from 12803 to 17175, while increasing the PD from 55.2% to 64.9%. For the moving variance technique (Figure 13(b)), increasing the time buffer from 0 seconds to 1 second causes little change. FP increases from 3464 to 3677 and PD from 82.5% to 84.2%.

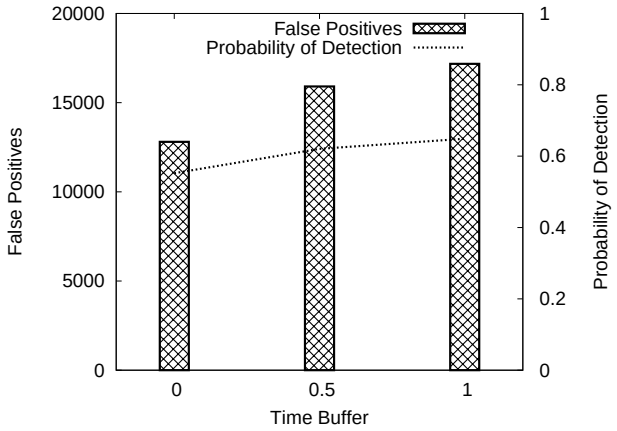
The parameters τ and r impact system sensitivity substantially (Figures 14 and 15). Increasing their values decreases both PD and FP. The decrease in average FP is substantial, from 31650 to 707 for the moving average threshold τ range and from 6835 to 784 for the moving variance r range. The decreases in PD for the same ranges are from 84.7% to 38.0% and 95.0% to 70.9% for the moving average and moving variance techniques respectively.

For the moving average technique, choice of the w_s parameter (Figure 16) is more important than the w_l parameter (Figure 17) for the ranges examined. FP drops from 26251 to 1514 for values of $w_s = 3$ and $w_s = 20$ respectively. PD drops from 74.0% to 47.0%. The w_l parameter has less effect on FP and PD over the range of $w_l = 20$ to $w_l = 200$. PD increased from 59.3% to 62.6%. FP varied between 10824 and 12329, but not as a monotone function of w_l.

For the moving variance window size parameter w (Figure 18), PD peaks slightly when $w = 40$. FP dropped from 5299 to 3997 from $w = 20$ to $w = 80$.

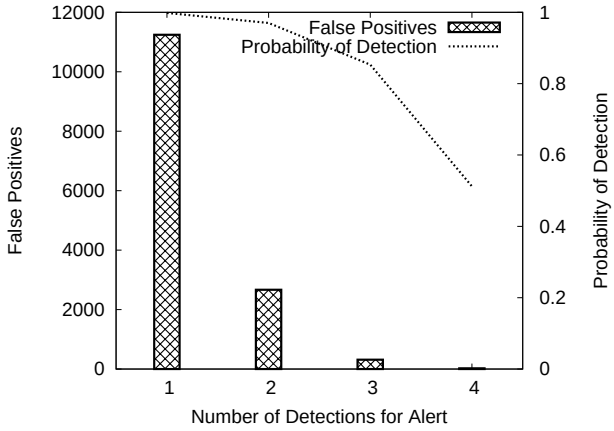


(a) Moving Average: Number of Detections for Alert N

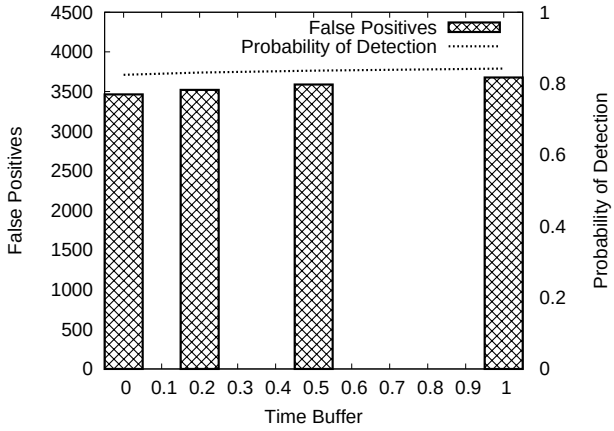


(b) Moving Average: Time Buffer b

Figure 12: Multiple Detection Parameters for Moving Average, with metrics averaged over other parameters



(a) Moving Variance: Number of Detections for Alert N



(b) Moving Variance: Time Buffer b

Figure 13: Multiple Detection Parameters for Moving Variance, with metrics averaged over other parameters

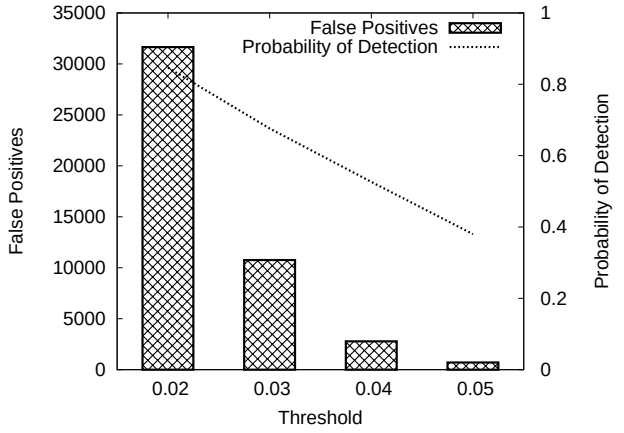


Figure 14: Moving Average: Threshold τ

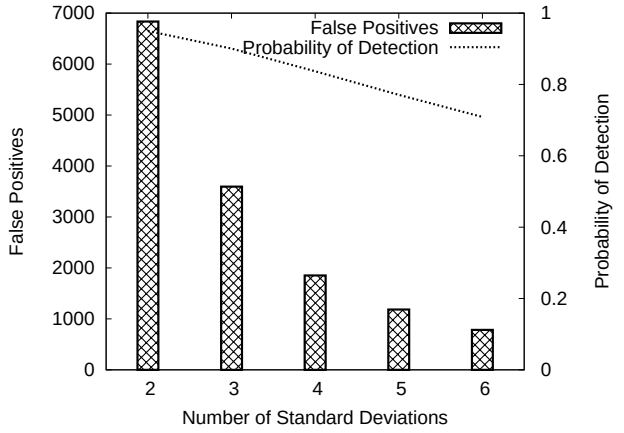


Figure 15: Moving Variance: Number of Standard Deviations r

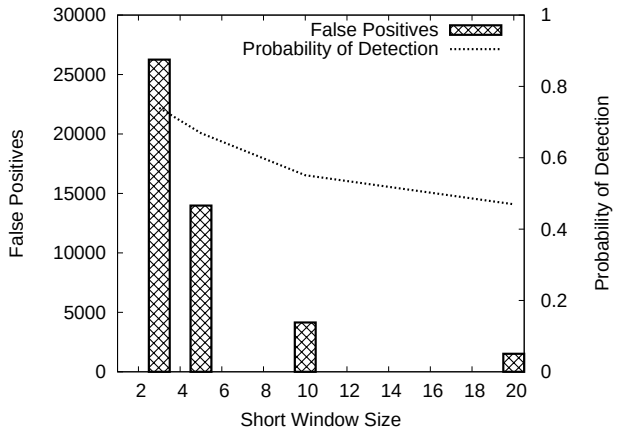


Figure 16: Moving Average: Short Window Size w_s

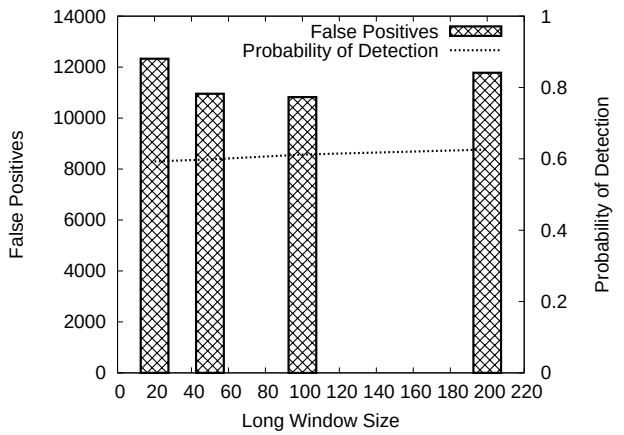


Figure 17: Moving Average: Long Window Size w_l

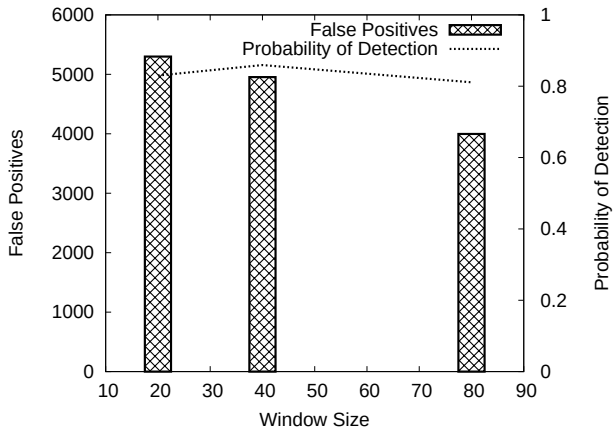


Figure 18: Moving Variance: Window Size w

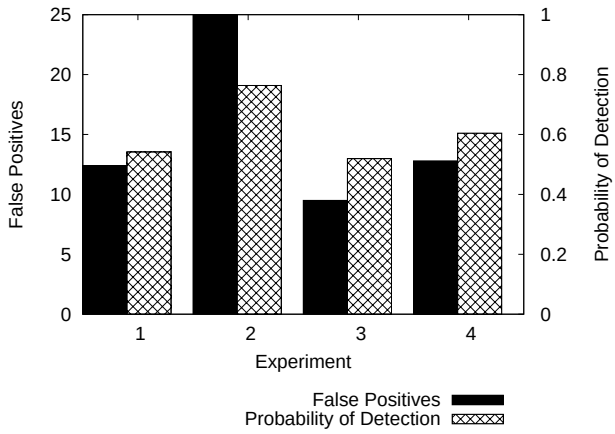


Figure 19: Averages of Moving Average Metrics by Experiment

5.3.1 Performance by Experimental Layouts

The summary results averaged over the moving average and moving variance parameters are shown in Figures 19 and 20. This analysis shows aggregate results only; particular parameters paired with a experimental setup could outperform others. The aggregate analysis is designed to indicate which experiment setups are more robust with respect to changes in the parameters.

In the aggregate analysis, the experiment 2 layout was the most sensitive under the moving average technique, having both the highest PD and FP. Under the variance technique, layout 2 had the fewest FP of any layout, and the 83.7% PD was slightly lower than the maximum of 86.5% for layout 4. For the other layouts, PD and FP increase or decrease together when moving from one layout to another.

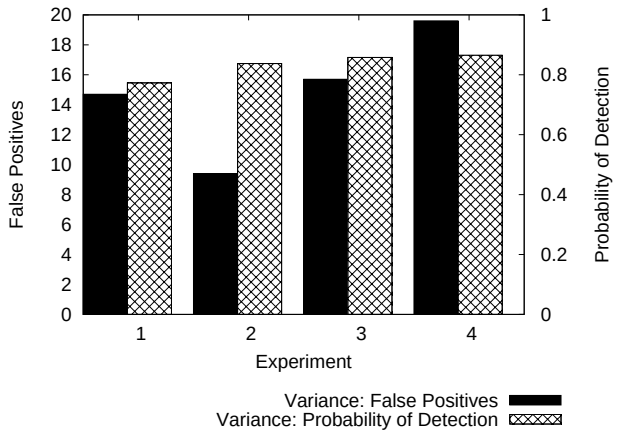


Figure 20: Averages of Moving Variance Metrics by Experiment

Layout	Moving Average	Moving Variance
1	3	0
2	44	37
3	32	5
4	63	20

Table 4: Number of Parameter Optimal Combinations by Experimental Layout

5.3.2 Optimal Parameter Combinations

The aggregate analysis of parameters thus far provides only a general indication of how changing parameters will affect system performance. To find optimal parameters maximizing probability of detection and minimizing false postives, it is necessary to examine particular parameter settings.

Both the moving average and moving variance techniques can recognize movement with high accuracy and few false positives for tuned performance parameters. Many different combinations of parameters successfully alerted for all 10 movement events with no false positives. The number of different combinations for each experimental setup are listed in Table 4. Further experimental measurements are required to further differentiate the performance of these parameter combinations.

The number of optimal combinations for each experimental layout suggest the ordering from best to worst should be 2 or 4 followed by 3 and 1. This is conjectured to be a result of the moving person impeding direct signal transmission from access point to monitoring point. Signals along direct paths are expected to have a greater contribution to signal strength than reflected signals.

Tables 5 and 6 show examples of optimal param-

Layout	w_l	w_s	τ	N	b
1	50	5	0.05	1	0
2	20	10	0.05	1	0
2	20	20	0.03	2	0
2	20	20	0.03	2	0.5
3	100	5	0.05	1	0
3	50	3	0.03	2	0
3	200	5	0.05	1	0
4	20	20	0.04	1	0
4	50	10	0.02	2	0

Table 5: Sample Moving Average Optimal Parameters

Layout	w	r	N	b
2	40	4	2	0
2	80	4	2	0
2	20	3	3	0
3	40	3	3	0
3	80	3	3	0
4	40	6	2	0
4	40	2	4	0

Table 6: Sample Moving Variance Optimal Parameters

eters that successfully alerted for all ten movement events while providing no false positives. These are examples only; as shown in Table 4, there are many more parameter combinations that are not listed.

Some parameter combinations performed well across all experimental layouts. Tables 5.3.2 and 5.3.2 show high performing parameter combinations for the moving average and variance techniques respectively. This is evidence these parameters are more robust than others because they were effective for multiple configurations, but the evidence is not conclusive.

6 Future Measurements

Future experimentation should include different movement patterns and more noisy experimental conditions to verify and expand upon this report's results. The experiments reported here used only short

Layout	PD	FP
1	0.8	0
2	1.0	1
3	0.8	0
4	1.0	0

Table 7: High performing average technique parameters: $w_l = 20, w_s = 3, \tau = 0.04, N = 2, b = 0$

Layout	PD	FP
1	0.9	1
2	0.9	0
3	0.9	0
4	1.0	0

Table 8: High performing variance technique parameters: $w = 40, r = 4, N = 3, b = 0.0$

bursts of movement followed by static periods. The techniques used in this report were designed to recognize this particular movement pattern, and should be tested over a wider range. A less controlled environment should be used to demonstrate the system is feasible in relevant, possibly noisy environments.

The variance technique is expected to generalize to other movement patterns with better performance than the moving average technique. In the four experiments performed, the moving person stopped in each position, where a new static measurement could be made. The moving average exploits this by estimating averages for two windows detecting when the averages are significantly different. If the moving person is in constant motion, the RSSI may fluctuate but give similar average values for the two windows. For the moving variance technique, any movement is expected to cause substantial signal changes relative to a static environment. As long as the variance in any window is significant, the system should detect motion.

7 Conclusions

In this report, we introduced the DfP system for intrusion detection and tracking in a WiFi network. The system uses the changes in the received RSSI to detect changes in the environment.

We described the DfP system's architecture and showed that the system works with the nominal WiFi equipment. We presented two techniques for intrusion detection and a technique for tracking single and multiple intruders. We also evaluated the performance of the DfP system for simple experiments.

Our results show that the system can detect movement with high probability and low false positive rate in controlled environments. Moreover, the system can track the intruder's position to within a few feet.

The experimental results are inconclusive for determining optimal DfP system configurations. Additional measurements are needed both for this purpose in the long-term goal of preparing a commercially deployable system. The results to date have established the proof of concept of the DfP technology.

References

[1] The Institute of Electrical and Electronics Engineers, Inc., IEEE Standard 802.11 - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, 1999.

[2] Paramvir Bahl and Venkata N. Padmanabhan, RADAR: An In-Building RF-based User Location and Tracking System, IEEE InfoCom 2000, Tel Aviv, Israel, March 26-30, 2000

[3] G. Chen and D. Kotz, A Survey of Context-Aware Mobile Computing Research, Dartmouth Computer Science Technical Report TR2000-381, 2000

[4] P. Krishnan, A. S. Krishnakumar, Wen-Hua Ju, Colin Mallows, Sachin Ganu, A System for LEASE: Location Estimation Assisted by Stationery Emitters for Indoor RF Wireless Networks, IEEE InfoCom 2004

[5] Moustafa Youssef, Ashok Agrawala, A. Udaya Shankar, WLAN Location Determination via Clustering and Probability Distributions," IEEE International Conference on Pervasive Computing and Communications (PerCom) 2003, Fort Worth, Texas, March 23-26, 2003.

[6] Moustafa Youssef and Ashok Agrawala, Handling Samples Correlation in the Horus System, IEEE InfoCom 2004, Hong Kong, March 7-11, 2004

[7] Moustafa Youssef, Ashok Agrawala, "Small-Scale Compensation for WLAN Location Determination Systems," IEEE Wireless Communications and Networking Conference (WCNC) 2003 New Orleans, Louisiana, March 16-20, 2003

[8] Moustafa Youssef, Ashok Agrawala, "The Horus WLAN Location Determination System," Third International Conference on Mobile Systems, Applications, and Services (MobiSys 2005), Seattle, WA, USA, June 2005.

[9] Moustafa Youssef and Adel Youssef and Chuck Rieger and Udaya Shankar and Ashok Agrawala, "PinPoint: An Asynchronous Time-Based Location Determination System," Fourth International Conference on Mobile Systems, Applications, and Services (MobiSys 2006), Uppsala, Sweden, June 2006.