applied sciences

MDPI

Article

Defeat Your Enemy Hiding behind Public WiFi: WiGuard Can Protect Your Sensitive Information from CSI-Based Attack †

Jie Zhang [1,‡], Meng Li [1,‡], Zhanyong Tang [1,*], Xiaoqing Gong [1], Wei Wang [1], Dingyi Fang [1] and Zheng Wang [2]

1 School of Information Science and Technology, Northwest University, Xi'an 710127, China; jz@stumail.nwu.edu.cn (J.Z.); lijmeng@stumail.nwu.edu.cn (M.L.); gxq@nwu.edu.cn (X.G.); wwang@nwu.edu.cn (W.W.); dyf@nwu.edu.cn (D.F.)

2 School of Computing and Communications, Lancaster University, Lancaster LA1 4YX, UK; z.wang@lancaster.ac.uk

* Correspondence: zytang@nwu.edu.cn

† Extension of a conference paper: A preliminary version of this article entitled "Protect Sensitive Information Against Channel State Information Based Attacks" by J. Zhang et al. appeared in the International Conference on Computational Science and Engineering (CSE), 2017. The extended version makes the following additional contributions over the conference paper: (1) it provides a more detailed description of the attack; (2) it describes how the user uses WiGuard to protect sensitive information and gives the user a choice for the position and channel to optimize the system performance; (3) it provides new experimental results to evaluate the influence of the packet loss rate on the success rate and provides proof for the channel switch; (4) it adds a new experiment to evaluate the diversity of the attacker wireless transmitter; (5) it includes new results to compare the recognition results with and without channel interference.

‡ Jie Zhang and Meng Li are co-first authors.

Received: 27 February 2018; Accepted: 23 March 2018; Published: 28 March 2018

Abstract: Channel state information (CSI) has been recently shown to be useful in performing security attacks in public WiFi environments. By analyzing how CSI is affected by finger motions, CSI-based attacks can effectively reconstruct text-based passwords and locking patterns. This paper presents WiGuard, a novel system to protect sensitive on-screen input information in a public place. Our approach carefully exploits WiFi channel interference to introduce noise to attacker's CSI measurements to reduce the success rate of CSI-based attacks. Our approach automatically detects when a CSI-based attack happens. We evaluate our approach by applying it to protect text-based passwords and pattern locks on mobile devices. Experimental results show that our approach is able to reduce the success rate of CSI-based attacks from 92–42% for text-based passwords and from 82–22% for pattern lock.

Keywords: CSI-based attack; channel interference; sensitive information protection

1. Introduction

Smartphones and tablets are usually used in public places (such as cafes, hotels, shopping malls, airports) and connected to public WiFi. However, it is not safe to use mobile devices in such an environment, because by analyzing the influence of user's finger movements on channel state information (CSI) when the user enters the password, the attackers can steal user's sensitive information, such as passwords, PINs, security codes, etc. We call this kind of attack a "CSI-based attack" [1].

Unlike traditional attacks, such as shoulder surfing attack [2], fingerprint attack [3] and video-based attack [4], which need to obtain the users' devices or additional support of video-based techniques, the CSI-based attack can recognize the users' sensitive input information from only

one public WiFi access point (AP) [5] and does not need any other vision-enhancing devices for a long-distance attack. Moreover, using commercial off-the-shelf (COTS) devices, such as Network Interface Controller (NIC) 5300, the attackers can conduct a successful CSI-based attack to obtain the user's passwords [6,7] even without obtaining any information displayed on the screen. Additionally, with professional techniques such as MIMO beamforming [8], the users' private information, such as lip-reading, can be leaked by analyzing CSI.

As shown in Figure 1, to launch the new attack, there is only one thing needed, and that is the attacker's toolkits and the target devices access the same online public WiFi simultaneously. Unfortunately, it seems that this happens all the time at KFC, Modoload, Starbucks coffee bars, etc.

(a) Scenario 1 (b) Scenario 2 (c) Scenario 3 (d) Scenario 4

Figure 1. Attack scenarios. The target is inputting sensitive information in a public place, and the attacker uses NIC as the receiver in Scenario 1 and Scenario 4, while in Scenario 2 and Scenario 3, the attacker uses her/his laptop to receive CSI.

Therefore, what makes the CSI-based attack easy to conduct for attackers? The key insight is that CSI characterizes the channel frequency response, and the signal at the receiver end is a superposition of multipath propagation, which is scattered from the wall and the surrounding objects. When a user inputs sensitive information, the movements of the finger motions will generate a unique pattern in time series CSI values, and different finger motions correspond to different patterns.

However, it is not enough to simply obtain CSI values, fine-grained CSI is required to conduct a CSI-based attack. In order to capture the subtle differences between finger motions, CSI must be measured at a fine-grained level. This is often done by sending high-frequency ICMP packets to the target AP (the public AP the attacker leverages) to obtain a high sample rate of CSI. For instance, Ali et al. [5] recognized keystrokes using CSI at a rate of 2500 ICMP packets per second. Therefore, obtaining high-frequency, fine-grained CSI measurements is key to the success of CSI-based attacks.

As analyzed above, the more fine-grained CSI is, the more easily the attacker will obtain the input sensitive information. Inspired by [9], in order to protect the input sensitive information, the user can reduce the rate of ICMP ping packets or make the attacker's receiver lose ICMP ping packets. A low rate of ICMP ping packets cannot capture the difference between different finger motions, and this will lead to the failure of the CSI-based attack. While there are a number of methods available to decrease ICMP responses [10], the communication quality of the target device cannot be ignored. Our solution is based on the fact that the target AP will lose ICMP packets if there exists another AP works on a channel next to the target AP's working channel.

This paper introduces WiGuard. As opposed to the prior work [11], which proposed a black sensor obfuscation technique and required additional hardware, WiGuard explores the potential of adjacent channel interference to defeat the CSI-based attack and prevent the public WiFi from leaking users' input sensitive information. To protect user's privacy, first knowing which public WiFi is being leveraged to obtain CSI values by an attacker is an important step. Simply put, if the network activity is normal without suspicious CSI collection in public WiFi, the users could use their wireless network normally; otherwise, the users need to take some protective measures before inputting sensitive information. First, the user needs to detect which channel the target public AP is on, then switch the channel of a safe wireless transmitter (as described in Section 6.1) to a proper channel to interfere

with the target public AP. All this effort is to make the attacker's receiver lose a massive amount of key packets of CSI measurements, so that the attacker cannot recover the corresponding finger motions correctly.

Our approach automatically detects when an attack is likely to happen by monitoring the network activities and runs the protection scheme if an attack is detected. Different from past works [12,13], which consider channel interference as detrimental and seek reasonable channel assignment methods to avoid channel interference [14–17], WiGuard exploits channel interference to prevent public WiFi from leaking users' privacy. To transform the above idea into a practical, feasible system, we need to solve the following challenges:

(1) When users access the public WiFi, how do they know whether there exists an attack in the current public WiFi? From the CSI-based keystrokes recognition [5], we know that if there exists a CSI-based attack, the attacker's receiver needs to continuously ping the public AP at a high rate, such as 2500 packets per second, and the user can monitor the number of ICMP packets in the network to decide whether there exist attacks in public places.

(2) How can one increase the packet loss rate of CSI channel so as to distort the CSI measurements of the corresponding finger motions obtained by attackers, while not affecting the normal network communication of public WiFi? After detecting the channel of the target public AP, the channel of a safe wireless transmitter is switched to interfere with the attacker's obtained CSI measurements. However, there are many adjacent channels that can be switched to interfere with the attacker. For example, when the target public AP works on Channel 6, the channel of the safe wireless transmitter can be switched to Channel 4 or Channel 5. Therefore, which channel should the safe wireless transmitter be switched to so that the channel interference between the safe wireless transmitter and the target public AP can achieve the maximum while ensuring that the users' normal network services on the target public AP are not affected by the channel interference?

(3) How does the system choose a proper distance for the safe wireless transmitter, and from this distance, there will not exist adjacent channel interference between the safe wireless transmitter and other normal APs? There may exist many public APs in public places. If the distance between the safe wireless transmitter and the normal APs is short, then the channel switching of the safe wireless transmitter may interfere with the normal public APs. Thus, we propose a CSI-based localization method for pubic APs and based on the localization results, the system will give a proper position for the safe wireless transmitter if the user chooses to use the system to protect his/her privacy.

Summary of the results: We build a prototype of WiGuard and evaluate it in different conditions. Our extensive experiments lead to the following findings:

- In order to interfere with the attacker's received CSI measurements, the channel spacing between the safe wireless transmitter and the target public AP should be one, and it can interfere with the target public AP to the greatest extent.
- In order not to interfere with the other normal public APs, the distance between the safe wireless transmitter and the normal public APs should be more than 4 m, and the longer the distance is, the smaller the impact will be on the normal public APs.
- The paper demonstrates that channel interference can defeat the CSI-based attack by recovering the unlock patterns for the smart phone and the keyboards of the PC. The attacker can achieve an accuracy of 82.33% and 92% respectively for patterns and keyboards when there exists no channel interference; and with channel interference, the recovery accuracy is respectively 21.67% and 42%.

Contributions: This paper makes the following contributions:

- It analyzes the essence of the CSI-based attack and introduces a protection system to defeat it. To the best of our knowledge, we are the first to propose solutions for such an attack.
- It presents a channel interference protection system that exploits channel interference to defeat CSI-based attack. As a result, the design delivers a good protective effect, and the success rate of CSI-based attack decreases dramatically.

- It is a working system, and we have evaluated it in a real-word environment. The results demonstrate that the system does not influence the normal network service.

2. Related Work

Our work lies at the intersections of CSI-based input sensitive information recognition and channel interference. This work leverages channel interference to defeat a new attack called the CSI-based attack. We will introduce the related work from the two following aspects.

2.1. CSI-Based Input Sensitive Information Recognition

There are many research works about CSI-based gesture recognition. Ali et al. [5] established a keyboard behavior recognition system called WiKey, and it can achieve more than 97.5% classification success rate for a keystroke and 96.4% recognition accuracy for a single key. It also can recognize keystrokes that are typed continuously with an accuracy of 93.5%. Li et al. [7] established a practical keystroke inference framework called WindTalker, which can recognize the sensitive keystrokes on a mobile device through CSI. WindTalker can achieve an average accuracy classification of 81.8% in Xiaomi, 73.2% in Nexus and 64% in Samsung. Wang et al. [8] presented WiHear, which enabled us to "hear" our speech using WiFi signal. WiHear can achieve an average recognition accuracy of 91% for a single individual speaking no more than six words and 74% for no more than three people talking simultaneously. It can be seen from the previous works that gesture recognition based on CSI has been able to achieve a higher recognition accuracy.

2.2. Channel Interference

Previous research works considered channel interference as detrimental and sought reasonable channel assignment methods, which is a common choice in resource management [18–24], and they mainly focused on two kinds of channel interference: one is interference between different communication systems [25], and the other is channel interference with respect to the 802.11 communication system [26].

2.2.1. Interference between 802.11 Networks and Other Networks That Work on 2.4 GHz

ISM (Industrial Scientific Medical) 2.4 GHz is an open frequency band worldwide, and many communication systems work on it, such as ZigBee, WiFi, Bluetooth and wireless USB. With the development of short-range wireless communication systems in recent years, more and more systems work on 2.4 GHz. However, the frequency band of 2.4 GHz is limited, and that will lead to the interference between different communication systems. The interference problem will be increasingly serious and inevitable with an increasing number of short-range wireless communication systems.

According to [12], previous research works have been classified into the following three categories:

- Interference mechanism/interference principle:
  Some research works focused on the interference mechanism/interference principle and tried to analyze the possible causes of interference appearing between different communication systems. For example, Yuan et al. [27] divided the interference between WiFi and ZigBee into four cases and analyzed whether there exists channel interference in these four cases. The study of the interference mechanism/interference principle will lay the foundation for the following two types of research works.
- Interference avoidance:
  The scheduling problem of spectrum resources is the essence of interference avoidance, and the core problem is how to allocate the spectrum resources in different communication systems to transmit data. Tytgat et al. [28] and Shi et al. [29] achieved interference avoidance between WiFi and ZigBee communication systems. Lee et al. [30] proposed a collaborative approach and a non-collaborative approach to solve the interference avoidance.

- Interference coexistence:
  When the spectrum resources are used, there will exist interference. How to make different communication systems coexist is a challenge. Yan et al. [31] achieved the coexistence of interference between WiFi and ZigBee, and Almeida et al. [32] achieved the coexistence of interference between WiFi and LTE.

2.2.2. Channel Interference in 802.11 Networks

Two types of interference in the 802.11 network have been proposed by Villegas et al. [13]: one is the co-channel interference, which is caused by the transmission on the same frequency channel, and the other is the adjacent channel interference, which is caused by the transmission on the adjacent channels or overlapped channels. Zubow et al. [33] analyzed the adverse effects of adjacent channel interference in 802.11 networks. Tan et al. [34] evaluated the effects of adjacent channel interference through extensive experiments. Previous studies on channel interference in 802.11 networks were mainly focused on how to allocate channels for these WiFi nodes to avoid co-channel interference and how to prove adjacent channel interference to assist the radio resources of different management mechanisms. Unlike previous work, which considered channel interference unfavorable on transmission systems, this paper leverages channel interference to defeat the CSI-based attack.

3. Background

3.1. Threat Model

A scenario is considered where attackers try to identify user's input sensitive information in time series CSI measurements generated by finger motions, and meanwhile, the attacker does not need to be close to the user. We assume that an attacker can access public WiFi and can ping a public WiFi AP at a high rate and use a receiver to receive the time series CSI measurements. Two representative scenarios for which the attack is reasonable are: (1) the receiver end of the attacker in public places is not obvious and in a hidden setting; (2) the attacker pretends to use his/her laptop to work in the public place, and he/she looks unsuspicious.

For Scenario 1, as shown in Figure 1a, the user unlocks the smart device while the attacker uses the network NICs to receive the CSI measurements. The attacker is far away from the user, and the prepared receiver is near the user. However, the location of the network NICs is hidden, and the user will not notice the receiver. For Scenario 2, as shown in Figure 1b, an attacker pretends to work on a laptop, which is used to receive CSI measurements. The attacker looks unsuspicious, so that the user will not perceive him/her.

3.2. CSI-Based Attack

With more and more public places deploying public WiFi, CSI has received much attention [35,36], and because of the rich information that CSI contains, it can be used to detect micro motions, such as finger motions [5,6] and mouth motions [8]. Using a commercial receiver, an attacker can obtain a user's PIN, password or other input sensitive information. In this section, we first show why CSI can detect and recover input sensitive information, and then, we will introduce a novel attack, the CSI-based attack.

3.2.1. Overview of CSI

Channel state information (CSI) describes the multi-path propagation scattered from the wall and surrounding objects, and it characterizes the variations in the wireless channel and provides more detailed fine-grained information of wireless signals. In our work, we leverage the multipath effect to recognize the input sensitive information, and different CSI modes, such as instantaneous CSI and statistical CSI, are not considered in this paper. That is also because the multipath effect will always exist no matter whether for instantaneous CSI and statistical CSI. CSI can be obtained by WiFi network

interface controllers (NICs). Let $X(f,t)$ be the transmitted signals at different subcarrier frequencies and $Y(f,t)$ be the received signals at different subcarrier frequencies, and the channel state information $H(f,t)$ at the receiver end can be calculated via $H(f,t) = \frac{Y(f,t)}{Y(f,t)}$. Let N_{Tx} represent the number of transmitter antennas and N_{Rx} the number of receiver antennas, the attacker received at the receiver end will be $30 \times N_{Tx} \times N_{Rx}$ CSI streams, and 30 means there are 30 subcarriers for each antenna pair.

3.2.2. CSI-Based Input Sensitive Information Recovery Model

When the user inputs sensitive information, the finger movements will introduce relative multi-path propagation of the wireless signal, and an unique pattern will be generated in time series CSI measurements, and different finger motions correspond to different multi-path propagation; and thus, it can be used to recognize the input sensitive information.

For the CSI-based sensitive information recovery model, there are several steps. First, noise needs to be removed from the obtained signal. After noise removal, it is necessary to extract the features and then use machine learning algorithms to recognize the input sensitive information, as shown in Figure 2.

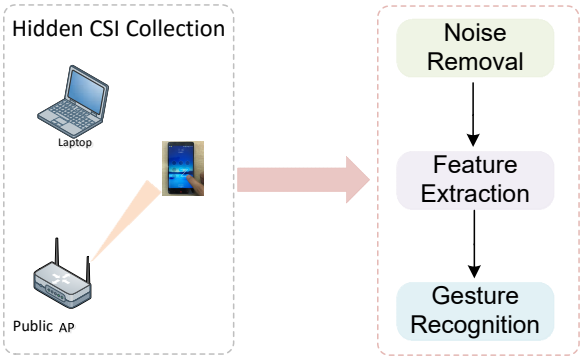


Figure 2. The process of CSI-based attack. After obtaining CSI measurements at the receiver end, the attacker needs to remove the noise, extract the features from the noise-removed signals and finally recognize the input sensitive information using machine learning algorithms.

(1) Noise removal:

The CSI measurements received by commercial WiFi NICs usually contain inherent noise, such as Gaussian white noise, because the transmission rates and internal CSI inference levels change frequently. In order to use CSI measurements to recover input sensitive information, such inherent noise needs to be removed from CSI time series measurements.

There are many methods to remove noise, such as MIMO beamforming or directional antennas to focus on the certain parts of the body, discrete wavelet decomposition to remove noise, a low-pass filter to remove high frequency noise, and so on.

(2) Feature Extraction:

The CSI measurements usually start being collected before the input sensitive information starts and finish being collected after the input sensitive information ends. Therefore, after removing noise from the obtained signals, the actual influenced signal traces need to be extracted from time series CSI measurements.

When the input sensitive information starts, the CSI waveforms will show a similar rising or falling trend. Thus, a simple method, sliding window, can be used to extract the features. However, the input sensitive information can be classified into two categories: one is consecutive finger motions, and the other is discrete finger motions. For consecutive finger motions, there exists no pause in the sensitive information performing process, such as unlock patterns on an Android screen and applications; while for discrete finger motions, there exists a pause in the sensitive information performing process,

such as keystrokes of laptops or digital unlock passwords. For discrete finger motions, the system first segments the time series CSI measurements into individual motions, then extracts the features for each individual motion.

After obtaining the starting and ending point, for each individual motion, the PCA (principal component analysis) method can be used to extract the principal components and then calculate the time-frequency features for each motion.

(3) Sensitive information recovery:

After extracting features, the machine learning algorithms will be applied to recover input sensitive information. There exists a similarity between speech recognition and gesture recovery; thus, a well-established technique, DTW (dynamic time warping), borrowed from speech recognition can be used to recover the input sensitive information. Besides, KNN (k-nearest neighbor), NB (naive Bayesian) and other classification algorithms can also be used to recover the input sensitive information using time-frequency features.

3.2.3. Requirements for CSI-Based Attack

The implementation of CSI-based attack only needs a receiver for the attacker, and the receiver can be a network NIC or a laptop. All the devices are commercial off-the-self (COTS) devices; thus, it can be easily achieved and deployed by an aggrieved attacker. Because the attacker does not need to be near the user or obtain any displayed information on the screen, so the attacker can mingle in the crowd and look unsuspicious, as shown in Figure 1.

After obtaining the CSI measurements, the input sensitive information can be recovered successfully by the attacker using the above techniques, as shown in Figure 2. However, a successful CSI-based attack needs the following several requirements, which can be equivalent to the following equation:

CSI-based attack $\Leftrightarrow$ (wireless transmitter, signal receiver, ICMP ping packets at a high rate from transmitter, communication channel between transmitter and receiver, Quality_{CSI})

The detailed information of the above equation can be interpreted as follows: there must be a wireless transmitter and a signal receiver. The wireless transmitter is used to transmit the wireless signal, and the signal receiver is used to receive the time series CSI measurements. In order to recover the input sensitive information, especially for those similar finger motions, the ICMP ping packets from the transmitter must be at a very high rate. In addition, the communication channel between the transmitter and the receiver must remain stable. If the communication channel between the transmitter and the receiver is disturbed and unstable, the receiver will not receive the complete ICMP ping packet, which will be unable to recover finger motions successfully. Quality_{CSI} describes the quality of received time series CSI measurements. If the wireless signal is interfered with in the multi-path propagation process, it will be changed at the receiver end.

4. WiGuard Overview

4.1. Channel Interference

The IEEE 802.11 is widely used for public WiFi, and it usually works on 2.4 GHz, which is between 2400 MHz and 2500 MHz. The 2.4 GHz is divided into 13 frequency bands (only Channel 1–Channel 13 are considered just because Channel 14 is only used in Japan and only 802.11b can support Channel 14 in Japan) [37], and each frequency band is 22 MHz. However, there are 13 channels in the 100-MHz frequency band, and that will lead to overlaps between frequency bands. The overlaps between frequency bands will cause channel interference.

However, when the central frequency spacing of two frequency bands is more than 22 MHz, there will exist no channel interference between these two frequency bands. Generally, Channel 1, Channel 6 and Channel 11 are chosen to be used simultaneously. Besides Channel 1, Channel 6 and Channel 11; if the devices support, there are two other groups of channels that do not interfere with each other, and they are: Channel 2, Channel 7, Channel 12; Channel 3, Channel 8 and Channel 13.

For those 13 channels, there are four channels that overlap the same channel. Thus, if an AP uses a certain channel, its neighbor AP must use the channel of the eight remaining un-overlapped channels; otherwise, there will exist channel interference between these two neighbor APs.

Furthermore, among the four overlapped channels, the channel interference is different between the two neighbor APs when the channel spacing between them is different, because the overlaps between the two channels are different. For example, the overlap between Channel 2 and Channel 1 is 77.27%, while the overlap between Channel 3 and Channel 1 is 54.55%. Thus, the channel interference between Channel 2 and Channel 1 is stronger than that between Channel 3 and Channel 1.

Prior research works have also demonstrated that the adjacent channel is harmful in the 802.11 network [33,38]. Akella et al. [17] validated that when there are plenty of wireless transmitters in a region, the co-channel interference will greatly reduce the network output: the output of TCP reduces from 9 Mbps–2 Mbps; the output of UDP also reduces, and it reduces from 9.7 Mbps–8.6 Mbps. In order to prevent the neighbor wireless transmitters from interfering with each other, there are many channel assignment methods proposed for WLANs [14–16,39].

4.2. System Overview

In order to defeat the CSI-based attack, a protection system, WiGuard, is designed in this paper. The key aspect of WiGuard is destroying the necessary requirements of a successful CSI-based attack by using channel interference. In the following sections, we will introduce the system design. First, the ICMP-based attacker AP acquirement detects whether there are abnormal ICMP ping packets caused by the CSI measurements collected by an attacker. If there is no abnormal ICMP ping packet, the user can input the sensitive information; if an attacker AP is detected, the user should detect the working channel of the target public AP and then switch the channel of a safe wireless transmitter to a proper channel to interfere with the target public AP. In order not to interfere with other normal public APs, the system will locate all the public APs and seek a proper position for the safe wireless transmitter, as shown in Figure 3.

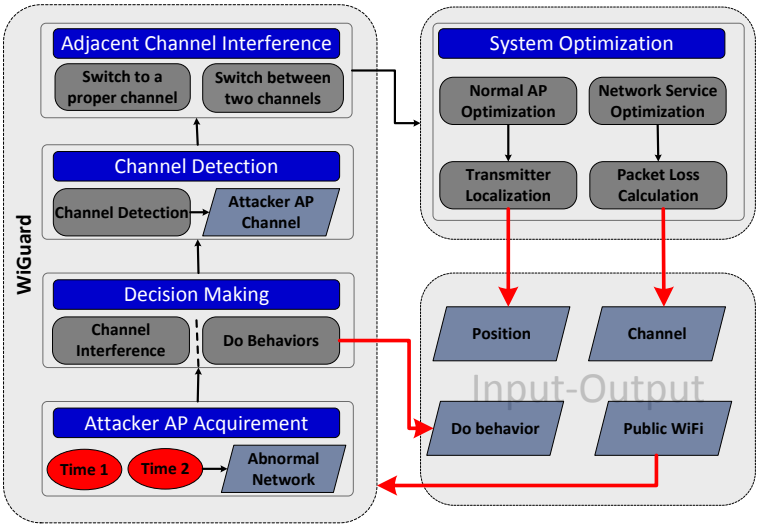


Figure 3. System overview.

5. ICMP-Based Attacker AP Detection

5.1. Attacker AP Characteristics

In order to recover the users' input sensitive information successfully, the fine-grained CSI measurements should be measured. Coarse-grained CSI values cannot characterize the difference

between finger motions, especially for micro motions, such as the digital unlock passwords of smart phones and keystrokes of laptops. However, CSI measurements are measured on ICMP ping packets. Thus, in order to obtain fine-grained CSI measurements, the attacker's receiver needs to continuously ping packets from the target public AP at a high rate, and the rate of ICMP ping packets is always thousands of packets/s, such as 2500 packets/s [5].

In normal cases, ICMP ping packets occur to test the network connectivity, and ICMP ping packets are sent at the rate of one packet per second [40]. Therefore, generally, there exist no ICMP ping packets or few ICMP ping packets for public AP. When an attacker leverages the public AP to collect CSI measurements, there will exist plenty of ICMP ping packets in the network.

5.2. Attacker AP Detection

Based on the analysis mentioned above, we know that when an attacker uses a public AP to collect CSI measurements, the number of ICMP ping packets in the network is far greater than normal cases. Thus, whether there exist ICMP ping packets and the number of ICMP ping packets per unit of time can be used to detect whether there exists a target public AP in public places. If a public AP is detected to have plenty of ICMP ping packets during different time periods, then it is very likely caused by an attacker who is pinging the public AP at a high rate, and we think there exists an attack in the public place.

However, in public places, there will be many public APs, and the attacker may use two or more public APs to improve the success rate of the CSI-based attack. Abdelnasser et al. [41] demonstrated that using multiple APs can improve the accuracy of gesture recognition. Therefore, in order to protect the input sensitive information thoroughly, users need to surf all public APs to detect how many public APs the attacker used.

When the user detects plenty of abnormal ICMP ping packets in the current network, the system will first detect on which channel the target public network AP is working. Channel detection is easy to implement, and there are many commercial applications that can support channel detection functions, such as WiFi analyzers.

6. Adjacent Channel Interference

After detecting the channels on which the target public APs work, adjacent channel interference will be used to protect the user's input sensitive information. However, how does the safe wireless transmitter change when the number of target public APs is different? Which channel should the safe wireless transmitter be switched to so that each public AP will be interfered with? Then, we will give the details of the adjacent channel interference protection method.

6.1. Safe Wireless Transmitter

In order to interfere with the target public APs, the channel of a safe wireless transmitter needs to be switched to the adjacent channel of target public APs. The safe wireless transmitter can be the normal public APs in the public place. Besides, the user can also use his/her smart devices with hotspot functionality as the safe wireless transmitters, such as smartphones or laptops. When the public wireless network is detected to be abnormal, the hotspot functionality of the user's devices can be turned on, and then, the channel of users' devices will be switched to interfere with the CSI measurements that the attacker has obtained.

6.2. Channel Switch

After detecting the channels of target public APs, a safe wireless transmitter will switch its channel to interfere with the target public APs. However, there are four adjacent channels that can interfere with the working channel of the target public APs. From the above analysis in Section 4.1, we know that when the channel spacing between two neighbor APs is different, the channel interference between them is also different; thus, the packet loss rate caused by the channel interference will also be different.

Therefore, which channel should the safe wireless transmitter be switched to so that the packet rate loss will be the maximum?

Theoretically, when the channel spacing between two adjacent APs is one, the channel interference between the two channels is the largest, because the overlap between the two channels is the largest.

However, in most cases, attackers can use two or more public APs to collect CSI measurements in order to improve the success rate of CSI-based attacks. Therefore, after detecting the channels of all target public APs, how does the safe wireless transmitter switch its channel to interfere with all the target public APs? There are two cases considered here: one is that the safe wireless transmitter only needs to switch its channel to a proper channel, and the other is that the safe wireless transmitter needs to switch its channel between two channels to interfere with all the target public APs.

(a) Switch to a proper channel:

There exists two cases in which the safe wireless transmitter can switch its channel to a proper channel to interfere with all target public APs. In the first case, there exists only one target public AP in the public place, and the channel of the safe wireless transmitter can be switched to an adjacent channel; for example, when the target public AP is working on Channel 6, the safe wireless transmitter can switch its channel to Channel 5 or Channel 7. In the second case, there exists two or more target public APs in the public place, and the channel spacing of target public APs is less than five. The channel of the safe wireless transmitter can be switched to the proper channel to interfere with the target public APs. For example, the channels of two target public APs are Channel 1 and Channel 6, and the safe wireless transmitter can switch its channel to Channel 3 or Channel 4.

In the second case, the safe wireless transmitter switches its channel to the proper channel to interfere with all target public APs, but in order to maximize the packet loss rate, the safe wireless transmitter can also switch its channel between two channels.

(b) Switch between two channels:

If the channel spacing between the target public APs is greater than five, the safe wireless transmitter can switch its channel between two channels to achieve adjacent channel interference. For example, when the channels of the two target public APs are Channel 1 and Channel 11, respectively, the safe wireless transmitter needs to switch its channel between Channel 2 and Channel 10.

7. System Performance Optimization

When the channel interference protection method is used to protect users' input sensitive information, in order not to affect the normal communication of the public wireless network, the system needs to be optimized in two ways: on the one hand, after switching the channel of the safe wireless transmitter, it should not affect the normal network service of the target public APs, so that the network service of the people who have already accessed the target public WiFi is not affected; on the other hand, there should exist no channel interference between the safe wireless transmitter and the normal public wireless transmitters.

The strength of channel interference between two neighbor wireless transmitters is related to the distance between them and the channel spacing between their channel. The smaller the channel spacing of their channel is, the stronger the channel interference between them. However, when two wireless transmitters are far away from each other, even when they work on adjacent channels, there will not exist channel interference between them.

From the analysis above, the safe wireless transmitter needs to be far away from normal public wireless transmitters and to be near the target public APs, so that after channel switching, the channel interference will not exist between the former, and it will only exist between the latter. Thus, we need to locate the distance between the safe wireless transmitters and all the public wireless transmitters, and based on the localization results, the system will give a proper position for the safe wireless transmitters when the WiGuard protection system is used.

7.1. System Optimization Model

We know that when two wireless transmitters are in a certain range of distance, if they work on the adjacent channels, there will exist channel interference between them, and we call the two wireless transmitters neighbors. The distance can be called $D_{neighbor}$.; However, when the distance between them is greater than $D_{neighbor}$, the channel interference will not occur even when they work on adjacent channels.

Based on the analysis above, the strength of channel interference can be mapped into a function f(d,channel), and an optimization model is built for the system. As shown in Figure 4, the channel interference can be mapped into two vectors, min vector and max vector, where min vector represents the channel interference between the safe wireless transmitter and the normal public wireless transmitters, while max vector represents the channel interference between the safe wireless transmitter and the target public APs.

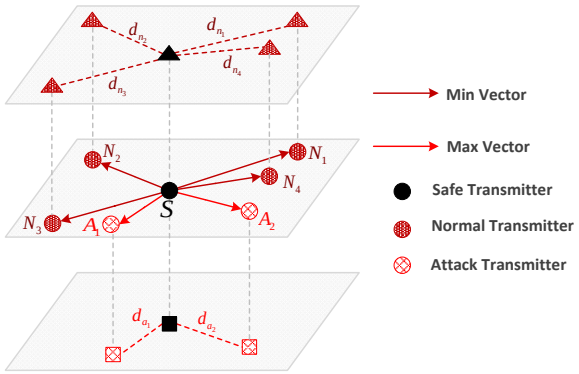


Figure 4. Interference vector.

In order not to interfere with the normal public wireless transmitters, min vector will give a proper position where the safe wireless transmitter is not the neighbor of the normal wireless transmitters, while max vector will give a proper channel.

The mapped expressions of min vector and max vector can be written as the following two equations:

min vector

$$f(d_{N_1}, channel) + ... + f(d_{N_i}, channel) + ... + f(d_{N_n}, channel) \quad (1)$$

max vector

$$f(d_{A_1}, channel) + ... + f(d_{A_j}, channel) + ... + f(d_{A_m}, channel) \quad (2)$$

under the following constraints:

(i) Distance constraint:

$$max\ d_{A_i} \leq D_{neighbor} \leq d_{N_i}$$

(ii) Channel constraints:

$$packet\ loss\ rate_{CSI\ values} \geq \delta$$

$$packet\ loss\ rate_{normal\ QoS} \leq \gamma$$

where d_{N_i} represents the distance between the safe wireless transmitter and normal public wireless transmitters, while n represents the number of normal wireless transmitters in the public place; d_{A_j} represents the distance between the safe wireless transmitter and the target public APs, while m represents the number of target public APs; $D_{neighbor}$ represents the distance at which the two wireless transmitters can be neighbors.

The distance constraints can be interpreted as follows: in order to interfere with the target public APs, the distance d_{A_i} should be shorter than $D_{neighbor}$, so that when they work on adjacent channels, there will exist channel interference between the safe wireless transmitter and the target public APs. In order not to interfere with the normal public wireless transmitters, the distance d_{N_j} should be large than $D_{neighbor}$, so that even when they work on adjacent channels, there will not exist channel interference between the safe wireless transmitters and normal public wireless transmitters.

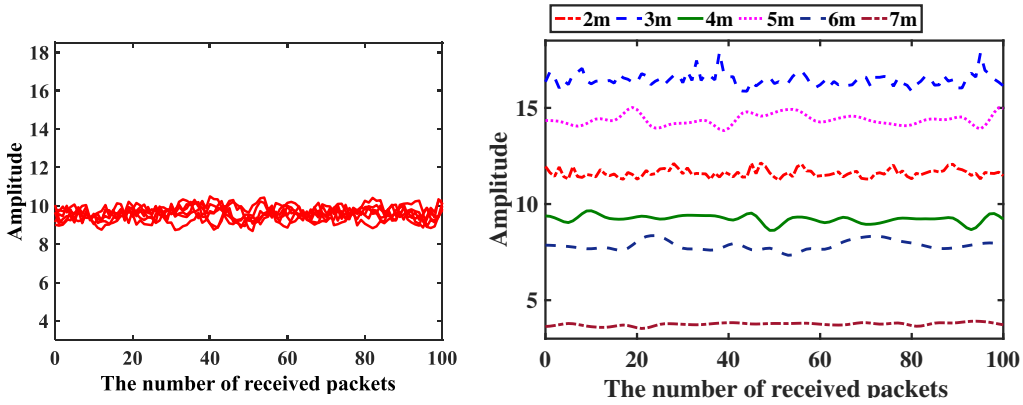
The interpretation of the channel constraints is as follows: in order to interfere with the CSI measurements at the receiver end so that the attacker cannot recover the input sensitive information, the packet loss rate for CSI measurements needs to be larger than the threshold δ; in order not to affect the normal network service, the packet loss rate of QoS should be smaller than the threshold γ.

7.2. CSI-Based Localization for Wireless Transmitters

There are many methods to locate public wireless transmitters. For example, Wang et al. [42] proposed an accurate localization method by using received signal strength (RSS). However, RSS is related to the transmit power of the public APs, and the attacker may change the transmit power to confuse the user to get the position of the public APs in the public place. Thus, the RSS-based localization method is not feasible in the public place, and the CSI-based localization method is used to locate the public APs in this paper.

As mentioned above, a kind of finger motion can generate a unique pattern in time series CSI measurements. In addition, different positions can also generate different patterns in CSI measurements; thus, CSI can also be used to locate public APs. As shown in Figure 5, the CSI measurements of the same position are always the same at different periods of time, and the CSI amplitude values in Figure 5a are from 8–11. We can see from Figure 5b that the CSI measurements of different positions are different.

When CSI values are used to do localization for public APs, first we need to remove the noise from the obtained CSI measurements, then PCA is used to reduce the dimension of CSI measurements, and the details of CSI-based localization are described in the following sections.



(a) Same position (b) Different positions

Figure 5. CSI measurements for different positions.

7.2.1. Noise Removal Using DWT

As mentioned in Section 3.2.2, the obtained CSI values contain much noise, so noise needs to be removed from received CSI values. In this paper, we apply a two-level discrete wavelet packet decomposition and Symlets wavelet filter to remove noise.

7.2.2. Dimension Reduction Using PCA

What is received at the receiver is a sequence of CSI values, and each CSI represents the amplitudes and phases on the group of subcarriers. In this paper, the dimensionality of CSI values is reduced by PCA, because PCA can recognize which subcarriers show the strongest correlation with the position, choose the most representative components from all CSI time series and remove the uncorrelated noisy components. The PCA-based dimension reduction includes the following steps.

Processing:

A matrix H presents the CSI time series measurements with $30 \times N_{TX} \times N_{RX}$ streams after noise removal. Every column of H represents the CSI measurements of each subcarrier, and the column of H will be $30 \times N_{TX} \times N_{RX}$. Then, the mean value of each column in H is calculated, and the corresponding mean values are subtracted in every column.

Correlation calculation:

Correlation matrix H_c is calculated as the following equation: $H^T \times H$. After obtaining the correlation matrix, then the eigenvalues and eigenvectors of covariance will be also calculated.

Main eigenvalues chosen:

Eigenvalues are sorted from large to small, and we choose the matrix k number of eigenvalues. Then, the corresponding k eigenvectors will form an eigenvector matrix.

7.2.3. Location Using DTW and SVM

As mentioned above, DTW (dynamic time warping) is widely used for classification and clustering tasks in isolated word speech recognition, gesture recognition, data mining and information retrieval. DTW calculates the distance between two samples, and the shorter the distance is, the more similar the two samples will be. For example, Ali et al. [5] used DTW techniques in keystroke classification and achieved an accuracy of 93.5%. Wang et al. [8] used DTW to achieve 87% accuracy for mouth recognition. Thus, in this paper, DTW is used to locate the public APs. Besides, we build a classifier to locate the wireless transmitters based on their waveform shapes and the DTW distances, and our classifier adopts the SVM classification scheme, which allows all the positions to be differentiated based on the training dataset. Support vector machines (SVMs) are supervised learning models with associated learning algorithms that analyze data used for classification and regression analysis [43]. It has been proven to be an effective method for sequence classification. For example, Wang et al. has established a gait recognition system called WifiUthat uses LibSVM to classify the human and achieves an accuracy of 93.05% [44]. The system can also use other machine learning algorithms to do the localization.

7.3. Packet Loss Rate Calculation

When channel interference is used to interfere with the attacker's obtained CSI measurements, the essence of channel interference is to make the attacker's receiver lose ICMP ping packets. However, how many packets does the attacker's receiver need to lose so that the attacker cannot recover the input sensitive information successfully? For public APs, in order not to influence the network service for normal users, the packet loss rate for the network service should be less than a threshold.

7.3.1. Packet Loss Rate (QoS)

For real-time applications, such as Internet telephony or video conferencing, the quality of service (QoS) will degrade when the packet loss is excessive [45]. However, the real-time applications are not sensitive to packet loss, and a packet loss rate of 1%∼3% is acceptable in most cases [46].

In public places, people often surf the Internet, watch online videos, chat online or play games using public WiFi, so the packet loss rate of the network service for normal users should be less than 3%, and the network service for normal users will not be affected.

7.3.2. Packet Loss Rate (CSI)

In order to obtain a high success rate for the CSI-based attack, the attacker needs to obtain fine-grained CSI measurements. In this part, we will discuss the influence of packet loss rate on success rate. What the attacker received at the receiver end is CSI time series, and the Quality_{CSI} is measured by the packet loss rate. For input sensitive information recovery, feature length (the number of received packets after feature extraction) can be a factor to differentiate different finger motions. For example, the feature lengths of simple unlock patterns and complex unlock patterns on smart devices are usually different. If the influenced signal traces that the attacker received are not complete, the attacker will recover the complex unlock patterns as simple unlock patterns.

However, if the packet loss rate is small and one to several packets are lost, it will not influence the final recovery results. However, if Quality_{CSI} is larger than a threshold, it will influence the CSI measurements greatly, and the success rate will decrease dramatically.

The attacker can use the DTW method to quantify the similarity of two influenced signal traces; the shorter the distance that DTW calculated is, the more similar the two influenced signal traces will be. In this part, the influence of the packet loss rate on calculated distance is considered instead of calculating the recovery accuracy in order to give a bottom view of the success rate calculation.

The DTW distances of CSI waveforms between 15 unlock patterns on smart phones is calculated, and the results are as shown in Figure 6. We can see from Figure 6 that with the increase of the packet loss rate, the distances between 15 unlock patterns become shorter, and the tested unlock pattern will be more similar to the 15 unlock patterns. Then, the tested unlock patterns will be recovered for one of those 15 unlock patterns according to the calculated distances; thus, the recovery accuracy will decrease.

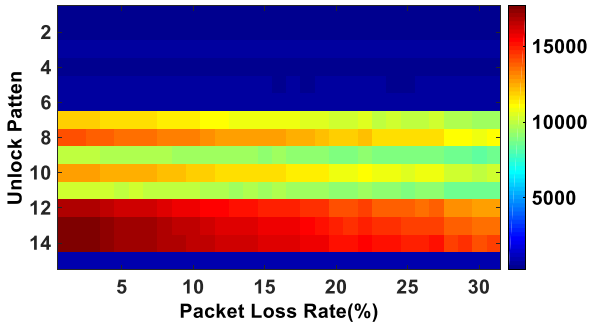


Figure 6. Influence of packet rate loss on calculated DTW distances between two samples.

8. Implementation

8.1. Experimental Setup

Wireless devices: In our work, the TP-Link wireless router (TP-Link WR 1043ND) and smart device with wireless hotspot functionality (iPhone 6 plus) are used as wireless transmitters, respectively, and the desktop with Intel 5300 NIC (Network Interface Controller) is used as a receiver. The transmitter and receiver both have three antennas. The receiver needs to be deployed with the Linux 802.11n CSI Tool [47], which is needed to open two terminals to ping data packets and collect data packets. The receiver continuously pings packets, and stores and processes the collected packets. The work of the transmitter follows the IEEE 802.11n protocol, and the firmware reports CSI to the upper layers. The collected packets are a sequence of data, and each packet contains the received signal strength indicator (RSSI) value of three antennas, the value of noise, CSI, and so on. Each CSI represents the phase and amplitude on a set of 30 OFDM subcarriers.

Scenarios: We implement WiGuard on current TP-Link wireless routers and smart devices with hotspot functionality in a corridor with a size of 2 m $\times$ 5 m and in a room in an indoor environment with a size of 5 m $\times$ 10 m.

Configurations: The safe wireless transmitters are placed at 0.5 meters to 7 meters away from the target public APs. Six conditions for safe wireless transmitters and target public AP are given, and they are separately $\{S_1, A_6\}$, $\{S_6, A_1\}$, $\{S_1, A_{11}\}$, $\{S_{11}, A_1\}$, $\{S_6, A_{11}\}$ and $\{S_{11}, A_6\}$. $\{S_1, A_6\}$ represents that the safe wireless transmitter works on Channel 1 and the target public AP works on Channel 6, while the other five configurations are in the same manner.

8.2. Parameters for Interference Evaluation

After detecting the channel of the public APs, then the safe wireless transmitter will switch to a proper channel to interfere with the target public APs. However, there are several adjacent channels that can interfere with the public APs. Which channel should the safe wireless transmitter be switched to so that the channel interference between the safe wireless transmitter and the target public APs maximum and the packet loss rate will be the maximum? In this paper, we will introduce four parameters to quantify the channel interference between the safe wireless transmitter and the target public APs, and they are the number of packets received, the packet loss rate, the interference strength and the active ratio [48], respectively.

The definition of the four parameters is as follows:

- The number of received packets:
  The parameters are obtained by actual experiments. What we have obtained is a sequence of CSI measurements, and the length of the sequence is the number of received packets.
- Packet loss rate:

$$Packet\ Loss\ Rate = \frac{RV\ of\ RP - IV\ of\ RP}{RV\ of\ RP} \tag{3}$$

  In the above equation, $RV\ of\ RP$ represents the reference number of received packets, and the packets are obtained when the safe wireless transmitter and target public APs work on different channels and there exists no channel interference between them. $IV\ of\ RP$ represents the interference number of received packets, and the packets are obtained when the safe wireless transmitter and the target public APs work on adjacent channels and there will exist adjacent channel interference between them. We assume that when the safe wireless transmitter and the target AP work on different channels and there exist no channel interference between them, the packet loss rate is zero.
- Interference strength:

$$IS = \sum_{i=0}^{RP} \frac{RSSI_{i\_noise\_removal}}{RP} \tag{4}$$

  In the above equation, $RSSI_{i\_noise\_removal}$ represents the RSSI value of the i-th packet from which the noise has been removed, and RP represents the reference number of the received packets. The value of IS represents the interference strength between the safe wireless transmitter and the target public AP; when the value of IS is greater, the interference strength between the safe wireless transmitter and the target public APs is stronger.
- Active ratio:

$$AR = \sum_{i=0}^{RP} U_i,$$

$$U_i = \begin{cases} if \frac{|RSSI_i + Noise_i|}{RSSI_{i\_noise\_removal}} \geq 1, & U_i = 1 \\ other, & U_i = 0 \end{cases} \quad (5)$$

In the above equation, $RSSI_i$ represents the RSSI value of the i-th packet and $Noise_i$ represents the noise value of the i-th packets; when the value of AR is greater, the noise contained in the received packets is lower, and the channel interference between the safe wireless transmitter and the target public APs will be weaker.

9. Evaluation

In this section, we first prove that the channel interference between two adjacent wireless transmitters is different when channel spacing between them is different, which lays the foundation of channel switching. Then we prove that when the distance of two wireless transmitters is greater than $D_{neighbor}$, there would be no channel interference between them. Finally, we reproduce the experiments of WiPass [6] and WiKey [5], and the results demonstrate that the channel interference can defeat the CSI-based attack.

9.1. Channel Interference on Public APs that the Attacker Leverages

In order to select a proper channel to interfere with the target public APs, it is necessary to carry out experiments with different channel spacing between two wireless transmitters. In this paper, the adjacent channel interference experiments are done, and first, the safe wireless transmitter and the target public AP work on different channels, then the safe wireless transmitters will switch their channel to interfere with the target public AP.

9.1.1. Channel

For public APs that can work in the same public place, in order to avoid channel interference between them, they always work on Channel 1, Channel 6 and Channel 11. Thus, there are six conditions of the channels for two neighbor wireless transmitters, and in this part, the experiments of these six conditions are done to demonstrate that when the channel spacing between two neighbor wireless transmitters is different, the channel interference between them will also be different. In these experiments, the distance between the two neighbor APs is 1 m, and the results are as shown in Figure 7.

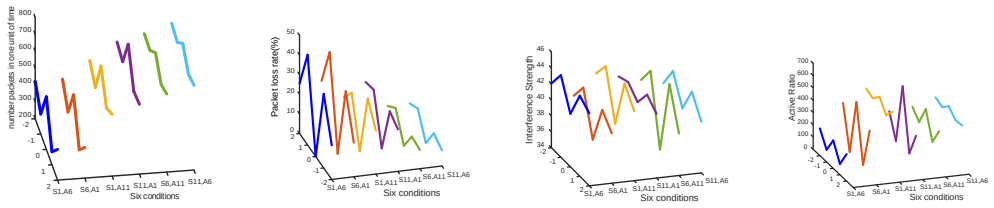
In Figure 7, the value "0" on the X-axis means that there exists no channel interference between the safe wireless transmitter and the target public AP; the values "−2" and "2" mean that the channel spacing between two wireless transmitters is two; the values "−1" and "1" mean the channel spacing between two wireless transmitters is one. "−" means that the channel of the target public AP is less than the channel of the safe wireless transmitter.

We can see from Figure 7 that the number of received packets is the maximum when there exists no channel interference between the safe wireless transmitters and the target public AP. The number of received packets is relatively low when there exists channel interference between the two wireless transmitters, and when the channel spacing between two wireless transmitters is one, the number of received packets is the minimum and the packet loss rate is the maximum. For example, in Figure 7a,b, when the channel of the safe wireless transmitter is 1 and the channel of the target public AP is 6; if the safe wireless transmitter switches its channel to Channel 5, the packet loss rate is 37.695%; if the safe wireless transmitter switches its channel to Channel 7, the packet loss rate is 45.894%; while if the safe wireless transmitter switches its channel to Channel 4, the packet loss rate is 17.383%; and if the safe wireless transmitter switches its channel to Channel 8, the packet loss rate is 25.392%. Thus, when the channel spacing between the safe wireless transmitter and the target public AP is one, the channel interference between them can achieve the maximum.

We can see from Figure 7c,d that when there exists no channel interference between safe wireless transmitter and the target public AP, the value of interference strength is the minimum, and the value

of the active ratio is the maximum. When the safe wireless transmitter switches the channel, the value of the interference strength will increase, and the value of the active ratio will decrease. When the channel spacing between the safe wireless transmitter and the target public AP is one, the value of the interference strength is the maximum, and the value of active ratio is the minimum. This is consistent with the analysis in Section 8.2.

Therefore, when the channel spacing between the safe wireless transmitter and the target public AP is one, the channel interference between them is maximum. Thus, the system can switch the channel of the safe wireless transmitter to an adjacent channel of the target public AP, and the channel spacing between them is one.



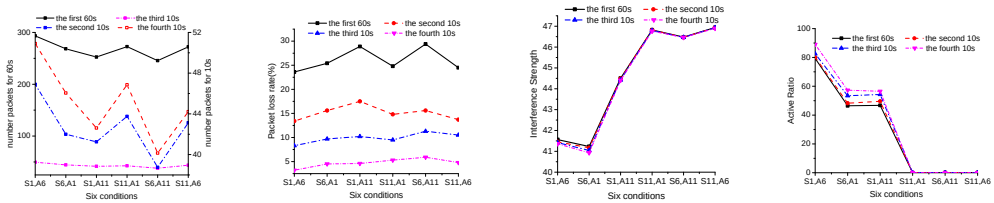
(a) Number of packets (b) Packet loss rate (c) Interference strength (d) Active ratio

Figure 7. Four parameters to characterize the channel interference between the safe wireless transmitter and the public AP that the attacker leverages under six conditions.

9.1.2. Time

For some wireless transmitters, a simple co-channel interference avoidance algorithm may be adopted. When AP detects channel interference, it will choose other proper channels for data transmission [49]. In order to demonstrate how long channel interference exists after switching the channel so that the users' input sensitive information can be completed during the interference time, we collected 90 s of data after switching the channel of the safe wireless transmitter.

We can see from Figure 8a,b that under the six conditions, the number of received packets of the fourth 10 s is the largest, in Figure 8c,d, the difference of the *IS* and *AR* values in different periods is relatively small. Therefore, after switching the channel, the channel interference between the safe wireless transmitter and the target public AP will be weakened with time elapsing; however, after 90 s, the channel interference still exists between them, and 90 s is enough to complete the input sensitive information. If the user inputs the sensitive information for a long time, the user can continuously detect the channel of the target public AP, and if the channel of the target public AP switches to another channel before finishing inputting the sensitive information, then the safe wireless transmitter switches its channel accordingly.



(a) Number of packets (b) Packet loss rate (c) Interference strength (d) Active radio

Figure 8. Four parameters to characterize the duration of channel interference between the safe wireless transmitter and the other normal public APs under six conditions.

9.1.3. Different Wireless Transmitters

The attacker can turn on the hotspot functionality of his/her smart devices to serve as a public wireless transmitter to emit wireless signals [6]; thus, whether the channel interference is also appropriate for the different kinds of wireless transmitters needs to be considered.

We can see from Figure 9 that for public APs and smart devices, the parameters that characterize the channel interference are different. The interference value of received packets and the packet loss rate of public AP are more than that of smart devices; for example, the packet loss rate of the public AP is 31.5%, while the packet loss rate of the smart device is 27.2%. Besides, the value of the interference strength of AP is more than that of the smart device, and the value of the active ratio of AP is less than that of the smart device. Through the analysis of IS and AR in Section 8.2, we know that the influence of channel interference on the public AP is stronger than that on smart devices. However, when the attacker leverages the smart phone to collect CSI measurements, the channel interference protection method also works.

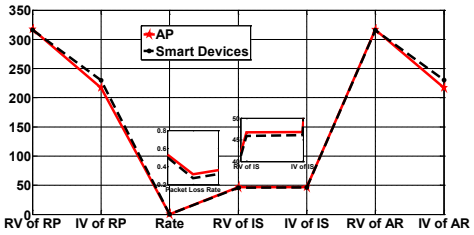
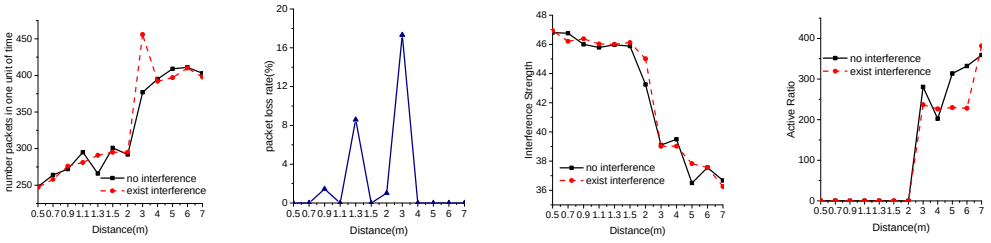


Figure 9. The parameters to characterize the channel interference for different wireless transmitters.

9.2. Channel Interference on Normal Public Wireless Transmitters

When the safe wireless transmitter is far away from the normal public APs, there is no channel interference between them. In order to choose an appropriate distance between the safe wireless transmitter and the other normal public APs, we carry out experiments on different distances, and in the experiment, the channel spacing between the safe wireless transmitter and the other normal public AP is one.

From Figure 10a,b, we know that when the distance between the safe wireless transmitter and other normal public wireless APs is from 0.5 m–2 m, the interference value of the received packets and the reference value of the received packets are almost the same. This is because the safe wireless transmitter and the other normal public APs are close, and even if there is no channel interference, it will also affect the normal communication. As the distance between them increases, the influence of channel interference will be weakened. As can be seen from Figure 10, when the channel interference between the safe wireless transmitter and the other normal public AP is more than 3 m, the channel interference between them will be weak.



(a) Number of packets (b) Packet loss rate (c) Interference strength (d) Active ratio

Figure 10. Four parameters under different distances.

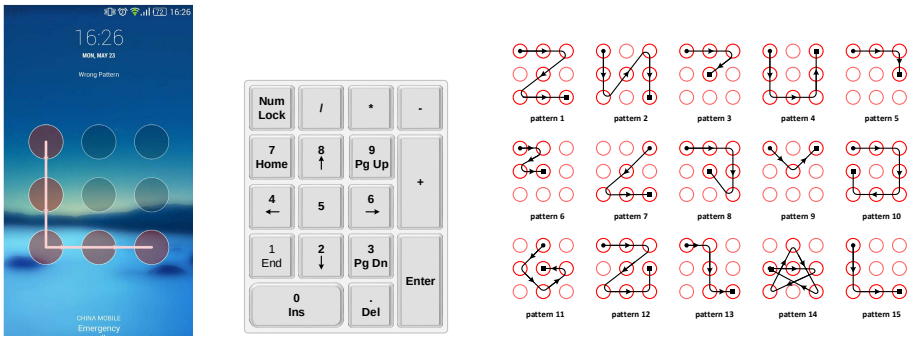
In Figure 10c,d, when the distance is less than 2 m, IS is high and AR is relatively low; when the distance is more than 3 m, IS decreases and AR increases sharply. Therefore, in order not to interfere with the other normal public APs, the distance between the safe wireless transmitter and the other normal public APs would be better when it is more than 4 m. When the distance is 4 m, the channel switch will not influence the communication of normal public APs. The longer the distance between the safe wireless transmitter and other normal public APs is, the smaller the impact of channel switching will be on the communication of normal public APs.

9.3. Case Study

There are two kinds of input sensitive information for CSI-based attacks, and we separately choose unlock patterns and keystrokes as the representative finger motions for consecutive motions and discrete motions to do the experiments. The results are as shown in Figure 11. Uellenbeck et al. [50] found that there exist typical strategies for frequently-used unlock patterns, such as the top left corner is usually used as a starting point, and straight lines are more popular in the patterns. According to this, 15 unlock passwords are randomly chosen as the tested unlock passwords according to the habits of people's daily use, and the 15 tested unlock passwords are shown in Figure 11c. Besides, Numpad 0–Numpad 9 on the right of the keyboard are chosen as the tested keystrokes, as shown in Figure 11b.

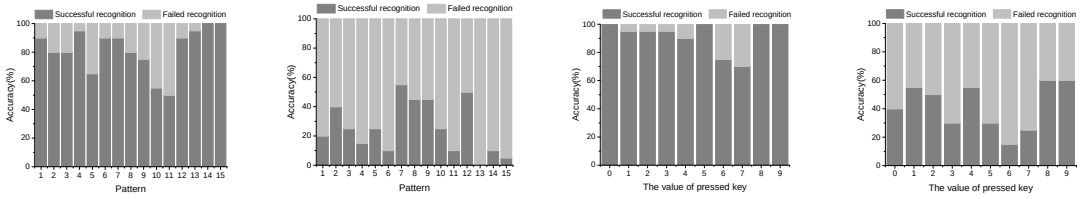
The results of the recovery accuracy of the two case studies are shown in Figure 12. From Figure 12a,c, we know that when there is no channel interference, the recovery accuracy is relatively high: the average recovery accuracy of the 15 unlock password patterns is 82.33%, and the average recovery accuracy of the 10 keypads is 92%. The results of unlock patterns and keyboard recovery indicate that the wireless signal will reveal the user's privacy, which should be a warning for users.

From Figure 12b,d, we know that when the channel interference exists, the recovery accuracy is relatively low, and the average recovery accuracy of the 15 unlock password patterns is 21.67%, and the detailed recovery results are shown in Figure 13; the average recovery accuracy of the 10 keypads is 42%, and the detailed recovery results of keypads for 20 times are shown in Figure 14. Compared with the recovery accuracy without channel interference, the recovery accuracy with channel interference significantly decreases. The results show that channel interference can defeat the CSI-based attacker effectively.



(a) (b) (c)

Figure 11. Two case studies. (**a**) Unlock patterns; (**b**) keystrokes; (**c**) 15 tested patterns for Android applications.



(a) (b) (c) (d)

Figure 12. Users' behavior recognition when there is no channel interference and exists channel interference. (**a**) Pattern recognition without interference; (**b**) pattern recognition with channel interference; (**c**) keyboard recognition without interference; (**d**) keyboard recognition with channel interference.

9.4. Channel Interference on the Network Service

If the target public AP is interfered with, the network services that ordinary users have accessed will also be interfered with. Watching online programs is done to test the impact of channel interference on network services. As can be seen from Figure 15, when users are watching the online program using the network services of the target public AP, after the safe wireless transmitter switches the channel, the network service can also be good, and the video is also smooth. Therefore, the impact of channel interference on network services is very small, and the users can have a normal network service on the target public AP.

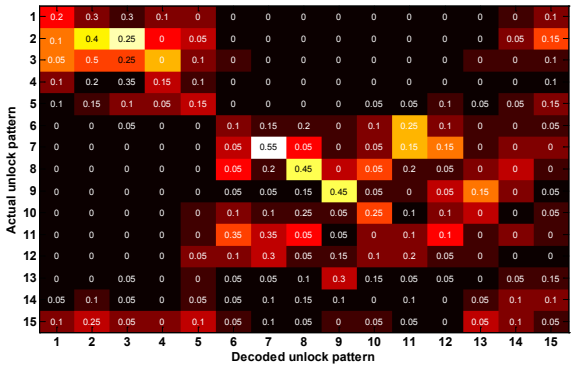


Figure 13. Recognition accuracy of the unlock pattern when there exists channel interference.

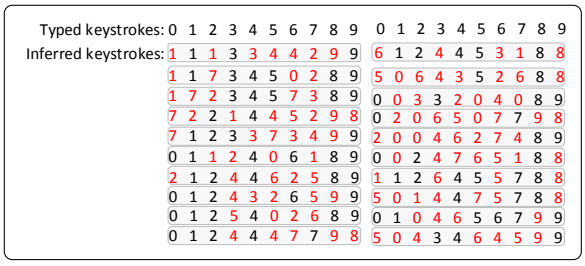


Figure 14. Recognition accuracy of keystrokes when there exists channel interference.

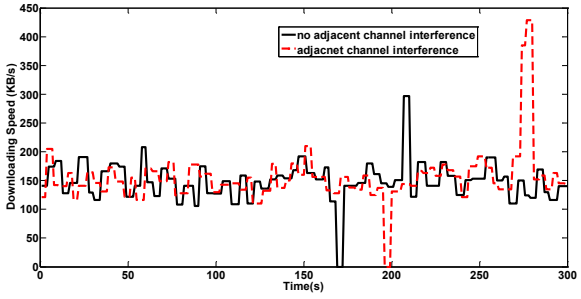


Figure 15. Evaluation of network service on the target public AP.

10. Conclusions

This paper presents a new method, called WiGuard, to defeat the CSI-based attack, which uses public WiFi to obtain user's input sensitive information. Our key insight of the design is that if we can interfere with the target public AP to distort the CSI measurements, then the attacker will not be able to successfully recover the input sensitive information. In order to distort the CSI measurements, WiGuard exploits the potential of channel interference to defeat the attack. WiGuard first detects the channel of the target public AP using the number of ICMP ping packets, because in order to obtain the fine-grained

CSI measurements to recover the input sensitive information, the attacker needs to ping the target public AP at a high rate. After detecting the channel, the user can switch a safe wireless transmitter to a proper channel to interfere with the target public AP. Extensive experiments demonstrate that when the channel spacing of the safe wireless transmitter and the target public AP is one, the channel interference between them can achieve the maximum, and the user can switch the safe wireless transmitter to that channel. When the distance between the safe wireless transmitter and the other normal public APs is more than 4 m, channel interference between them becomes weak, and $D_{neighbor}$ can be seen as 4 m. Therefore when the distance between them is more than 4 m, the channel switching of the safe wireless transmitter will not influence the other normal public APs. Evaluation of the network service demonstrates that channel interference will not influence the normal network service. The results of two case studies show that when there exists channel interference, the recovery accuracy decreases dramatically; thus, our system WiGuard is effective, and channel interference can be used to defeat CSI-based attack.

Acknowledgments: This work was partially supported by projects of the National Natural Science Foundation of China (No. 61672427, No. 61672428); the International Cooperation Foundation of Shaanxi Province, China (No. 2015KW-003, No. 2017KW-008); the Service Special Foundation of Shaanxi Province Department of Education (No.16JF028); the Research Project of Shaanxi Province Department of Education (No. 15JK1734); the Key Research Project of Shaanxi Province of China (No. 2017GY-191); the Research Project of CCF-NSFOCUS Kunpeng Science Foundation; the U.K. Engineering and Physical Sciences Research Council under Grants EP/M01567X/1 (SANDeRs) and EP/M015793/1 (DIVIDEND); and a Royal Society International Collaboration Grant (IE161012).

Author Contributions: Jie Zhang and Zhanyong Tang conceived and designed the system, and Jie Zhang wrote the paper; Meng Li performed the experiments; Xiaoqing Gong and Wei Wang analyzed the data and modified the experimental part; Dingyi Fang and Zheng Wang contributed analysis tool and Zheng Wang modified the system design part.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CSI	channel state information
PIN	personal identification number
AP	access point
COTS	commercial off-the-shelf
NIC	network interface controller
MIMO	multiple input multiple output
ICMP	Internet control messages protocol
PC	personal computer
USB	Universal Serial Bus
PCA	principal component analysis
DTW	dynamic time warping
KNN	k-nearest neighbor
NB	naive Bayesian
TCP	transmission control protocol
UDP	user datagram protocol
QoS	quality of service
RSS	received signal strength
SVM	support vector machine
OFDM	orthogonal frequency division multiplexing
RSSI	received signal strength indicator

References

1. Zhang, J.; Tang, Z.; Li, R.; Chen, X.; Gong, X.Q.; Fang, D.; Wang, Z. Protect Sensitive Information against Channel State Information Based Attacks. In Proceedings of the 2017 IEEE International Conference on Computational Science and Engineering, Guangzhou, China, 21–24 July 2017; pp. 203–210.

2. William R. Trumble. In *Shorter Oxford English Dictionary*, 6th ed.; Oxford University Press: Oxford, UK, 2007.
3. Zhang, Y.; Xia, P.; Luo, J.; Ling, Z.; Liu, B.; Fu, X. Fingerprint attack against touch-enabled devices. In Proceedings of the ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, Raleigh, NC, USA, 19 October 2012; pp. 57–68.
4. Shukla, D.; Kumar, R.; Serwadda, A.; Phoha, V.V. Beware, Your Hands Reveal Your Secrets! In Proceedings of the ACM Sigsac Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 904–917.
5. Ali, K.; Liu, A.X.; Wang, W.; Shahzad, M. Keystroke recognition using wifi signals. In Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, ACM, Paris, France, 7–11 September 2015; pp. 90–102.
6. Zhang, J.; Zheng, X.; Tang, Z. Privacy Leakage in Mobile Sensing: Your Unlock Passwords Can Be Leaked through Wireless Hotspot Functionality. *Mob. Inf. Syst.* **2016**, *2016*, doi:10.1155/2016/8793025.
7. Li, M.; Meng, Y.; Liu, J.; Zhu, H.; Liang, X.; Liu, Y.; Ruan, N. When CSI Meets Public WiFi: Inferring Your Mobile Phone Password via WiFi Signals. In Proceedings of the ACM Sigsac Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 1068–1079.
8. Wang, G.; Zou, Y.; Zhou, Z. We can hear you with Wi-Fi! In Proceedings of the 20th Annual International Conference on Mobile Computing and Networking, Maui, HI, USA, 7–11 September 2014; pp. 593–604.
9. Rouf, I.; Mustafa, H.; Xu, M. Neighborhood watch: Security and privacy analysis of automatic meter reading systems. *ACM Conf. Comput. Commun. Secur.* **2012**, 462–473, doi:10.1145/2382196.2382246.
10. Wikipedia. Denial-Of-Service Attack. Available online: https://en.wikipedia.org/wiki/Denial-of-service_attack/ (accessed on 10 August 2016).
11. Qiao, Y.; Zhang, O.; Zhou, W.; Srinivasan, K.; Arora, A. PhyCloak: Obfuscating sensing from communication signals. In Proceedings of the Usenix Conference on Networked Systems Design and Implementation, Santa Clara, CA, USA, 16–18 March 2016.
12. Xu, R.; Shi, G.; Luo, J. Muzi: Multi-channel zigbee networks for avoiding wifi interference. In Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, Dalian, China, 19–22 October 2011; pp. 323–329.
13. Villegas, E.G.; Lopez-Aguilera, E.; Vidal, R. Effect of adjacent-channel interference in IEEE 802.11 WLANs. In Proceedings of the CrownCom 2007 2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, Orlando, FL, USA, 1–3 August 2007; pp. 118–125.
14. Mishra, A.; Banerjee, S.; Arbaugh, W. Weighted coloring based channel assignment for WLANs. *ACM SIGMOBILE Mob. Comput. Commun. Rev.* **2005**, *9*, 19–31.
15. Lee, Y.; Kim, K.; Choi, Y. Optimization of AP placement and channel assignment in wireless LANs. In Proceedings of the LCN 2002. 27th Annual IEEE Conference on Local Computer Networks, Tampa, FL, USA, 6–8 November 2002; pp. 831–836.
16. Akl, R.; Arepally, A. Dynamic channel assignment in IEEE 802.11 networks. In Proceedings of the PORTABLE07 International Conference on Portable Information Devices, Orlando, FL, USA, 25–29 May 2007; pp. 1–5.
17. Akella, A.; Judd, G.; Seshan, S. Self-management in chaotic wireless deployments. *Wirel. Netw.* **2007**, *13*, 737–755.
18. Cordeschi, N.; Amendola, D.; Shojafar, M.; Baccarelli, E. Distributed and adaptive resource management in Cloud-assisted Cognitive Radio Vehicular Networks with hard reliability guarantees. *Veh. Commun.* **2015**, *2*, 1–12.
19. Zahra, P.; Kang-Cheng, C.; Chia-Mu, Y.; Mauro, C. RARE: Defeating Side Channels based on Data-Deduplication in Cloud Storage. In Proceedings of the International Conference on Computer Communications: Cloud Computing Systems, Networks, and Applications (INFOCOM CCSNA), Honolulu, HI, USA, 15–19 April 2018; pp. 1–6.
20. Nosrat-Makouei, B.; Andrews, J.G.; Heath, R.W. MIMO Interference Alignment Over Correlated Channels With Imperfect CSI. *IEEE Trans. Signa Process.* **2011**, *59*, 2783–2794.
21. Nauryzbayev, G.; Seilov, S. Impact of antenna correlation and imperfect csi on interference alignment in compound MIMO BC. In Proceedings of the International Conference on Information and Communication Technology Convergence, Jeju, Korea, 19–21 October 2016; pp. 544–548.
22. Chen, X.; Yuen, C. On Interference Alignment With Imperfect CSI: Characterizations of Outage Probability, Ergodic Rate and SER. *IEEE Trans. Veh. Technol.* **2016**, *65*, 47–58.

23. Yu, H. A Review on Interference Alignment in Multiuser Interference Channels. *Wirel. Pers. Commun.* **2015**, *83*, 1751–1764.
24. Lau, V.K.N.; Rao, X.; Ruan, L. CSI Feedback Reduction for Mimo Interference Alignment. *IEEE Trans. Signa Process*. **2015**, *61*, 4428–4437.
25. Zhang, J.; Lei, X.; Shi, J.; De, L. Simulation study and performance analysis on Zigbee system with CCI. In Proceedings of the Wireless and Optical Communication Conference, Chengdu, China, 21–23 May 2016; pp. 1–4.
26. Backes, F.; Vacon, G.; Callahan, P.; Hawe, W.R.; Durand, R. Program for Adjusting Channel Interference between Access Points in a Wireless Network. U.S. Patent US7774013A1, 10 August 2010.
27. Yuan, W.; Wang, X.; Linnartz.; J.-P.M.G. A Coexistence Model of IEEE 802.15.4 and IEEE 802.11b/g. In Proceedings of the 2007 14th IEEE Symposium on Communications and Vehicular Technology in the Benelux, Delft, The Netherlands, 15 November 2007; pp. 1–5.
28. Tytgat, L.; Yaron, O.; Pollin, S. Analysis and experimental verification of frequency-based interference avoidance mechanisms in IEEE 802.15. 4. *Netw. IEEE/ACM Trans.* **2015**, *23*, 369–382.
29. Shi, G.; Xu, R.; Shu, Y. Exploiting temporal and spatial variation for WiFi interference avoidance in ZigBee networks. *Int. J. Sens. Netw.* **2015**, *18*, 204–216.
30. Lee, L.; Kang, G.; Zhang, X. An interference avoidance strategy for zigbee based WeHealth monitoring system. In Proceedings of the IEEE, International Conference on E-Health Networking, Applications and Services, Beijing, China, 10–13 October 2012; pp. 68–72.
31. Yan, Y.; Yang, P.; Li, X.Y. Wizbee: Wise zigbee coexistence via interference cancellation with single antenna. *Mob. Comput. IEEE Trans.* **2015**, *14*, 2590–2603.
32. Almeida, E.; Cavalcante, A.M.; Paiva, R.C.D. Enabling LTE/WiFi coexistence by LTE blank subframe allocation. In Proceedings of the 2013 IEEE International Conference on Communications (ICC), Budapest, Hungary, 9–13 June 2013; pp. 5083–5088.
33. Zubow, A.; Sombrutzki, R. Adjacent channel interference in IEEE 802.11n. In Proceedings of the 2012 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, China, 1–4 April 2012; pp. 1163–1168.
34. Tan, W.L.; Bialkowski, K.; Portmann, M. Evaluating Adjacent Channel Interference in IEEE 802.11 Networks. In Proceedings of the IEEE Vehicular Technology Conference, Taipei, Taiwan, 16–19 May 2010; pp. 1–5.
35. Xiao, J.; Wu, K.; Yi, Y. Pilot: Passive device-free indoor localization using channel state information. In Proceedings of the 2013 IEEE 33rd International Conference on Distributed Computing Systems (ICDCS), Philadelphia, PA, USA, 8–11 July 2013; pp. 236–245.
36. Abdel-Nasser, H.; Samir, R.; Sabek, I.; Youssef, M. MonoPHY: Mono-stream-based device-free WLAN localization via physical layer information. In Proceedings of the Wireless Communications and Networking Conference (WCNC), Shanghai, China, 7–10 April 2013; pp. 4546–4551.
37. Draft, W.G. *Telecommunications and Information Exchange Between Systems-LAN/MAN Specific Requirements-Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specification: Specification for Radio Resource Measurement*; IEEE Stdandard: Piscataway, NJ, USA, 2003.
38. Angelakis, V.; Papadakis, S.; Siris, V.A.; Traganitis, A. Adjacent channel interference in 802.11a is harmful: Testbed validation of a simple quantification model. *Commun. Mag. IEEE* **2011**, *49*, 160–166.
39. Chieochan, S.; Hossain, E.; Diamond, J. Channel assignment schemes for infrastructure-based 802.11 WLANs: A survey. *IEEE Commun. Surv. Tutor.* **2010**, *12*, 124–136.
40. Sin, T.W.; Halim, M.N.; Naredula, J.R.; Fang, M.H.; Payne, K. Quality of Transmission across Packet-Based Networks. U.S. Patent US20020051464A1, 2 May 2002.
41. Abdelnasser, H.; Youssef, M.; Harras, K.A. Wigest: A ubiquitous wifi-based gesture recognition system. In Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM), Kowloon, Hong Kong, China, 26 April–1 May 2015; pp. 1472–1480.
42. Wang, J.; Xie, B.; Fang, D.; Chen, X.; Liu, C.; Xing, T.; Nie, W. Accurate Device-Free Localization with Little Human Cost. In Proceedings of the 1st International Workshop on Experiences with the Design and Implementation of Smart Objects, Paris, France, 7 September 2015; pp. 55–60.
43. Chang, C.C.; Lin, C.J. LIBSVM: A library for support vector machines. *ACM Trans. Intell. Syst. Technol.* **2011**, *2*, 1–27.

44. Wang, W.; Liu, A.X.; Shahzad, M. Gait recognition using wifi signals. In Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing, Heidelberg, Germany, 12–16 September 2016; pp. 363–373.
45. Borella, M.S.; Swider, D.; Uludag, S.; Brewster, G.B. Internet Packet Loss: Measurement and Implications for End-to-End QoS. In Proceedings of the International Conference on Parallel Processing Workshops, Minneapolis, MN, USA, 14 August 1998; pp. 3–12.
46. Zhao, L.; Fan, C. Enhancement of QoS differentiation over IEEE 802.11 WLAN. *Commun. Lett. IEEE* **2004**, *8*, 494–496.
47. Halperin, D.; Hu, W.; Sheth, A.; Wetherall, D. Linux 802.11n CSI Tool. Available online: http://dhalperi.github.io/linux-80211n-csitool/ (accessed on 20 March 2017).
48. Zhang, Z.L.; Chen, H.M.; Huang, T.P. A channel allocation scheme to mitigate Wifi interference for wireless sensor networks. *Jisuanji Xuebao (Chin. J. Comput.)* **2012**, *35*, 504–517.
49. H3C, The Leader in Digital Solution. H3C Corp. Available online: http://www.h3c.com.hk (accessed on 10 April 2017.).
50. Uellenbeck, S.; Dürmuth, M.; Wolf, C.; Holz, T. Quantifying the security of graphical passwords: The case of android unlock patterns. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany, 4–8 November 2013; pp. 161–172.