Violating Privacy Through Walls by Passive Monitoring of Radio Windows

Arijit Banerjee
University of Utah
Salt Lake City, UT, USA
arijit@cs.utah.edu

Dustin Maas
Xandem Technology
Salt Lake City, UT, USA
dustin@xandem.com

Maurizio Bocca
Politecnico di Milano
Milano, Italy
maurizio.bocca@polimi.it

Neal Patwari
University of Utah & Xandem Technology
Salt Lake City, UT, USA
npatwari@ece.utah.edu

Sneha Kasera
University of Utah
Salt Lake City, UT, USA
kasera@cs.utah.edu

ABSTRACT

We investigate the ability of an attacker to passively use an otherwise secure wireless network to detect moving people through walls. We call this attack on privacy of people a "monitoring radio windows" (MRW) attack. We design and implement the MRW attack methodology to reliably detect when a person crosses the link lines between the legitimate transmitters and the attack receivers, by using physical layer measurements. We also develop a method to estimate the direction of movement of a person from the sequence of link lines crossed during a short time interval. Additionally, we describe how an attacker may estimate any artificial changes in transmit power (used as a countermeasure), compensate for these power changes using measurements from sufficient number of links, and still detect line crossings. We implement our methodology on WiFi and ZigBee nodes and experimentally evaluate the MRW attack by passively monitoring human movements through external walls in two real-world settings. We find that achieve close to 100% accuracy in detecting line crossings and determining direction of motion, even through reinforced concrete walls.

Categories and Subject Descriptors

C.2 [**Computer-Communication Networks**]: Miscellaneous

Keywords

Radio Window; WiFi; Signal strength; Line Crossing

1. INTRODUCTION

We investigate an attack to the privacy of the people moving in an area covered by a wireless network. People moving in an area covered by one or more wireless networks affect the way radio signals propagate. We demonstrate that the presence, location and direction of movement of people not carrying any wireless device can be "eavesdropped" by using the channel information of wireless links artificially created by an attacker by deploying sensing devices or *receivers* that can passively "hear" *transmitters* such as WiFi access points (APs), composing the legitimate wireless network. Radio signals from transmitters passing through non-metal external walls are analogous to light from light bulbs passing through glass windows in that either can be used to "see" where building occupants are moving from outside of the building. Hence, we call this attack on privacy of people an "monitoring radio windows" (MRW) attack.

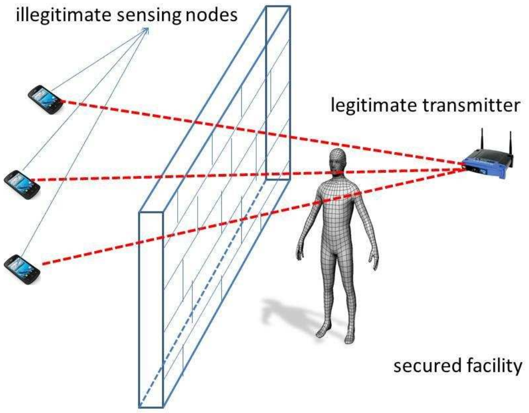


Figure 1: Monitoring Radio Windows (MRW) attack example.

Consider a building where security is important (e.g., an embassy) with a concrete exterior wall. One or more wireless networks may have been set up in this building to transfer different types of data, including voice and video. We can expect these networks to implement advanced data security protocols to prevent eavesdropping of data. However, an attacker can still deploy receivers outside the wall of the building to passively measure different parameters of the received

WiSec'14, July 23–25, 2014, Oxford, UK.
Copyright 2014 ACM 978-1-4503-2972-9/14/07 ...$15.00.
http://dx.doi.org/10.1145/2627393.2627418.

radio signals. By measuring the channel state information (CSI) or received signal strength (RSS), for example, of the links from the transmitters inside the building to the receivers deployed, the attacker can monitor the movements of people and objects inside the building in the area behind the wall in Figure 1. The information about people's movements can be put to malicious use including planning a physical attack on the personnel inside the building.

In this paper, we design and implement the MRW attack methodology for through wall people localization. Our methodology relies on reliably detecting when people cross the link lines between the legitimate transmitters and the attack receivers. We first develop a majority-vote based detection algorithm that reliably detects line of sight (LOS) crossing between the legitimate transmitter and the attack receivers by comparing short-term variances in link channel information with their long-term counterparts. We also develop a method to estimate the direction of movement of a person from the sequence of link lines crossed during a short time interval. Next, we implement our methodology on WiFi and ZigBee nodes and experimentally evaluate the MRW attack by monitoring people's movements through walls in two real-world settings – a hallway of a university building separated from the outside by a one-foot thick concrete wall, and a residential house. When we use two WiFi 802.11n nodes with normal antenna separation, or two groups of ZigBee nodes as attack receivers, we find that our methods achieve close to 100% accuracy in detecting line crossings and the direction of movement. We also find that our methods achieve $90-100\%$ accuracy when we use a single 802.11n attack receiver. We note that our goal in this paper is not to precisely estimate the location of a moving person but rather, only detect line crossings and determine the direction of movement through walls. This coarse-granular location information violates the person's privacy and can be used by an attacker.

To protect the privacy of the location information from the MRW attack, the owner of the legitimate network may choose to implement a countermeasure in which the transmitters vary their transmit power during successive transmissions. The artificial transmit power changes can be either random or follow a pre-defined profile replicating the typical channel variations introduced when a person crosses a link line. This countermeasure is expected to introduce additional variability in the received signal measured by the attack receivers, which can be wrongly interpreted by the attacker as caused by moving people or objects crossing the link lines. In this paper, we demonstrate that an attacker who can measure a sufficient number of links can accurately estimate the artificial transmit power change, compensate for it, and ultimately locate people and monitor their movements. We base our compensation strategy on the following intuition: an artificial transmit power change at a transmitter will impact the measurements at all attack receivers with approximately the same magnitude of change, whereas genuine power changes due to human movement are likely to impact receivers each with a different magnitude. This intuition also suggests that protecting against radio window attacks is a very hard problem because any change at the source of transmission can be possibly compensated for by correlating measurements across multiple attack receivers.

The idea of using radio signals through walls for obtaining location information is not new and has been used in existing efforts including Radio Tomographic Imaging (RTI) [25], WiVi [2], and WiTrack [1], among others. However, the existing literature does not demonstrate that an attacker can obtain location information 1) without transmitting (and thus not subject to jamming or source localization); and 2) through thick external walls (such as reinforced concrete) and in large buildings. Wilson et al. developed RTI [25] to track human movement through walls by deploying dozens of transceivers throughout or on many sides of a room in a residential home. However, RTI requires active transmission from all the deployed nodes, and, hence it can be detected by source localization and/or countered by jamming. Note that for solid external walls, penetration loss can be very high, e.g., about 20 dB/ft through concrete at 2.4 GHz [21]. Since the signal must penetrate external walls twice, once to enter and once to exit the building, transmit power must be very high in order to achieve useful range.

Adib et al. [2] developed WiVi to track moving humans through walls inside a closed room using WiFi signals. In a follow up work, Adib et al. [1] developed a 3-D through-wall motion tracking system, WiTrack, that can be used to track the 3D location of a moving person inside a room, and to detect falls and simple gestures. Though efficient, these methods also depend on active probing requiring custom hardware to send WiFi signals through a barrier (e.g., a wall) and measure the way it reflects back from objects on the other side. Like RTI, these methods are vulnerable to detection and jamming, and must penetrate an external wall twice. Note that WiTrack was demonstrated through drywall [1], which has a 0.5 dB penetration loss at 2.4 GHz [26]. Our work is stealthier in that purely *passive* receivers are deployed by an attacker to measure signals from the transmitters already deployed in existing infrastructure. The attack receivers do not transmit any signal or interfere with the existing transmissions in any way - hence they can not be detected using source localization and are immune to jamming. Furthermore, the active signal transmission from outside the wall, forces WiVi and WiTrack to perform a costly "nulling" procedure to counteract the flash effect - the strong reflection from the wall that overshadows signals reflected back from inside the room. We rely only on the transmitted signal from the existing infrastructure inside the facility to detect a person's movement, hence the flash effect does not apply. We can perform our location detection with simpler algorithms and off the shelf hardware. Unlike WiVi and WiTrack, our method enables the attacker to see through dense wall material, including 12 inch thick reinforced concrete walls. In a related work that is not directly concerned with location privacy [18], Pu et al. showed that Doppler shifts resulting from multipath distortions, due to reflections of wireless signals from a human body, can be used to identify human gestures. However, their work relies on classification of gestures based on extensive learning. One must actively perform a startup sequence of gestures in the direction of the wireless receiver(s) to get into the control system before sending the real gesture commands. Our research does not consider human gestures and hence does not require an extensive learning phase.

The remainder of the paper is organized as follows. Section 2 describes the adversary model, while in Section 3 we introduce the methods developed. Experimental setup and results are presented in Sections 4 and 5, respectively. Additional existing research in the area of location privacy attacks is discussed in Section 6. Conclusions are given in Section 7.

2. ADVERSARY MODEL

We make the following assumptions about the attacker (In this paper, we use the term attacker for anyone, whether malicious or genuine, who is trying to detect human movement):

- The attacker is able to deploy multiple wireless sensing devices within the transmission range of the legitimate transmitter(s) outside the area being monitored. The attacker is able to measure the physical layer information (RSS and/or CSI) of the links between the transmitter(s) and the attack receivers.
- The attacker does not have access to the content of the packets transmitted by the legitimate network nodes.
- The attacker does not deploy any transmitters, nor does it have any control over the legitimate transmitters. However, it requires the legitimate transmitters to transmit packets frequently to allow it perform the line crossing detections.
- The attacker does not make any assumption regarding the transmit power profile of the transmitters.
- The attacker nodes do not associate or interfere in any manner with the transmissions of the legitimate transmitter(s).
- The attacker may not know the precise location of the transmitters, however, we do assume that the transmitter is located well inside the perimeters of buildings for network coverage.
- The attacker may deploy the MRW attack when it is dark to minimize the chance of getting detected.

3. METHODOLOGY

In this section, we first develop a methodology to detect line crossings of a single person based on a majority vote for WiFi 802.11n receivers. We also develop a method that uses a sequence of line crossings to determine the direction of the movement. Next, we present our approaches for estimating transmit power change and its compensation, when the transmit power is artificially changed by the owner of the wireless transmitters, inside a secure building, with the hope of preserving location privacy. Last, we show how we adapt our methodology for IEEE 802.15.4 ZigBee attack receivers.

3.1 Line Crossing Detection

Many modern WiFi networks use the 802.11n standard, in which transceivers are equipped with multiple antennas in order to leverage the spatial diversity of the wireless channel. While these multiple-input multiple-output (MIMO) systems provide high data rates, they also provide a rich source of channel information to an adversary interested in localizing people inside a building.

The 802.11n wireless standard uses the well-known orthogonal frequency-division multiplexing (OFDM) modulation scheme, which encodes and transmits data across multiple subcarriers for each transmitter-receiver antenna pair. When an 802.11n receiver receives a packet, it estimates the effect of the wireless channel on each MIMO OFDM subcarrier for the purpose of channel equalization. Since this channel state information (CSI), represented as a complex gain for each subcarrier, is measured during the unencrypted preamble of each WiFi packet, an adversary without legitimate access to data on the network can still measure the CSI for every packet.

We apply a windowed variance method for detecting abrupt changes in the CSI for a WiFi link. Let $H_{j,k}(n)$ be the magnitude of the signal strength for the jth transmitter-receiver antenna pair and the kth OFDM subcarrier for the nth packet. We define the windowed variance measurement at packet n as follows. Let

$$v^{w}_{j,k}(n) = \frac{1}{w-1} \sum_{i=n-w+1}^{n} (H_{j,k}(i) - \bar{H}^{w}_{j,k})^2, \qquad (1)$$

where, w is the number of previous CSI samples in the window and $\bar{H}^{w}_{j,k}(n)$ is the average signal strength for the jth transmitter-receiver antenna pair computed over w.

We define the subcarrier-average variance and standard deviation for packet n for a given antenna pair j as

$$V^{w}_{j}(n) = \frac{1}{N} \sum_{k} v^{w}_{j,k}(n), S^{w}_{j}(n) = \frac{1}{N} \sum_{k} \sqrt{v^{w}_{j,k}(n)}. \qquad (2)$$

where N is the number of subcarriers. We track both $V^{w}_{j}(n)$ and $S^{w}_{j}(n)$ over a short-term time window w_s, and a long-term time window w_l, and detect a line crossing when

$$\sum_{n \in D} V^{w_s}_{j}(n) - V^{w_l}_{j}(n) > \gamma(n), \qquad (3)$$

where D is the most recent contiguous set of packets for which $V^{w_s}_{j}(n) - V^{w_l}_{j}(n) > 0$ and the threshold $\gamma(n)$ is defined as

$$\gamma(n) = V^{w_l}_{j}(n) + CS^{w_l}_{j}(n). \qquad (4)$$

$\gamma(n)$ determines the sensitivity of the detection system, smaller values of $\gamma(n)$ will ensure low missed detection rate but will increase the probability of false alarms. On the other hand, larger values of $\gamma(n)$ will lower false alarm rates at the expense of higher missed detection rates. The constant C is included to allow the user to adjust the trade-off between false alarms and missed detections.

To improve robustness, in the case where there are more than two antenna pairs, we take the majority vote between antenna pairs over the short-term window to decide if a line crossing has occurred. More specifically, when a receiver antenna detects a line crossing, we count the line crossing detections for all the receiver antennas over the short-term window, w_s. For a 3×3 MIMO transmitter and receiver, this would mean computing a majority vote over nine measurements. When the majority of the receiver antennas detect a line crossing within w_s, we infer that a person has crossed the link line between the transmitter and the receiver. We will show that this majority vote method improves the performance of our detector by decreasing false alarms and missed detections.

We note that our window-based variance method differs from the method presented in [19,28]. In [19,28], Youssef et al. compare recent window-based variance measurements of RSSI at multiple WiFi links to measurements made during a static calibration period when nobody is moving in the area of interest. If a certain number of WiFi links within the area of interest detect motion within a certain time interval, a motion event is detected in the area of interest. Our attacker does not know if and/or when people are moving inside of the building, and therefore cannot create calibration measurements based on a static environment. Instead, we compare a short-term window variance to a long-term windowed variance. The long-term window allows us to capture the behavior of the wireless links when the majority of measurements are likely made while there is nobody crossing the link line. Additionally, in the case of 802.11n, we exploit the effect that line crossings have on each OFDM subcarrier and MIMO antenna pair.

3.2 Determining Direction of Motion

If the adversary measures the CSI at multiple receivers, or if a single receiver includes multiple antennas as is the case with 802.11n, it is also possible to infer the direction that a person is walking when line crossings are detected. The direction of motion is inferred from the time differences between the line crossing detections at each receiver, in the case of multiple receivers, or at each transmitter-receiver antenna pair, when the receivers include multiple antennas.

Consider the scenario where the attacker arranges the MIMO antenna array of an 802.11n receiver such that the antennas are roughly parallel to a hallway as shown in Figure 2(a). The spatial order of the antennas with reference to the hallway is known, and each transmitter-receiver antenna is given an index according to its spatial order. Based on the adversary model assumption that a transmitter is located well inside the perimeter, the attacker, even without knowing the precise location of the transmitter or the arrangement of its antennas, may treat the antennas of the wireless transmitter as if they are co-located and still achieve reliable results.

In the single WiFi receiver case, if a link crossing is detected by majority vote for a given short-term window, we find the line that best fits the set of points $\{(d_j, n_j) : j \in P\}$, where d_j is the spatial index of antenna pair j representing it's location relative to the other links, n_j is the packet index indicating when a detection occurred at antenna pair j according to (3), and P is the set of antenna pairs ending at the WiFi receiver which detected a line crossing during the short-term window. The sign of the slope of this line indicates the direction of motion. Figure 2 shows an example which uses CSI measurements from three antennas at the WiFi transmitter and three antennas at WiFi RX1 (9 antenna pairs). In the case of two single-input single-output (SISO) WiFi receivers, a similar method may be applied, but the two spatial and packet indexes directly determine the line and its slope.

3.3 Compensation of Transmit Power Change

In this subsection, we propose a methodology to detect artificial transmit power changes (if any) and compensate for the same. The signal strength for the jth transmitter-receiver antenna pair and the kth OFDM subcarrier for packet n is given by

$$H_{j,k}(n) = T_x(n) + G_t + G_r - L_{j,k}(n) + \Psi_{j,k}(n), \tag{5}$$

where $T_x(n)$ is the transmit power of the transmitter for packet n, G_t and G_r are the transmitter and receiver antenna gains, respectively, $L_{j,k}(n)$ is the path loss, and $\Psi_{j,k}(i)$ is a noise term.

The attacker does not know the transmit power or antenna gains, so she relies on the difference between the signal strength for the packet n and the reference packet ($n = 0$) as follows.

$$h_{j,k}(n) \triangleq H_{j,k}(n) - H_{j,k}(0). \tag{6}$$

From (5), we see that

$$h_{j,k}(n) = t_x(n) - l_{j,k}(n) + \psi_{j,k}(n), \tag{7}$$

where $t_x(n) = T_x(n) - T_x(0)$, $l_{j,k}(n) = L_{j,k}(n) - L_{j,k}(0)$, and $\psi_{j,k}(n) = \Psi_{j,k}(n) - \Psi_{j,k}(0)$.

In absense of any transmit power changes, $h_{j,k}(n)$ is dominated by path loss changes caused when a person crosses the link and abrupt variation in $h_{j,k}(n)$ can be used to detect line crossings. However, any transmit power change (introduced artificially) at the transmitter dominates the $h_{j,k}(n)$ term and masks the effect of channel variation caused by human movement. A transmitter could thus presumably preserve location privacy by changing its transmit power frequently to introduce artifical signal strength variations.

We now propose a method that a smart attacker can use to estimate and remove the artificial power changes and accurately detect line crossings. In our method, the attacker estimates the artificial transmit power change amplitude by correlating measurements across all antenna pairs and all subcarriers, and removes the effect of transmit power changes from the received signal strength measurements. We propose to use the median of $h_{k,j}(n)$ for all available transmitter-receiver antenna pairs and corresponding subcarriers, as an estimator of the artificial transmit power change, as shown in the equation below:

$$\hat{t}_x(n) = \text{median}\left\{h_{j,k}(n) \forall j, k\right\}. \tag{8}$$

Our choice of this estimator is based on the following observations. First, we observe that $t_x(n)$ appears in the equation for $h_{k,j}(n)$ for all j and k. This is because, any change in transmit power affects measurements across all transmitter-receiver antenna pairs and corresponding subcarriers simultaneously. We also know that the change in the path loss $l_{j,k}$ is just as likely to be positive as negative. Furthermore, any change due to human movement will not affect all the links simultaneously.

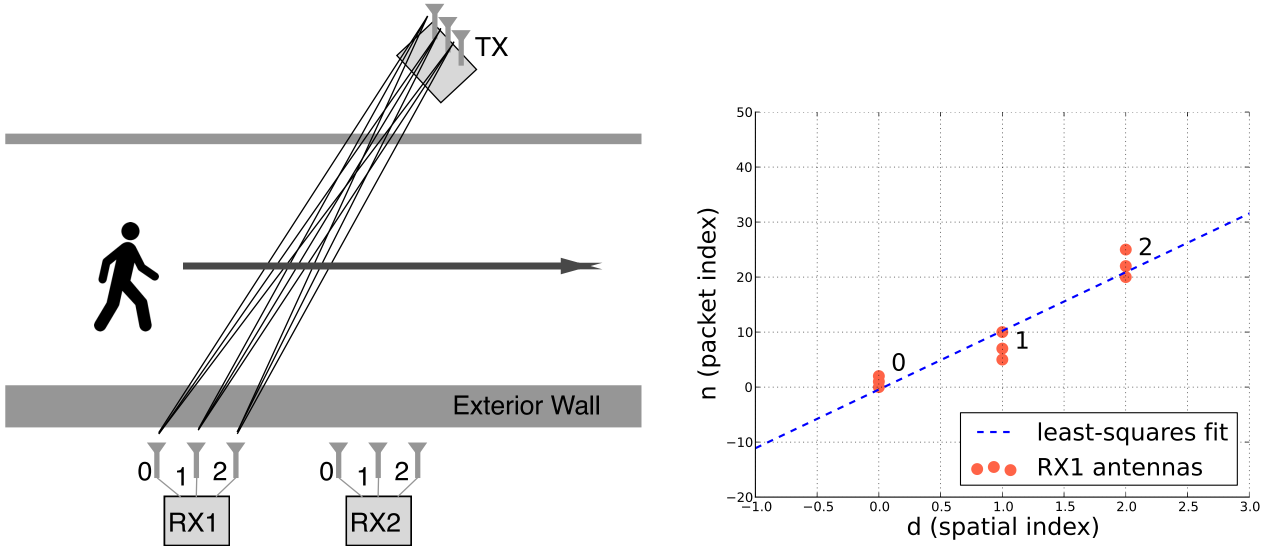
In the absence of an artificial transmit power change, $\hat{t}_x(n)$ is likely to be close to zero, i.e., our estimator does not require us to detect whether or not there is an artificial transmit power change for packet n.

The compensated signal strength for packet n, which we denote $\hat{H}_{j,k}(n)$, is given by

$$\hat{H}_{j,k}(n) = H_{j,k}(n) - \hat{t}_x(n). \tag{9}$$

Although the reference packet was sent with unknown transmit power $T_x(0)$, for $n > 0$, we consider $T_x(n)$ to be the relative dB shift in transmit power compared to $T_x(0)$. $\hat{H}_{j,k}(n)$ essentially, is an estimate of the subcarrier signal strength if there were no transmit power changes between the reference packet and packet n.

It is clear that, any error in the estimation of the transmit power changes amplitude will introduce additional noise in the measurements. However, the dynamics of the signal are still preserved and an attacker can use any variation in the



(a)

(b)

Figure 2: (a) The MIMO antenna array used for line crossing detection.(b) Direction of motion is determined by slope of the line fitted to the points created by the spatial indexes of the antennas and the packet indexes.

signal over a short time period in order to notice motion of a person near the link line.

3.4 ZigBee Networks

The methodologies described above are also applicable for IEEE 802.15.4 ZigBee nodes. However, the ZigBee nodes are generally equipped with a single antenna, so the MIMO setup is not available. Moreover, ZigBee nodes do not use OFDM for communication, so we use channel information from a single frequency channel (instead of averaging across all subcarriers as in the case of OFDM) to evaluate our methodologies. Furthermore, there is no tool to get the complete CSI at the receiver. Instead, we rely on the RSS value obtained from the receiver hardware. Thus, in the case of ZigBee we set $H_{j,k}(n)$ to the RSS value measured in decibel units for the jth transmitter-receiver antenna pair for packet n, also $k = 1, \forall j$ as we have measurements from a single channel only.

In order to create spatial diversity we use three closely located ZigBee receivers together to form a group as described in Section 4. We detect line crossings by applying our majority vote approach on the three links formed between the transmitter and the three receivers in the group. We detect direction of motion using two groups of receivers and observing sequence of groups crossed over a short time window. We estimate and compensate for artificial transmit power changes (if any) by applying the methods described in Section 3.3, and utilizing the fact that any change in transmit power affects all receivers simultaneously across all groups.

4. EXPERIMENTS

In this section, we describe the experimental setup. Section 4.1 describes the tools we use to measure the wireless channel, Section 4.2 describes the transmit power changes we apply, and Section 4.3 describes two real-world experimental deployments.

4.1 Tool Description

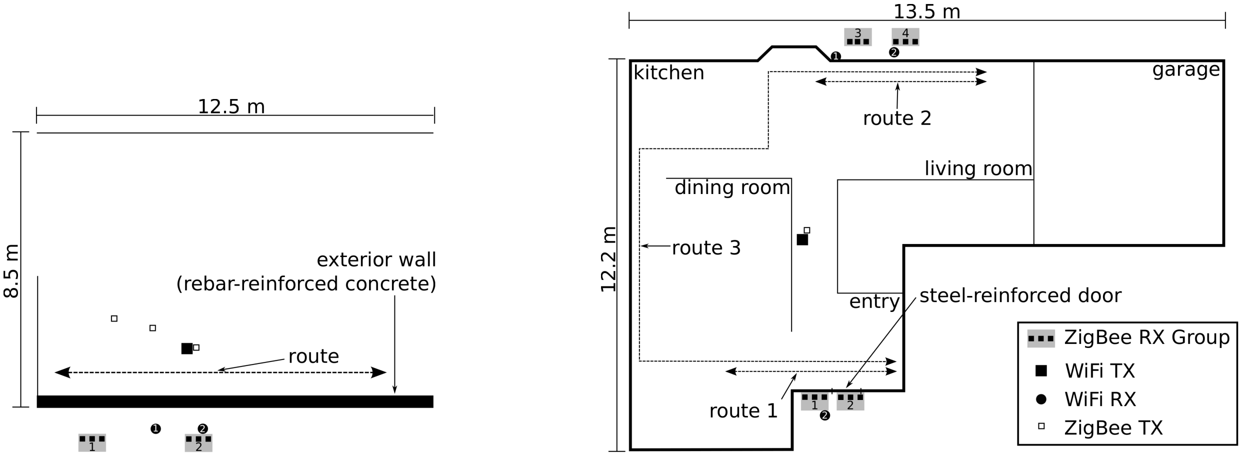
We use the following tools to measure the wireless channel and detect line crossings.

WiFi: We use laptops with Intel 5300 NICs that have three-antenna MIMO 802.11n radios. We use the CSI Tool [9], that has been built for these radios, to get channel state information from the WiFi transmitter. The CSI tool extracts 802.11n channel state information for 30 subcarrier at each antenna pair. Since we use three antennas at each node for communication, for each transmitter-receiver pair, we have $3 \times 3 = 9$ links each with 30 subcarrier groups. We use two kinds of antenna separations - in the normal case (WiFi_NORM), we place the antennas 6 cm apart, in the other case (WiFi_SEP), we use a larger antenna separation of 30 cm. The increased separation is accomplished by connecting the antennas to the Intel 5300 NIC with standard RF cables that are long enough to provide up to 30 cm separation. We program the transmitter to transmit packets at a rate of 10 Hz which is similar to beacon frame rates of a standard wireless access point. The attack receivers use the CSI Tool to obtain channel state information from the received packets which in turn is used to detect line crossings as described in Section 3.1.

ZigBee: For the ZigBee experiments, we use Texas Instrument CC2531 USB dongles [22], which are equipped with low-power, IEEE 802.15.4-compliant radios operating in the 2.4 GHz ISM band. The transmission frequency in this case is 12 Hz. A laptop is used to process the measured data at the attack receivers. There is no tool to obtain the CSI information in the case of ZigBee nodes. Therefore, we use the RSS value (in dBm) measured by the receiver hardware for our analysis, as described in Section 3.4.

4.2 Transmit Power Variations

We consider three different settings of transmit power variations for our experiments:



(a) University hallway.

(b) Residential.

Figure 3: Network layouts. We show maps of the University Hallway and the Residential House and mark the location of the legitimate transmitter(s) and the attack receivers. We also highlight the route(s) followed by the walking person.

TX_NORMAL: In this case, the transmitters transmit with fixed transmit power and variations in RSS are due to person movement and noise only.

TX_LINECROSS: For finer control, we simulate the effect of transmit power change (for both WiFi and ZigBee) by modifying received data according to a power profile that replicates typical signal attenuation introduced by a person crossing the link line. We randomly select different time points in the measurements to introduce effect of transmit power change.

TX_RANDOM: Here, we experimentally implement or simulate the scenario where the transmitter may use a different power level for each transmission by randomly selecting from a predefined set of power levels supported by the hardware. For ZigBee nodes, we program the transmitter(s) to change its transmit power at each transmission by randomly selecting one among four pre-defined transmit power levels, *i.e.*, $+4.5$ dBm, -1.5 dBm, -6 dBm, and -10 dBm. However, we are unable to program the random power changes in WiFi nodes and hence, we simulate these power changes.

While simulating effects of transmit power change we rely on the fact that any change in the transmit power at a time instant is observed across all subcarriers for all transmitter-receiver antenna pairs in case of WiFi and across all receivers in case of ZigBee at the same instant and we change the received signal parameters accordingly. We also add a zero mean Gaussian random variable (with standard deviation 0.67) to each $H_{j,k}(n)$ measurement, in addition to the the transmit power change $t_x(n)$, to account for errors due to environmental noise.

4.3 Experimental Deployments

We evaluate our methodologies in two different real world settings.

4.3.1 University Hallway

We choose a hallway inside a university building as the area being monitored (Figure 3(a)). The hallway is adjacent to a 30 cm thick and 3.5 m tall rebar-reinforced concrete boundary wall. We note that this type of a wall causes significant RF attenuation at WiFi frequencies and represents a worst-case scenario among typical exterior walls for our purposes [20]. We place the attack receivers outside the boundary wall parallel to the hallway approximately 1 m away from the wall, at a height of 1.2m.

For the WiFi experiment, we deploy one transmitter inside the building across the hallway, and two attack receivers separated by 3 m outside the concrete wall (Figure 3(a)). Similarly, for the ZigBee network, we deploy one transmitter across the hallway and six receivers outside the boundary wall. The attack receivers are placed in two groups of three nodes each, with the distance between the groups being 3 m (Figure 3(a)). Nodes in the same group are almost 30 cm apart. We perform both TX_NORMAL and TX_RAND experiments with the same ZigBee setup.

During the experiment, a person is walking back and forth along a predefined path (shown as route in Figure 3(a)) along the corridor between the transmitter and the attack receivers. With the help of a metronome, the person walks at a constant speed of 0.5 m/s. We collect over $12,000$ data samples for WiFi and over $20,000$ data samples for ZigBee in this experiment. In our evaluation, we use $w_s = 4$ s (short time window), and $w_l = 40$ s (long term window) (Section 3.1). Note that, w_s must be chosen such that it effectively captures the effect of short term variation in signal strength due to human movement in the vicinity of the link. We observe that, for typical movements these variations last for about 2-6 seconds (Figure 5). We use the mean value for our evaluation (our results do not change significantly if we other values in the 2-6 seconds range). On the other hand, w_l must be large enough to capture the long term behavior of the link, and should not get affected by short term movements. We select a moderately large value for w_l that effectively captures the long term link behavior, and keeps the computation complexity under reasonable bounds so that the detection can be performed in real time.

4.3.2 Residential House

In this experiment, we monitor two sides of a residential house (Figure 3(b)) to detect people movement. We perform two sets of experiment with the WiFi nodes. In the first experiment (House 1), we place the WiFi transmitter in a corridor centrally located inside the house and two WiFi receivers with normal antenna separation (WiFi_NORM) in the backyard of the house outside the external wall as shown in the Figure 3(b). The receivers are placed approximately 1 m away from each other, both at a height of 1.2m. For the second experiment (House 2), we use two WiFi receivers with larger antenna separation (WiFi_SEP) and place one of them in the backyard and the other outside the front entrance. The transmitter is placed in the same position as in experiment House 1.

For the ZigBee network, we place two groups of receivers, each group with three nodes, on either side of the house outside the external walls. As shown in Figure 3(b), the ZigBee groups 1 & 2 are placed outside the front entrance, and groups 3 and 4 are placed in the backyard, approximately 1 m away from the walls. Nodes in the same group are almost 30 cm apart while the inter-group distance on either side being at least 1 m. The ZigBee transmitter is placed inside the house co-located with the WiFi transmitter.

During these residential experiments, a person walks inside the house back and forth first near the front entrance of the house (route 1 in the Figure 3(b)), and then in the living room which is near the rear end of the house (shown as route 2 in the Figure 3(b)). Finally, the person makes a few rounds inside the house as shown in route 3 in the Figure 3(b). We collect over $10,000$ data samples for each set of ZigBee and WiFi experiments. We video record the line crossings to test the accuracy of our detection method against ground truth. For the residential experiments, we use $w_s = 2$ s (short time window), $w_l = 20$ s (long term window) and $\Delta = 4$ s (Section 3.1). We use smaller window sizes for detection of line crossings as the person walks at a faster speed as compared to the University Hallway experiments.

In our experiments, we place the transmitter on a stand that is approximately 1.2 m high. We understand that transmitters are sometimes placed on a ceiling. However, given that transmitters are typically placed well inside boundary walls for coverage reasons, we can assume that movement behind boundary walls will still result in line of sight crossings between the transmitter and receivers that an attacker deploys at low heights. Furthermore, even if transmitter and receiver are both at ceiling height, there should be changes in CSI observed, as shown by [29]. An attacker may also use existing works on source localization [16, 17] to determine the location of the wireless transmitter, and plan the target area of detection accordingly.

We end this section by noting that while our experiments consider only one wireless transmitter, it is very likely that multiple transmitters will be present in a common home/university setting. However, WiFi transmitters actively avoid interfering with each other due to the 802.11 MAC protocol. Wireless devices, such as WiFi access points, also attempt to operate on different channels for minimizing transmission overlap. Therefore, signals from wireless transmitters can still be received at the attack receivers. Additionally, we can identify the transmitter a packet is coming from using RSS-based or other signatures. We will thoroughly investigate the impact of multiple transmitters on detection accuracy in our future work.

5. RESULTS

We evaluate the performance of the MRW attack in terms of false alarm and missed detection rates. False alarm (FA) rates are calculated as the number of line crossings wrongly detected by the system over the number of sample points. Missed detection (MD) rates are calculated as the number of actual line crossings not detected by the system over the total number of actual line crossings.

5.1 Detection of Line Crossing

In this section, we present the accuracy of detection of line crossings using the methodology as described in Section 3.1.

5.1.1 University Hallway

Table 1 lists the results obtained in the University Hallway experiment using our majority vote detection. We achieve almost 100% detection rate with few false alarms and missed detections. Using a WiFi 802.11n receiver with normal antenna separation, we get zero false alarms and only 1.92% missed detections. We compare the detected crossing times with those in the recorded video footage of the experiment and find that we can detect the crossing times with an average error of 0.79 s, with minimum and maximum errors of 0.03 s and 2.73 s respectively.

We obtain zero false alarms and missed detections when using a 802.11n WiFi receiver with a large spatial separation between antennas, the mean error in this case being 1.22 s. For ZigBee, using a group of three closely located receivers, we get a 2.66% false alarm rate and a 1.67% missed detection rate in line crossing detection with an average error of 1.22 seconds. We use two groups of receivers and experiment with three different transmitter locations in case of ZigBee. We obtain the above results by averaging over all transmitter location and receiver group pairs.

Note that, while computing the errors as compared to the ground truth, we consider the line connecting the centroid of transmitter antenna locations (or the transmitter location in case of ZigBee) and the centroid of the receiver antenna locations (or the centroid of the receiver locations in the group in case of ZigBee) as the representative link line.

5.1.2 Residential House

We present the detection accuracy of the Residential House experiment in Table 2. We achieve greater than 94% detection accuracy with a 0.043% false alarm rate while using WiFi receivers with normal antenna separation (WiFi_NORM). With larger antenna separation (WiFi_SEP) the accuracy is greater than 95% with a 0.005% false alarm rate. The mean error in detection of line crossings is $1.06s$ in case of WiFi_NORM, the same being $0.56s$ for WiFi_SEP.

For ZigBee, we achieve greater than 99% accuracy in detection with a false alarm rate of 0.004% only. The average error in time-of-crossing estimation in this case is 1.63 s. Note that during this experiment, we placed one group of ZigBee nodes (group 2) directly in front of the metal-plated entrance door. The packet reception rates for receivers in this group are much lower than the receivers in the other groups. Also, perhaps due to attenuation through the door, the RSS measurements made by this group are more noisy than those made by the other groups, leading to further degradation in performance. The missed detection rate for this group is almost 30%, about 60 times more than the

Table 1: Detection Accuracy (Hallway).

Hallway	Accuracy		Error (sec)		
Experiment:	FA%	MD%	Min	Max	Mean
WiFi_NORM	0	1.92	0.03	2.73	0.79
WiFi_SEP	0	0	0.27	2.37	1.22
ZigBee	0	1.02	0.27	2.37	1.22

Table 2: Detection Accuracy (House).

House	Accuracy		Error (sec)		
Experiment:	FA%	MD%	Min	Max	Mean
WiFi_NORM	0.043	5.70	0.29	2.78	1.06
WiFi_SEP	0.005	4.35	0.03	1.82	0.56
ZigBee	0.004	0.49	0.10	3.55	1.63

average missed detection rate of other groups (results presented in Table 2 are averaged over the other three groups). Thus, we conclude that, although an MRW attack can penetrate concrete and brick walls, metallic structures in the line of sight path of the radio signals degrades the detection accuracy significantly.

5.2 Determining Direction of Motion

In this section, we present the accuracy we achieve in detecting the direction of motion for each experiment.

5.2.1 University Hallway

In the university hallway experiment, the corridor was crossed by a moving person an equal number of times in either direction. We achieve 100% accuracy in detecting direction of movement on either side of the corridor while using two WiFi receivers or two groups of ZigBee nodes using the method described in Section 3.2.

We also achieve an accuracy as high as 90.38% in detecting direction of motion with only a single WiFi 802.11n receiver by increasing the spatial separation of the MIMO antennas. The accuracy with a single WiFi receiver with standard antenna separation is 59.62%, which is slightly better than guessing the direction of motion.

5.2.2 Residential House

For the experiment performed in the residential house we again achieve 100% accuracy in detection while using two WiFi receivers with standard antenna separation (experiment House 1) or two groups of ZigBee nodes on either side of the house. Individual detection accuracy of the two WiFi receivers (with standard antenna separation placed on the same side of the house as in experiment House 1) used are 100% (RX1) and 68% (RX2) respectively. Detection accuracy with spatially separated antennas for these receivers (when they are placed on opposite sides of the house as in experiment House 2) are 96% (RX1) and 52.6% (RX2) respectively. These results differ from the University Hallway experiment where we get better accuracy in detecting direction of movement while using large spatial separation between antennas as compared to using normal antenna separation. The degradation in accuracy with antenna separation in Residential House experiment may be due to the fact that during the House 2 experiment, walking speed of the person was about 20% faster as compared to the House 1 experiment with normal antenna separation, hence crossing times for individual antennas overlapped with each other in some cases.

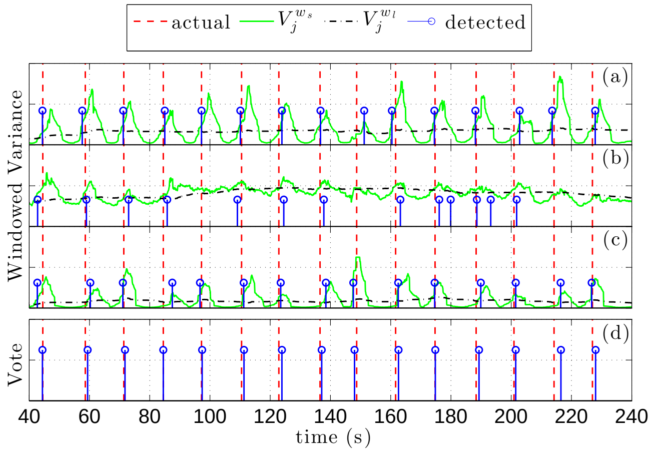
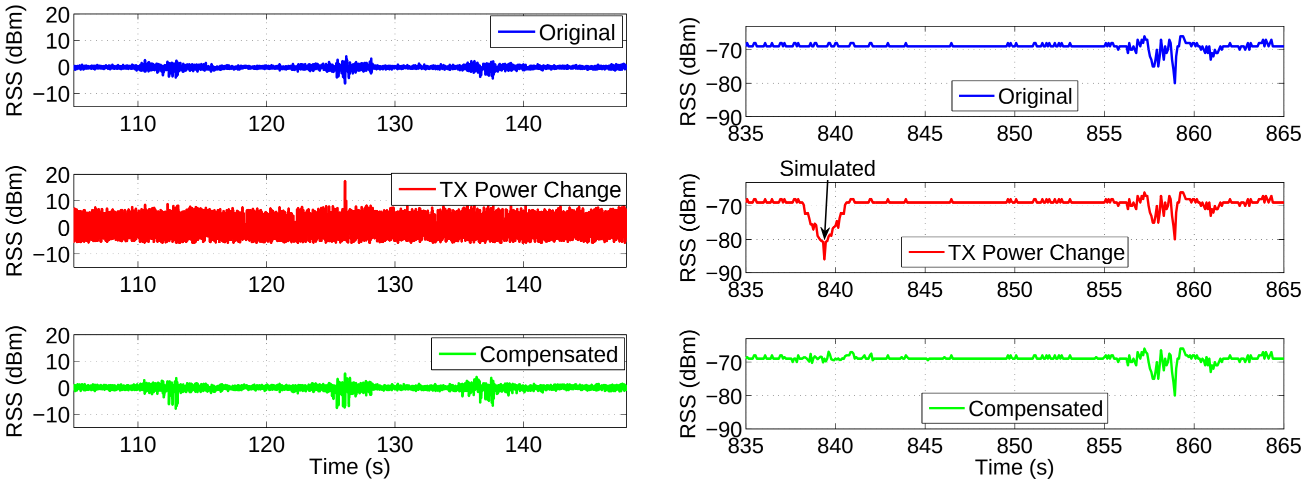


Figure 4: The majority vote over transmitter-receiver antenna pairs reduces false alarms and missed detections. (a),(b), and (c) show the results of the windowed variance based line crossing detection for three antenna pairs using Wifi. In (d), we see that the majority vote eliminates false alarms and missed detections.

To summarize, a MRW adversary should use two WiFi receivers or two groups of ZigBee nodes to detect direction of motion accurately. It is possible to achieve high accuracy even with a single WiFi receiver in some cases (e.g. RX1 in experiments House 1 and House 2), however the results depend on the environment and need further investigation.

5.3 Advantages of Majority Vote

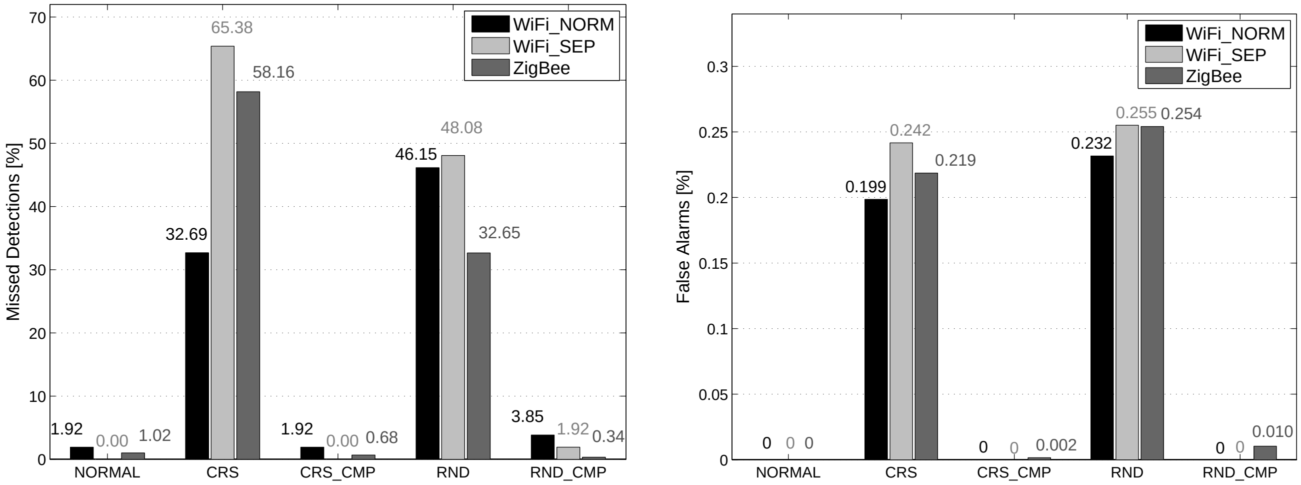
In this section, we show how our majority vote approach helps overcome inherent uncertainties in wireless links. All wireless links are not equally sensitive to motion occurring in their vicinity and the sensitivity varies with link fade level along with other factors. Since it is not possible for an adversary to know beforehand whether a link is good or bad for detecting LOS crossings, he relies on correlation among multiple closely located links and infers a line crossing only when majority of these closely located links indicates a crossing. In our experiments, $3 \times 3 = 9$ links between the MIMO transmitter-receiver antenna pairs are considered for majority vote in the WiFi case, and groups of 3 single-antenna receivers in the ZigBee case. Figure 4 shows one scenario where our majority vote algorithm helps get rid of some false alarms and missed detections due to one bad WiFi link (for clarity we show three out of the nine links) from the University Hallway experiment. As can be seen the link in Figure 4(b), fails to detect a line crossing that occurs around 100 s, however the other two links (Figure 4(a) & Figure 4(c)) detect the crossing and a majority vote among these three links detects the crossing at that time (Figure 4(d)). Similarly, we see that the link in Figure 4(b) flags a false alarm at 180 s but the other two links do not indicate any crossing. Hence again the majority vote gets rid of the false alarm at time 180 s (Figure 4(d)), thereby improving the overall accuracy of the system.



(a) TX_RANDOM (WiFi)

(b) TX_LINECROSS (ZigBee)

Figure 5: Measured CSI and RSS (top) without and (middle) with TX power change; and (bottom) after compensation.



(a) Missed Detections

(b) False Alarms

Figure 6: Compensation accuracy in the University Hallway Experiment.

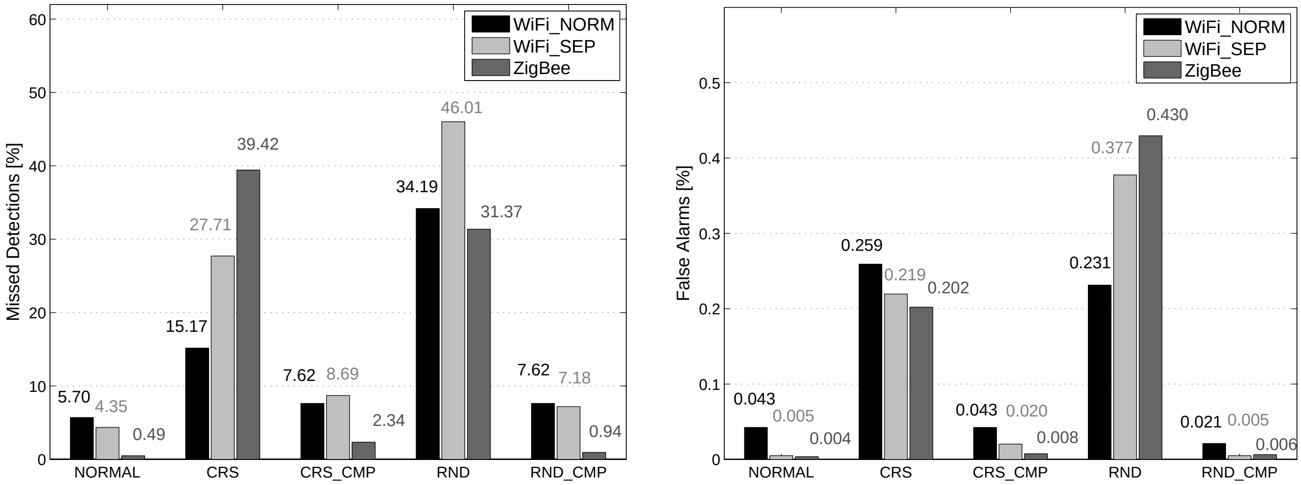


Figure 7: Compensation accuracy in the Residential House Experiment.

To summarize - a single wireless link suffices in some cases in detection of line crossings between a transmitter and a receiver, however the results are not always reliable due to inherent uncertainties in link sensitivity to object movements. We can improve accuracy and reliability by correlating detections across multiple co-located links using a majority vote approach.

5.4 Compensation for Transmit Power Change

In this section, we show how transmit power changes (random or strategic) affect line crossing detection accuracy and how our compensation method nullifies the effect of such power changes. Figure 5(a) shows the effect of random transmit power changes on line crossing detection for a WiFi link between a single transmitter-receiver antenna pair that is crossed three times by a moving person. The top figure corresponds to the case when there is no transmit power change. This figure clearly shows distinct short time periods of high variance in the CSI corresponding to the times when the person crosses the link. However, transmit power change masks these distinct short term variance regions and renders line crossing detection ineffective as can be seen in the figure in the middle. The bottom figure plots the CSI for the same link after compensating for the transmit power changes as described in Section 3.3. Clearly, our compensation method almost nullifies the masking effect of transmit power changes and the attacker can detect three line crossings (high short term variance region) from the compensated signal. Similarly, Figure 5(b) shows how strategic power changes can be used to simulate link line crossings, and how our compensation method eliminates these artificial variations. The top figure plots the RSS in dBm for a ZigBee link that is crossed during the time interval 856-860 s. The figure in the middle shows one additional line crossing (high variance region) introduced in the link by strategic transmit power changes during time interval 838-841 s. However, as seen from the bottom figure, our compensation method gets rid of the false alarm introduced by strategic power change and we can detect the original line crossing from the compensated signal.

In the Figure 6 we show false alarms and missed detections induced by transmit power changes and the accuracy of our compensation method in the University Hallway experiment. In the figure, NORMAL corresponds to the case when the transmitter transmits with fixed transmit power, CRS is when strategic power changes are introduced in the data using TX_LINECROSS simulation, CRS_CMP corresponds to the results when we apply our compensation method on TX_CRS. Similarly, RND shows results when the transmitter is changing its transmit power randomly with each transmission, while RND_CMP is the corresponding compensation results.

As an example, in the University Hallway experiment, a strategic transmit power change at the WiFi transmitter increases the missed detections rate from 1.92% to 32.69% and the false alarms rate from 0% to 0.199% when using a WiFi receiver with normal antenna separation. However, our compensation method gets rid of all the additional false alarms and missed detections. Similarly, random power changes for the ZigBee experiment increases the false alarms rate from 0% to 0.254%, but our compensation method brings it back to only 0.010%. We obtain similar results in the Residential House experiment (Figure 7). For example, for random power changes at the ZigBee transmitter, the missed detections rate increases to 31.37% from 0.94% and the false alarms rate increases to 0.429% from 0.003% but our compensation method brings down the missed detection and false alarm rates to only 0.94% and 0.006%, respectively.

To summarize our findings, transmit power changes (strategic or random) increase the false alarm and missed detection rates significantly. However, using our compensation method, an attacker can accurately estimate the transmit power change amplitude and compensate for the same to get rid of the adverse effect caused by such changes and, still sense people location and motion with high accuracy.

5.5 Detection with Varying Transmission Rate

ZigBee applications in modern facilities use different transmission rates for communication. To understand the effect of lower transmission rates on detection accuracy, we use the data from TX_NORMAL for both the University Hallway and Residential House experiment to simulate lower transmission rates. Note that the original transmission rate is approximately 12 Hz. We simulate three additional transmission rates - 6 Hz, 4 Hz and 2 Hz respectively from the original data. Figure 8 shows the results of our simulation. We find that the overall detection rates decrease with lower transmission rates. For the transmission rate of 6 transmissions/second, accuracy of the detector is over 98% for the University Hallway experiment and over 96% for the Residential House experiment. These results are similar to what we observe for original transmission frequency of 12 Hz. The accuracy is worst for transmission frequency of 2 Hz with the detection rate being as low as 71% for the Residential House experiment. For the transmission rate of 4Hz, the detection rate degrades to 87% in the University Hallway experiment, although it remains greater than 96% for the Residential House experiment. We do not see any noticeable change in the false alarm rates with varying transmission rate.

6. ADDITIONAL RELATED WORK

In recent years, device-free localization (DFL), in which people who are not carrying any radio transmitters are located by a static deployed network, has been the subject of intense research. Our MRW attack is significantly different from traditional DFL work in that the MRW attack is practical for large buildings, is stealthy because no transmitters are deployed by the attacker, and is immune from jamming. DFL systems such as the ones in [4, 11–13, 15, 24, 24, 25, 30] require dozens of radio transceivers deployed throughout or on many sides of the target area. Further, through-building DFL systems such as [25, 31] assume the transmitted signal penetrates through two external walls and any internal walls in between, and as such have been tested only in buildings of small (18 - 42 m^2) size. In this paper, we show access to one side is sufficient for an MRW attack, and it requires a signal from inside a building to penetrate only one external wall. Other fingerprint-based DFL systems [14, 19, 23, 27] require collection of training data with a person in each possible location in the environment. In our MRW attack, we do not assume that an attacker has prior access to the inside of the building to be able to perform such data collection. Further, to perform DFL, an attacker must deploy some nodes which transmit, exposing them to being detected and located by RF source localization, while an MRW attack is stealthier in that purely passive receivers are deployed by an attacker. Finally, DFL systems' signals could be interfered

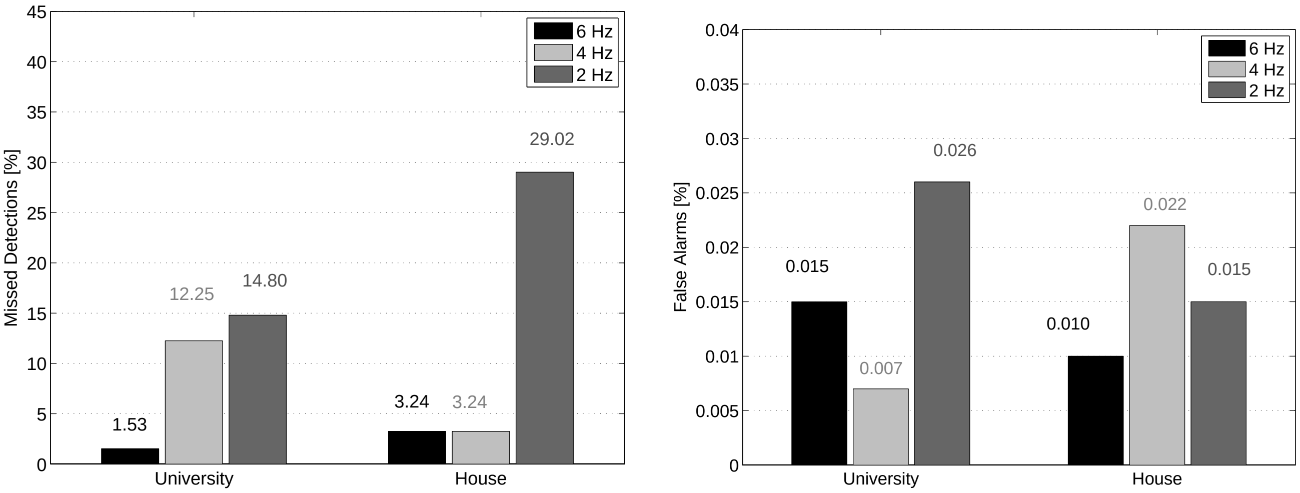


Figure 8: Detection accuracy with varying transmission rates (ZigBee).

with by a powerful jammer. In the method in this paper, any transmitter in the building, including a jammer, could be used as a source for MRW. The work in [5] presents a through-walls passive WiFi radar system. In it, a receiver is situated outside the target building and a Wi-Fi AP placed inside the building and having a narrow-beamwidth directional antenna is used as transmitter. The signal received by the passive radar detector is then used to create a range-Doppler surface and detect a moving target. Our work is complementary to [5], first, because we use different measurements. Doppler information in [5] is used to estimate relative velocity; in our work, received power or CSI is used to infer presence (even when stationary) on the link line. In theory, both could be used to improve localization accuracy. For example, while a person is crossing perpendicular to the link line, the cause no Doppler shift, but our system would detect their direction of motion. Second, we note that the receiver in [5] is a specialized radar receiver with a PC for intensive offline processing. In comparison, our system uses standard transceivers and requires little processing, and thus is suitable for real time monitoring by an adversary with only standard hardware. We demonstrate that, random or pre-defined transmit power change, used as a possible countermeasure, can not protect the privacy of the location of people inside the target area. To the best of our knowledge, no previous work on location privacy can function accurately in presence of purposeful transmit power changes.

Several existing works focusing on location privacy typically assume that the *victims* of the attack are carrying an actively communicating wireless device [3, 6–8, 10]. We focus on obtaining location information where the person being monitored does not actively participate in the detection process.

7. CONCLUSION

We investigated the ability of an attacker to surreptitiously use an otherwise secure wireless network to detect a moving person through walls. We designed and implemented an attack methodology, to passively obtain through wall person movement information, that reliably detects when a person crosses the link lines between the legitimate transmitters and the attack receivers by using physical layer measurements. We also developed a method to determine the direction of movement of a person from the sequence of link lines crossed during a short time interval. Additionally, we described how an attacker may estimate any artificial changes in transmit power (used as a countermeasure), compensate for these power changes using measurements from sufficient number of links, and still detect line crossings. We implemented our methodology on WiFi and ZigBee nodes and experimentally evaluated the MRW attack by monitoring people movements through walls in two real-world settings. We found that our methods achieve close to 100% accuracy in detecting line crossings and the direction of movement. The limitation of our proposed methodology is that it works for detecting movement of only a single person at a time. Future work must develop methodology for passively locating multiple people through walls in more dynamic environments.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant Nos. #0748206, #0855261, #1035565, and by the ARL MURI Grant #W911NF-07-0318. The many comments from our shepherd Dr. Di Ma and anonymous reviewers greatly improved the final version of the paper.

8. REFERENCES

[1] F. Adib, Z. Kabelac, D. Katabi, and R. C. Miller. 3d tracking via body radio reflections. In *Presented as part of the 11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14)*, Seattle, WA, 2014. USENIX.

[2] F. Adib and D. Katabi. See through walls with wifi! In *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*, pages 75–86. ACM, 2013.

[3] P. Bahl, V. N. Padmanabhan, and A. Balachandran. Enhancements to the radar user location and tracking system. Technical report, 2000.

[4] X. Chen, A. Edelstein, Y. Li, M. Coates, M. Rabbat, and M. Aidong. Sequential Monte Carlo for simultaneous passive device-free tracking and sensor localization using received signal strength measurements. In *ACM/IEEE Information Processing in Sensor Networks (IPSN)*, April 2011.

[5] K. Chetty, G. Smith, and K. Woodbridge. Through-the-wall sensing of personnel using passive bistatic wifi radar at standoff distances. *Geoscience and Remote Sensing, IEEE Transactions on*, 50(4):1218 –1226, april 2012.

[6] B. Danev, D. Zanetti, and S. Capkun. On physical-layer identification of wireless devices. *ACM Computer Survey*, 45(1):6:1–6:29, 2012.

[7] B. Greenstein, R. Gummadi, J. Pang, M. Y. Chen, T. Kohno, S. Seshan, and D. Wetherall. Can ferris bueller still have his day off? protecting privacy in the wireless era. In *Proceedings of the 11th USENIX workshop on Hot topics in operating systems*, HOTOS'07, pages 10:1–10:6, Berkeley, CA, USA, 2007. USENIX Association.

[8] M. Gruteser and D. Grunwald. Enhancing location privacy in wireless lan through disposable interface identifiers: a quantitative analysis. *Mob. Netw. Appl.*, 10(3):315–325, June 2005.

[9] D. Halperin, W. Hu, A. Sheth, and D. Wetherall. Tool release: gathering 802.11n traces with channel state information. *SIGCOMM Comput. Commun. Rev.*, 41(1):53–53, Jan. 2011.

[10] T. Jiang, H. J. Wang, and Y.-C. Hu. Preserving location privacy in wireless LANs. In *In Proceedings of 5th International Conference on Mobile Systems, Applications, and Services (MobiSys 2007*, pages 246–257. ACM Press, 2007.

[11] O. Kaltiokallio and M. Bocca. Real-time intrusion detection and tracking in indoor environment through distributed rssi processing. In *2011 IEEE 17th Intl. Conf. Embedded and Real-Time Computing Systems and Applications (RTCSA)*, volume 1, pages 61 –70, Aug. 2011.

[12] O. Kaltiokallio, M. Bocca, and N. Patwari. Follow @grandma: Long-term device-free localization for residential monitoring. In *Local Computer Networks Workshops (LCN Workshops), 2012 IEEE 37th Conference on*, pages 991 –998, oct. 2012.

[13] M. A. Kanso and M. G. Rabbat. Compressed RF tomography for wireless sensor networks: Centralized and decentralized approaches. In *5th IEEE Intl. Conf. on Distributed Computing in Sensor Systems (DCOSS-09)*, Marina Del Rey, CA, June 2009.

[14] A. E. Kosba, A. Saeed, and M. Youssef. Rasid: A robust WLAN device-free passive motion detection system. In *2012 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 180–189, 2012.

[15] R. K. Martin, C. Anderson, R. W. Thomas, and A. S. King. Modelling and analysis of radio tomography. In *CAMSAP*, pages 377–380, 2011.

[16] D. Niculescu and B. Nath. Ad hoc positioning system (aps) using aoa. In *INFOCOM*, volume 3, pages 1734–1743. IEEE, 2003.

[17] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan. The cricket location-support system. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 32–43. ACM, 2000.

[18] Q. Pu, S. Gupta, S. Gollakota, and S. Patel. Whole-home gesture recognition using wireless signals. In *Proceedings of the 19th annual international conference on Mobile computing & networking*, pages 27–38. ACM, 2013.

[19] M. Seifeldin, A. Saeed, A. Kosba, A. El-Keyi, and M. Youssef. Nuzzer: A large-scale device-free passive localization system for wireless environments. *Mobile Computing, IEEE Transactions on*, PP(99):1, 2012.

[20] W. C. Stone. Nist construction automation program report no. 3: Electromagnetic signal attenuation in construction materials. *Building Fire Res. Lab., Nat. Inst. Standards Technol., Gaithersburg, MD, Tech. Rep. NISTIR*, 6055, 1997.

[21] C. D. Taylor, S. J. Gutierrez, S. L. Langdon, K. L. Murphy, and W. A. Walton III. Measurement of RF propagation into concrete structures over the frequency range 100 MHz to 3 GHz. In *Wireless Personal Communications*, pages 131–144. Springer, 1997.

[22] Texas Instruments. A USB-enabled system-on-chip solution for 2.4 GHz IEEE 802.15.4 and ZigBee applications.

[23] F. Viani, P. Rocca, M. Benedetti, G. Oliveri, and A. Massa. Electromagnetic passive localization and tracking of moving targets in a WSN-infrastructured environment. *Inverse Problems*, 26:1–15, March 2010.

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

[25] J. Wilson and N. Patwari. See Through Walls: Motion Tracking Using Variance-Based Radio Tomography Networks. *IEEE TMC*, 2010.

[26] R. Wilson. Propagation losses through common building materials 2.4 GHz vs 5 GHz. Technical Report E10589, Magis Networks, Inc., August 2002.

[27] C. Xu, B. Firner, Y. Zhang, R. Howard, J. Li, and X. Lin. Improving RF-based device-free passive localization in cluttered indoor environments through probabilistic classification methods. In *IPSN*, pages 209–220, 2012.

[28] M. Youssef, M. Mah, and A. K. Agrawala. Challenges: device-free passive localization for wireless environments. In *MOBICOM*, pages 222–229, 2007.

[29] D. Zhang, J. Ma, Q. Chen, and L. M. Ni. Dynamic clustering for tracking multiple transceiver-free objects. In *IEEE PerCom'09*.

[30] D. Zhang, J. Ma, Q. Chen, and L. M. Ni. An RF-based system for tracking transceiver-free objects. In *Fifth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom-07)*, pages 135–144, 2007.

[31] Y. Zheng and A. Men. Through-wall tracking with radio tomography networks using foreground detection. In *IEEE WCNC*, pages 3278–3283, 2012.