Using Channel State Information for Tamper Detection in the Internet of Things

Ibrahim Ethem Bagci, Utz Roedig
School of Computing and Communications
Lancaster University
Lancaster, UK
{i.bagci, u.roedig}@lancaster.ac.uk

Ivan Martinovic
Computer Science Department
University of Oxford
Oxford, UK
ivan.martinovic@cs.ox.ac.uk

Matthias Schulz, Matthias Hollick
Secure Mobile Networking Lab
Technische Universität Darmstadt
Darmstadt, Germany
{mschulz, mhollick}@seemoo.tu-darmstadt.de

ABSTRACT

The Internet of Things (IoT) is increasingly used for critical applications and securing the IoT has become a major concern. Among other issues it is important to ensure that tampering with IoT devices is detected. Many IoT devices use WiFi for communication and Channel State Information (CSI) based tamper detection is a valid option. Each 802.11n WiFi frame contains a preamble which allows a receiver to estimate the impact of the wireless channel, the transmitter and the receiver on the signal. The estimation result - the CSI - is used by a receiver to extract the transmitted information. However, as the CSI depends on the communication environment and the transmitter hardware, it can be used as well for security purposes. If an attacker tampers with a transmitter it will have an effect on the CSI measured at a receiver. Unfortunately not only tamper events lead to CSI fluctuations; movement of people in the communication environment has an impact too. We propose to analyse CSI values of a transmission simultaneously at multiple receivers to improve distinction of tamper and movement events. A moving person is expected to have an impact on some but not all communication links between transmitter and the receivers. A tamper event impacts on all links between transmitter and the receivers. The paper describes the necessary algorithms for the proposed tamper detection method. In particular we analyse the tamper detection capability in practical deployments with varying intensity of people movement. In our experiments the proposed system deployed in a busy office environment was capable to detect 53% of tamper events ($TPR = 53\%$) while creating zero false alarms ($FPR = 0\%$).

Categories and Subject Descriptors

C.2.3 [**Computer-Communication Networks**]: Network Operations—*Network Monitoring*

Keywords

Tamper Detection; 802.11n; Wireless; Security; PHY; OFDM; Channel State Information

1. INTRODUCTION

A large number of IoT systems are using WiFi as a means of communication [2]. Many of these systems require a high level of security. An example is a surveillance system using WiFi based cameras integrated with antennas to monitor critical infrastructures such as an airport or power plant. Traditional cryptographic operations can be used to authenticate data transmitted from the camera devices. However, tampering with a device (e.g. movement or change of viewpoint) cannot be detected using cryptographic methods. Using CSI analysis of transmitted data from camera devices would allow us to introduce an additional layer of defence which can detect these tamper events. CSI based tamper detection is a valuable security building block for critical systems using wireless communication. In addition, CSI values can be extracted from existing transmissions and the overhead for implementing CSI based tamper detection is low.

Each 802.11n WiFi frame contains a preamble which allows a receiver to estimate the impact of the wireless channel and of the transmitter on the received signal. Amplitude changes and phase shifts of several subcarriers used to transmit the signal are estimated at the receiver using the preamble information. The resulting CSI is used by a receiver to extract successfully the transmitted information. However, as the CSI depends on the communication environment and the transmitter hardware, it can also be used for security purposes. If an attacker tampers with a transmitter, either by replacing the device or by moving it, it will have an effect on the CSI measured at a receiver.

Unfortunately, not only tamper events lead to CSI fluctuations, modifications of the communication environment have an impact too. In particular, movement of people in the communication environment has a noticeable influence on the CSI. In our previous work [1] we have been shown that tamper detection based on CSI analysis is generally possible but that it is hard to distinguish tamper events from natural changes in the communication environment. Thus, it is difficult to construct a practical security system based on CSI analysis as a high number of false positives and a low number of true positives are detected. Figure 1 illustrates this

challenge. The changing CSI amplitude value over time for just one subcarrier is shown. As can be seen, tamper events and environmental changes (in this case a person walking between sender and receiver) manifest in very similar ways.

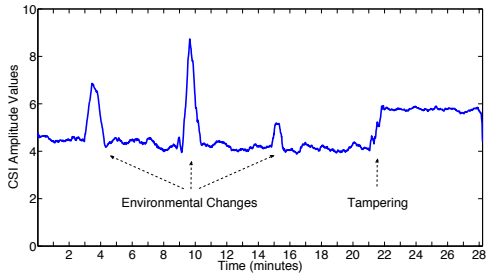


Figure 1: Effects of environmental changes and tampering on CSI amplitude values of the 9^{th} subcarrier of the 2^{nd} antenna. Environmental changes and tamper events have a similar effect on CSI amplitude values.

To address this problem we propose to analyse CSI values from a single transmission simultaneously at multiple receivers to improve distinction of tamper and movement events. A moving person is expected to have an impact on some but not all communication links while a tamper event is noticeable at all receivers. In this paper we describe the necessary algorithms for the proposed CSI tamper detection method using multiple receivers. In particular we analyse the tamper detection capability in practical deployments with varying intensity of people movement. Specific contributions of this paper are:

- *Multi-Receiver CSI Tamper Detection:* We describe CSI algorithms for tamper detection using multiple receivers.
- *Tamper Detection Evaluation:* We analyse the tamper detection capability of the proposed method using realistic deployment environments. We describe system capability in these environments in terms of achievable False Positive Rate (FPR) and True Positive Rate (TPR).
- *Tamper Detection Implementation:* We describe how the proposed algorithms can be put to action in practical deployments. We discuss their application in the future IoT.

In our experiments the proposed system deployed in a busy office environment was capable to detect 53% of tamper events ($TPR = 53\%$) while creating zero false alarms ($FPR = 0\%$).

The paper is organized as follows. The next section describes the threat model. Section 3 discusses related work. Section 4 describes the algorithms used for multi-receiver CSI tamper detection. In Section 5.1 the system capability is analysed in a controlled environment where people move within the setup in a known and controlled way. In Section 5.2 the system capability is analysed in an uncontrolled, more challenging environment. An office setup is used in which people move freely throughout the day; during daytime a lot of movement is present while at night the environment is more quiet and less movement occurs. In Section 6 we discuss how the proposed mechanisms can be put to work within real IoT applications. Section 7 concludes the paper.

2. THREAT MODEL

In this paper we are considering an attacker who is capable of physically tampering with a device. We assume that the attacker is able to move or rotate the device. Our aim is to detect such device movements with a high detection reliability and a low false alarm rate.

In this work we do not consider physical tampering with internal components of the device. We do not aim to detect replacement of device components such as the microcontroller. Additionally, we do not assume the attacker is able to change the software running on the device. To protect against internal device tampering other protection methods than the one discussed in this paper have to be used.

An example application scenario for which the tamper detection method described in this paper is useful is a wireless surveillance system where WiFi enabled cameras integrated with antennas are deployed to monitor an area. An attacker would aim to prevent observation of a particular section (i.e. to pass undetected through the observed area). This can be achieved by moving the device to alter the camera's view. This kind of attack cannot be detected by using conventional security protocols. Our proposed system aims to detect these tampering attacks. Obviously a low false positive rate is necessary for such a system as any alarm would require unnecessary investigation of the camera system. On the other hand, high true positive rates are desirable to ensure reliable tampering detection.

3. RELATED WORK

PHY-layer information has been used to secure wireless networks in many ways. The application areas that are related to our work are transmitter location distinction and transmitter identification, which can ultimately be used for transmitter tamper detection.

Transmitter location distinction aims to determine transmitter location changes by using the received signal characteristics. Channel Frequency Response (CFR) [11] and Channel Impulse Response (CIR) [13, 17] are used in Direct Sequence Spread Spectrum (DSSS) modulated networks, and recently CSI [1] is used in Orthogonal Frequency Division Multiplexing (OFDM) modulated networks. DSSS modulation is of no importance for WiFi systems any more, and 802.11n fully adapts OFDM modulation. The work by Bagci et al. [1] is the closest to ours in terms of source of PHY-layer information, encoding methods and test devices. The work shows that transmitter location distinction based on CSI is possible for OFDM networks in static deployment environments. Their work also shows that natural changes in the communication environment make it hard to distinguish actual location changes and that these changes cause false alarms. In practical deployments, natural changes in the communication environment are unavoidable. We propose to use multiple receivers to improve the location distinction for CSI based detection systems in practical deployments.

Transmitter identification uses received signal characteristics to identify the transmitter device or the class of the device. Modulation errors caused by modulator circuitry are used in [3] to identify 802.11 devices. Ureten et al. [15]

and Danev et al. [4] use the transient part of the RF signal to identify 802.11 and 802.15.4 devices, respectively. RFID transponders are identified by using RF burst information in [5]. WiFi stations are identified by using the angle-of-arrival information of incoming signals in [16]. Most recently, CSI is used to identify 802.11n devices in [1]. More comprehensive information about transmitter identification based on PHY-layer information can be found in [6].

Another usage of PHY-layer information in security is detecting spoofing attacks. A source-authentication method to detect spoofing attacks on 802.11n management frames (MFs) by using CSI is proposed by Jiang et al. [10]. The work uses CSI for the source of information as we do in our work, however it is not aimed at tamper detection. They show that amplitude of CSI changes in injected frames. Received Signal Strength (RSS) information is also used to detect spoofing attacks in [7]. Here, RSS is used to create *signalprints* to detect identity-based attacks.

In summary, our work differs from the existing work in three ways: (i) In contrast to existing work, we analyze multiple and more complex tampering scenarios. (ii) Most other tamper detection systems are not designed for 802.11n OFDM. (iii) Existing tamper detection systems do not work in practical deployments as they do not address properly the separation of environmental and tamper events.

4. CSI TAMPER DETECTION

As thoroughly described in [9], CSI information in 802.11n systems is extracted from the HT-LTF preamble that consists of training symbols on each OFDM subcarrier. These symbols are known by both the transmitters and the receivers. The received preamble differs from the transmitted one due to the effects of the wireless channels and the pre-filtering at the transmitter, as well as, the effects of the transmitter's and receivers' hardware. To extract the transmitted data streams at the receiver, the previously described effects on the preamble need to be inversely applied to the data parts of the wireless frames, as each subcarrier in an OFDM system can be represented as a linear combination of the described effects. Similar to previous work [1], we use the CSI information that is extracted on every frame reception as tamper evidence. The main challenge of our work is to cope with tamper unrelated events such as moving people that change the wireless channel which influences the CSI. In an optimal case, our system should detect all tampering events without being disturbed by other environmental changes.

4.1 Beamforming and Spatial Expansion

As mentioned above, the data transmission on each subcarrier sc can be described by a linear system. According to [1], we use $T_1^{sc} \dots T_T^{sc}$ to describe the signals sent by the transmitter's antennas on each subcarrier and $R_1^{sc} \dots R_R^{sc}$ as the corresponding received signals. Together with the channel coefficient matrix $\mathbf{H}_{R\times T}^{sc}$ containing the CSI values between each pair of transmit and receive antennas, the following linear system can be formulated:

$$\mathbf{R}^{sc} = \mathbf{H}_{R\times T}^{sc}\mathbf{T}^{sc}$$

Instead of directly transmitting one data stream per antenna, the transmitter can decide to use transmit filters to either cancel channel effects (beamforming) or to distribute a lower number of data streams to a higher number of antennas (spatial expanding). To perform the filtering operation, the transmitter uses filtering matrices $\mathbf{F}_{T\times S}^{sc}$ to distribute S spatial streams to T transmit antennas:

$$\mathbf{T}^{sc} = \mathbf{F}_{T\times S}^{sc}\mathbf{S}^{sc}$$

To extract the data streams $\mathbf{S}^{sc}$, the receivers need to invert the linear combination $\mathbf{M}_{R\times S}^{sc}$ of $\mathbf{H}_{R\times T}^{sc}$ and $\mathbf{F}_{T\times S}^{sc}$. To simplify the receiver, the preamble to estimate the CSI is also passed through the filter $\mathbf{F}_{T\times S}^{sc}$, so that the receiver always estimates $\mathbf{M}_{R\times S}^{sc}$.

If the transmitter sends the packets in broadcast mode (i.e., receiver agnostic) it only uses one spatial stream. In this work, we assume this mode of operation; nodes transmit periodic broadcast beacons which can be picked up by multiple receivers for CSI based tamper detection.

4.2 Basic Tamper Detection

As transmitters send their packets in broadcast mode only one spatial stream is used ($S = 1$). Therefore, we simplify the representation of the CSI matrices and use $\mathbf{M}_R^{sc}$ in the remainder of the paper.

In the tamper detection algorithm, receivers collect and store τ CSI measurements $\mathbf{M}_{R,i\in 1\dots\tau}^{sc}$. These CSI measurements are collected while the transmitter is in a tamper free state and will be used for comparison with newly received CSI measurements $\mathbf{M}_{R,i>\tau}^{sc}$. A distance metric is used as existing works show that such algorithms work well in this context (see related work [1, 13, 17] as discussed in the previous section). If the distance is above a certain threshold, the algorithm decides there is a tamper event and triggers an alarm.

We consider three distance algorthims: (i) *Euclidean distance*, (ii) *Mahalanobis distance* and (iii) *Earth Mover's distance*. The Euclidean distance gives the distance between two points; in our case the distance of two CSI vectors. Mahalonobis distance gives the distance between a point and a distribution, in our case the distance of a new CSI vector and a distribution of τ CSI vectors. And lastly, Earth Mover's distance gives the distance between two distributions, in our case the distance of the distribution of two CSI vectors.

The algorithm uses only the amplitude information of a CSI measurement and omits the phase information. The amplitude information is normalized by taking the Euclidean norm of all values in dimensions sc and r. Euclidean distance D_i is obtained by calculating the Euclidean distance between the stored τ CSI measurements and a new CSI measurement $\mathbf{M}_{R,i}^{sc}$.

$$D_i = \frac{1}{\tau}\sum_{j=1}^{\tau}\sqrt{\sum_{r=1}^{R}\sum_{sc=1}^{SC}\left(\frac{|M_{r,i}^{sc}|}{||M_{r,i}^{sc}||_2^{sc,r}} - \frac{|M_{r,j}^{sc}|}{||M_{r,j}^{sc}||_2^{sc,r}}\right)^2}$$

Similarly, we omit the phase information in $\mathbf{M}_{R,i}^{sc}$ and use normalized amplitude information when computing Mahalanobis and Earth Mover's distance. We omit the details of Mahalanobis and Earth Mover's distance algorithms here as they are well documented in the literature [12, 14]. We show in the evaluation Section 5.1 that the simplest distance computation method (Euclidean distance) is sufficient and that the more sophisticated methods of Mahalanobis and Earth Mover do not provide significantly better results.

To decide if tampering occurred, we need to set a threshold γ. If D_i is greater than γ the algorithm will detect tam-

pering ($q_i = 1$), and otherwise a tamper free state ($q_i = 0$) is assumed:

$$q_i = \begin{cases} 0 & \text{if } D_i < \gamma \\ 1 & \text{if } D_i \geq \gamma \end{cases}$$

4.3 Multi-Receiver Tamper Detection

When using one link (one receiver) to evaluate tampering it is not possible to distinguish tamper situations and environmental changes. Both events can push the distance value above the threshold. We will demonstrate this effect in Section 5.1. To overcome this limitation we aim to use multiple receivers for CSI analysis. The assumption is that a tamper event will push the distance observed at all receivers above the set threshold while a change in the environment will not result in a sufficiently significant distance change at all receivers. We decided against an approach where a majority vote is used (i.e. the distance is above the threshold at the majority of receivers to declare tampering). Tampering with the transmitter device clearly must influence all links and not just some.

Formally the overall tampering decision Q^i with q_i^n being the tampering decision at the individual receivers for a new received frame is:

$$Q^i = \begin{cases} 0 & \text{if } \sum_{n=1}^{N} q_i^n < N \\ 1 & \text{if } \sum_{n=1}^{N} q_i^n = N \end{cases}$$

Where N is the number of receivers. Here, the packet i must be received by all the receivers for a decision to be made. This situation can occur in practice as the transmitted beacon used for tamper detection may not be received at all stations.

4.4 Threshold Selection

The performance of the tamper detection largely depends on the selected threshold γ. If the threshold is selected too high some tamper events might be missed. If the threshold is too low the system is too sensitive and a large number of false detections may occur. In this work we consider 3 methods for threshold selection: (i) *Maximum Distance*, (ii) *Equal Error Rate* and (iii) *Zero False Negative*.

A simple and straightforward approach is to use the maximum distance of all captured CSIs during the training phase $\mathbf{M}^{sc}_{R\times S, i\in 1\ldots\tau}$ as the threshold:

$$D^{\tau}_{i,j} = \sqrt{\sum_{r=1}^{R}\sum_{sc=1}^{SC}\left(\frac{|M^{sc}_{r,s,i}|}{||M^{sc}_{r,s,i}||_2^{sc,r}} - \frac{|M^{sc}_{r,s,j}|}{||M^{sc}_{r,s,j}||_2^{sc,r}}\right)^2}$$

$$\max(D^{\tau}) = \max_{\forall i,j}\left(D^{\tau}_{i,j}\right)$$

This threshold works well when the environment is static as we will show. However, the algorithm doesn't provide good performance in terms of false alarms when the environment is dynamic.

We use False Positive Rate (FPR), False Negative Rate (FNR) and True Positive Rate (TPR) metrics to assess the detection mechanism. False Positive (FP) occurs when the algorithm falsely decides there is tampering but actually there is not, False Negative (FN) occurs when the algorithm misses a true tampering, and True Positive (TP) occurs when the algorithm catches a tamper situation. We can create a Receiver Operating Characteristic (ROC) curve by evaluating all possible thresholds. A ROC curve displays the trade-off between FPR and TPR for a given system. A balanced threshold can be found for a system by looking at the Equal Error Rate (EER). EER is the point where FPR equals FNR on the ROC curve.

CSI data collected during a training phase can be used to calculate a ROC. The threshold that gives the EER on the ROC curve, γ_{EER}, can be used as a threshold. This threshold gives a balanced result in terms of FPRs and TPRs. However, as we will show in Section 5.2.2, γ_{EER} is often too high. It gives very good FPR results, but at the same time it causes very low TPRs. We thus need to decrease the threshold, and to this end we propose to pick the maximum threshold where the ROC curve gives FNR $= 0$, $\gamma_{FNR=0}$. We will show in Section 5.2.2 that this threshold gives fair TPRs and, unfortunately, provides FPR > 0. We propose to apply time-wise filtering to the overall decision to address this issue which we detail next.

4.5 Time-Wise Filtering

We apply a time-wise moving average filter to the overall decision Q^i to reduce the FPRs. We consider the points t_i—when a packet i was received by all the receivers—and make a decision over a window t_w. The overall time-wise filtered decision Q^{i,t_w} is considered tampered if all individual decisions in the window t_w were tampered:

$$Q^{i,t_w} = \begin{cases} 0 & \text{if } \sum_{\substack{j \\ t_j\in(t_i-t_w,t_i)}} Q^j < \text{count}(t_j) \\ 1 & \text{if } \sum_{\substack{j \\ t_j\in(t_i-t_w,t_i)}} Q^j = \text{count}(t_j) \end{cases}$$

Note that although time-wise filtering helps to reduce the FPRs, it will also reduce the TPRs. This is a trade-off that needs to be considered. Also, before a decision can be made, data points covering a full window must be collected. This increases the time until a decision can be made (tamper detection is delayed).

5. EVALUATION

We start our evaluation with a controlled movement experiment. In this experiment only one person is present and movement of the person in the deployment area is known. This experiment is used to analyse how distance values extracted from the CSI are affected by movement. Furthermore, the experiment shows that the use of multiple receivers is an effective measure for distinguishing movement and tamper events.

Thereafter an experiment with uncontrolled movement is carried out. Nodes are deployed in an office environment in which office workers move around during the day. At night there is less activity but occasionally people are present. In this experiment we do not record the number of people or their movements. The purpose of this experiment is to see how different configurations of the tamper detection algorithm handle realistic environments with different levels of activity. We use this experiment as well to evaluate several different tamper situations to see how likely different tamper

Figure 2: A laptop and an antenna used in the experiments. Only the antenna is tampered (moved or rotated) during the experiments.

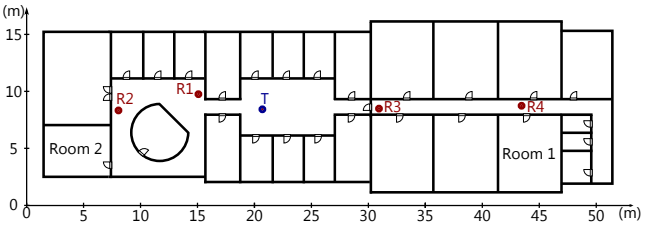


Figure 3: Controlled movement experiment layout. Receivers are shown as R1-4, and transmitter is shown as T. The environment is static during the experiment. A person is walking occasionally or waiting in Room 1 or Room 2.

situations are to be detected.

We use off-the-shelf Toshiba NB250-108 laptops equipped with an Intel 5300 network interface card (NIC) for our experiments. The laptops run Ubuntu 14.04 LTS with the 3.5.7 kernel. We use the Linux 802.11n CSI Tool [8] to extract CSI from the Intel 5300 NICs. Each NIC is equipped with a triple TP-Link TL-ANT2403N 802.11n omni-directional antenna. Figure 2 shows one of the laptops with antenna. To induce tampering the antenna is moved or rotated.

5.1 Controlled Movement

We use 4 receivers and one transmitter deployed in an office building as shown in Figure 3. The transmitter sends broadcast beacons at the rate of 1 packet/second. All receivers listen for these packets and extract the CSI from incoming packets.

A history size of $\tau = 100$ CSI readings is required before receivers calculate distance values. Figure 4 shows as an example how the CSI amplitude values develop over time. Values as received by the 2^{nd} antenna of Receiver 3 are shown; similar data is available for the other 2 antennas. The x-axis shows the time in minutes, and the y-axis shows the amplitude at each OFDM subcarrier. It can be seen that amplitude values change occasionally due to movement of a person until tampering happens at time $t = 21.5$ min which is clearly visible. We detail movement patterns and tampering events in the next paragraphs.

Figures 5, 6, and 7 show the distance value development over time at all 4 receivers using Euclidean, Mahalanobis, and Earth Mover's distance algorithms. We show the Maximum Distance threshold $\max(D^\tau)$ in the figures. Figure 8 shows the resulting tamper detection decision q_i considering each receiver individually when using the Euclidean distance (We do not show the result for Mahalanobis, and Earth Mover as these are very similar). The overall tamper decision Q^i considering all 4 receivers combined is shown in Figure 9 for Euclidean, Mahalanobis, and Earth Mover's distance algorithms. The tamper event at $t = 21.5$ min is clearly identified; movement events before this time do not lead to a tampering report.

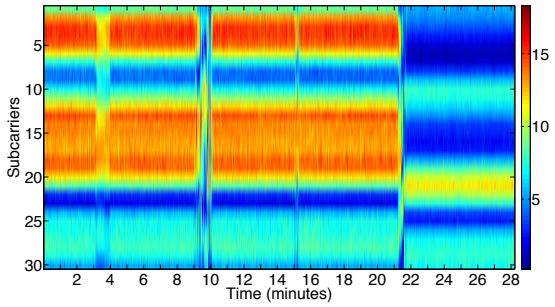
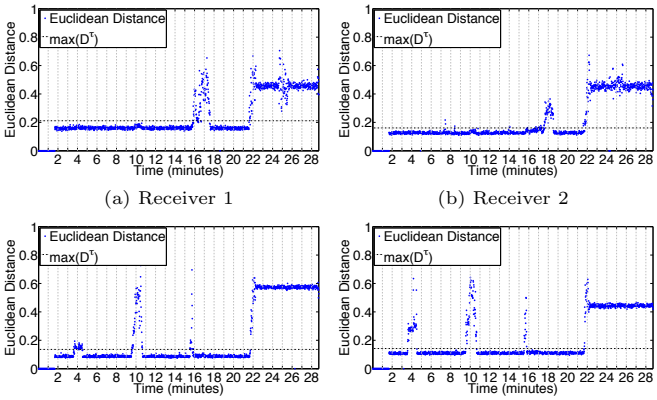


Figure 4: CSI amplitude values of 2^{nd} antenna of Receiver 3 during the controlled movement experiment. Amplitude values change occasionally due to movement until a tamper event at time $t = 21.5$ min.



(a) Receiver 1 (b) Receiver 2

(c) Receiver 3 (d) Receiver 4

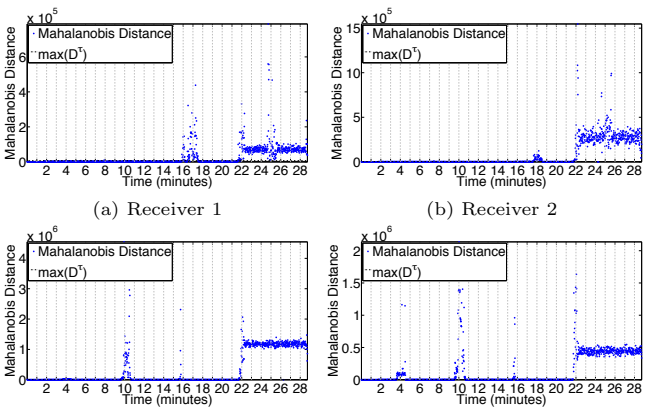
Figure 5: Euclidean distance in the controlled movement experiment. Tampering is induced at $t = 21.5$ min. Distance values at each receiver increase occasionally until this time due to movement.

All the receivers start to report distance values after 100 seconds. At the beginning of the experiment, a person is waiting in Room 1.

At time $t = 3.5$ min, the person walks close to Receiver 4, waits next to Receiver 4 for a minute, and then enters Room 1. We can see in the figures that this affects distance values at Receiver 4 and very slightly at Receiver 3. Since we do not see any increase on distance values of Receiver 1 and Receiver 2, the system will not create a false alarm when considering data from all receivers.

At time $t = 9.5$ min, the person walks very close to Receiver 3, waits next to Receiver 3 for a minute, and then enters Room 1. This affects the distance values of Receiver 3 and Receiver 4. Again, there is no significant change on the distance values of Receiver 1 and Receiver 2.

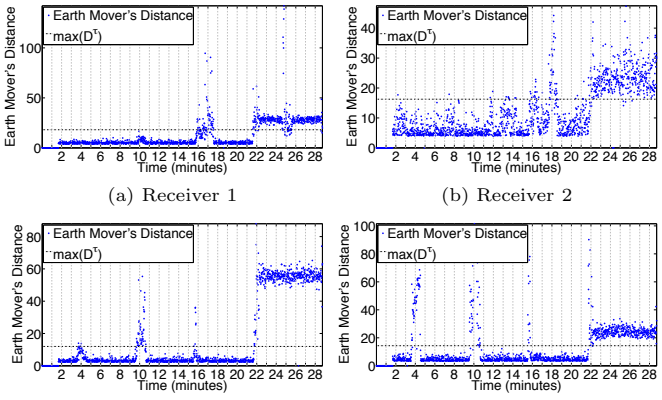
At time $t = 15.5$ min, the person walks very close to Receiver 1, waits next to Receiver 1 for two minutes, then moves to Receiver 2 at time $t = 17.5$ min and waits next to Receiver 2 for a minute, and finally enters Room 2. We



(a) Receiver 1 (b) Receiver 2

(c) Receiver 3 (d) Receiver 4

Figure 6: Mahalanobis distance in the controlled movement experiment. Tampering is induced at $t = 21.5$ min. Distance values at each receiver increase occasionally until this time due to movement.



(a) Receiver 1 (b) Receiver 2

(c) Receiver 3 (d) Receiver 4

Figure 7: Earth Mover's distance in the controlled movement experiment. Tampering is induced at $t = 21.5$ min. Distance values at each receiver increase occasionally until this time due to movement.

can see from the figures that distance values increase for Receiver 3 and Receiver 4 at time $t = 15.5$ min. This is because the person needs to pass by Receiver 3 and Receiver 4 to go to Receiver 1. Distance values for Receiver 3 and Receiver 4 go back to normal as distance values for Receiver 1 increase. The system does not create a false alarm when considering all receivers together as it does not see distance value increases above the threshold at all receivers at the same time.

At time $t = 21.5$ min, the person rotates the antenna of the transmitter 90° clockwise, and enters Room 2. Now the system creates an alarm, since distance values of all the receivers increase.

At time $t = 24.5$ min, the person walks very close to Receiver 1, waits next to Receiver 1 for a minute, and enters Room 2. Distance values of Receiver 1 and Receiver 2 slightly change during this period but remain above the threshold. Thus, the tamper situation remains. The experiment terminates around time $t = 28.5$ min.

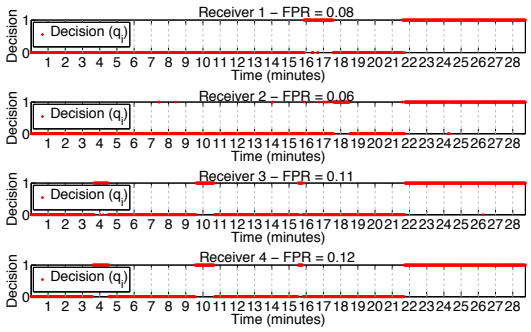


Figure 8: Tamper decisions (q_i) for each individual receiver in the controlled movement experiment using Euclidean distance and max(D^τ) as threshold. False alarms due to movement are present before the tampering event at $t = 21.5$ min.

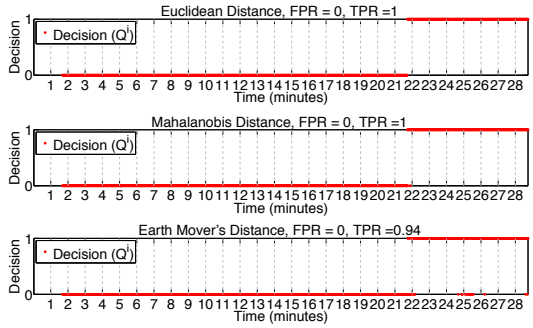


Figure 9: Multi-receiver tamper decisions (Q^i) for the controlled movement experiment. All receivers are taken into account and max(D^τ) is used as threshold. False alarms are avoided (FPR = 0) while the tamper event is correctly identified (For Euclidean and Mahalanobis distance algorithms with TPR = 1 and for the Earth Mover's distance algorithm with TPR = 0.94).

Figure 8 shows decisions q_i for each receiver (considering individual receiver results) when using Euclidean distance algorithm and max(D^τ) as the threshold. The x-axis shows the time in minutes, and y-axis shows the decisions. Decision 0 means there is no tampering, and decision 1 means there is tampering.

From Figure 8 we can see that false alarms exist when considering individual receivers. FPRs are 0.08, 0.06, 0.11, and 0.12 for Receivers 1, 2, 3, and 4, respectively.

However, from Figure 9 we can see that multi-receiver tamper detection provides the desired results. All the distance algorithms provide FPR = 0 result. Both Euclidean and Mahalanobis distance algorithms have a TPR = 1, however, the Earth Mover's distance algorithm provides only TPR = 0.94.

Euclidean, Mahalanobis, and Earth Mover's distance algorithms perform very similarly. This is somewhat surprising as they operate quite differently and one would have expected that more complex distance algorithms capturing more information would provide better results.

5.2 Uncontrolled Movement

The uncontrolled movement experiment is carried out in the same environment as the controlled movement experiment. However, the transmitter and the 4 receivers are

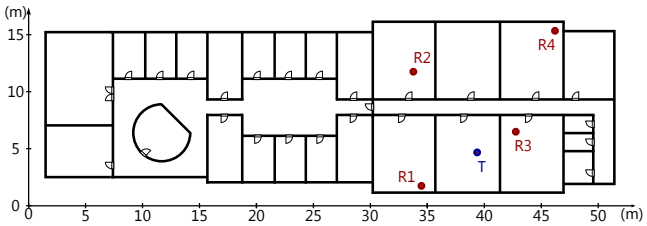


Figure 10: Uncontrolled movement experiment layout. People are moving in the rooms and in the corridor inducing CSI variations.

Day				Night			
Time	**Type**	**Time**	**Type**	**Time**	**Type**	**Time**	**Type**
12:00	90° cw	12:10	180° cw	20:00	90° cw	20:10	180° cw
12:20	270° cw	12:30	360°(0°) cw	20:20	270° cw	20:30	360°(0°) cw
12:40	1 cm up	12:50	1 cm right	20:40	1 cm up	20:50	1 cm right
13:00	1 cm down	13:10	1 cm left	21:00	1 cm down	21:10	1 cm left
13:20	2 cm up	13:30	2 cm right	21:20	2 cm up	21:30	2 cm right
13:40	2 cm down	13:50	2 cm left	21:40	2 cm down	21:50	2 cm left
14:00	3 cm up	14:10	3 cm right	22:00	3 cm up	22:10	3 cm right
14:20	3 cm down	14:30	3 cm left	22:20	3 cm down	22:30	3 cm left
14:40	4 cm up	14:50	4 cm right	22:40	4 cm up	22:50	4 cm right
15:00	4 cm down	15:10	4 cm left	23:00	4 cm down	23:10	4 cm left
15:20	4 cm up	15:30	5 cm right	23:20	4 cm up	23:30	5 cm right
15:40	5 cm down	15:50	5 cm left	23:40	5 cm down	23:50	5 cm left
16:00	30 cm left	16:10	60 cm left	00:00	30 cm left	00:10	60 cm left
16:20	Original			00:20	Original		

Table 1: The different tamper events and their times.

located in different rooms as shown in Figure 10. People use the offices and corridors and may also move chairs and other objects. Movement events of people and objects may lead to false tamper detection which we aim to avoid. The transmitter sends broadcast beacons for tamper detection at the rate of 1 packet/second.

The experiment starts while the transmitter is in a tampered state. The transmitter antenna is rotated by 90° anticlockwise from its intended position. After a while the antenna is rotated to its intended position, i.e., it is transited to the untampered state. In both states (tampered and untampered) data for threshold selection as described in Section 4.4) is collected. A history size of $\tau = 100$ CSI data is also collected during the untampered state when we can ensure that the environment is free of movement. Then, the setup is left for a long time in an untampered state. Then different tamper states are induced during day time and later as well at night. The Euclidean distance metric is used for evaluation. Figure 11 shows this distance value over time for all 4 receivers.

The experiment starts at 18:00 on 18th of May when the antenna of the transmitter is rotated 90° anticlockwise from its intended position. The antenna is rotated to its intended position at 12:06 on 19th of May. Several tamper situations are induced from 12:00 until 16:20 on May 20th (see Table 1 for details). To compare tamper detection in busy and more quiet periods, the same tamper events are applied again starting 20:00 on May 20th. Training CSI values are collected at 01:00 on May 20th (shown as vertical black line in Figure 11). Maximum distance values within the training data are also shown in the figure as $\max(D^\tau)$. The distance values of the packets not received by a receiver are shown as 0 in Figure 11. Tamper events are shown in Figure 11 with vertical dashed lines at their corresponding times.

FPR		TPR	
Night time (01:02 - 08:00)	0	Night time (20:00 - 00:30)	0.999
Day time (08:00 - 12:00)	0.831	Day time (12:00 - 16:00)	0.966
Overall (01:02 - 12:00)	0.769		

Table 2: FPRs and TPRs when using $\max(D^\tau)$ as the threshold.

Tampered state	18:00 18th of May - 12:06 19th of May
Untampered state	12:06 19th of May - 01:00 20th of May

Table 3: Time ranges of tampered and untampered states for ROC calculation.

Receiver 1	Receiver 2	Receiver 3	Receiver 4
0.032	0.148	0.036	0.258

Table 4: EERs for all the receivers in the uncontrolled movement experiment.

5.2.1 *Maximum Distance Threshold*

Figure 11 shows that distance values are above $\max(D^\tau)$ during office hours when there is no tampering. In a busy environment, $\max(D^\tau)$ is too sensitive and a high FPR is the consequence. Using $\max(D^\tau)$ as the threshold results in FPRs and TPRs as shown in Table 2 considering the overall decisions Q^i. FPR results are divided into three time regions: (i) Night time between 01:02 and 08:00 when the experiment environment is less dynamic, (ii) Day time between 08:00 and 12:00 when the experiment environment is dynamic, and (ii) Overall (day and night combined). TPR results are also divided into two time regions: (i) Night time between 20:00 and 00:30 when the experiment environment is less dynamic, (ii) Day time between 12:00 and 16:00 when the experiment environment is dynamic. TPRs from different tamper events are averaged resulting in a single TPR value (We will analyse TPR of individual tamper states later). Although we obtain a high TPR for both time durations and also 0 FPR during night time, we observe a high FPR during day time. We thus conclude that using the maximum distance threshold $\max(D^\tau)$ is not suitable for busy environments.

5.2.2 *Equal Error Rate Threshold*

The experiment starts while the transmitter is in a tampered state, then it is transited to untampered state after a while. We can use the distance values from the initial tampered and untampered state to calculate the ROC curve. The ROC curve can then be used to select a threshold based on the desired FPR and TPR rates as previously discussed in Section 4.4. Table 3 shows the time ranges of tampered and untampered states for ROC calculation. Figure 12 shows the ROC curve of our 4 different receivers during this training time. Thresholds ranging from 0.001 to 1 with 0.001 intervals are applied to the distance values.

We calculate the EER for each receiver. The EER is the rate where the FPR and FNR are equal. Table 4 shows the EERs for all the receivers. Figure 13 shows the achievable FPRs and TPRs for the overall decision Q^i using this threshold γ_{EER}.

γ_{EER} reduces the FPRs dramatically. The FPR during the day is 0.00024 and it averages 0.00022 over the entire experiment. Unfortunately, the resulting detection capabil-

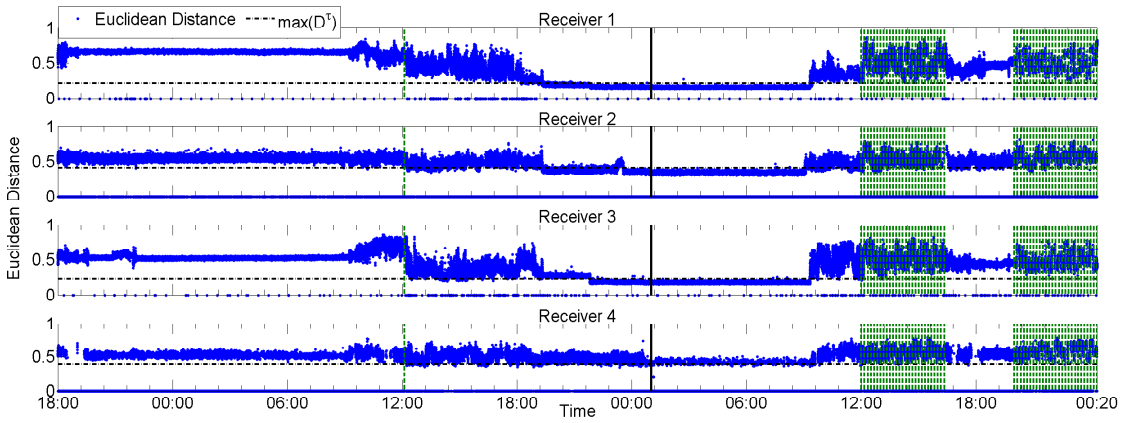


Figure 11: Euclidean distance for the uncontrolled movement experiment. Tamper events are indicated with vertical lines. Distance values of each receiver show tampering and also movement during office hours.

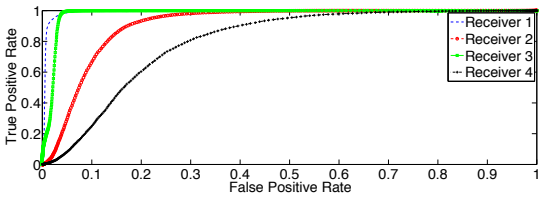


Figure 12: ROC curve of the 4 receivers.

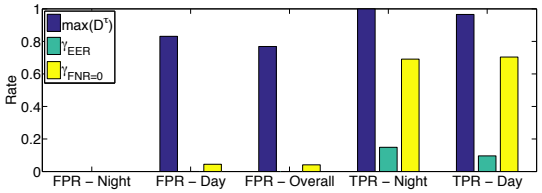


Figure 13: FPRs and TPRs with different thresholds. FPRs are always 0 during the night time. $\max(D^\tau)$ gives high FPRs. γ_{EER} reduces both FPRs and TPRs. $\gamma_{FNR=0}$ gives more balanced results.

ity of the system is low; TPRs of only 0.148 during night time and 0.096 during day time are achieved. However, for some applications it might be acceptable to have such a low TPR.

5.2.3 *Zero False Negative Threshold*

If we select a threshold lower than the EER threshold we may have a chance to increase the TPR. We select the maximum threshold where the ROC curve gives a FNR = 0, $\gamma_{FNR=0}$. Table 5 shows the all thresholds for each receiver, and Figure 13 shows the result Q^i based on this threshold. This threshold helps to increase TPRs (0.69 during night and 0.7 during the day), but we also increase the FPRs (0.045 during day and 0.041 overall). This threshold achieves a good TPR but the FPR is too high for many practical applications. We apply time-wise filtering to address this issue.

5.2.4 *Time-Wise Filtering*

We use window sizes of $t_w \in \{10, 30, 60\}$ seconds, and the decision is made that there is tampering when it was decided there was tampering for all individual packets within the window. Figure 14 shows the effect of time-wise filtering

	Receiver 1	Receiver 2	Receiver 3	Receiver 4
$\max(D^\tau)$	0.204	0.406	0.219	0.390
γ_{EER}	0.577	0.519	0.500	0.507
$\gamma_{FNR=0}$	0.419	0.386	0.355	0.396

Table 5: Threshold values for each receiver.

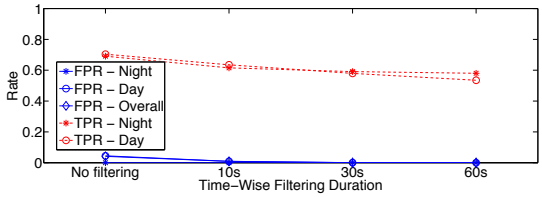


Figure 14: Effect of time-wise filtering on FPRs and TPRs when using $\gamma_{FNR=0}$ as the threshold. $t_w = 60\,\mathrm{s}$ reduces FPRs to 0, but it also reduces TPRs.

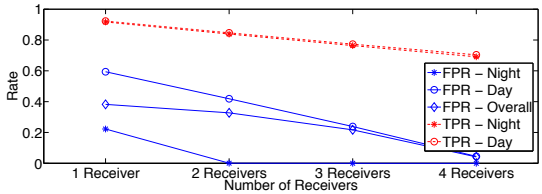


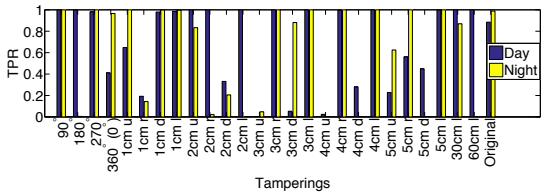
Figure 15: Effect of number of receivers to make a decision on FPRs and TPRs, when using $\gamma_{FNR=0}$ as the threshold and without using time-wise filtering. Increasing the number of receivers reduces both FPR and TPR.

over FPRs and TPRs when using $\gamma_{FNR=0}$ as the threshold. Increasing t_w decreases the FPR. The FPR is reduced from 0.045 to 0 during day time, and it is reduced from 0.04 to 0 overall when $t_w = 60\,\mathrm{s}$. However, using a 60 s window reduces the average TPR from 0.69 to 0.58 during night time, and from 0.7 to 0.53 during day time.

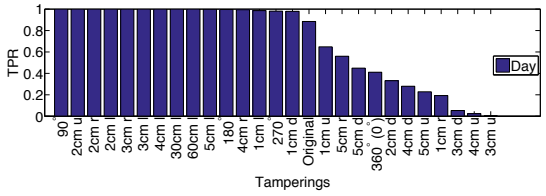
Clearly, it is possible even in a busy environment to use CSI based tamper detection without risking false alarms while detecting a reasonable number of tamper situations.

5.2.5 *Using Multiple Receivers*

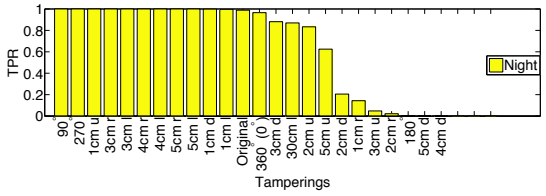
Until now, all of the decisions were made by using reports from all the receivers. All of the receivers needed to receive the packet, and that packet had to provide a distance above the thresholds for all receivers. The question is how many



(a) Tamperings during the day and the night times.



(b) Tamperings during the day time, sorted by TPRs.



(c) Tamperings during the night time, sorted by TPRs.

Figure 16: TPRs for different tamper events when using $\gamma_{FNR=0}$ as the threshold and without using time-wise filtering.

receivers should be used and what the contribution is of each additional receiver to FPRs and TPRs.

We used a total of $N = 4$ receivers in the experiment. We can use 1, 2, 3, or all of them to make a tamper decision. Figure 15 shows the tamper decision results when using $\gamma_{FNR=0}$ as the threshold and without using time-wise filtering. Results are averaged for different combinations of receivers for a given number of receivers, n. For example, if we use $n = 3$ we calculate the results using receivers {1, 2, 3}, {1, 2, 4}, {1, 3, 4}, and {2, 3, 4} in groups and take the average.

Figure 15 shows that using an increasing number of receivers n decreases the FPRs. If we use more than 4 receivers to make a decision, we might obtain even better FPRs. However, using more receivers also decreases TPRs.

5.2.6 *Tamper Event Detectability*

Previously all the TPRs from different tamper events were averaged and shown as a single result. In this section, we analyse individual TPRs for the different tamper states. We applied different tamper events during the day and night. These tamper events are shown in Table 1.

Figure 16 shows the results when using $\gamma_{FNR=0}$ as the threshold and without using time-wise filtering. All the receivers are used to make a decision. Some receivers could not receive beacons during the events 2 cm left at night, 4 cm up at night, and 60 cm left at night. These results are not shown in the figure.

Figure 16a shows TPRs for tamper events in order of their execution while Figure 16b and Figure 16c show them ordered by TPR night and day values. We can see from this that the magnitude of tampering (moved distance) does not correlate with detectability. It can also be seen that most tamper events can clearly be detected while a minority are hard to detect.

The minimum TPR value during the day time is 0.0034, the maximum is 1, and the average is 0.704. During the night time, the minimum TPR value is 0, the maximum is 1, and the average is 0.691.

6. DEPLOYMENT CONSIDERATIONS

In the previous sections we have described and analysed multi-receiver CSI tamper detection. Now we discuss how these methods can be put to work in practice to secure a WiFi based IoT setup. We first discuss potential capabilities of such a system based on the previously shown evaluations. We then discuss how a practical WiFi based system can incorporate the described methods and finally we describe how such a system can be operated in a practical setting.

6.1 System Capability

Many IoT systems are used to monitor and control critical infrastructure such as airports, refineries, hospitals or military installations. Additional layers of defence guarding the installation against tampering and other attacks are desirable. CSI tamper detection is a valuable building block in this context.

The evaluation has shown that in different deployment settings different FPR and TPR rates are achievable. The level of tolerable FPR and required TPR depends very much on the application scenario. The question is: in which application scenarios could the described system be employed?

A large number of IoT systems are deployed in areas with little variation in the environment. For example, systems are used to monitor and control production processes in refineries or power plants. Workers move throughout these installations but movement is limited; times of high activity are often known in advance (e.g. scheduled maintenance). In these settings a minimal FPR is required (ideally zero) as false alarms require costly investigation of the situation. On the other hand a high TPR is required to ensure that tampering with devices is detected. Our evaluation shows that requirements of such a setup can be fulfilled.

Other IoT setups are in relatively busy environments. For example, a wireless camera system used to monitor an office building would experience high levels of movement. In such a setting a zero FPR can also be achieved but only when making some sacrifices on the achievable TPR. However, if CSI tamper detection is used as an additional layer of defence and not the only security mechanism a TPR below 1 may already bring significant added value to the overall security of the system.

From our evaluations we conclude that CSI tamper detection is feasible with (i) perfect FPR ($FPR = 0$) and perfect TPR ($TPR = 1$) in settings with limited movement; and (ii) perfect FPR ($FPR = 0$) and good TPR ($TPR = 0.53$) in settings with high levels of movement.

6.2 System Design

A system using WiFi enabled nodes would likely operate in an infrastructure mode. Devices such as cameras would transmit data via access points interconnected by a fixed wired backbone. It can be assumed that multiple access points are in communication range of a device. We therefore suggest extending the functionality of access points to collect CSI information. The collected CSI information is then forwarded to a central system which carries out CSI based

tamper detection. To enable CSI collection at multiple access points nodes must transmit broadcast frames. This can be achieved by having nodes transmit periodic beacons for the purpose of tamper detection (in our experiments a one second interval was used). Using regular data transmissions of the nodes is less suitable as 802.11n adjusts the number of spatial streams and CSI is dependent on the number of spatial streams (see [1]). However, existing beaconing of nodes can be reused for the purpose of tamper detection. The system must allow secure collection of CSI data at access points which we believe is not trivial but achievable. The full specification of a CSI collection framework and extension of the 802.11n standard to incorporate appropriate beaconing for tamper detection is out of scope of this paper. However, we believe the outlined requirements can be addressed.

6.3 Deployment and Operation

A system using multi-receiver CSI tamper detection requires a training phase when it is deployed. Depending on the application requirements, different thresholds might be used ($\max(D^\tau)$, γ_{EER} and $\gamma_{FNR=0}$) to achieve the desired FPR and TPR rates. The different thresholds have different complexity in terms of deployment and training.

Using $\max(D^\tau)$ requires a very short training phase. In our experiments we used 100 packets transmitted over a period of 100s. However, during the transmission of these packets it must be ensured that the system is in an untampered state and that the environment is quiet.

Using γ_{EER} and $\gamma_{FNR=0}$ requires training data which contains a tampered state. This can be achieved by treating the initial placement location of a node as a tampered reference state in which data is collected over a period of time. Thereafter the node is placed in its operation location which is the untampered state. During the tampered and untampered state training data are collected to calculate the thresholds as previously described.

We believe that the described setup procedure is feasible for many application scenarios. For example, when a security system is deployed in a restricted area it is possible to ensure no movement in this area during installation.

Once a system is deployed it may happen that the communication environment changes naturally and the initial selected thresholds are invalidated. For example, smaller building alterations would change the observed CSI. These situations can be identified by an increase in the FPR rate and a re-initialisation of the system is required. An analysis of how often such re-calibration is necessary is not included in this paper and we will address this issue in future work.

7. CONCLUSION

The IoT is used for critical applications and to monitor and control critical infrastructure. Thus, it is important to provide secure IoT solutions. In particular it is desirable to detect tampering with IoT devices. In this paper we have shown that analysis of 802.11n CSI concurrently at multiple receivers allows us to provide a reliable tamper detection mechanism.

Although many IoT devices make use of 802.11n for communication, other transceiver types are also in use. The proposed methods can directly be applied to other communication systems based on OFDM. Other systems will describe the wireless channel differently. However, we believe that any information describing the communication channel is useful input for a tamper detection mechanism.

Acknowledgment

This work has been partly funded by the German Research Foundation (DFG) in the Collaborative Research Center (SFB) 1053 "MAKI – Multi-Mechanism-Adaptation for the Future Internet" and by LOEWE CASED. We thank our shepherd, Charles Wright.

8. REFERENCES

[1] I. E. Bagci, U. Roedig, M. Schulz, and M. Hollick. Short Paper: Gathering Tamper Evidence in Wi-fi Networks Based on Channel State Information. In *Proc. Wisec'14*, 2014.

[2] M. Bor, A. King, and U. Roedig. Lifetime bounds of Wi-Fi Enabled Sensor Nodes. In *Proc. IUPT'15*, 2015.

[3] V. Brik, S. Banerjee, M. Gruteser, and S. Oh. Wireless Device Identification with Radiometric Signatures. In *Proc. MobiCom'08*, 2008.

[4] B. Danev and S. Capkun. Transient-based Identification of Wireless Sensor Nodes. In *Proc. IPSN'09*, 2009.

[5] B. Danev, T. S. Heydt-Benjamin, and S. Capkun. Physical-layer Identification of RFID Devices. In *Proc. USENIX'09*, 2009.

[6] B. Danev, D. Zanetti, and S. Capkun. On Physical-layer Identification of Wireless Devices. *ACM Comput. Surv.*, 45(1):6, 2012.

[7] D. B. Faria and D. R. Cheriton. Detecting identity-based attacks in wireless networks using signalprints. In *Proc. WiSe'06*, 2006.

[8] D. Halperin, W. Hu, A. Sheth, and D. Wetherall. Tool Release: Gathering 802.11n Traces with Channel State Information. *ACM SIGCOMM CCR*, 41(1):53, 2011.

[9] IEEE 802.11 Working Group. IEEE 802.11n-2009. *IEEE Std*, 802:1–51, 2010.

[10] Z. Jiang, J. Zhao, X.-Y. Li, J. Han, and W. Xi. Rejecting the Attack: Source Authentication for Wi-Fi Management Frames using CSI Information. In *Proc. INFOCOM'13*, 2013.

[11] Z. Li, W. Xu, R. Miller, and W. Trappe. Securing wireless systems via lower layer enforcements. In *Proc. WiSe'06*, 2006.

[12] P. C. Mahalanobis. On the generalized distance in statistics. *Proceedings of the National Institute of Sciences (Calcutta)*, 2:49–55, 1936.

[13] N. Patwari and S. K. Kasera. Robust location distinction using temporal link signatures. In *Proc. MobiCom'07*, 2007.

[14] Y. Rubner, C. Tomasi, and L. J. Guibas. The earth mover's distance as a metric for image retrieval. *International journal of computer vision*, 40(2):99–121, 2000.

[15] O. Ureten and N. Serinken. Wireless security through RF fingerprinting. *Electrical and Computer Engineering, Canadian Journal of*, 32(1):27–33, 2007.

[16] J. Xiong and K. Jamieson. SecureArray: Improving Wifi Security with Fine-grained Physical-layer Information. In *Proc. MobiCom'13*, 2013.

[17] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera. Advancing Wireless Link Signatures for Location Distinction. In *Proc. MobiCom'08*, 2008.