Detection and Localization of Hidden Wi-Fi Cameras

Rhys Cunningham
School of ICT
Griffith University
Australia
rhys.cunningham@griffithuni.edu.au

Wee Lum Tan
School of ICT
Griffith University
Australia
w.tan@griffith.edu.au

***Abstract*— The widespread availability of Wi-Fi networks in our workplaces, schools, hotels, and public spaces provides us with access to the Internet from just about anywhere. An increasing range of devices are being developed with Wi-Fi capabilities including devices such as surveillance or "spy" cameras that allow for remote viewing of a live feed. News reports have shown hidden cameras being placed illegally, or without consent, in places including hotel rooms, workplaces, schools, and rental homes. This is a malicious invasion of privacy and has potential to facilitate extortion or blackmail. Current methods of finding hidden cameras typically involve manual surveying of the environment, radio frequency detectors, or the use of some smartphone cameras that cause infrared light to become visible. These methods can be ineffective, unreliable, or incur extra costs for hardware. The addition of Wi-Fi functionality in these maliciously placed devices, while enabling ease of remote viewing and access for the intruder, also creates a means of identifying and localizing them. In this paper, we investigate potential signal metrics to detect and localize hidden Wi-Fi cameras. We use signal metrics such as Received Signal Strength Indicator (RSSI), Channel State Information (CSI) and Power Delay Profile (PDP) to determine the direction of the received Wi-Fi signal as well as estimate the distance to the hidden Wi-Fi camera. Our results show that these signal metrics can be used to detect and localize a hidden Wi-Fi device, with the CSI and PDP signal metrics achieving the best performance in scenarios with line-of-sight and non-line-of-sight to the hidden camera.**

Keywords— Hidden Wi-Fi camera, RSSI, CSI, PDP

I. Introduction

Advancements in technology have led to widespread availability of wireless networks in our homes, schools, workplaces, and public spaces. Wi-Fi functionality has also become prevalent in many electronic devices. Examples of this are surveillance or "spy" cameras that are now available with Wi-Fi capabilities. Such cameras provide access to cloud storage or the ability to view video feeds in real-time from anywhere in the world. Spy cameras are becoming more compact which makes them much easier to hide. News articles have shown hidden cameras being found in inappropriate locations such as bathrooms, hotel rooms, schools, and rented homes [1]–[3]. This is an incredible invasion of privacy. Currently, these malicious hidden cameras are discovered accidentally or require visual investigations of the environment to locate. Technologies that can assist with detection are radio frequency detectors [4], front-facing phone cameras that can display infrared signals, and smartphone applications that map the local wireless network to identify connected devices [5], [6]. These methods can be tedious, time-consuming, or simply do not provide enough information to identify the location of the device. With the inclusion of Wi-Fi functionality, transmissions from hidden cameras can be used in Wi-Fi-based detection and localization techniques. This would provide a faster and more accurate means of securing an environment of these Wi-Fi-based hidden cameras.

In this paper, we utilize the hidden camera's Wi-Fi traffic and its associated signal metrics to detect and localize its location. It is well-known that the strength of an RF signal is inversely correlated with the distance to the transmitting device. By constantly measuring the signal strength and moving towards the direction where the signal strength grows stronger, we should be able to eventually locate the transmitting device. Using the Nexmon tool [7] installed on a Raspberry Pi, we extract and process the signal information from the hidden camera's Wi-Fi transmissions to produce three signal metrics: Received Signal Strength Indicator (RSSI), Channel State Information (CSI) and Power Delay Profile (PDP). We compare the performance of these metrics in determining the direction of the received Wi-Fi signal as well as estimate the distance to the hidden camera. We perform multiple experiments with the Wi-Fi camera and Raspberry Pi in the same room (line-of-sight scenario), in different rooms (non-line-of-sight scenario) as well as with the camera "uncovered" and "covered" (to emulate a hidden camera scenario). Our results show that RSSI metric only performs well in the direct line-of-sight scenario, and leads to poor performance in non-line-of-sight scenarios. On the other hand, both the CSI and PDP metrics perform well in both line-of-sight and non-line-of-sight scenarios, irrespective of whether the camera is "covered" or "uncovered".

The remainder of the paper is organized as follows. We briefly discuss related works in Section II, and describe the hidden camera detection methodology, signal metrics and data collection and processing procedures in Section III. We present and discuss the experiment results in Section IV and conclude this paper in Section V.

II. Related Works

Since hidden Wi-Fi cameras typically need to send video feeds or recordings across the network, their network transmissions can be used against them. There are a couple of works that detect the presence/existence of a hidden Wi-Fi camera by analysing wireless traffic to recognize the distinct traffic patterns of wireless cameras [8], [9]. Unfortunately these works only detect the existence of a Wi-Fi camera but cannot identify the location of the camera. In this paper our focus is on the localization of the hidden camera, and that the presence of the hidden camera has already been established through these traffic analysis methods.

There are also works that have used measurements of received signal strength in path loss propagation models to perform distance estimation between a wireless transmitter and receiver [10]–[12]. Localization in these works rely on the triangulation method using the estimated distances to multiple

wireless transmitters in order to locate the receiver. Our work differs from them in that there is only one wireless transmitter (i.e. the hidden Wi-Fi camera) and we are using the Raspberry Pi as the receiver in order to locate the transmitter. The related work that is closest to ours is [13] where the authors used the CSI of Wi-Fi signals to localize a rogue AP (or any other wireless transmitter). Their proposed framework consists of the direction determination and position estimation components. Whilst our work utilized a similar direction determination approach, we also compare the performance of three Wi-Fi signal metrics (RSSI, CSI and PDP) in direction determination as well as distance estimation to the hidden Wi-Fi camera.

III. Hidden Wi-Fi Camera Detection Procedure

A. Overview

In our work, we focus on the localization of the hidden Wi-Fi camera. The presence of the hidden camera and its associated MAC address are identified through the traffic analysis methods proposed in [8], [9].

Localizing a single wireless transmitter (the hidden Wi-Fi camera) using just a single receiver is challenging. While we could measure the received signal strength and use path loss propagation models to estimate the distance between the receiver and transmitter, this by itself only narrows down the transmitter's location to a circle with a radius corresponding to the estimated distance. We could take multiple measurements at three different positions and then use the triangulation method to locate the transmitter, however this can be a bit cumbersome and its accuracy is highly dependent on the distance estimation calculations. To make the search more efficient, a direction is required. The work in [13], [14] showed the effects of disrupting the line-of-sight (LOS) between a transmitter and receiver. If there is a direct, non-blocking LOS between the transmitter and receiver, then the received signal strength would be strong. On the other hand, if there is an object blocking the LOS between the transmitter and receiver, then the received signal strength would be weak. Using these observations, by holding the receiver device close to the body and simply turning on the spot until the LOS is broken, the direction of the received signal (i.e. the direction of the transmitter) can be determined as shown in Fig. 1.

The localization process is then to determine the direction of received signals, estimate the distance in the identified direction, walk in the identified direction, and the device will be in the area that is approximately the estimated distance away. This should be a simple and direct process in LOS conditions. In non-line-of-sight (NLOS) scenarios where for example the transmitter and receiver devices are in different rooms, the determined direction may follow the signal path around obstacles (e.g. furniture, doors) that are blocking the LOS. In these situations where one encounters an obstacle, the localization process can be modified as follows: bypass the obstacle, for example walk around the furniture or walk through the door, and then repeat the direction determination process. If the determined direction leads to a dead end, e.g. a corner or a wall, we also repeat the direction determination process at that dead end. In addition we also repeat the direction determination process if there is a drop in the received signal strength due to us walking too far away from the transmitter. We use the term "adjustment" to refer to this repeat of the direction determination process in these NLOS situations.

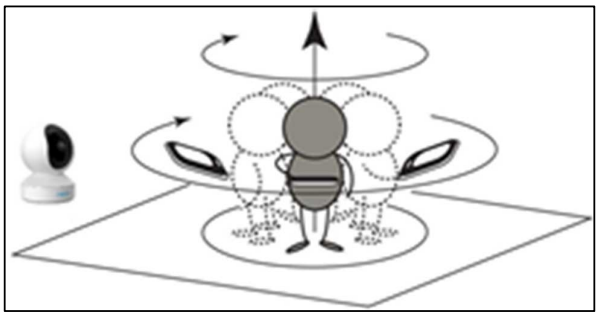


Fig. 1. Direction determination procedure to determine the direction of the received signal [14]

B. Signal Metrics

We perform the direction determination and distance estimation processes using three signal metrics: Received Signal Strength Indicator (RSSI), Channel State Information (CSI) and Power Delay Profile (PDP).

As the wireless signal propagates from the transmitter to the receiver, it will naturally decay in strength the further it travels. Indoor environment with obstacles (e.g. furniture, walls, people) additionally introduces effects such as absorption, scattering and reflection of the signal that can be detrimental to signal propagation and reception. The receiver typically receives multiple copies of the same signal, with each copy of the signal experiencing different delay and attenuation in their respective signal paths. This is known as multipath. The three signal metrics above are used to represent a measurement of the signal strength at the receiver, whilst handling the multipath effect in different ways.

RSSI is a popular signal metric used for localization due to it being easily accessible on many wireless devices. RSSI is a coarse-grained measured value that represents the average power across all copies of received signals. Due to its inability to filter out signals disproportionately impacted by multipath effects, RSSI values can greatly vary as shown in Fig. 2. Averaging the RSSI values over a period of time while filtering for outliers can reduce the overall volatility.

CSI is a set of fine-grained physical information that measures the channel conditions between the transmitter and receiver [7]. Its purpose is to provide information on how the signals are being received so the transmitter can adaptively optimise the communication throughput according to the

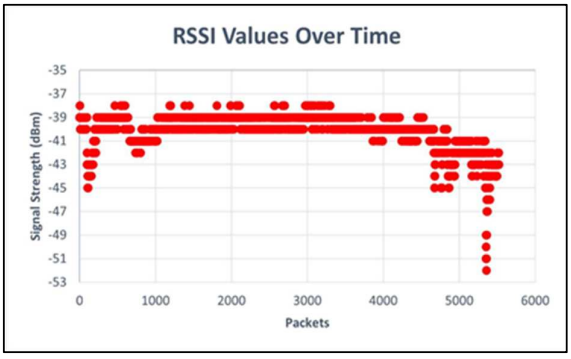


Fig. 2. RSSI values across 5500 packets

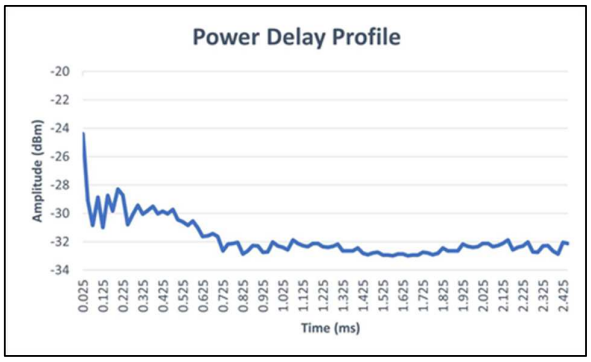


Fig. 3. Power delay profile showing amplitudes of received signals over time

wireless environment. Compared to the RSSI metric that is a coarse-grained average power over all the OFDM subcarriers and hence provides only one RSSI value per packet, the CSI metric is a 3D matrix that describes the received amplitude and phase of each OFDM subcarrier. The CSI metric provides a better representation of the received signal strength than the RSSI metric in complex indoor environment where multipath signals are prevalent.

The PDP metric captures the strength of different received signal paths over time (see Fig. 3). It is obtained by converting the CSI from the frequency domain into the time domain using the Inverse Fast Fourier Transform (IFFT) algorithm. The first signal component in the PDP is known as the direct path signal, i.e. it traversed the least distance amongst all the received signal paths. In LOS conditions the direct path signal likely travelled in a straight line to the receiver. In [13], it was shown that when blocking the LOS it was only the direct path signal that contained a noticeable decrease in signal strength. This makes the direct path signal useful in obtaining a more representative signal strength measurement that better reflects the path loss between the transmitter and receiver.

C. Data Collection and Processing

A Reolink E1 Pro camera using the Wi-Fi standard 802.11n was selected as the hidden device to be localized. We used a Raspberry Pi model 4B+ as the receiver device to detect and localize the hidden camera. The Raspberry Pi monitors the Wi-Fi channels to extract the MAC address of the hidden camera and measures the received signal strength. It runs a modified version of the Nexmon firmware [7] that could extract both the RSSI and CSI signal metrics from received Wi-Fi frames. The main purpose of Nexmon is to extract signal information from Wi-Fi transmissions. It does this by configuring the device's Wi-Fi chip for monitor mode where it will listen to a Wi-Fi channel. Upon reception of a Wi-Fi frame, Nexmon will collect the signal measurements from the appropriate registers as the Wi-Fi chip is processing the frame. This information is then placed into a UDP packet and forwarded to port 5500 where it can be captured by any applications that are listening on that port.

The process for data collection consists of:

1) The Wi-Fi camera sends a live video feed to a remote server.
2) The Raspberry Pi running Nexmon detects the Wi-Fi transmissions.
3) Nexmon extracts the source MAC address, RSSI value, and CSI matrix.
4) For each Wi-Fi frame, a UDP packet containing the extracted information is crafted and forwarded to port 5500.
5) Tcpdump is configured to listen on port 5500 and collects the UDP packets to be stored in a PCAP file.
6) The PCAP file is then read using CSIKit [15], a python-based CSI processing tool

The raw signal measurements that are obtained contain some contaminations in the CSI amplitude values due to hardware imperfections and signal processing limitations [16]–[18]. We used specific processes to remove these contaminants as described below. The sanitised dataset also contains outliers that will skew the measured values and create inaccuracies in the localization. Once the outliers have been filtered, the remaining CSI amplitude values can be averaged and applied to the direction determination and distance estimation methods.

Automatic Gain Control: Nexmon collects the CSI data after it passes through the Automatic Gain Control (AGC) process which multiplies the received amplitudes by an unknown factor for stability. To mitigate the effects of the AGC, we used the method proposed in [16] to obtain a scaling coefficient using the RSSI and CSI of the received frame. CSIKit [15] uses the scaling coefficient to scale the CSI automatically while it is being read from the PCAP file.

Subcarrier Removal: The received CSI matrix contains information for all pilot, null, guard, and data OFDM subcarriers in the channel. The pilot subcarriers are used as reference markers for the rest of the subcarriers while null and guard subcarriers are used to protect against interference. Data subcarriers are used to transmit the required data. The pilot, guard, and null subcarriers are either not modulated or use a different modulation from the data subcarriers [17]. They can contain extreme or arbitrary values that skew the dataset and reduce the accuracy of the measurements, and thus are removed.

Outlier Removal and Averaging: We continuously process a moving window of 500 UDP data packets in the tests to produce the signal metrics. Given the random multipath effects on subcarrier signals, averaging across these packets after filtering for outliers is used to stabilise the received values. Signal amplitudes that are outside of two standard deviations of the mean are considered outliers and removed from the dataset. This was applied to the RSSI values and PDP direct path signals across all packets, and CSI subcarriers within each packet. After the removal of the outliers, the RSSI and PDP values are then averaged across all packets while the CSI amplitudes are averaged per subcarrier across all packets.

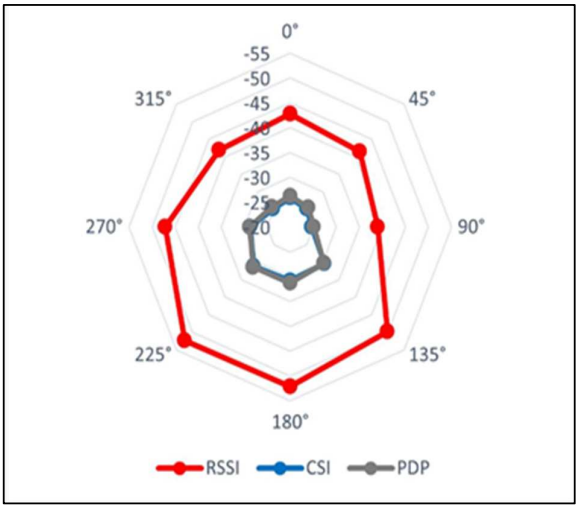
IV. Results And Discussions

We conducted several experiments to evaluate the performance of the three signal metrics in localizing the hidden Wi-Fi camera. Our experiments are conducted indoors in a residential home shown in Fig. 4. We first evaluated the accuracy of the signal metrics in the direction determination process. We placed the camera on a stool chair in the lounge room at a height of 1.3m to be in line with the height of the Raspberry Pi when held. We captured the Wi-Fi signal transmissions from the camera at several locations in the home: lounge room, dining room and bathroom, while standing and turning at 45-degrees increment at a spot. The distances of the three locations from the camera are approximately 2m, 6m, and 12m away respectively.

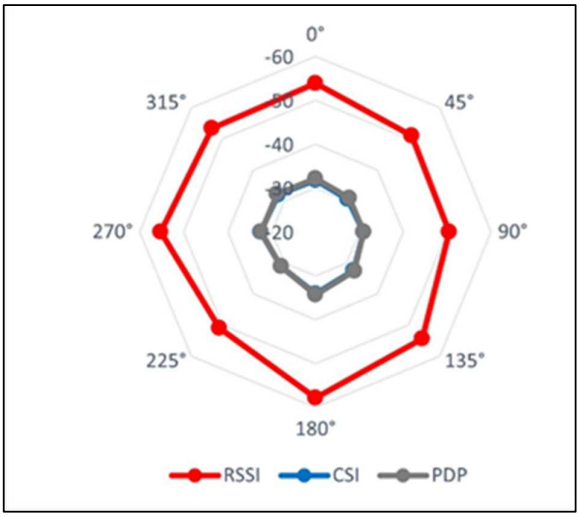
Fig. 4. Camera placement and Wi-Fi signal capture locations in 45-degrees increment

The radar graphs in Fig. 5 show the average signal amplitudes for RSSI, CSI, and PDP in eight directions in the lounge room, dining area, and bathroom, respectively. Note that the graphs for CSI and PDP are overlapping each other due to their very similar results in this experiment. At each location, the zero degrees (0°) direction is the direction facing towards the camera. We see that for the lounge room and the dining room, the direction of 180° has the weakest signal amplitude. This corresponds to the NLOS scenario where the human body holding the Raspberrry Pi is blocking the camera's signal. Thus we can infer that the camera is located in the opposite direction (i.e. the 0° direction). In the bathroom location, the 270° direction has the weakest signal amplitude. Since the entrance to the bathroom is approximately the 90° direction, this suggests the camera's signal path through the bathroom's entrance may have been the strongest and is then obstructed by the human body, leading to the 270° direction having the weakest signal amplitude. Overall, we see that the three signal metrics provide reasonably good performance in determining the direction of the Wi-Fi camera.

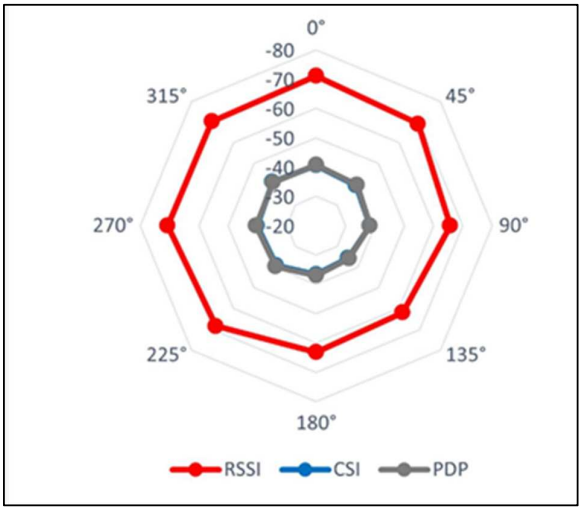
Next we conducted experiments to evaluate the signal metrics performance in localizing the hidden Wi-Fi camera. We hid the camera in various locations in the lounge room: in a basket on the floor covered by a blanket, on a stool placed in a corner and surrounded by cushions, and on top of a wall-mounted air-conditioning unit at about ceiling level. We start the localization process at the entrance to the lounge room, and evaluated the performance of the three signal metrics in terms of the number of "adjustments" that we need to make in order to successfully locate the hidden camera. Recall that an adjustment is basically repeating the direction determination process in cases where an obstacle or a dead end is encountered, or when there is a drop in the received signal amplitude.



(a) Lounge Room

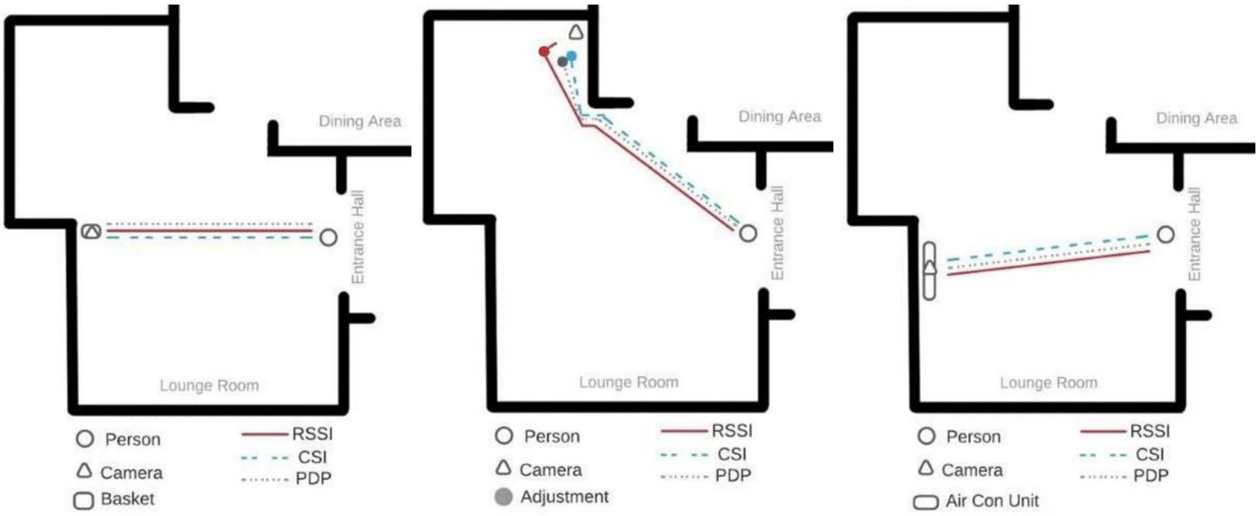


(b) Dining Room



(c) Bathroom

Fig. 5. Average signal amplitudes measured in the lounge room, dining room, and bathroom across 8 directions from the camera



(a) Camera hidden in basket covered by blanket

(b) Camera placed on a stool around a corner, surrounded by cushions

(c) Camera hidden above a wall-mounted air-conditioning unit

Fig. 6. Paths taken to localize the hidden Wi-Fi camera for three locations in lounge room

Fig. 6 shows the experiment results where we see the hidden camera in the scenarios in the basket and on the air-conditioning unit was immediately identified by the three signal metrics in the localization process. In the scenario where the hidden camera was located in the corner of the room, the localization process initially led to the wall behind which the camera was located. An adjustment was made after walking around the wall, and subsequently all the three signal metrics successfully pointed towards the hidden camera. These results show that the hidden camera can be localized at various heights as well as when it is covered by materials such as blankets and cushions.

The final experiment was to locate the hidden Wi-Fi camera when we start the localization process from a room that is much further away. The camera is again hidden in a basket covered by a blanket in the lounge room, while we start the localization process in the bathroom that is approximately 12m away. Fig. 7 shows the paths determined via the CSI and PDP signal metrics. Both signal metrics initially led us out of the bathroom to the far end of the dining room where an adjustment was made, which then led us through the entrance to the lounge room where another adjustment was made to finally locate the hidden camera. On the other hand, the RSSI signal metric was unable to help us determine the direction of the covered camera in the bathroom and hence couldn't be used to locate the hidden camera. In this complex environment, the results show that adjustments are required when there is no LOS between the transmitter and receiver.

Fig. 7. Paths taken to localize the hidden Wi-Fi camera in lounge room from a starting location in the bathroom

V. Conclusions

In this paper, we identified the problem of the malicious placement of hidden cameras that invade the privacy of unsuspecting employees, students, hotel patrons, and rental tenants. We have devised a method for the detection and localization of hidden Wi-Fi cameras in an indoor environment. Localization of the detected device made use of collected signal measurements for direction determination and distance estimation. This was performed using the Nexmon tool to monitor a Wi-Fi channel and extract signal metrics from the Wi-Fi camera's transmissions. We conducted experiments to compare the performance of three signal metrics RSSI, CSI, and PDP in locating the hidden camera. Our results show that RSSI metric only performs well in direct LOS scenario, and leads to poor performance in NLOS scenarios. On the other hand, both the CSI and PDP metrics perform well in both LOS and NLOS scenarios, irrespective of whether the camera is "covered" or "uncovered". The proposed localization method can successfully lead a user to locate a hidden Wi-Fi camera. This work can be utilised in smartphone applications to provide a means of securing the user's surroundings from malicious Wi-Fi devices, hence creating some sense of safety or reassurance.

REFERENCES

[1] "Sydney landlord jailed over hidden cameras", 2020. Available: https://7news.com.au/news/crime/sydney-landlord-jailed-over-hidden-cameras-c-39493.

[2] "Workers sue Illinois dental practice over hidden cameras found in bathroom", 2020. Available: https://nypost.com/2020/12/11/workers-suedental-practice-over-hidden-cameras-found-in-bathroom/.

[3] "Hundreds of motel guests were secretly filmed and live-streamed online", 2019. Available: https://edition.cnn.com/2019/03/20/asia/south-korea-hotel-spy-cam-intl/index.html.

[4] "Best hidden camera detector in 2022: hunt out bugs, trackers and spy cams", Available: https://www.digitalcameraworld.com/au/buying-guides/best-hidden-camera-detector.

[5] "How to find hidden cameras in your Airbnb or hotel room", 2021. Available: https://toomanyadapters.com/find-hidden-cameras/.

[6] "How to find hidden cameras in any place you stay", 2021. Available: https://www.rd.com/list/find-out-hidden-camera-hotel-room/.

[7] F. Gringoli, M. Schulz, J. Link and M. Hollick, "Free your CSI: A channel state information extraction platform for modern Wi-Fi chipsets", in Procs of the 13th International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization - WiNTECH, 2019.

[8] Y. Cheng, X. Ji, T. Lu and W. Xu, "On detecting hidden wireless cameras: a traffic pattern based approach", in IEEE Transactions on Mobile Computing, vol. 19, no. 4, pp. 907-921, 2020.

[9] K. Wu and B. Lagesse, "Do you see what I see? Detecting hidden streaming cameras through similarity of simultaneous observation," in Procs. IEEE International Conference on Pervasive Computing and Communications (PerCom), 2019.

[10] A. Zanella and A. Bardella, "RSS-based ranging by multichannel RSS averaging", in IEEE Wireless Communications Letters, vol. 3, no. 1, pp. 10-13, 2014.

[11] K. Wu, Jiang Xiao, Youwen Yi, Min Gao and L. M. Ni, "FILA: Fine-grained indoor localization," in Procs IEEE INFOCOM, 2012.

[12] R. Yang, X. Yang, J. Wang, M. Zhou, Z. Tian and L. Li, "Decimeter level indoor localization using WiFi channel state information," in IEEE Sensors Journal, vol. 22, no. 6, pp. 4940-4950, March, 2022.

[13] C. Wang, X. Zheng, Y. Chen and J. Yang, "Locating rogue access point using fine-grained channel information," in IEEE Transactions on Mobile Computing, vol. 16, no. 9, pp. 2560-2573, Sept. 2017

[14] H. Zhang, X. Zhou, W. Zhang, Y. Zhang, G. Wang, B. Zhao, and H. Zheng, "I am the antenna: accurate outdoor AP location using smartphones," in Procs ACM MobiCom 2011.

[15] G. Forbes, "CSIKit: Python CSI processing and visualisation tools for commercial off-the-shelf hardware", https://github.com/Gi-z/CSIKi/

[16] Z. Gao, Y. Gao, S. Wang, D. Li and Y. Xu, "CRISLoc: Reconstructable CSI fingerprinting for indoor smartphone localization," in IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3422-3437, Mar. 2021.

[17] A. R. Voggu, V. Vazhayil and M. Rao, "Decimeter level indoor localisation with a single WiFi router using CSI fingerprinting," in Procs. IEEE Wireless Communications and Networking Conference (WCNC), 2021.

[18] N. Tadayon, M. T. Rahman, S. Han, S. Valaee and W. Yu, "Decimeter ranging with channel state information," in IEEE Transactions on Wireless Communications, vol. 18, no. 7, pp. 3453-3468, July 2019.