Journal Title
XX(X):1–15
©The Author(s) 2017
Reprints and permission:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/ToBeAssigned
www.sagepub.com/
SAGE

Defeat Your Enemy Hiding Behind Public WiFi: WiGuard Can Protect Your Sensitive information from CSI-based Attack*

Jie Zhang[1], Zhanyong Tang[1], Meng Li[1], Xiaojiang Chen[1], Dingyi Fang[1], Zheng Wang[2]

Abstract

As WiFi becomes increasingly popular, CSI-based attack has attracted much attention , which uses channel state information (CSI) of public Wi-Fi to exploit the strong correlation between the CSI fluctuation and the pattern lock or keystrokes to infer the user's input. Obviously, this new attack form can obtain the gesture privacy more far away from target and without any displayed information on the screen, so past proposals will perform poorly in the new attack scenarios.

To defeat CSI-based attack, we propose a protection system WiGuard. Unlike prior work that considers channel interference as a harmful effect to avoid, our design exploits channel interference to protect gesture sensitive information. The intuition underlying our design is that we can interfere the attacker's wireless transmitter to distort the CSI signal. We explore a simple but functional hop channel solution to increase the packet loss of CSI channel, our approach automatically detects when a CSI-based attack happens, and it also determines where to place a safe wireless transmitter to introduce interference without greatly affecting normal network traffics. We evaluated our approach by applying it to protect the user's pattern lock on mobile phones and the keystroke records of pc. Experimental results show that our approach is able to reduce the success rate of CSI-based attack from 92%to 42% for single keystrokes and from 82.33% to 21.67% for unlock patterns.

Keywords
CSI-based attack, channel interference, sensitive information protection

Introduction

Smartphones and tables are usually used in public places (such as cafes, hotels, shopping malls, airports, etc.) and connected to the public WiFi. However, in such an environment, using mobile devices, by analyzing the influence of user's fingertip movement on the channel state information (CSI) of WIFI signals when they enter the password, we can open the back door for attackers who can steal user passwords.We call this kind of attack as "CSI-based attack".

Unlike traditional shoulder surfing attack uses direct observation techniques, looking over someone's shoulder, to get information such as passwords, PINs, security codes, and similar data oxf (2007). CSI-based attack can recognize the users' gesture privacy (PIN, Pattern Lock, Keystrokes etc.) only by one Public Wi-Fi AP Ali et al. (2015), but not need to use any other vision-enhancing devices in long distance. Moreover, using Commercial Off-The-Shelf (COTS) such as NICs 5300, the adversaries can commit a successfully attack to get your pattern lock Zhang et al. (2016) even without obtaining any information displayed on themishra:weighted screen. Worst of all, with professional techniques such like MIMO beamforming Wang et al. (2014), the more fine-grained CSI of mouth motions could leakage your whipers.

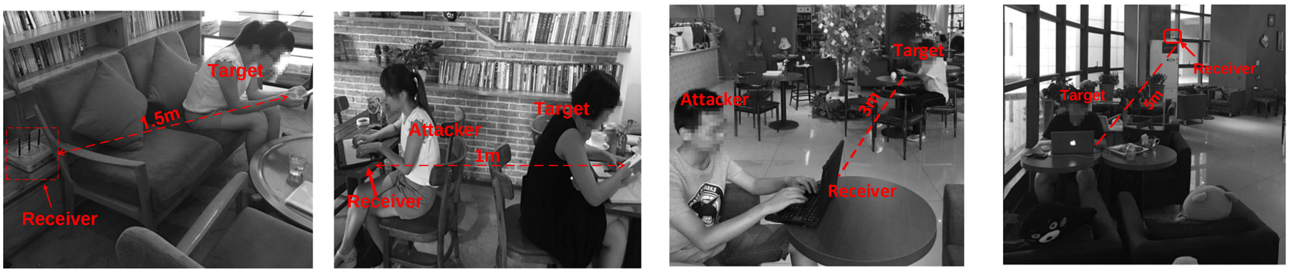
As shown in Figure 1, to launch the new attack called CSI-based attack, there is only just one thing needed, and it is that the attacker toolkits and the target devices access the same online public WiFi simultaneously. Unfortunately, these things almost happen all the time in KFC, Modoload, or StarBack Coffee Bar, etc.

So what is the rationale that goes behind making these CSI-based attack so easy for attackers? The key sight of these attacks is that CSI characterizes the channel frequency response, and the signal at the receiver end is a superposition of multipath propagation, which the multipath comes from the wall and the surrounding objects. When a user performs

[1]School of Information Science and Technology, Northwest University, Xi'an, P.R. China
[2]School of Computing and Communications, Lancaster University, UK

Corresponding author:
Zhanyong Tang
Email: zytang@nwu.edu.cn

*Extension of Conference Paper: a preliminary version of this article entitled "Protect Sensitive Information Against Channel State Information Based Attacks" by J. Zhang et el. appeared in International Conference on Computational Science and Engineering(CSE), 2017 Zhang et al. (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 use WiGuard to protect sensitive information and give the user a choice for position and channel to optimize the system performance; (3) it provides new experimental results to evaluate the influence of packet loss rate on success rate and provides proof for 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.



(a) scenario 1 **(b)** scenario 2 **(c)** scenario 3 **(d)** scenario 4

Figure 1. Attack Scenarios. The target is doing gesture privacy in public place, and the attacker receives the gesture-related CSI values using NICs in scenario 1 and scenario 4 while in scenario 2 and scenario 3, the attacker using her laptop to receive the gesture-related CSI values.

different gestures, the multipath for different gestures will be different, thus different gestures will generate their unique patterns in time-series CSI values.

However, it is not enough to simply obtaining CSI values, the fine-grained of CSI is reuqired to commit a CSI-based attack well. In order to capture the subtle differences between gestures, the CSI must be measured at a fine-grained level. This is often done by sending high-frequent ICMP packets to the target AP[†] to obtain a high frequent sample rate by analyzing the response packets sent by the target AP. For instance, the work presented in Ali et al. (2015) requires the attacker to send at least 2500 ICMP packets per second to the target AP. Therefore, obtaining high-frequent, fine-grained CSI measurements is key to the success of CSI-based attacks.

As analyzed above, the more fine-grained the CSI is, the easier the attacker will obtain gesture privacy. For users to protect their gesture privacy, inspired by Rouf et al. (2012), the user can reduce the rate of the ICMP ping packets or make the attacker's receiver lose ICMP ping packets, a low ICMP ping packets cannot capture the difference details between different gestures, and the attacker will not decode the gestures successfully. While there are a number of methods available to drop ICMP responses Wikipedia (2016), the communication quality of the target device cannot be ignored. Our approach to this issue is to exploit the fact that the communication quality of the target AP will decrease if there exists another AP uses a channel next to the target APs working channel.

This paper introduces WiGuard, unlike prior work Qiao et al. (2016), which proposes a black sensor obfuscation technique, needs additional hardwares, WiGuard explores the potential of adjacent channel interference to defeat the CSI-based attack and prevent public WiFi from leaking users' gesture privacy. In order to do so, knowing which public WiFi is being leveraged to obtain CSI values by an attacker is an important first step for an user to take measures of protection. 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 detect which channel the target public AP works on, then switch a safe wireless transmitter (as described in section) to a proper channel to interfere the target public AP. All in an effort is to make the wireless receiver end to lose massive key packets of CSI data, so that the attackers can't recover the corresponding gesture privacy signals correctly.

To reduce the impact to the user, our approach automatically detects when an attack is likely to happen by monitoring the network activities, and only switches on the protected scheme if an attack is detected. Different from past approaches Xu et al. (2011) Villegas et al. (2007), which consider channel interference as detrimental and seeks reasonable channel assignment method to avoid channel interference Mishra et al. (2005) Lee et al. (2002) Akl and Arepally (2007) Akella et al. (2007). WiGuard exploits channel interference to prevent wireless signals from leaking users' privacy. To transform the above idea into a practical, feasible system, we need to solve the following challenges:

(1) *When the users access the public WiFi, how do they know whether there exists an attacker in current public WiFi?* From the CSI-based keystrokes recognition Ali et al. (2015), we know that the receiver needs to continuously pings the wireless transmitter 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 the public place.

(2) *How to increase the packet loss of CSI channel so as to distort the corresponding gesture privacy signals obtained by attackers, while does not affect the public WiFi network to correspond normally?* After detecting the channel of public wireless transmitter, the channel of a safe wireless transmitter is switched to interfere the attacker's obtained wireless signals. However, there are many adjacent channels that can be switched to interfere the attacker. For example, when the target public AP is 6, the safe wireless transmitter can switch to channel 4 or channel 5, which channel should the safe wireless transmitter switch so that the channel interference between the safe wireless transmitter and the target public AP can achieve the maximum meanwhile the normal users' network services on the target public AP are not affected by the channel interference.

(3) *How can we choose a proper distance for 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 the public places, if the distance between the safe wireless transmitter and the normal APs is short, then the channel switch of the safe wireless transmitter

[†] We define the public AP that the attacker leverages as target public AP.

may interfere the normal public APs[‡]. If the safe wireless transmitters are far away from the normal public APs, then the channel switch of the safe wireless transmitter will not influence 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 if the user choose their smart devices as the safe wireless transmitter; if the user choose the normal public AP as the safe wireless transmitter, the system will give a choice of normal public AP.

Summary of Results: We built a prototype of WiGuard and evaluated it in different conditions. Our extensive experiments lead to the following findings:

- In order to interfere the attacker's received packets, the channel spacing between safe wireless transmitter and the target public AP is 1, which can interfere the target public AP to the greatest extent.
- in order not to interfere the other normal public APs, the distance between the safe wireless transmitter and the normal public APs should be less tan 4m.
- The paper demonstrates that channel interference can defeat CSI-based attack by recovering the unlock patterns for smart phone and the keyboards of pc. The recovery accuracy of them are separately 82.33% and 92% when there exists no channel interference; when there exists channel interference, the recovery accuracy of them are separately 21.67% and 42%.

Contributions: This paper makes the following contributions:

- It analyzes the essence of CSI-based surfing 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 good protective effect and the success rate of CSI-based attack decreases dramatically.
- It is a working system and evaluates it in real-word environment. The results demonstrate that the system doesn't influence the normal network service.

Background

Threat Model

A scenario is considered where attackers try to identify user's gesture privacy in a series of time series CSI values generated by user gestures, and attackers do not need to be close to users or on user screens. We assume that an attacker can access public WiFi at a high rate of Ping public WiFi AP and use a receiver to receive the time series CSI value. Two representative scenarios the attack is reasonable are: (1) the receiving end of attackers in public places is not obvious to be ready (for example NIC) in public places, or in the hidden settings receiver suspicious; (2) the attackers pretend to use his laptop to work in a public place, he looks normal.

For scenario 1, as shown in Figure 1a, the user unlocks the device while the attacker uses the network NICs to receive the CSI value, the attacker is away from the user, and the prepared network NICs stays near the user. However, the location of the network NICs is hidden, and the user does not notice the receiver. For scenario 2, as shown in Figure 1b, an attacker pretends to work on a laptop computer used to receive CSI values. The attacker looks normal so that the user won't perceive him/her.

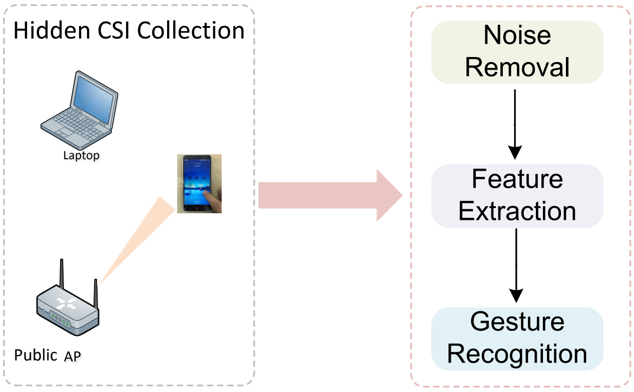


Figure 2. The process of CSI-based attack. When the attacker obtains the CSI values of gesture privacy, after noise removal, feature extraction, the attacker will decode the gesture successfully.

CSI-based Attack

With more and more public places deploying public WiFi, CSI has received much attention Xiao et al. (2013) Abdel-Nasser et al. (2013), and because of rich information that CSI contains, it can be used to detect micro motions, such as finger motions Ali et al. (2015) Zhang et al. (2016) and mouth motions Wang et al. (2014).Using a commercial receiver, an attacker can obtain a user's PIN, password, or other gesture information for gestures. In this section, we first show why CSI can detect and restore gesture privacy, and then will introduce a novel attack, CSI-based attack.

Overview of CSI

Channel state information(CSI) contains fine-grained information of wireless signals and it is the characterization of variations in the wireless channel and it can be obtained by WiFi network interface controllers (NICs). Let N_{Tx} represents the number of transmitting antennas, N_{Rx} represents the number of receiving antennas, what received at the receiver end will be $30 \times N_{Tx} \times N_{Rx}$ CSI streams, which 30 means there are 30 subcarriers for a received packet.

CSI-based Gesture Privacy Recovery Model

The CSI value can be used to restore gesture privacy .movement from a particular part of the body will introduce relative multi-path propagation of the wireless signal when the user is gesturing privacy,and different motions correspond to different multi-path propagation, therefore a

[‡] Definition 1: When two wireless transmitters are in the 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 and the distance ca 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.

unique pattern will be generated in the sequence CSI value by a certain motion, and the uniqueness can be used to restore the privacy of the gesture.

For the CSI-based gesture privacy recovery model, several steps are required to successfully identify. First, noise needs to be removed from the signal obtained. After noise removal, it is necessary to extract the actual affected part of the signal track from the collected signal, and then use the gesture recovery methods to restore the gesture privacy, as shown in Figure 2.

1)Noise Removal

The CSI values 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 values to recover gesture privacy, such inherent noise need to be removed from CSI time-series values.

There are many methods for CSI-based gesture privacy recovery system 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 values usually start to be collected before the gestures start and end to be collected after the gestures end. So, after removing noise from obtained signals, the actual influenced signal traces need to be extracted from time-series CSI values.

When the gesture starts, the CSI waveforms will show a similar rising or falling tends. Thus, a simple method, sliding window, can be used to extract the features. However, the gestures that users always do can be classified into two categories, one is consecutive gestures, and another is discrete gestures. For consecutive gestures, there exists no pause in gestures performing process, such as unlock patterns on Android screen and applications; while for discrete gestures, there exists pause in gesture performing process, such as keystrokes of laptops or digital unlock passwords. For discrete gestures, the system first segments the time-series CSI values into individual motions, then extract the features for each individual motion.

After making sure the starting and ending point, for each gesture, Pricipal Component Analysis (PCA) method can be used to extract the signals that only contain variations caused by the certain gestures on the filtered subcarriers so that even for similar gestures, the extracted features are also different and the system can get a high recovery accuracy for those similar gestures.

3) Gesture Privacy Signal Recovery

After extracting features, gesture privacy recovery methods will be applied to recover gestures. There exists similarity between speech recognition and gesture recovery, thus, a well-established technique, Dynamic time warping (DTW) that borrowed from speech recognition can be used to recover the gesture privacy.

DTW calculates the distance between the two waveforms and the shorter the distance is, the more similar the two waveforms will be. A hierarchical approach can be used to reduce the computational complexity and computational cost, or the DTW distance can be used as the input and the system will train a classifiers using the distance and all those gesture features. Then the system will recover the gestures from each classifier.

CSI-based Attack

Shoulder surfing attack, which the attacker obtain the users' passwords by direct observation or by recording the user's authentication session, is a known risk and a special concern when people input their personal privacy information in public places Wiedenbeck et al. (2006). The user's defense is to shield the screen with an object or his/her body. However, in public places, the attacker can obtain your gesture privacy information through public WiFi instead of direct observation and it is called CSI-based attack. Unlike traditional shoulder surfing attack, the attacker doesn't observe the user's screen directly, as shown in Figure 1, the attacker is far away from the user and doesn't need to have control of the user's screen. Qiao et al. Qiao et al. (2016) also demonstrate that gesture privacy can be obtained by using WiFi signals.

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

After obtaining the wireless signals associated with gesture privacy, the gestures can be decoded successfully by the attacker using noise removal, feature chosen and gesture recognition techniques, as shown in Figure 2. In order to achieve CSI-based attack, there are several requirements that the attacker successfully decode the gesture privacy,which can be equivalent to the following equation:

$$\textit{CSI-based Attack} \Leftrightarrow (\textit{Wireless Transmitter, Signal Receiver, ICMP ping packets at a high rate from transmitter, Communication Channel between Transmitter and Receiver, } Quality_{CSI})$$

The specific understanding of the above equation is 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 values . In order to characterize the fine-grained degree of different gestures, especially for those similar gestures, the ICMP Ping packets from the emitter must be at a very high speed. In addition, the communication channel between the transmitter and the receiver must remain stable. Once the communication channel is disturbed and unstable, the receiver will not receive the ICMP Ping packet from the sending side, which will lead to incomplete the time-series CSI values. $Quality_{CSI}$ describes the quality of received time-series CSI values, if the wireless signal interference in multi-path propagation,it will be changed when it reaches the receiving end, and the received time-series CSI values will be different, this will cause the CSI waveform distortion.

WiGuard Overview

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. 2.4 GHz is divided into 13 frequency bands[§] Draft (2003), and each frequency band is 22 MHz. However, there are 13 channels in 100 MHz frequency band. That will lead to more or less overlaps between frequency bands and the overlaps between frequency band will cause channel interference.

However, when the cental frequency spacing of two frequency bands is more than 22MHz, 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 other two groups of channels that doesn't interfere with each other, and they are channel 2, channel 7, channel 12; channel 3, channel 8 and channel 13. For 13 channels, there are 4 channels that are overlapped with the same channel. Thus, if an AP uses a ceratin channel, its neighbor AP must use one channel of the remaining unoverlapped 8 channels, otherwise, there will exist channel interference between these two neighbor APs.

Furthermore, among the overlapped 4 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 overlaps between channel 2 and channel 1 is 77.27% while the overlaps between channel 3 and channel 1 is 54.55%. Thus, the channel interference between channel 2 and channel 1 is different from that between channel 3 and channel 1.

Prior researches have also demonstrated that adjacent channel is harmful Angelakis et al. (2011) Zubow and Sombrutzki (2012) in 802.11 network, Akella et al. Akella et al. (2007) validate that when there are a plenty of wireless transmitters in a region, the co-channel interference will greatly reduce the network output and the output of TCP reduces from 9Mbps to 2Mbps, the output of UDP also reduces and it reduces from 9.7Mbps to 8.6Mbps. In order to keep the neighbor wireless transmitters non-interfering with each other, there are many channel assignment methods proposed for WLANs Mishra et al. (2005) Lee et al. (2002) Chieochan et al. (2010) Akl and Arepally (2007).

System Overview

In order to resist the CSI-based attack, a protection system WiGuard is designed which destroys the $Quality_{CSI}$ with channel interference,and is a necessary condition for the success of the CSI-based attack. In this section, we introduce the system design. First, *ICMP based Attacker AP Acquirement* detects whether there are abnormal ICMP Ping packets caused by the CSI value collected by an attacker. So, if there is no abnormal ICMP Ping packet, the user can do their gestures; instead, if it exists, the user should detect the target public AP work in which channel,and then switch the channel of a safe wireless transmitter to a proper channel to interfere with the attacker, as shown in Figure 3.

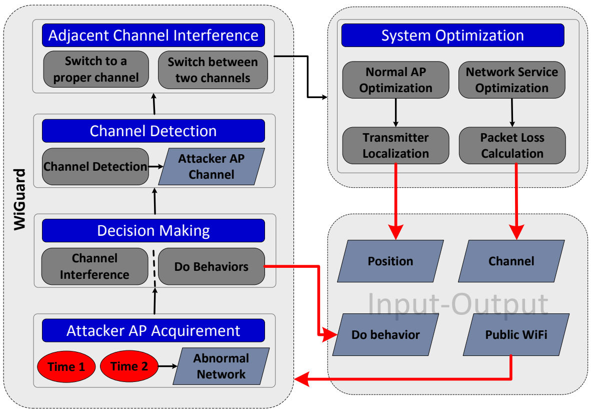


Figure 3. System overview.

Attacker AP Detection

Attacker AP Characteristics

In order to successfully decode the users' gesture privacy information, the attacker should have a fine-grained CSI values. Coarse-grained CSI values can't characterize the difference between gestures, especially for those micro motions, such as digital unlock passwords of smart phones, keystrokes of laptops. However, CSI values are measured on ICMP ping packets. Thus, in order to obtain fine-grained CSI values, the attacker's receiver needs to continuously ping packets from public AP at a high rate, such as in order to decode the keystrokes of laptops successfully, the rate of ICMP ping packets should be 2500 packets/s Ali et al. (2015).

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 Sin et al. (2002). So, 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 values, the attacker's receiver will continuously ping packets from public AP at a high rate, and there will exist plenty of ICMP ping packets in the network.

Attacker AP Detection

Based on the analysis mentioned above, xxxx , whether there exist ICMP ping packets and the number of ICMP ping packets per unit of time can be used to detect whether the public AP is leveraged by the attacker to collect CSI values. If a public AP is detected to exist plenty of ICMP ping packets during different time periods, then it is very likely caused by an attacker who is pinging the public AP st a high rate, and we think there exist an attack in the public place.

However, generally in public places, there is not only one public AP, an attacker may use two or more public APs to improve the CSI-based attacks success rate, Abdelnasser et al. Abdelnasser et al. (2015) demonstrated using multiple APs can improve the accuracy of recovery. Thus, in public

[§] In this paper, only channel 1 to channel 13 are considered just because the channel 14 is only used in Japan and only 802.11b can support the channel 14 in Japan.

places, attackers can use more public APs, not just one public AP to decode gestures privacy successfully. Therefore, in order to ensure that attackers don't use all potential public AP to collect CSI values, users need to surf all public APs to detect how many public APs the attacker used.

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

Adjacent Channel Interference

After detecting the channel that the target public APs work on, adjacent channel interference will be used to protect the user's gesture privacy. However, how should the channel of a safe wireless transmitter change when the number of target public APs is different? Which channel should the safe wireless transmitter switch so that the packet loss rate caused by channel interference is the maximum? Then we will give details of adjacent channel interference protection method.

Safe Wireless Transmitter

In order to interfere the channel of the target public APs, the channel of a safe wireless transmitter need to be switched. The safe wireless transmitter can be the normal public APs in the public place. The user can also use his/her devices with hotspot functionality as the safe wireless transmitters, such as his/her 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 the attacker.

Channel Switch

After detecting the channels, a safe wireless transmitter will switch its channel to interfere the attacker. However, there are four adjacent channels that can interfere the same channel, from the above analysis in section , 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 that caused by the channel interference will also be different, so which channel should the safe wireless transmitter switch to interfere the attacker so that the packet rate loss will be the maximum?

Theoretically, when the channel spacing between two adjacent AP is 1, the channel interference between the two channels is the largest, because the overlap between the two channels is the largest. Therefore, switching the safe wireless transmitter to the adjacent channel can achieve the purpose of jamming the attacker. The channel spacing between the secure wireless transmitter and the target public AP is 1.

However, in most cases, attackers can use two or more public APs to collect CSI values in order to improve the success rate. How the secure wireless transmitter switch channel to interfere with all the target public APs.There are two cases considered here. One is the secure wireless transmitter only needs to switch to the right channel. The other is the secure wireless transmitter needs to switch between two channels to interfere all the target public APs, so as to prevent attackers from acquiring CSI values.

(a) **Switch to a proper channel**

When the channel of the secure wireless transmitter switches to the appropriate channel, the CSI signals that the attacker receives will lose the packets in two different cases. In the first case, the public places have only one target public AP, the channel of wireless transmitter can be switched to a adjacent channel, for example,when the target public AP is working on channel 6, users will be able to switch the channel of the secure wireless transmitter to channel 5 or channel 7. In another case, when the public places have two or more public APs, and the channel spacing of all target public APs is less than 5, the channel of the secure wireless transmitter can be switched to the right channel to interfere with attackers, for example,the channels of two target public APs are channel 1 and channel 6, then the secure wireless transmitter can switch to channel 3 or channel 4.

In the second case, we can switch the secure wireless transmitter to the appropriate channel to interfere with the attacker, but in order to maximize the packet loss rate, we can switch the secure wireless transmitter between the two channels.

(b) **Switch between two channels**

If the channel interval between the target public AP is greater than 5, the secure wireless transmitter can switch between the two channels to achieve interference. For example, when there are abnormal network activities detected in two public APs, and the channels of the two target public APs are channel 1 and channel 11 respectively, then the secure wireless transmitter needs to switch between channel 2 and channel 10.

System Performance Optimization

When channel interference protection method is used to protection users' gesture privacy, in order not to affect the normal communication of public wireless network, the system need to be optimized from two folds: in 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. In another 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 comes from the distance between them and the channel spacing between their channel. The smaller channel spacing is, the stronger the channel interference between those two wireless transmitters will be. However, when the two wireless transmitters are far away from each other, even when they work on adjacent channel, there will not exist channel interference between them.

From the analysis above, the safe wireless transmitter can be set to be far away from normal public wireless transmitters and to be near to the target public APs, so that after switching the channel of the safe wireless transmitter, the channel interference will not exist between the former and it will only exist between the latter. Thus, we need to localize the distance between the safe wireless transmitters

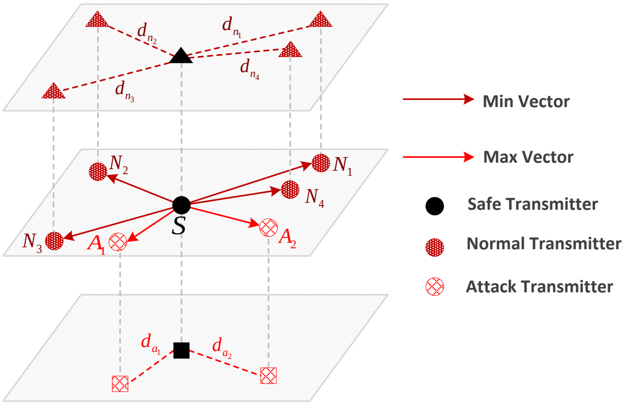


Figure 4. Interference vector

and all the public wireless transmitters,and then after the localization, the system will give a proper position for the safe wireless transmitters when the user uses his own devices as the safe wireless transmitters, or the system will give a proper choice for the safe wireless transmitters from all those normal wireless transmitters.

System Optimization Model

Based on the analysis above, the strength of channel interference can be mapped into a function *f(d,channel)*, then a 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*, which *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.

In order not to interfere the normal public wireless transmitters, *min vector* will give a proper position where the safe wireless transmitter is not the neighbor of normal wireless transmitters and is the neighbor of the target public AP. In order not to affect the normal network service of target public AP, *max vector* will give a proper channel which after the safe wireless transmitter switches to the channel, the channel interference between the safe wireless transmitters and the target public APs is the strongest, and the packet loss rate for the attacker received CSI values can achieve maximum while the packet loss rate for the normal network service can achieve minimum. The mapped expressions of *min vector* and *max vector* can be written as the following two equations:

min vector

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

max vector

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

under the following constraints:

(i) Distance constraint:

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

(ii) Channel constraints:

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

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

Which 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 that the two wireless transmitters can be neighbors, as shown in the definition of neighbors in definition 1, the footnote in Page 2.

The distance constraint can be interpreted as follows: in order to interfere 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 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.

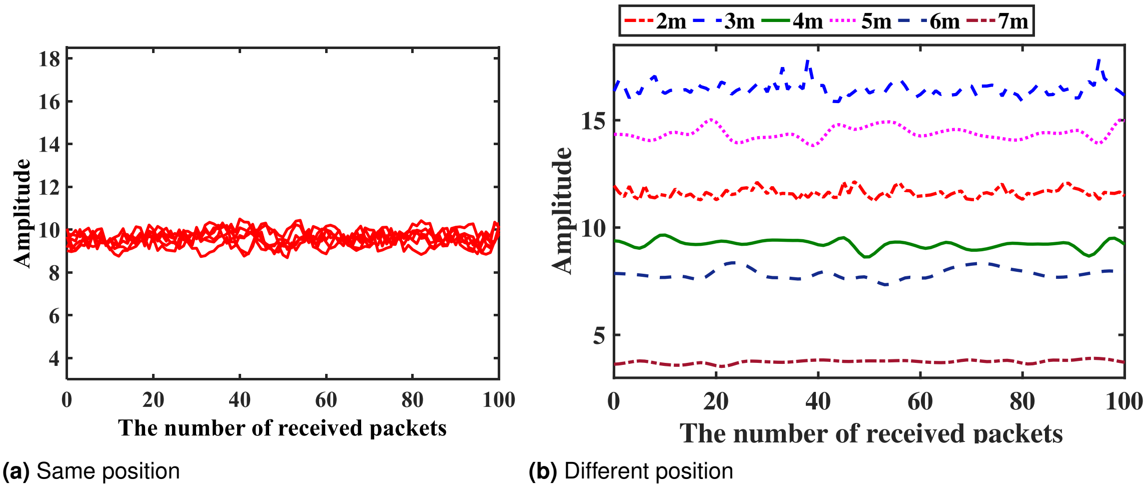
The interpretation of channel constraint is as follows: in order to interfere the CSI values that the attacker received so that the attacker can't recover the gesture privacy, the packet loss rate for CSI values need to be larger than the threshold δ; in order not to effect the normal network service, the packet loss rate of QoS should be smaller than the threshold γ.

CSI-based Localization for wireless transmitters

There are many methods to locate the public wireless transmitters, for example, Wang et al.Wang et al. (2015) propose an accurate localization method by using received signal strength (RSS). However, RSS is related to the transmit power of the APs, and the attacker may change the transmit power to confuse the user to get the position of the public wireless transmitters in the public place. Thus, RSS-based localization method is not feasible in the public place and CSI-based localization method is used to locate the public wireless transmitters in this paper.

As mentioned above, a gesture can generate an unique pattern in CSI values, however, different positions can also generate different patterns in CSI values, thus, CSI can be used to do localization for public wireless transmitters. As shown in Figure 11a, the CSI values of the same position are always the same at different periods of time, and the CSI amplitude values in Figure 11a are from 8.6 to 10.6. We can see from Figure 11a that the CSI values of different positions are different and when two positions are near each other, their CSI values are also similar; when the two positions are far away from each other, their CSI values will be totally different.

When CSI values are used to do localization for public wireless transmitters, first we need to remove the noise from obtained signals, then in order to reduce the computational complexity, PCA is used to reduce the dimension of CSI values, then the system will locate the public wireless transmitters. The following will introduce the details.



(a) Same position **(b)** Different position

Figure 5. CSI values for different positions

Noise Removal using DWT

As mentioned in section , the obtained CSI values contain much noise, so noise need 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.

Dimension Reduction using PCA

What received in the receiver is a sequence of CSI values and each CSI represents the amplitudes and phases on group of subcarriers. For example, when the receiver is Intel 5300 NICs with N_{TX} transmit antennas and N_{RX} receiver antennas, the CSI vales in the receiver end will be $30 \times N_{TX} \times N_{RX}$ streams. Thus, when CSI values are used to do localization, dimension of CSI values need to be reduced in order to reduce the computational cost.

In this paper, the dimensionality of CSI values is reduced by PCA, because PCA can recognize which subcarries 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 on CSI values dimension reduction includes the following steps.

Processing:

A matrix H presents the CSI time-series data with $30 \times N_{TX} \times N_{RX}$ streams that is after noise removal. Every column of H represents the CSI data 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 calculate and the corresponding mean values is 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 eigenvalues and eigenvectors of covariance will be also calculated.

Main Eigenvalues Chosen:

Eigenvalues is sorted from large to small and we choose the matrix k number of Eigenvalues. Then the corresponding k Eigenvectors will form a Eigenvector matrix.

Location using DTW and SVM

As mentioned above, DTW is used to compare the waveforms of different gestures, it can also be used to compare the waveforms of different positions. In this paper, DTW is used to localize the public wireless transmitters. DTW calculates the distance between the waveforms of two positions, and the shorter the distance is, the more similar the two waveforms will be. We build a classifier to localize the wireless transmitters based on their waveform shapes and the DTW distances, and our classifier adopts SVM classification scheme, which allows all the positions to be differentiated based on the training dataset.

Packet Loss Rate Calculation

When channel interference is used to interfere the attacker's obtained CSI values, the essence is making attacker lose ICMP ping packets. However, how many packets the attacker lose so that the attacker can't decode the gestures privacy successfully? For public APs, in order not to influence the network service for the normal users, the packet loss rate for the network service should be less than a threshold.

Packet Loss Rate (QOS)

For real-time applications, such as Internet telephony or video conference, the quality of service (QoS) will degrade when the packet loss is excessive Borella et al. (1998). However, the real-time applications are not sensitive to packet loss, and the packet loss rate of $1\% \sim 3\%$ is acceptable in most cases Zhao and Fan (2004).

In public places, people often surf the Internet, watch online videos, online chat 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.

Packet Loss Rate (CSI)

In order to obtain a high success rate of gesture privacy, the attacker need to obtain fine-grained CSI time-series values. In this part, we will discuss the influence of packet loss rate on success rate. What the attacker received from his receiver is a sequence of CSI values and the $Quality_{CSI}$ is measured by packet loss rate. For gestures recovery, feature length (the number of received packets after feature chosen) can be a factor to differentiate different gestures. For example, the feature lengths of simple unlock patterns and complex

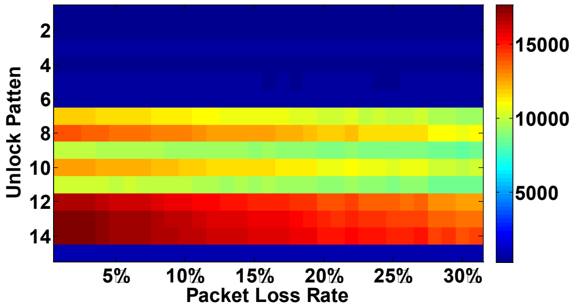


Figure 6. Influence of packet rate loss on success rate

unlock patterns on smart devices are usually different. If the influenced signal traces that the attacker received is not complete, the attacker will decode the complex unlock patterns as simple unlock patterns.

However, if the packet loss rate is small and just lose several packets, it will not influence the results of success rate. However, if $Quality_{CSI}$ is large than a threshold, it will influence the results of success rate greatly and the success rate will decrease dramatically.

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

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

Implementation

We implement WiGuard on current TP-Link wireless routers in the corridor and in a room in indoor environment.

Experiments setup

The TP-Link wireless router and intelligent device with wireless hotspot functions are wireless transmitters respectively, and the desktop with Intel 5300 NIC (Network Interface Controller) is used as a receiver. The work of the transmitter follows the IEEE 802.11n protocol. The receiver is deployed with 3 antennas, and the firmware reports CSI to the upper layers. One end of the receiver continuously pings packets, and the other end stores and processes the collected packets. The collected packets are a sequence of data, each packet contains the 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.

Parameters for interference evaluation

After detecting the channel of public APs the target public AP, then the safe wireless transmitter will switch to a proper channel to interfere the target public APs. However, there are several adjacent channels that can interfere the public APs, which channel should the safe wireless transmitter switch to make the channel interference between the safe wireless transmitter and the target public APs maximum so that the packet loss rate can achieve maximum. In this paper, we will introduce four parameters to quantify the channel interference between the secure wireless transmitter and the target public APs, which are the number of packets received, the packet loss rate, the interference strength Zhang et al. (2012) and the active ratio Zhang et al. (2012), respectively.

The definition of the four parameters is as follows:

- **The number of the received packets.**
  The parameters are obtained by actual experiments, and what we have obtained is a sequence of CSIs, and the length of the sequence is the number of the received packets.
- **Packet loss rate.**

$$Packet\ Loss\ Rate = \frac{RV\,of\,RP - IV\,of\,RP}{RV\,of\,RP} \quad (3)$$

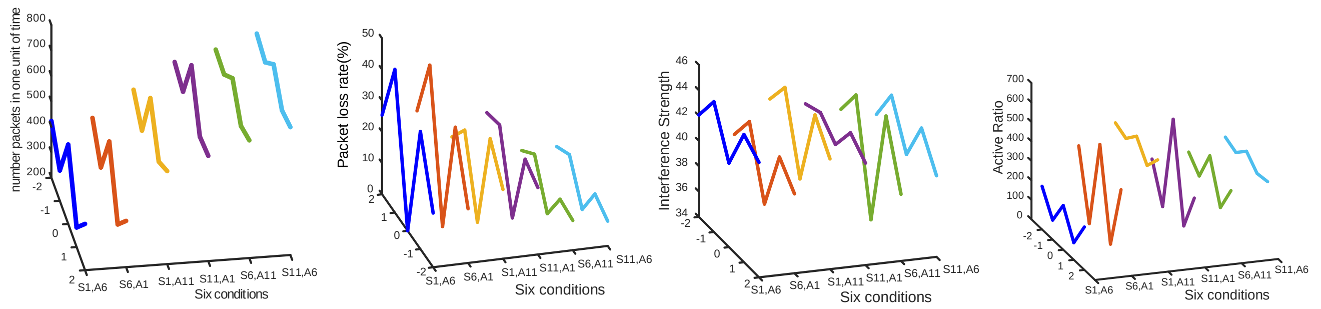
  In the above equation, $RV\ of\ RP$ represents the reference number of received packets, which the packets are obtained when the safe wireless transmitter and target public APs work on different channels and there exist no channel interference between them[¶]. $IV\ of\ RP$ represents the interference number of received packets, which 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.
- **Interference strength.**

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

  In the above equation, $RSSI_{i\_noise\_removal}$ represents the RSSI value of $i-th$ packets that has been removed noise, 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, the value of IS is greater, the interference strength between the safe wireless transmitter and the target public APs is stronger.
- **Active ratio.**

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

[¶] We assume that when the safe wireless transmitter and the public APs that the attacker leverages work on different channels and there exist no channel interference between them, the packet loss rate is 0.



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

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

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

Evaluation

In this section, we first prove that the channel interference between two adjacent wireless transmitters is different when the channel spacing between them is different , and lays the foundation for channel switching, then we prove that when the distance of two wireless transmitters is greater than $D_{neighbor}$, between them there would be no channel interference, finally we reproduce the experiments of WiPass Zhang et al. (2016) and WiKey Ali et al. (2015), which proves the channel interference can beat CSI-based attack.

Channel Interference on Public APs that Attacker Leverages

In order to select a suitable channel to interfere with the target public APs, it is necessary to carry out experiments with different channel spacing between two wireless transmitters. For some public APs, the simple co-channel interference avoidance algorithm can be used to prove that the channel interference can last enough time to ensure gesture privacy operation completely done, and then do the experiments of the last time of channel interference.

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 1m and the results are as shown in Figure 7.

In Figure 7 the value “0” in X-axis means that there exists no channel interference between two wireless transmitters, the value “-2” and “2” means that the channel spacing between two wireless transmitters is 2 ; the value “-1” and “1” means the channel spacing between two wireless transmitters is 1. “$-$” 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 two neighbor wireless transmitters. 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 1, the number of received packets is the minimum and the packet loss rate is the maximum. For example, in Figure 7a and Figure 7b, when the channel of safe wireless transmitter is 1, the channel of the target public AP is 6, if the safe wireless transmitter switches to channel 5, the number of received packets is 319 and the packet loss rate is 37.695%; if the safe wireless transmitter switches to channel 7, the number of received packets is 277 and the packet loss rate is 45.894%; while if the safe wireless transmitter switches to channel 4, the number of received packets is 423 and the packet loss rate is 17.383%; and if the safe wireless transmitter switches to channel 8, the number of received packets is 382 and the packet loss rate is 25.392%. Thus, when the channel spacing between the safe wireless transmitter and the target public AP is 1, the channel interference between them can achieve the maximum.

We can see from Figure 7c and Figure 7d 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 active ratio is the maximum. When the safe wireless transmitter switches the channel, the value of interference strength will increase and the value of the active ratio will decrease. When channel spacing between the safe wireless transmitter and the target public AP is 1, the value of the interference strength is the maximum and the value of active ratio is the minimum. That is consistent with the analysis in section .

Therefore, when the channel spacing between the secure wireless transmitter and the target public AP is 1, the channel interference between them is maximum. Thus,users can switch the secure wireless transmitter to the adjacent channel, and make the channel spacing between the security wireless transmitter and the target public AP be 1, so as to interfere with the attacker.

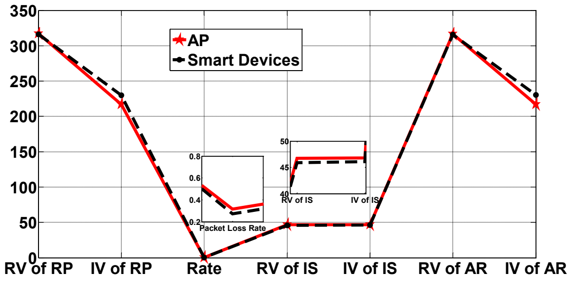


Figure 9. The parameters to characterize the channel interference for different wireless transmitters

Time

For some wireless transmitters, a simple co-channel interference avoidance algorithm may be adopted. When AP detects channel interference, it will choose other suitable channels for data transmission H3C (2016). In order to demonstrate how long channel interference exists between the secure wireless transmitter and the target public AP after switching the channel of secure wireless transmitter so that the users gesture privacy can be completed during the interference time, we collected 90s data after switching the channel of the safe wireless transmitter.

We can see from Figure 8a that under the six conditions, the number of the fourth 10s received packets is the largest, in Figure 8b, the difference for IS and AR values in different periods is relatively small. So as time grows, the channel interference between the secure wireless transmitter and the target public AP will be weakened, however, after 90s, the channel interference is still existed between the secure wireless transmitter and the target public AP, and 90s is enough to complete some gesture privacy. If the user does the gesture privacy for a long time, the user can detect the channel of the target public AP, and if the channel of target public AP switches to another channel during the time when gesture privacy is done, then the safe wireless transmitter switches its channel accordingly.

Different wireless transmitters

The attacker can turn on the hotspot functionality of his smart devices to serve as a public wireless transmitter, and the smart devices is used as the transmitter to emit wireless signals Zhang et al. (2016), thus whether the channel interference is also appropriate for the different kinds of wireless transmitters.

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

Channel Interference on Normal Public Wireless Transmitters

When the secure wireless transmitter is far away from the normal public APs, there is no channel interference between the two. In order to choose an appropriate distance between the secure wireless transmitter and the other public APs, we carry out experiments on different distances, and on the condition of that the channel spacing between the secure wireless transmitter and the other normal public AP is 1.

From Figure 10a, we can see when the distance between the secure wireless transmitter and other normal public wireless AP is from 0.5m to 2m, the interference value of the received packets and the reference value of the received packets is almost the same, which is because the secure wireless transmitter and the wireless transmitter of attacker is close enough, even if there is no channel interference, it will also affect the number of packets received. As the distance between them increases, the influence of channel interference will be weakened, and the number of packets received will be increased. As can be seen from Figure 10a, when the channel interference between the secure wireless transmitter and the other normal public AP is more than 3m, the channel interference between them will be weakened.

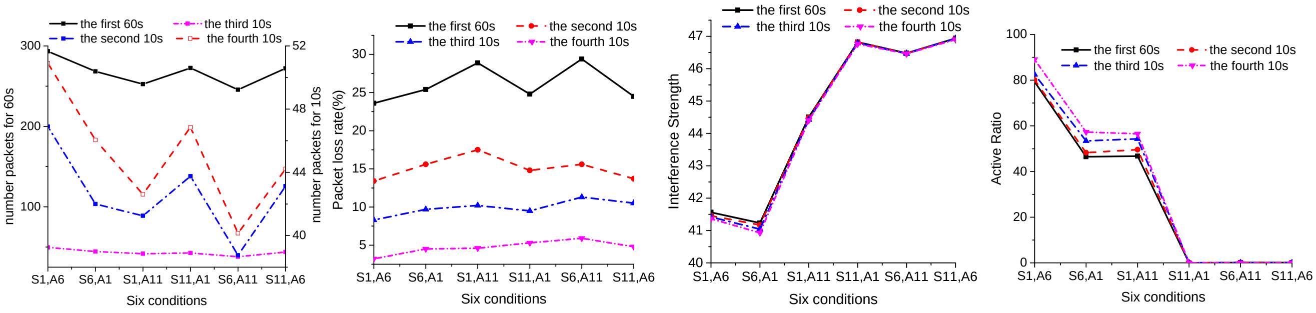
In Figure 10b, when the distance is less than 2m, IS is high and AR is relatively low, when the distance is more than 3m, IS decreases and AR increases sharply. So in order not to interfere the other normal public APs, the distance between the safe wireless transmitter and the other normal public APs would be better when it is more than 4m.

Case Study

There are two kinds of gestures for CSI-based attack, and we separately choose unlock patterns and keystrokes as the representative gestures for consecutive gestures and discrete gestures to do the experiments, and the results are as shown in Figure 11. Uellenbeck et al.S et al. (2013) 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 their patterns. According to it, 15 unlock passwords are randomly chosen as the tested unlock passwords according to the habits of people's daily use, and the tested 15 unlock passwords are shown in Figure 11c. Besides, numpad 0 to numpad 9 in the right of the keyboard are chosen as the tested keystrokes, as shown in Figure 11b.

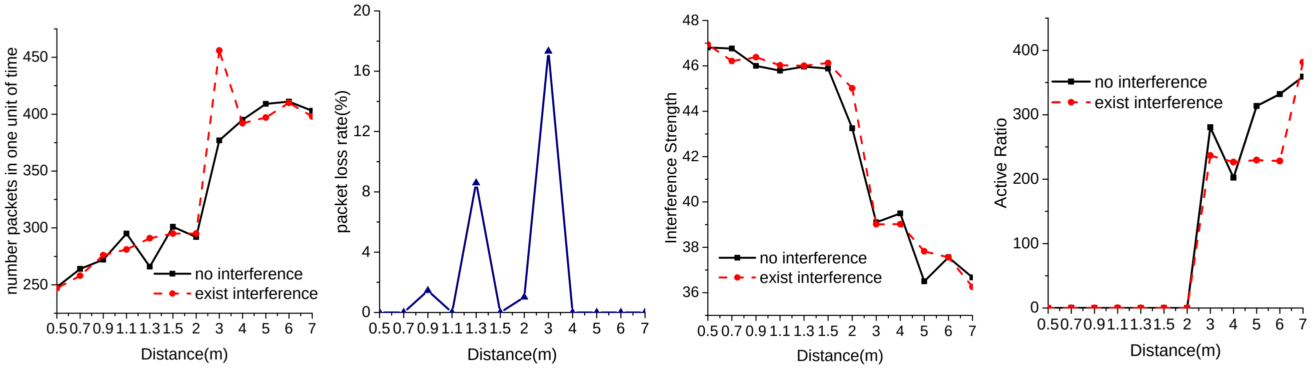
The results of the recovery of the two case studies are shown in Figure 12. From Figure 12c, we can see that when there is no channel interference, the recovery accuracy is relatively high, the average recovery accuracy of the 15 unlock password patterns is 82.33%, and the average recovery accuracy of the 10 keypads is 92%, as shown in Figure 12d. 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 12, we can see 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%, the recovery results are shown in Figure 13; the average recovery accuracy of the 10 keypads is 42%,



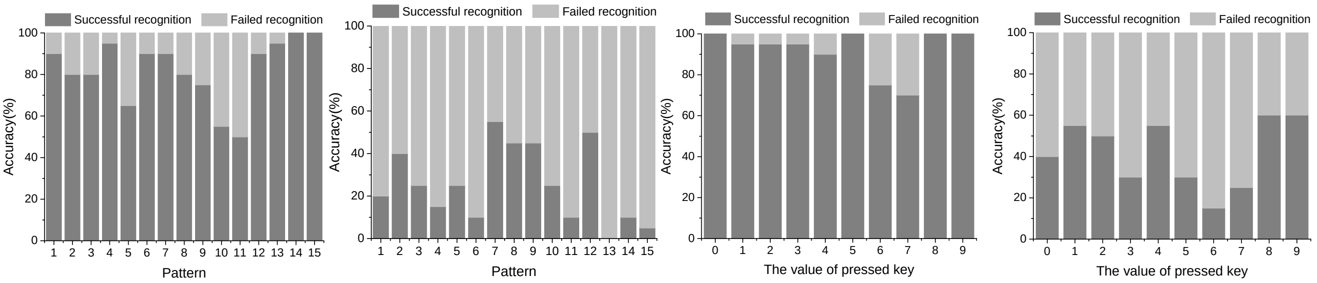
(a) Number of packets **(b)** Packet loss rate **(c)** Interference strength **(d)** Active radio

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



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

Figure 10. Four parameters under different distances



(a) Pattern recognition without interference **(b)** Pattern recognition with channel interference **(c)** Keyboards recognition without interference **(d)** Keyboards recognition with channel interference

Figure 12. Users' behavior recognition when there exists no channel interference and channel interference

and the recovery results of keypads for 20 times are shown in Figure 14. Compared with the recovery accuracy without channel interference, the recovery accuracy of the presence of channel interference is significantly reduced. The results show that the channel interference can effectively defeat CSI-based attacker effectively.

Channel Interference on the Network Service

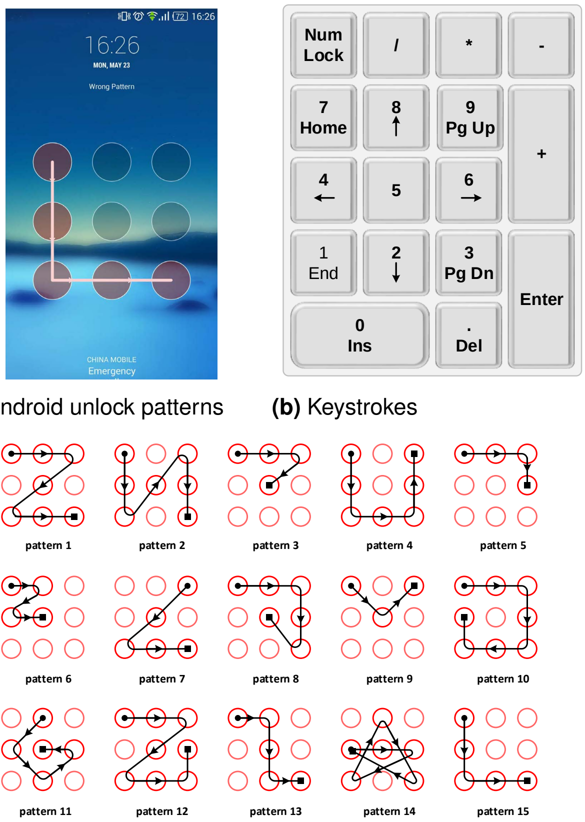
If the target public AP is disturbed, the network services that ordinary users have accessed will also be disturbed. Watching online programs is to test the impact of channel interference on network services. As can be seen from Figure 15, when users are watching the online program with the target public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

Related Work

Previous researches mainly focus on two kinds of channel interference, one is interference between different communication systems, and the other is channel interference between 802.11 communication systems.

Interference between 802.11 networks and other networks that works on 2.4GHz

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



(a) Android unlock patterns **(b)** Keystrokes

(c) 15 tested unlock passwords for Android unlock patterns

Figure 11. Two case studies

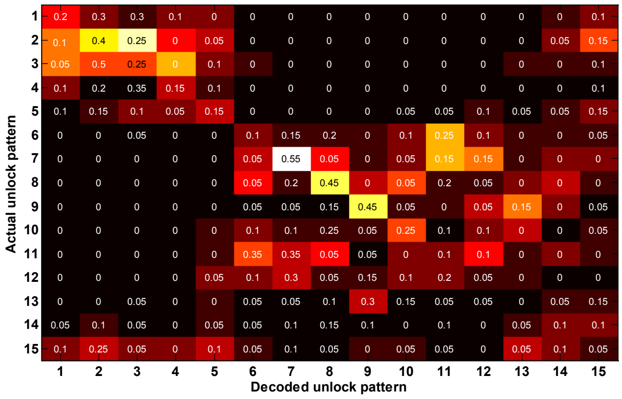
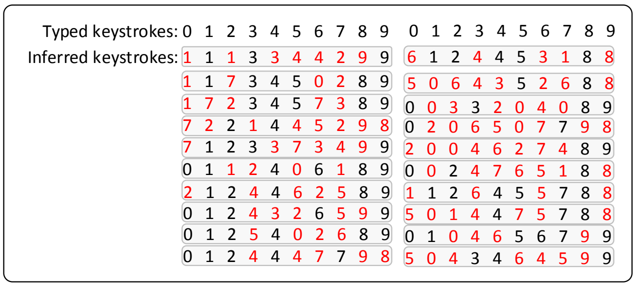


Figure 13. Recognition accuracy of unlock pattern when there exist channel interference.



Typed keystrokes:	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
Inferred keystrokes:	1	1	1	3	3	4	4	2	9	9	6	1	2	4	4	5	3	1	8	8
	1	1	7	3	4	5	0	2	8	9	5	0	6	4	3	5	2	6	8	8
	1	7	2	3	4	5	7	3	8	9	0	0	3	3	2	0	4	0	8	9
	7	2	2	1	4	4	5	2	9	8	0	2	0	6	5	0	7	7	9	8
	7	1	2	3	3	7	3	4	9	9	2	0	0	4	6	2	7	4	8	9
	0	1	1	2	4	0	6	1	8	9	0	0	2	4	7	6	5	1	8	8
	2	1	2	4	4	6	2	5	8	9	1	1	2	6	4	5	5	7	8	8
	0	1	2	4	3	2	6	5	9	9	5	0	1	4	4	7	5	7	8	8
	0	1	2	5	4	0	2	6	8	9	0	1	0	4	6	5	6	7	9	9
	0	1	2	4	4	4	7	7	9	8	5	0	4	3	4	6	4	5	9	9

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

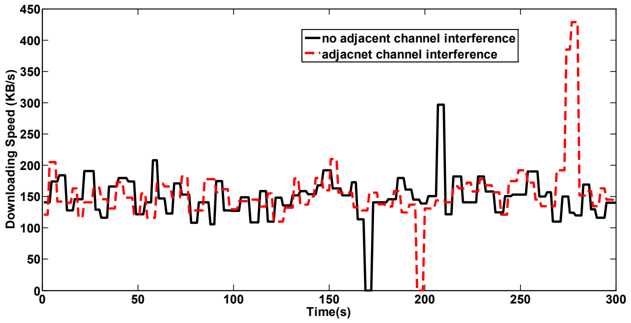


Figure 15. Evaluation on good AP

communication systems in recent years, more and more systems work on 2.4GHz. However, the frequency band of 2.4GHz 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 Xu et al. (2011), previous researches have been classified into the following three categories:

- **Interference mechanism/Interference principle.** Some researches focused on the interference mechanism/interference principle try to analyze the possible causes of interference appeared between different communication systems. For example, Yuan et al. Yuan et al. (2007) divided the interference between WiFi and ZigBee into four cases, and analyze whether there is channel interference in these four cases. The study of interference mechanism/interference principle will lay the foundation for the following two types of researches.
- **Interference avoidance.** The scheduling problem of spectrum resources is the essence of interference avoidance, in which the core problem is how to allocate the spectrum resources in different communication systems to transmit data. Tytgat et al. Tytgat et al. (2015) and Shi et al. Shi et al. (2015) achieve interference avoidance between WiFi and ZigBee communication systems. Lee et al. Lee et al. (2012) propose collaborative approach and non-collaborative approach to solve the interference avoidance.
- **Interference coexistence.** When the spectrum resources are fully used, there must be interference. How to make different communications and interference coexist is a challenge. The study Yan et al. (2015) achieves the coexistence of interference between WiFi and ZigBee, and Almeida et al. Almeida et al. (2013) achieves the coexistence of interference between WiFi and LTE.

Channel Interference in 802.11 networks

Two types of interference in the 802.11 network has been proposed by Villegas et al. Villegas et al. (2007), one is the co-channel interference, which is caused by the transmission on the same frequency channel; another is the adjacent channel interference, which is caused by the transmission on the adjacent channels or overlapped channels. Zubow et al. Zubow and Sombrutzki (2012) analyze the adverse effects of adjacent channel interference in the 802.11 networks. Tan et al. Tan et al. (2010) evaluate the effects of adjacent channel interference through extensive experiments. Previous studies on channel interference in 802.11 networks mainly focus 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 considered unfavourable to channel interference, this paper uses channel interference to defeat CSI-based attack.

Conclusion

This paper presents a new method to break the CSI - based attack, called WiGuard, which uses public WiFi to obtain user's gesture privacy. Our idea of design is that if we can interfere with the attacker's wireless transmitter to distort the CSI signal, then the attacker will not be able to successfully restore gesture privacy. In order to distort the CSI signal, WiGuard uses the realization possibility of channel interference to defeat the attacker. 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 values to recover gesture privacy, the attacker need 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 the attacker. Extensive experiments demonstrate that when the channel spcing of safe wireless transmitter the target public AP is 1, the channel interference between them can achieve 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 4m, channel interference between them becomes weak, and $D_{neighbor}$ can be seen as 4m, so when the distance between them is more than 4m, the channel switch of the safe wireless transmitter will not influence the other normal public APs. Evaluation on network service demonstrate that channel interference will not influence the normal network service. Unlock passwords and keyboards recovery experiments show that when there exists channel interference, the recovery accuracy decrease dramatically, thus, our system WiGuard is effective and channel interference can be used to defeat CSI-based attack.

References

1. Shorter oxford english dictionary (6th ed.). *Oxford University Press,*, 2007.
2. H. Abdel-Nasser, R. Samir, I. Sabek, and M. Youssef. Monophy: Mono-stream-based device-free wlan localization via physical layer information. pages 4546–4551, 2013.
3. H Abdelnasser, M Youssef, and K A Harras. Wigest: A ubiquitous wifi-based gesture recognition system. *Computer Communications (INFOCOM), 2015 IEEE Conference on. IEEE*, pages 1472–1480, 2015.
4. A Akella, G Judd, and S Seshan. Self-management in chaotic wireless deployments. *Wireless Networks*, 13(6):737–755, 2007.
5. R Akl and A Arepally. Dynamic channel assignment in ieee 802.11 networks. *Portable Information Devices, 2007. PORTABLE07. IEEE International Conference on. IEEE*, pages 1–5, 2007.
6. Kamran Ali, Alex X. Liu, Wei Wang, and Muhammad Shahzad. Keystroke recognition using wifi signals. *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, ACM*, pages 90–102, 2015.
7. E Almeida, A M Cavalcante, and R C D Paiva. Enabling lte/wifi coexistence by lte blank subframe allocation. *Communications (ICC), 2013 IEEE International Conference on. IEEE*, pages 5083–5088, 2013.
8. V. Angelakis, S. Papadakis, V. A. Siris, and A. Traganitis. Adjacent channel interference in 802.11a is harmful: Testbed validation of a simple quantification model. *Communications Magazine IEEE*, 49(3):160–166, 2011.
9. Michael S. Borella, Debbie Swider, Suleyman Uludag, and Gregory B. Brewster. Internet packet loss: Measurement and implications for end-to-end qos. In *International Conference on Parallel Processing Workshops*, pages 3–12, 1998.
10. S Chieochan, E Hossain, and J Diamond. Channel assignment schemes for infrastructure-based 802.11 wlans: A survey. *IEEE Communications Surveys & Tutorials*, 12(1):124–136, 2010.
11. W G Draft. 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 Std*, 2003.
12. WA Series Access Points Configuration Guide-6W112 H3C. H3c corp. *http://www.h3c.com.hk*, 2016.
13. L Lee, G Kang, and X Zhang. An interference avoidance strategy for zigbee based wehealth monitoring system. *IEEE, International Conference on E-Health Networking, Applications and Services. IEEE*, pages 68–72, 2012.
14. Y Lee, K Kim, and Y Choi. Optimization of ap placement and channel assignment in wireless lans. *Local Computer Networks, 2002. Proceedings. LCN 2002. 27th Annual IEEE Conference on. IEEE*, pages 831–836, 2002.
15. A Mishra, S Banerjee, and W Arbaugh. Weighted coloring based channel assignment for wlans. *ACM SIGMOBILE Mobile Computing and Communications Review*, 9(3):19–31, 2005.
16. Yue Qiao, Ouyang Zhang, Wenjie Zhou, Kannan Srinivasan, and Anish Arora. Phycloak: obfuscating sensing from communication signals. In *Usenix Conference on Networked Systems Design and Implementation*, 2016.
17. I Rouf, H Mustafa, and M Xu. Neighborhood watch: security and privacy analysis of automatic meter reading systems. *ACM Conference on Computer and Communications Security*, pages 462–473, 2012.
18. Uellenbeck S, Rmuth M, and Wolf C. Quantifying the security of graphical passwords: the case of android unlock patterns. *ACM Sigsac Conference on Computer & Communications Security*, pages 161–172, 2013.
19. G Shi, R Xu, and Y Shu. Exploiting temporal and spatial variation for wifi interference avoidance in zigbee networks. *International Journal of Sensor Networks*, 18(3-4):204–216, 2015.
20. Tam Wee Sin, Mohd Noor Halim, Janardhana Reddy Naredula, Mao Hui Fang, and Kevin Payne. Quality of transmission

across packet-based networks, 2002.

21. W L Tan, K Bialkowski, and M Portmann. Evaluating adjacent channel interference in ieee 802.11 networks. *IEEE Vehicular Technology Conference. IEEE*, pages 1–5, 2010.
22. L Tytgat, O Yaron, and S Pollin. Analysis and experimental verification of frequency-based interference avoidance mechanisms in ieee 802.15. 4. *Networking, IEEE/ACM Transactions on*, 23(2):369–382, 2015.
23. E G Villegas, E Lopez-Aguilera, and R Vidal. Effect of adjacent-channel interference in ieee 802.11 wlans. *Cognitive Radio Oriented Wireless Networks and Communications, 2007. CrownCom 2007. 2nd International Conference on. IEEE*, pages 118–125, 2007.
24. G Wang, Y Zou, and Z Zhou. We can hear you with wi-fi! *Proceedings of the 20th annual international conference on Mobile computing and networking. ACM*, pages 593–604, 2014.
25. Ju Wang, Binbin Xie, Dingyi Fang, Xiaojiang Chen, Chen Liu, Tianzhang Xing, and Weike Nie. Accurate device-free localization with little human cost. In *The International Workshop*, pages 55–60, 2015.
26. Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, and Jean Camille Birget. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Working Conference on Advanced Visual Interfaces, AVI 2006, Venezia, Italy, May*, pages 177–184, 2006.
27. Wikipedia. Denial-of-service attack. https://en.wikipedia.org/wiki/Denial-of-service_attack/, 2016. [Online; accessed 10-August-2016].
28. J Xiao, K Wu, and Y Yi. Pilot: Passive device-free indoor localization using channel state information. *Distributed computing systems (ICDCS), 2013 IEEE 33rd international conference on IEEE*, pages 236–245, 2013.
29. R Xu, G Shi, and J Luo. Muzi: Multi-channel zigbee networks for avoiding wifi interference. *Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing, IEEE*, pages 323–329, 2011.
30. Y Yan, P Yang, and X Y Li. Wizbee: Wise zigbee coexistence via interference cancellation with single antenna. *Mobile Computing, IEEE Transactions on*, 14(12):2590–2603, 2015.
31. Wei Yuan, Xiangyu Wang, Linnartz, and J.-P.M.G. A coexistence model of ieee 802.15.4 and ieee 802.11b/g. *Communications and Vehicular Technology in the Benelux, 2007 14th IEEE Symposium on*, pages 1–5, 2007.
32. J Zhang, X Zheng, and Z Tang. Privacy leakage in mobile sensing: Your unlock passwords can be leaked through wireless hotspot functionality. *Mobile Information Systems*, 2016(2):1–14, 2016.
33. Jie Zhang, Zhanyong Tang, Rong Li, Xiaojiang Chen, Xiao Qing Gong, Dingyi Fang, and Zheng Wang. Protect sensitive information against channel state information based attacks. In *IEEE International Conference on Computational Science and Engineering*, pages 203–210, 2017.
34. Z L Zhang, H M Chen, and T P Huang. A channel allocation scheme to mitigate wifi interference for wireless sensor networks. *Jisuanji Xuebao(Chinese Journal of Computers)*, 35 (3):504–517, 2012.
35. Liqiang Zhao and Changxin Fan. Enhancement of qos differentiation over ieee 802.11 wlan. *Communications Letters IEEE*, 8(8):494–496, 2004.
36. A Zubow and R Sombrutzki. Adjacent channel interference in ieee 802.11n. *2012 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1163–1168, 2012.