Protect Sensitive Information Against Channel State Information Based Attacks

Jie Zhang[1], Zhanyong Tang[1*], Xiaojiang Chen[1], Dingyi Fang[1], Rong Li[1], Zheng Wang[2]
[1]School of Information Science and Technology, Northwest University, Xi'an, 710127, P.R. China
[2]School of Computing and Communications, Lancaster University, UK

***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 the 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 gestures in a public place. Our approach carefully exploits the WiFi channel interference to introduce noise into the attacker's CSI measurement to reduce the success rate of the attack. 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 reduces the success rate of CSI attacks from 92% to 42% for text-based passwords and from 82% to 22% for pattern lock.**

Keywords: CSI-based attack, privacy protection, channel interference

I. Introduction

Smartphones and tables are often used in public places (e.g. coffee shops, hotels, shopping malls, airports etc.) and connects to a public WiFi. Using mobile devices in such environments, however, opens up a backdoor for attackers who can steal the user's passwords by analyzing how the channel state information (CSI) of the WIFI signal is affected by the user's fingertip movement when entering a password. This type of attacks is known as CSI-based attacks. It has been demonstrated to be effective in reconstructing PIN-based passwords [1] and text-based passwords [2] as well as locking patterns [3].

The simple setup of a CSI-based attack makes it a real threat for mobile users. Figure 1 depicts some typical scenarios where a CSI-based attack can be successfully performed. In all these scenarios, the attacker only needs to place a WiFi receiver (e.g. a wireless router or a laptop) next to the victim, with a distance ranges from 1 meter to 5 meters. Such a setting is unlikely to raise suspicion to many users in public places.

The underlying principal of a CSI-based attack is to use the CSI measurements to characterize the change of the multipath propagation of WFI signals caused by nearby gesture movements. The CSI readings can be mapped a keystroke or a pattern because each fingertip movement and location can be mapped to a unique CSI value. 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 [2] 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.

(a) scenario 1 (b) scenario 2

(c) scenario 3 (d) scenario 4

Fig. 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.

This paper presents WiGuard, a system to protect sensitive on-screen gestures against CSI-based attacks. Our key insight is that a CSI-based attack is likely to fail if the messages sent in response to the attacker's ICMP packets are lousy. While there are a number of methods available to drop ICMP responses [4], 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 AP's working channel. 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.

As a departure from prior work that all consider the channel interferences as a harmful effect and make every effort to prevent it from happening [5], [6], [7], [8], [9], our approach carefully utilizes the interference for information protection. Our design overcomes a number of practical challenges. These include: how to detect a CSI-based attack? how to introduce noises to the attack without significantly affecting the network performance? All these challenges require novel solutions to be constructed in this new application context.

We have evaluated our approach by using it to protect text-based passwords and locking patterns in public WiFI environments. We show that WiGuard can successfully defeat CSI-based attacks by reducing the accuracy of keystroke and pattern recognition from 92% and 82% respectively to 42% and 22%, with little impact to the communication quality.

Contributions: This paper makes the following contributions:

- It proposes a novel approach for protecting sensitive gestures against CSI-based attacks;
- It is the first work to exploit channel interference to protect sensitive information to be leaked from mobile devices;
- Experimental results show that the proposed approach can effectively defeat CSI-based attacks.

II. CSI-based Attack

With more and more public places deploying public WiFi, CSI has received much attention [10] [11], and because of rich information that CSI contains, it can be used to detect micro motions, such as finger motions [2] [3] and mouth motions [12]. With a commercial receiver, the attacker can obtain the users' PIN, passwords or other gesture privacy information. In this section, first we introduce why CSI can detect and recover the gesture privacy, and then will introduce a novel attack, CSI-based attack.

A. 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).

B. CSI-based Gesture Privacy Recovery Model

The reason why CSI values can be used to recover gesture privacy is that while a user does gesture privacy, the motions that come from the certain parts of the body will introduce relative muti-path propagation of wireless signals, and different motions correspond to different multi-path propagation, thus a certain motion will generate a unique pattern in the time-series CSI values, and the uniqueness can be exploited to recover the gesture privacy.

For CSI-based gesture privacy recovery model, there are several steps for a successful recognition. First, noise need to be removed from the obtained signals. After noise removal, the actual influenced signal traces need to be extracted and then the gesture recovery methods will be applied to recover the gesture privacy, as shown in Figure 2.

C. CSI-based Attack

After receiving the wireless signals that are related to gesture privacy, the attacker can decode the gestures successfully using noise removal, feature chosen and gesture recognition techniques. However, in order to achieve CSI-based attack, there are several requirements that the attacker successfully decode the gesture privacy and it can be equivalent with 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 interpretation of above equations is as follows: there must be a wireless transmitter and a signal receiver. The wireless transmitter is used to emit wireless signals while the signal receiver is used to receive the time-series CSI values. In order to characterize the fine-grained gestures, especially for those similar gestures, ICMP ping packets from the transmitter must be at a high rate. Besides, the communication channel between transmitter and receiver must be stable, if the communication channel is interfered and is not stable, the receiver will not receive the ICMP ping packets from the transmitter, that will lead to incomplete time-series CSI values. $Quality_{CSI}$ describes the quality of obtained time-series CSI values that are received by the receiver, if the wireless signals are interfered during the multi-path propagation process, , the received time-series CSI values will be changed at the receiver end, that will lead to the distortions of CSI waveforms.

III. Threat Model

We consider a scenario where an attacker seeks to identify the users' gesture privacy in a sequence of time-series CSI values generated by the users' gestures, the attacker doesn't need to be near to the user or have any displayed information on the users' screen. We assume that the attacker can access the public WiFi, ping the public WiFi AP at a high rate and receive the time-series CSI values using a receiver. Two representative scenarios the attack is plausible are: (1) the attacker inconspicuously leaves a prepared receiver end (e.g. network NICs) in the public place, perhaps in a hidden setting where the receiver is not suspicious; (2) the attacker pretends to work in a public place using his laptop and he looks unsuspicious.

For scenario 1, the user is unlocking the device while the attacker receives the CSI values using network NICs, the attacker is far away from the user and he leaves the prepared network NICs near to the user. However, the position of the network NICs is hidden and the user will not notice the receiver. For scenario 2, the attacker pretends to work on her laptop, which is used to receive the CSI values. The attacker looks unsuspicious and the user will not be aware of him/her.

IV. Prior Knowledge

The IEEE 802.11 is widely used for public WiFi and it usually works on 2.4 GHz, which is between 2400 MHz and

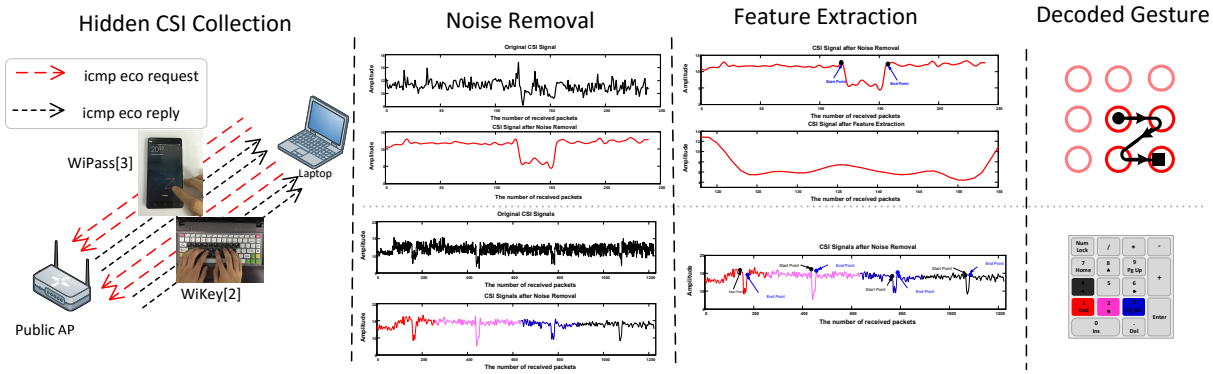


Fig. 2: The process of CSI-based attack. There are two kinds of gesture privacy presented in this figure, and one is consecutive gesture (unlock patterns of smart phones), and another is discrete gesture (keystrokes). When the attacker obtains the CSI values of gesture privacy, after noise removal, feature extraction, the attacker will decode the gesture successfully.

2500 MHz. 2.4 GHz is divided into 13 frequency bands[1][13], 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 [14] [15] in 802.11 network, Akella et al.[16] 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 [7] [8] [17] [9].

[1]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.

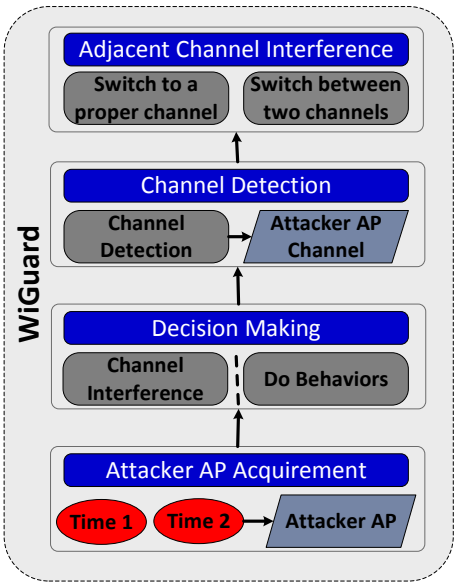
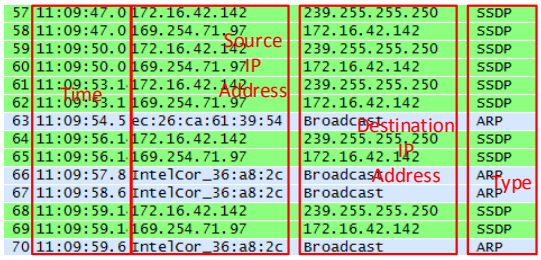


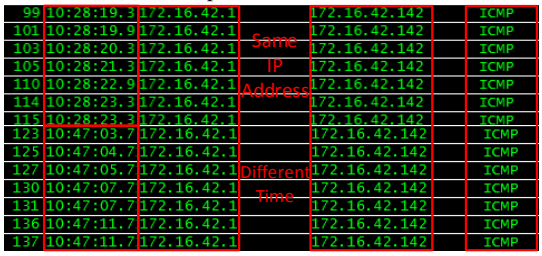
Fig. 3: System Overview of WiGuard

V. System Design

In order to defeat the CSI-based attack, we design a protection system WiGuard, which uses channel interference to destroy the $Quality_{CSI}$, the necessary requirements that the CSI-based attack can succeed. In this section, we introduce the system design. First, *ICMP based Attacker AP Acquirement* is used to detect whether there exist abnormal ICMP ping packets, which is caused by CSI values collection by an attacker. Then, if there is no abnormal ICMP ping packets, the user can do their gestures; if there exist abnormal ICMP ping packets, the user should detect which channel the target public AP works on and then switch the channel of a safe wireless



(a) WiFi packets in normal case



(b) attacker collects CSI values

Fig. 4: Public WiFi packets analysis using wireshark. When the attacker collect gesture CSI values, there will exist plenty of ICMP packets in different time.

transmitter to a proper channel to interfere the attacker, as shown in Figure 3.

A. ICMP based Attacker AP Acquirement

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 the rate of ICMP ping packets should be 2500 packets/s [2], in order to decode the keystrokes of laptops successfully.

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 [18]. So, generally, there exist no ICMP ping packets or few ICMP ping packets for public AP, as shown in Figure 4a. 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, as shown in Figure 4b.

Thus, 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 at a high rate, and we think there exist an attack in the public place.

However, sometimes, there will not exist only one public AP in the public place, and the attacker may use two or more public APs to improve the success rate of CSI-based attack, Abdelnasser et al.[19] demonstrate that the recovery accuracy will be improved using multiple APs. So, in public place, the attacker can use more public APs instead of just only public AP to decode the gesture privacy successfully. Thus, in order to make sure that the attacker does not leverage all potential public APs to collect CSI values, the user need to surf all the public APs to detect how many public APs are used by the attacker.

B. Decision Making

After detecting the number of public APs that may be used by the attacker, the user can make a decision whether it is safe in the public place to do gesture privacy. When the network is normal, and is without suspicious CSI values' collection, the user can do his/her gesture privacy immediately. However, when the network activity is abnormal with suspicious CSI values' collection, the user will need to adopt the channel interference protection system before doing his/her gesture privacy.

The channel interference protection system is mainly divided into two parts, and the first part is detecting which channel the target public AP works on, and then the channel of a safe wireless transmitter will be switched to a proper adjacent channel to interfere the attacker. The following two subsections will introduction the details.

C. Channel Detection

When the user detect that there exist abnormal ICMP ping packets in the network, first, the system will detect which channel the target public APs work on. The channel detection is easily achieved, and there are also many commercial applications that can support the channel detection functionality, such as WiFi Analyzer.

D. 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.

1) 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.

2) 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 IV, 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 neighbor APs is 1, the channel interference between them is the maximum because the overlaps between the two channels is the maximum. Thus, the safe wireless transmitter can switch to an adjacent channel to interfere the attacker, which the channel spacing between the safe wireless transmitter and the target public AP is 1.

However, the attacker may use two or more public APs to collect CSI values in order to improve the success rate, so how the channel of safe wireless transmitter switch to interfere all the target public APs? There are two kinds of conditions, and one is that the safe wireless transmitter only just need to switch to a proper channel, another is that the safe wireless transmitter need to switch between two channels to interfere all the target public APs to prevent the attacker from obtaining CSI values.

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

There are two different cases that the attacker's received CSI signals will lose the packets when the channel of the safe wireless transmitter is switched to a proper channel. In the first case, there is only one target public AP in the public place, the safe wireless transmitter can switch the channel to adjacent channel, for example, when the target public AP works on channel 6, then the user can switch the channel of a safe wireless transmitter to channel 5 or channel 7. In another case, there are two or more target public APs in the public place, and channel spacing of all the target public APs is smaller than 5, then the channel of the safe wireless transmitter can switch to a proper channel to interfere the attacker, for example, the channels of two target public APs are separately channel 1 and channel 6, then the safe wireless transmitter can switch to channel 3 or channel 4.

Although in the second case, the safe wireless transmitter can switched to a proper channel to interfere the attacker, however, in order to make the packet loss rate be maximum, the safe wireless transmitter can switch between two channels.

(b) **Switch between two channels**

If the channel spacing between the target public APs are larger than 5, then the safe wireless transmitter should switch between two channels. For example, there are two public APs detected to exist abnormal network activity, and the channel of the two target public APs are separately channel 1 and channel 11, then the safe wireless transmitter need to be switched between channel 2 and channel 10.

VI. Implementation

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

A. Experiments setup

TP-Link wireless routers and smart devices with wireless hotspot functionality are separately as the wireless transmitters, and the receiver is a desktop equipped with Intel 5300 NIC(Network Interface Controller). The transmitter operates in IEEE 802.11n. The receiver has 3 antennas and the firmware reports CSI to upper layers. The receiver continuously pings packets and the receiver stores and processes the collected packets. The collected packets are a sequence of data and each packet contains the RSSI values of three antennas, the value of noise, CSI, and so on. Each CSI represents the phases and amplitudes that are on a group of 30 OFDM subcarriers.

B. 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 introduce four parameters to quantify the channel interference between safe wireless transmitter and the target public APs, and one is the number of the received packets, one is packet loss rate, one is interference strength [20], and the last is active ratio [20]. We define the four parameters as follows:

- **The number of the received packets.**
  What we have obtained at the receiver is a sequence of CSI values, and the length of the sequence is the number of the received packets.
- **Packet loss rate.**

$$Packet\ Loss\ Rate = \frac{RV\ of\ RP - IV\ of\ RP}{RV\ of\ RP} \quad (1)$$

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[2]. $IV\ of\ RP$ 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.

[2]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.

- **Interference strength.**

$$IS = \sum_{i=0}^{RP} \frac{RSSI_{i\_noise\_removal}}{RP} \tag{2}$$

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.**

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

$$U_i = \begin{cases} if \frac{|RSSI_i + Noise_i|}{RSSI_{i\_noise\_removal}} \geq 1, & U_i = 1 \\ other, & U_i = 0 \end{cases} \tag{3}$$

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.

VII. Evaluation

In this section, first we demonstrate that the channel interference between two neighbor wireless transmitters is different when the channel spacing between them is different, and that lays a foundation for channel switch, then we demonstrate that when the distance of two wireless transmitters is longer than $D_{neighbor}$, there will not exist channel interference between them, finally we reappear the experiments of WiPass [3] and WiKey [2], and demonstrate that the channel interference can defeat CSI-based attack.

A. Channel Interference on Public APs that Attacker Leverages

In order to choose a proper channel to interfere the target public APs, first the experiments of different channel spacing between two wireless transmitters are done. For some public APs, they may adopt simple co-channel interference avoidance algorithm, in order to demonstrate that the channel interference can last enough time so that the gesture privacy can be done, then the experiemnts of the last time of channel interference are done.

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 1m and the results are as shown in Figure 5.

In Figure 5 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 smaller than the channel of the safe wireless transmitter.

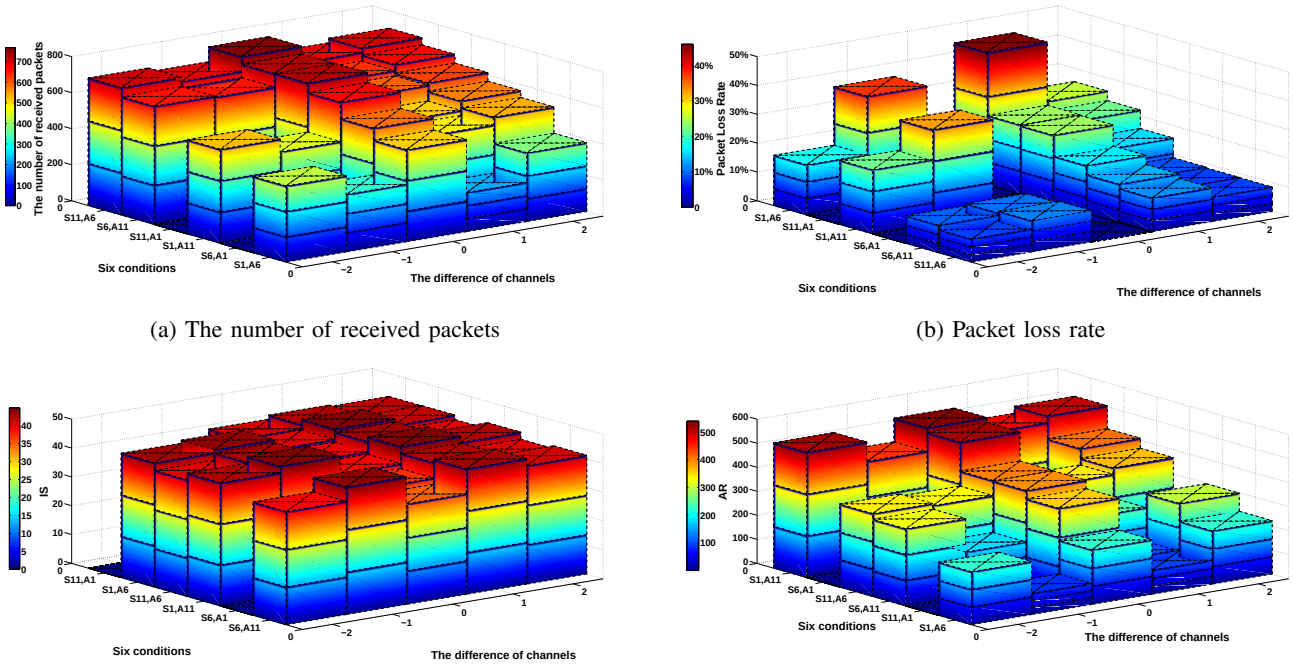
We can see from Figure 5 that the number of received packets is the maximum when there exists no channel interference between the two neighbor wireless transmitters. The number of received packets is relatively low when there exists channel interference between the two wireless transmitters, and when 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 5a and Figure 5b, 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 5c and Figure 5d 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 VI-B.

Thus, when the channel spacing between the safe wireless transmitter and the target public AP is 1, the channel interference between them achieve the maximum. So, the user can switch the safe wireless transmitter to adjacent channel to interfere attacker, and the channel spacing between the safe wireless transmitter and the target public AP is 1.

2) Time:

For some wireless transmitters, they may adopt simple co-channel interference avoidance algorithm, and when the APs detect channel interference, they will choose another proper cannel to transmit data [21]. In order to demonstrate how long the channel interference will exist between the safe wireless



(a) The number of received packets

(b) Packet loss rate

(c) Interference strength

(d) Active ratio

Fig. 5: Four parameters to characterize the channel interference under six conditions for the safe wireless transmitter and the public AP that the attacker leverages

transmitter and the target public AP after switching the channel of safe wireless transmitter so that the users' gesture privacy can be completely done during the interference time, we collected 90s data after switching the channel of the safe wireless transmitter.

We can see from Figure 6a that the number of received packets for the fourth 10s is the maximum under the six conditions, in Figure 6b, the difference for the value of IS and AR between different periods is small. So with the increase of time, the channel interference between the safe wireless transmitter and the target public AP will weaken, however, there still exists channel interference between the safe wireless transmitter and the target public AP after 90s, 90s is enough to do 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.

B. Channel Interference on Normal Public Wireless Transmitters

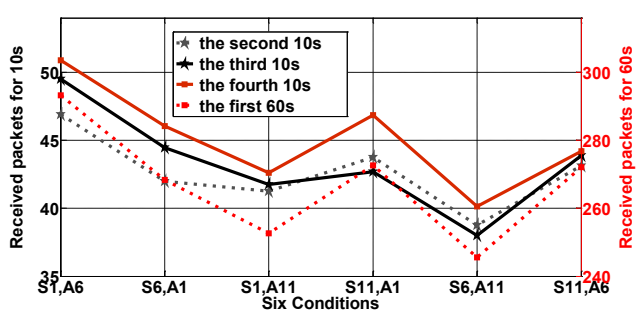
When the safe wireless transmitter is far away from the normal public APs, there will not exist channel interference between them. In order to choose a proper distance between the safe wireless transmitter and the other normal public APs, the experiments of different distances are done and the experiments are done when the channel spacing between the safe wireless transmitter and the other normal public AP is 1.

We can see from Figure 7a that when the distance between the safe wireless transmitter and the other normal pubic AP is from 0.5m to 2m, the reference value of received packets and the interference value of received packets are almost the same, that just because when the safe wireless transmitter and the attacker's wireless transmitter are near enough, even when there exist no channel interference between them, it will also influence the number of the received packets. With the increase of distance between them, the influence of channel interference will weaken and the number of received packets will increase. We can see from Figure 7a that when the distance between safe wireless transmitter and the other normal public AP is more than 3m, the channel interference between them will become weak.

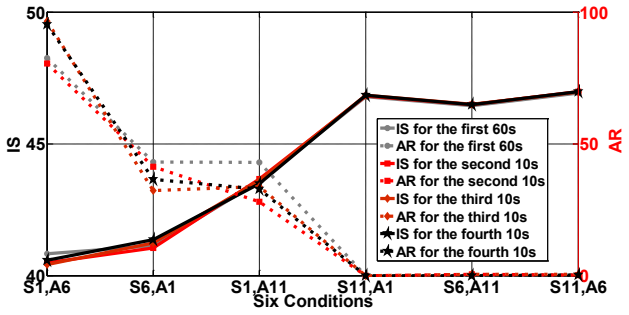
In Figure 7b, when the distance is less than 2m, IS is high and AR is relatively low, when the distance is more than 3m, IS decreases and AR increases dramatically. So in order not to interfere the other normal public APs, the distance between the safe wireless transmitter and the other normal public APs would be better when it is more than 4m.

C. 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 8. Uellenbeck et al.[22] found that there exist typical

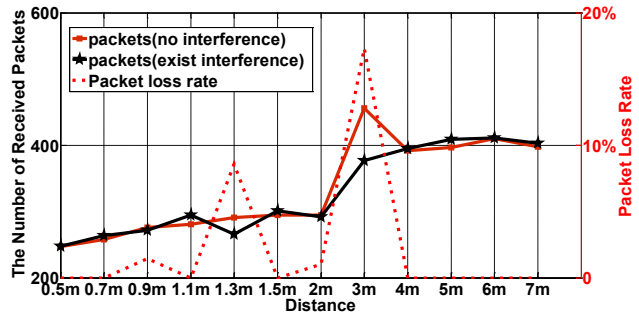


(a) The number of received packets and packet loss rate

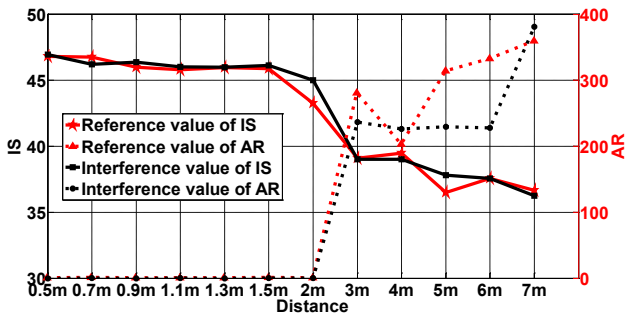


(b) The interference strength and active radio

Fig. 6: Four parameters to characterize the duration of channel interference under the six conditions for the safe wireless transmitter and the other normal public APs

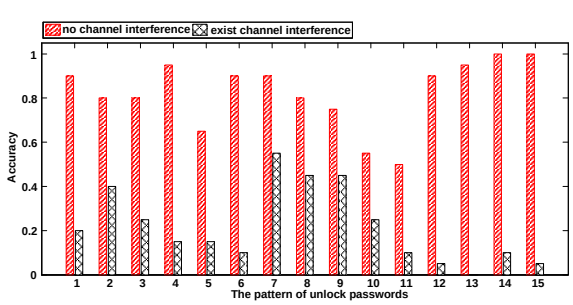


(a) The number of received packets and packet loss rate

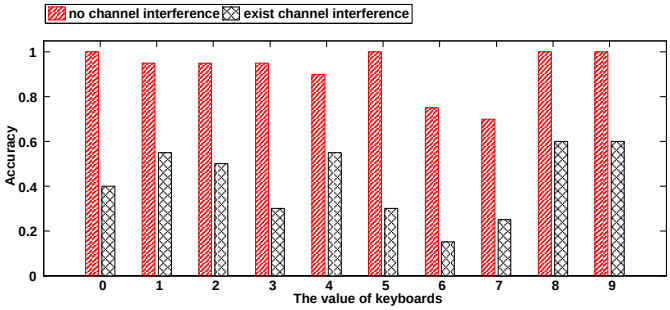


(b) Interference strength and active ratio

Fig. 7: Four parameters under different distances



(a) Unlock passwords recognition



(b) Keyboards recognition

Fig. 9: Users' behavior recognition when there exists no channel interference and channel interference

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 8. Besides, numpad 0 to numpad 9 in the right of the keyboard are chosen as the tested keystrokes.

The recovery results of the two case studies are shown in Figure 9. We can see from Figure 9a that when there exists no channel interference, the recovery accuracy is relatively high, and the average recovery accuracy of 15 unlock password patterns is 82.33%, and the average recovery accuracy of 10 keypads is 92%, as shown in Figure 9b. The results of unlock patterns and keyboard recovery demonstrate that wireless signals can leak the users' privacy and it should be a warning for users.

We can see from Figure 9 that when there exists channel interference, the recovery accuracy is relatively low, and the average recovery accuracy of 15 unlock password patterns is 21.67%, the average recovery accuracy of 10 keypads is 42%. Comparing to the recovery accuracy when there exists

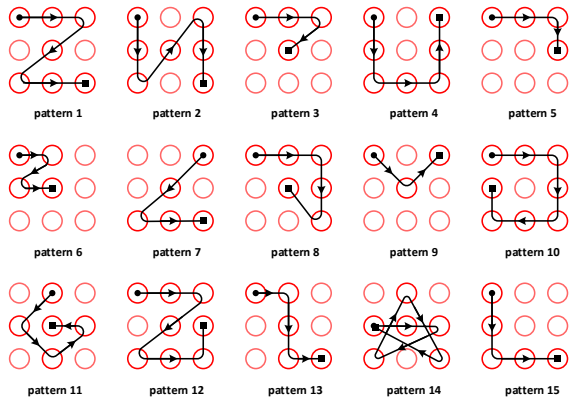


Fig. 8: 15 tested unlock passwords for Android unlock patterns

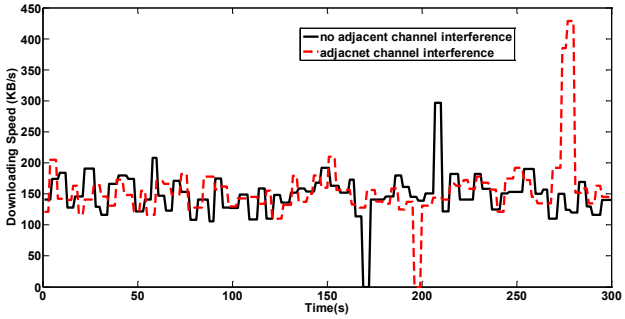


Fig. 10: Evaluation on good AP

no channel interference, the recovery accuracy when there exists channel interference decreases dramatically. The results demonstrate that channel interference can defeat CSI-based attacker effectively.

D. Channel Interference on the Network Service

If the target public AP is interfered, the network service for normal users who have accessed it will also be interfered. Watching a online show is chosen to test the influence of channel interference on network service. We can see from Figure 10 that when a user is watching a online show using 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. Thus, the influence of channel interference on network service is small and the user can also have a normal network service.

VIII. Related Work

The prior researches paid their attention on two kinds of channel interferences and one is interference between different communication systems and another is channel interference between 802.11 communication system.

A. 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 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 [5], previous researches have been classified into the following three categories:

- **Interference mechanism/Interference principle.**
  The researches that paid their attention on interference mechanism/interference principle try to analyze the reason why the interference can appear between different communication systems, such as, Yuan et al.[23] divided the interferences between WiFi and ZigBee into four cases, and analyze whether there exist channel interference in the four cases. The researches on interference mechinism/interference principle will lay a foundation for the following two categories of researches.
- **Interference avoidance.**
  The essence of interference avoidance is spectrum resource scheduling problem, and the core problem is how to allocate the spectrum resource to transmit the data in different communication systems. Tytgat et al.[24] and Shi et al.[25] achieve interference avoidance between WiFi and ZigBee communication systems. Lee et al.[26] propose collaborative approach and non-collaborative approach to solve the interference avoidance.
- **Interference coexistence.**
  When spectrum resource is occupied completely, the interference is inevitable, and how to make different communication coexist with the interference is a challenge. The research [27] achieve interference coexistence between WiFi and ZigBee, Almeida et al.[28] achieve interference coexistence between WiFi and LTE.

B. Channel Interference in 802.11 networks

Villegas et al.[6] propose that there are two types of interference in 802.11 networks, and one is co-channel interference, which is caused by the transmissions that are carried out on the same frequency channel; and another is adjacent channel interference, which is caused by the transmissions that are carried out on adjacent channels or partially overlapped channels. Zubow et al.[15] analyze the adverse effects of adjacent channel interference in 802.11 networks. Tan et al.[29] evaluate the effects of adjacent channel interference through extensive experiments. Previous researches on channel interference in 802.11 networks mainly paid their attention on how to allocate the channels for those WiFi nodes to avoid co-channel interference, how to justify the adjacent channel

interference to assist different management mechanisms radio resource. Different from prior work, which thinks channel interference as detrimental, however, in this paper, channel interference is exploited to defeat CSI-based attack.

IX. Conclusion

This paper presents WiGuard, a novel method that can defeat CSI-based attack, which exploits public WiFi to obtain the users' gesture privacy. The intuition underlying our design is that if we can interfere the attacker's wireless transmitter to distort the CSI signal, then the attacker will not recover the gesture privacy successfully. In order to distort the CSI signal, 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 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 spacing 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 set 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] Mengyuan Li, Yan Meng, Junyi Liu, Haojin Zhu, Xiaohui Liang, Yao Liu, and Na Ruan. When csi meets public wifi: Inferring your mobile phone password via wifi signals. In *ACM Sigsac Conference on Computer and Communications Security*, pages 1068–1079, 2016.

[2] Ali K, Liu A X, and Wang W. Keystroke recognition using wifi signals. *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, ACM*, pages 90–102, 2015.

[3] Zhang J, Zheng X, and Tang Z. Privacy leakage in mobile sensing: Your unlock passwords can be leaked through wireless hotspot functionality. *Mobile Information Systems*, 2016(2):1–14, 2016.

[4] Wikipedia the free encyclopedia. Denial-of-service attack. https://en.wikipedia.org/wiki/Denial-of-service_attack/, 2016. [Online; accessed 10-August-2016].

[5] Xu R, Shi G, and Luo J. 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.

[6] Villegas E G, Lopez-Aguilera E, and Vidal R. 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.

[7] Mishra A, Banerjee S, and Arbaugh W. Weighted coloring based channel assignment for wlans. *ACM SIGMOBILE Mobile Computing and Communications Review*, 9(3):19–31, 2005.

[8] Lee Y, Kim K, and Choi Y. 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.

[9] Akl R and Arepally A. Dynamic channel assignment in ieee 802.11 networks. *Portable Information Devices, 2007. PORTABLE07. IEEE International Conference on. IEEE*, pages 1–5, 2007.

[10] Xiao J, Wu K, and Yi Y. 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.

[11] 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.

[12] Wang G, Zou Y, and Zhou Z. We can hear you with wi-fi! *Proceedings of the 20th annual international conference on Mobile computing and networking. ACM*, pages 593–604, 2014.

[13] by 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 Std*, IEEE 802.11k/D0.7.2003.

[14] 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.

[15] Zubow A and Sombrutzki R. Adjacent channel interference in ieee 802.11n. *2012 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1163–1168, 2012.

[16] Akella A, Judd G, and Seshan S. Self-management in chaotic wireless deployments. *Wireless Networks*, 13(6):737–755, 2007.

[17] Chieochan S, Hossain E, and Diamond J. Channel assignment schemes for infrastructure-based 802.11 wlans: A survey. *IEEE Communications Surveys & Tutorials*, 12(1):124–136, 2010.

[18] Tam Wee Sin, Mohd Noor Halim, Janardhana Reddy Naredula, Mao Hui Fang, and Kevin Payne. Quality of transmission across packet-based networks, 2002.

[19] Abdelnasser H, Youssef M, and Harras K A. Wigest: A ubiquitous wifi-based gesture recognition system. *Computer Communications (INFOCOM), 2015 IEEE Conference on. IEEE*, pages 1472–1480, 2015.

[20] Zhang Z L, Chen H M, and Huang T P. A channel allocation scheme to mitigate wifi interference for wireless sensor networks. *Jisuanji Xuebao(Chinese Journal of Computers)*, 35(3):504–517, 2012.

[21] H3C WA Series Access Points Configuration Guide-6W112. H3c corp. *http://www.h3c.com.hk*, 2016.

[22] 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.

[23] 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.

[24] Tytgat L, Yaron O, and Pollin S. 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.

[25] Shi G, Xu R, and Shu Y. Exploiting temporal and spatial variation for wifi interference avoidance in zigbee networks. *International Journal of Sensor Networks*, 18(3-4):204–216, 2015.

[26] Lee L, Kang G, and Zhang X. 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.

[27] Yan Y, Yang P, and Li X Y. Wizbee: Wise zigbee coexistence via interference cancellation with single antenna. *Mobile Computing, IEEE Transactions on*, 14(12):2590–2603, 2015.

[28] Almeida E, Cavalcante A M, and Paiva R C D. Enabling lte/wifi coexistence by lte blank subframe allocation. *Communications (ICC), 2013 IEEE International Conference on. IEEE*, pages 5083–5088, 2013.

[29] Tan W L, Bialkowski K, and Portmann M. Evaluating adjacent channel interference in ieee 802.11 networks. *IEEE Vehicular Technology Conference. IEEE*, pages 1–5, 2010.