Detection of Suspicious Objects Concealed by Walking Pedestrians Using WiFi

Bao Zhou, Zuona Chen, Ziyuan Gong, Rui Zhou
School of Information and Software Engineering, University of Electronic Science and Technology of China
Email:ruizhou@uestc.edu.cn

***Abstract*—Security is of vital importance in public places. Detection of suspicious objects such as metal and liquid often requires dedicated and expensive equipment, preventing its wide deployment. This paper proposes a pervasive device-free method to detect suspicious objects concealed by walking pedestrians using WiFi Channel State Information (CSI). By analyzing the different variations of subcarrier amplitude caused by different materials, the proposed method is able to detect suspicious objects such as metal and liquid concealed by pedestrians, when they walk through the transmission link of the WiFi transmitter and receiver. The proposed method employs Convolutional Neural Network (CNN) to classify suspicious objects, on which majority voting is applied to vote for the final result, in order to improve the detection accuracy for walking pedestrians. Evaluations show that the proposed method with majority voting achieve the detection accuracy of 93.3% for metal and liquid concealed by walking pedestrians, 95.6% for exposed metal and liquid carried by walking pedestrians, and 100% for metal and liquid carried by standing pedestrians.**

***Index Terms*—Channel State Information, Convolutional Neural Network, majority voting, suspicious object detection.**

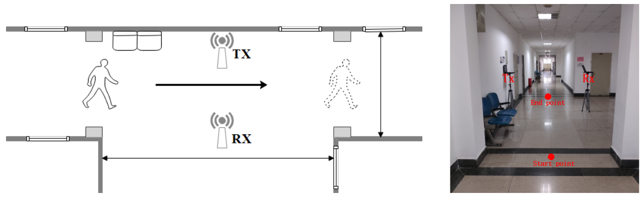
I. Introduction

Security is of vital importance in public places, such as schools, amusement parks, shopping plazas and public transportation. However, security protection measures in these places are often weak. Suspicious objects like knives and explosive liquid are easy to be carried to these places without being detected. Common approaches of suspicious object detection include handheld metal detector, X-ray screening machine and security gate, which are deployed in airports and railway stations. However, deploying such dedicated equipment is impractical in most public places, due to high cost, inconvenience or harmfulness. There is a great need of a convenient, low cost and harmless approach to detect suspicious objects carried by pedestrians.

There have been some solutions to detect suspicious objects. Camera-based schemes identify suspicious objects by analyzing their shape, color and texture [1], [2]. As cameras work in line of sight, camera-based schemes cannot detect concealed objects. Radio Frequency Identification (RFID) systems detect objects by attaching tags to them and collecting information from these tags [3], [4]. However, criminals would not attach tags on their objects to be detected. Radar is able to detect and locate objects on the basis of Doppler effect [5], but radar is expensive and restricted in sale, hindering its civilian use. X-ray [6] and Computed Tomography (CT) [7] are able to detect hidden objects. However, exposure to X-ray may increase the risk of cancer, thus they are not suitable for detecting objects carried by pedestrians.

Ubiquitous WiFi offers an opportunity to replace dedicated equipment for suspicious object detection. Due to Multiple-Input Multiple-Output (MIMO) and Orthogonal Frequency Division Multiplexing (OFDM) techniques, fine-grained Channel State Information (CSI) can be retrieved from the physical layer of wireless channels. CSI provides finer and stabler information than the commonly used Received Signal Strength Indication (RSSI) and has attracted considerable attentions in recent years. Researchers have explored the use of CSI for novel applications, such as user identification [8], [9], activity recognition [10], [11] and indoor localization [12], [13]. Pioneer studies also explored the use of CSI to detect objects. TagFree [14] aimed to distinguish multiple exposed objects. The system in [15] could detect metal and liquid objects in baggage and estimate their shape or volume. Wi-Metal [16] could detect metal carried by a standing pedestrian and calculate the distance between the metal and the detector. The method in [17] could identify a large exposed metal sheet carried by a walking pedestrian. The existing work of object detection using WiFi CSI could detect in-baggage objects, exposed objects, or large objects. However, suspicious objects are often concealed by pedestrians and need to be detected during normal walking. Both pedestrian walking and object concealing introduce noise into the detection process, making object detection more difficult.

Hence in this paper we propose a WiFi CSI-based device-free method to detect metal and liquid objects concealed by walking pedestrians. The application scenarios are as Fig. 1 shows, in which a pair of WiFi transmitter (TX) and receiver (RX) acts as the detectors. When a pedestrian walks through the transmission link, the concealed suspicious objects can be detected by analyzing its influence on wireless signals. The contributions of the paper are summarized as follows. (1) Propose a method to detect suspicious objects concealed by walking pedestrians using WiFi CSI. (2) Apply Convolutional Neural Network (CNN) to classify suspicious objects by analyzing CSI amplitude. (3) Apply majority voting on the results of CNN classification to achieve high accuracy for walking pedestrians. (4) In addition to detecting suspicious objects concealed by walking pedestrians, the method is able to detect concealed and exposed objects carried by walking and standing pedestrians as well as in baggage. (5) Compare the proposed method with the existing methods and analyze



(a) The setup (b) The environment

Fig. 1: The evaluation environment.

the impact of parameters on detection accuracy.

The remainder of the paper is organized as follows. Section II introduces CSI briefly and explains the rationale of suspicious object detection. Section III proposes the method of detecting suspicious objects concealed by walking pedestrians using CNN and majority voting. Section IV reports the experimental evaluations. Section V concludes the paper.

II. Preliminary and Rationale

Channel Impulse Response (CIR) is often used to describe the multipath effect of wireless channels, represented as

$$h(\tau) = \sum_{i=1}^{n} a_i e^{-j\theta_i}\delta(\tau - \tau_i) \tag{1}$$

where a_i, θ_i and τ_i denote the amplitude, phase and time delay of the i-th path, n is the number of paths, and $\delta(\cdot)$ is the Dirac delta function. Channel Frequency Response (CFR) can be acquired by Fourier Transform of CIR. Leveraging commodity Network Interface Card (NIC) with modified firmware and driver [18], a discrete version of CFR can be revealed to the upper layers in the format of CSI, described as

$$H(f_k) = |H(f_k)|e^{j\angle H} \tag{2}$$

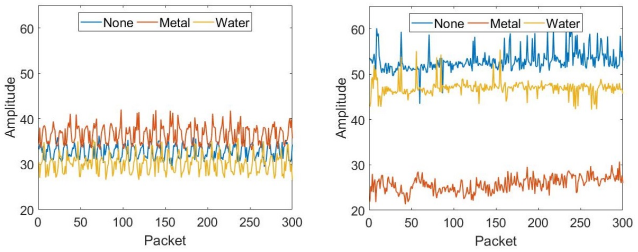
where $H(f_k)$ represents the subcarrier whose central frequency, amplitude and phase are denoted as f_k, $|H(f_k)|$ and $\angle H$. Assume N_{tx} and N_{rx} represent the numbers of transmitting and receiving antennas, the raw CSI data contain the CSI matrix H, expressed as

$$H = (H_{ij})_{N_{tx}\times N_{rx}} \tag{3}$$

where H_{ij} is the CSI of transmitting antenna i and receiving antenna j, consisting of N_s subcarriers

$$H_{ij} = [H(f_1), H(f_2), \cdots, H(f_{N_s})] \tag{4}$$

To verify the feasibility of suspicious object detection using CSI, we conduct experiments to demonstrate that different types of suspicious objects concealed by pedestrians can cause different influence on wireless signals. In the experiments, the volunteer walks through the transmission link between the transmitter and the receiver for three times, carrying nothing, hiding a metal knife in sleeve, and hiding a bottle of water in pocket, respectively. Fig. 2(a) plots the CSI amplitude of one subcarrier for the three walks. As a comparison, Fig. 2(b) plots the CSI amplitude of one subcarrier when a bag moves through the transmission link, containing nothing, a metal knife and a bottle of water, respectively. The two figures show that different types of suspicious objects cause different amplitude patterns, which can be analyzed to identify the objects. Due to the influence of human body, the amplitude patterns of different objects carried by pedestrians do not differ as much as in baggage, hence it is more challenging to detect suspicious objects concealed by pedestrians than in baggage. Even though, the CSI amplitude patterns of different suspicious objects hidden by walking pedestrians still have obvious differences, indicating the possibility of distinguishing them, but requiring a strong classifier.



(a) By pedestrian (b) In baggage

Fig. 2: CSI amplitude of one subcarrier when concealing different objects by pedestrian or in baggage.

III. Detection Method

Device-free detection of suspicious objects is deployed in the scenarios as shown in Fig. 1. When a pedestrian walks through the transmission link between the WiFi transmitter and receiver, the proposed method can detect whether the pedestrian carries suspicious objects and what objects they are. The structure of the proposed detection method is illustrated in Fig. 3. The raw CSI data are collected by the receiver during the pedestrians walking. After denoising by filtering, the detection segments are extracted from the CSI data and converted to images. The images labeled with the corresponding object types are used to train the CNN classification model. For object detection, the testing images converted from the CSI data are input to the CNN model to obtain the classification results, on which majority voting is applied to obtain the final voted decision. The object with the maximal votes is regarded as the final object.

A. Data collection

The WiFi transmitter sends packets to the receiver. The CSI data are retrieved from the received packets. The raw CSI data contain the information of all the subcarriers, expressed as:

$$\bar{r} = [h_1, h_2, \cdots, h_i, \cdots, h_N] \tag{5}$$

where h_i is a complex containing the amplitude and phase of subcarrier i, $N = N_{tx}N_{rx}N_s$ represents the number of subcarriers. As the phase information has random shift, we

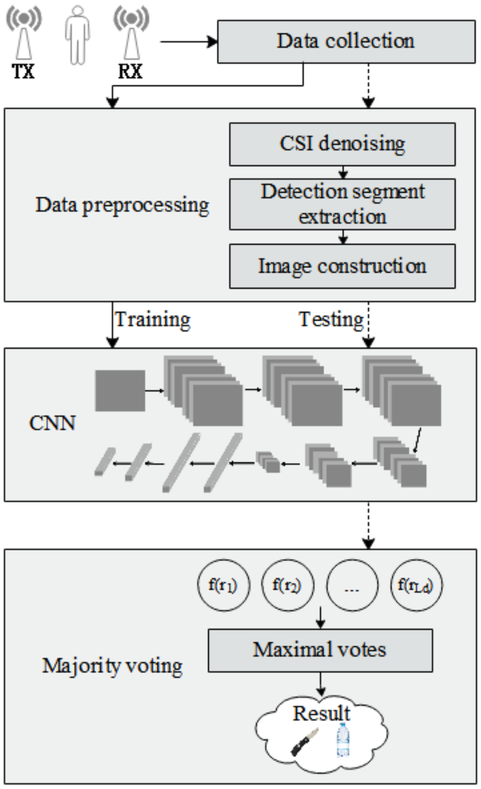


Fig. 3: Structure of the proposed detection method.

exploit the amplitude information to realize suspicious object detection. Hence we obtain the vector of CSI amplitude

$$r = [|h_1|, |h_2|, \cdots, |h_i|, \cdots, |h_N|] \tag{6}$$

where $|h_i|$ represents the amplitude of subcarrier i. A low-pass filter is applied on r to reduce the noise.

B. Detection segment extraction

When no pedestrian passing, the environment is relatively static, thus the CSI amplitude is relatively stable. When a pedestrian passes through the transmission link, the CSI amplitude will fluctuate significantly. The significant fluctuation part is the active segment. We apply the anomaly detection algorithm based on Local Outlier Factor (LOF) [19] to detect and extract the active segment S_a, denoted as a sequence of CSI amplitude vectors:

$$S_a = [r_1, r_2, \cdots, r_i, \cdots, r_{L_a}] \tag{7}$$

in which r_i represents a CSI amplitude vector, and L_a is the length of the active segment. The time complexity of LOF is $O(n^2)$, n is the number of CSI vectors. For each passing approximately 500 CSI vectors are collected. LOF takes 0.0049s to detect the active segment on an Intel i5 3.2GHz processor.

Not all the CSI amplitude vectors in the active segment contribute to detecting suspicious objects. As the WiFi signals begin to fluctuate when a pedestrian is approaching and the fluctuation weakens when the pedestrian is leaving, the middle part of the active segment is the most important, where the pedestrian is just crossing the transmission link. Therefore, we extract the middle part of the active segment to form the detection segment. From the central point of the active segment, we extract every other vector forwards and backwards along the sequence to form the detection segment. The central point in the active segment S_a is $r_{\lceil L_a/2 \rceil}$. The detection segment S_d can be expressed as

$$S_d = [\cdots, r_{\lceil L_a/2 \rceil - 2}, r_{\lceil L_a/2 \rceil}, r_{\lceil L_a/2 \rceil + 2}, \cdots] \tag{8}$$

with the segment length of L_d. Each CSI amplitude vector in the detection segment is converted to an image as the input to the CNN detection model for classification.

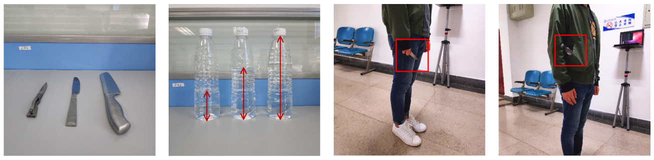
C. CNN detection model

We consider suspicious object detection as a classification problem. Each type of suspicious objects corresponds to a class and unsuspicious objects correspond to a class. Our method focuses on three classes: none, metal and liquid. For the rationale of our method is to analyze the different amplitude patterns caused by different suspicious objects, which is a typical classification problem, we employ a CNN model to automatically extract the features from the images converted from the CSI amplitude vectors and classify them to the corresponding objects. The CNN model consists of 11 layers, with 1 input layer, 3 convolutional layers, 3 max-pooling layers, 1 batch normalization layer, 2 fully connected layers and 1 output layer. The optimizer is Adam and the activation function is Rectified Linear Units (ReLU). The detailed model parameters are listed in Table I. The inputs to the CNN model are the images converted from the CSI amplitude vectors in the detection segments, and the outputs are the object types.

D. Majority voting

For suspicious object detection, the CNN model performs well for standing pedestrians, for which the suspicious objects can be detected with an accuracy of nearly 100% using only one CSI amplitude vector. However, for walking pedestrians, the detection accuracy of the CNN model alone can not meet the application requirements. To deal with this problem, we propose a majority voting algorithm to improve the detection accuracy. During the pedestrian passing through the transmission link, a sequence of CSI amplitude vectors are collected, from which we extract the detection segment from the middle part of the sequence. We first input the image of each CSI vector of the detection segment into the CNN model to obtain the initial classification results, then all the initial classification results vote for the final detection result, the object with the maximal votes is the finally determined object.

Assume the detection segment is represented as $S_d = [r_1, r_2, \cdots, r_{L_d}]$, in which r_i represents the i-th vector, L_d is the length of the detection segment. The CNN classification result of the vector r_i can be represented as $f(r_i)$. Majority voting is to obtain the final detection result for the walking scenario by doing voting on the L_d initial classification results,



(a) Metal objects (b) Liquid objects (c) Hiding knife (d) Hiding water

Fig. 4: Concealed suspicious objects.

the object that gets the maximal votes is regarded as the final result of the detection. The algorithm can be expressed as:

$$\begin{cases} v_j = \sum_{i=1}^{L_d} I(f(r_i) = o_j) \\ o = \arg\max_{o_j} v_j \end{cases} \tag{9}$$

in which, v_j represents the votes of the object o_j, $I(\cdot)$ is the indicator function which equals to 1 if $f(r_i) = o_j$ and 0 otherwise, and o is the final result of detection.

IV. Evaluations

A. Experimental setup

To evaluate the proposed detection method, we conduct experiments on the corridor outside our laboratory. We deploy two laptops equipped with Intel Wireless Link 5300 (IWL5300) NIC on both sides of the corridor, one as the transmitter and the other as the receiver, each with 3 antennas, as Fig. 1 shows. CSI can be retrieved from IWL5300 [18], which contains the amplitude and phase information of 30 groups of subcarriers. As the transmitter and the receiver have 3 antennas each, there are 270 subcarriers altogether. The WiFi devices work in 5GHz and the sampling rate is set as 100Hz. During a pedestrian walking through the transmission link, the CSI data are collected and analyzed, through which suspicious object detection is performed.

In the experiments, we regard knife and water as suspicious objects. Thus there are 3 classes: carrying nothing, hiding a knife and hiding water. We test 3 different sizes of metal knives and 3 different volumes of water, shown in Fig. 4(a) and 4(b). The sizes of the metal knives are small (16cm×1.2cm), medium (22.5cm×1.5cm) and large (30cm×3.5cm). The volumes of water are 180ml (1/3 bottle), 360ml (2/3 bottle), and 540ml (full bottle). The knives are totally or nearly totally hidden in the sleeves, the water bottles are partially hidden in the pockets or totally hidden in the handbags, as Fig. 4(c) and 4(d) illustrate.

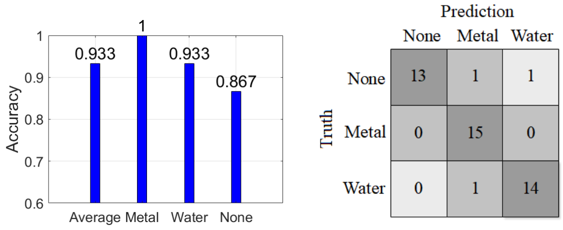
B. CNN model training

The volunteers walk through the transmission link between the transmitter and the receiver at normal speeds. To train the CNN detection model, we conduct 105 walks, which are 15 walks of carrying nothing, 45 walks of hiding a knife (15 walks for each size) and 45 walks of hiding water (15 walks for each volume). After denoising and detection segment extraction with the length of 120, there are 12600 CSI amplitude vectors. They are converted to images to train the CNN detection model. The parameters of the model are listed in Table I.

TABLE I: The CNN detection model.

Input layer	(18 × 15) 2D matrix
2D convolution	Filters=32, Kernel size=(5,5), Activation=ReLU
2D max pooling	Pool size=(2,2)
2D convolution	Filters=32, Kernel size=(5,5), Activation=ReLU
2D max pooling	Pool size=(2,2)
2D convolution	Filters=16, Kernel size=(3,3), Activation=ReLU
2D max pooling	Pool size=(2,2)
1st hidden layer	Nodes=256, Activation=ReLU
2nd hidden layer	Nodes=64, Activation=ReLU
Output layer	Nodes=3, Activation=Softmax
Compiler	Optimizer=Adam, Loss=Cross entropy

For detection testing, we conduct 45 tests/walks, which are 15 walks of carrying nothing, 15 walks of hiding a knife (5 walks for each size) and 15 walks of hiding water (5 walks for each volume). For each test/walk, after denoising and detection segment extraction, each CSI amplitude vector in the detection segment is converted to an image and input to the CNN detection model to obtain the initial classification results, which then vote to decide the final suspicious object for the test/walk.

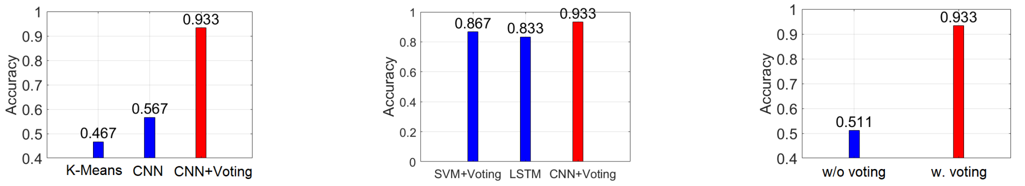


(a) Accuracy (b) Confusion matrix

Fig. 5: Detection accuracy and confusion matrix.

C. Evaluation results

The evaluation results are shown in Fig. 5(a). The average detection accuracy (i.e. correct rate) of concealed suspicious objects by walking pedestrians is 93.3%, with mixed metal sizes and mixed water volumes. To be specific, the proposed method detects metal with the accuracy of 100%, detects water with the accuracy of 93.3%, and detects carrying nothing with the accuracy of 86.7%. The confusion matrix of them is shown in Fig. 5(b). Out of 15 tests of carrying nothing, two tests are detected as metal and water. Out of 15 tests of carrying water, one test is detected as metal. All the 15 tests of carrying metal are detected correctly. The true positive rate (TPR) of suspicious object detection is 100% and the false positive rate (FPR) is 13.3%. To ensure that suspicious objects can be detected, TPR is more important than FPR. High TPR ensures high detection accuracy of suspicious objects. For each detection, the preprocessing takes 0.036s and the prediction takes 0.983s on NVIDIA GeForce MX250.



(a) Comparison with existing work (b) Comparison with other classifiers (c) Impact of majority voting

Fig. 6: Comparison with different methods.

D. Method analysis

1) Compare with existing work: We compare our method with the existing work of suspicious object detection using WiFi. Wi-Metal [16] used K-Means to detect metal and calculate the distance between the metal and the detector. The system in [17] utilized CNN to detect a metallic sheet about 30cm×30cm placed in front of the chest of the pedestrian. We implement two methods based on the two papers and conduct the same experiments. The comparison of them is illustrated in Fig. 6(a), showing that our method achieves the highest accuracy of 93.3% for walking pedestrians with concealed metal and water. As for computational complexity, running on NVIDIA GeForce MX250, our method takes 0.983s for a prediction, CNN takes 0.99s, and K-Means takes 0.0006s.

2) Compare with other classifiers: The proposed detection method employs CNN with majority voting to classify the suspicious objects. We compare CNN with other classifiers: Support Vector Machines (SVM) with majority voting, and Long Short-Term Memory (LSTM) using CSI sequence data without voting. The comparison is illustrated in Fig. 6(b), which shows that CNN with majority voting outperforms SVM with majority voting and LSTM.

3) Impact of majority voting: To improve the accuracy of suspicious object detection for walking pedestrians, we apply majority voting on the results of CNN classification. To prove its effect, we compare the accuracy with and without majority voting, as illustrated in Fig. 6(c). Majority voting improves the accuracy by a large margin from 51.1% to 93.3%.

E. Parameter analysis

1) Concealed vs. exposed: We conduct experiments to compare the accuracy of detecting exposed objects and concealed objects by walking pedestrians. The results are shown in Fig. 7(a). The exposed objects can be detected with the accuracy of 95.6%, slightly higher than the concealed objects. Totally concealed objects and nearly totally concealed objects achieve comparable results.

2) Walking vs. standing: We also conduct evaluations on detecting concealed objects by standing pedestrians, which achieve the accuracy of 100%, much higher than the accuracy of 93.3% for walking pedestrians. The results are shown in Fig. 7(b). As walking introduces noise into wireless signals, it is easier to detect objects concealed by standing pedestrians than walking pedestrians.

3) Pedestrian vs. baggage: We compare the accuracy of detecting concealed objects in baggage and by pedestrians. The in-baggage detection achieves the accuracy of 97.9%, higher than the accuracy of 93.3% by pedestrians, as shown in Fig. 7(c), indicating that human body has more significant impact on object detection than baggage.

4) Pedestrian: To investigate the impact of pedestrian numbers on object detection, 1 to 4 volunteers conduct the experiments with a medium metal knife and 2/3 bottle of water. As shown in Fig. 7(d), the accuracy decreases as the number of pedestrians increases. To investigate the impact of different pedestrians on object detection, 4 volunteers of different Body Mass Index (BMI) conduct the experiments. The results are shown in Fig. 7(e). All the pedestrians achieve the accuracy of more than 90%.

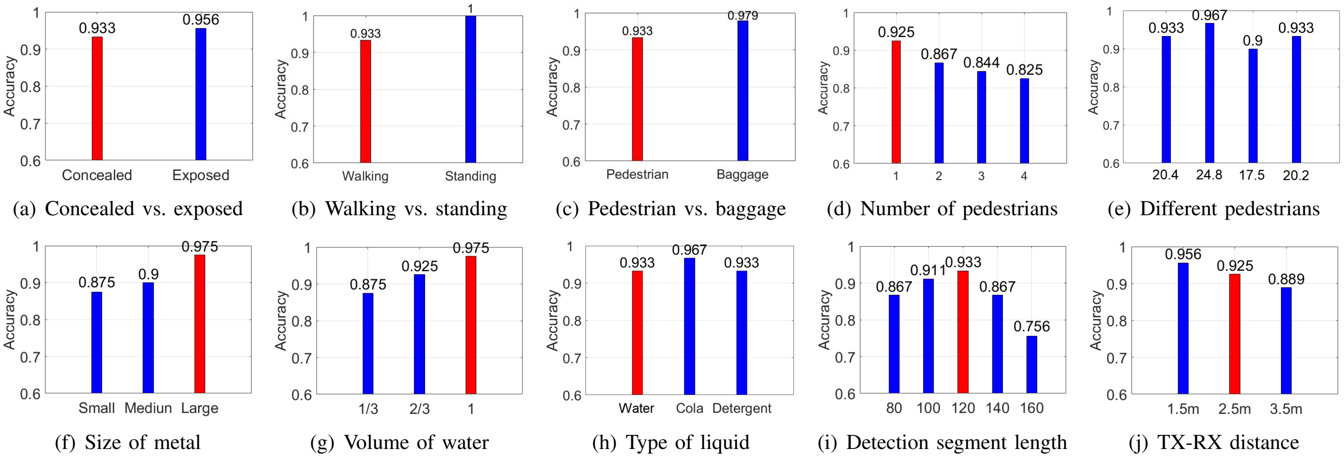
5) Size of metal: We choose different sizes of metal knives to evaluate the impact of metal size on object detection. We conduct 3 groups of experiments: carrying nothing, hiding a metal knife with the size of small, medium and large for each group respectively, and hiding a bottle of water. As shown in Fig. 7(f), the accuracy increases with the metal size.

6) Volume of water: We also choose different volumes of water to evaluate the impact of liquid volume on object detection. We conduct 3 groups of experiments: carrying nothing, hiding a metal knife, and hiding 1/3, 2/3 and a full bottle of water for each group respectively. As shown in Fig. 7(g), the accuracy increases with the liquid volume.

7) Type of liquid: To evaluate the impact of different liquid types on object detection, we conduct 3 groups of experiments: carrying nothing, hiding a metal knife, and hiding a bottle of water, cola and detergent respectively for each group. The results are shown in Fig. 7(h). The detection accuracy is comparable for water, cola and detergent.

8) Length of detection segment: To investigate the impact of the length of the detection segment on object detection, we set the length as 80, 100, 120, 140 and 160 respectively. The results are shown in Fig. 7(i). The length of 120 achieves the highest accuracy of 93.3%. If the detection segment is too short, the data are not enough for a successful model training, while if the detection segment is too long, the data contain irrelevant information, degrading the detection performance.

9) Distance between TX and RX: We place the transmitter and the receiver at a distance of 1.5m, 2.5m, and 3.5m respectively and investigate the impact of the distance. The pedestrian walks through carrying a medium metal knife or



(a) Concealed vs. exposed (b) Walking vs. standing (c) Pedestrian vs. baggage (d) Number of pedestrians (e) Different pedestrians

(f) Size of metal (g) Volume of water (h) Type of liquid (i) Detection segment length (j) TX-RX distance

Fig. 7: Impact of parameters

2/3 bottle of water. The results are shown in Fig. 7(j). The accuracy achieves 95.6% with the distance of 1.5m, 92.5% with 2.5m and 88.9% with 3.5m.

10) Walking direction: The walking directions of pedestrians are perpendicular to the transmission link between the transmitter and the receiver, hence walking in either direction has almost the same impact on object detection. Evaluations for each walking direction achieve comparable results.

V. Conclusion

Suspicious object detection plays an important role in public security. Existing approaches require dedicated equipment and are deployed in specific scenarios such as airports and railway stations. To ensure daily public security with low cost and pervasiveness, this paper exploits commodity WiFi devices to realize suspicious object detection, metal and liquid in particular, concealed by walking pedestrians. The method treats suspicious object detection as a classification problem and employs CNN with majority voting to solve it. Evaluations show that the proposed method detects metal and water concealed by walking pedestrians with the accuracy of 93.3%, detects exposed metal and water with the accuracy of 95.6%. For standing pedestrians, the accuracy achieves 100%. The detection accuracy may degrade with the increment of pedestrians. This issue will be tackled in our future research.

References

[1] C. Su, S. Zhang, J. Xing, W. Gao, and Q. Tian, "Deep attributes driven multi-camera person re-identification," in *European conference on computer vision*. Springer, 2016, pp. 475–491.

[2] S. Chi and C. H. Caldas, "Automated object identification using optical video cameras on construction sites," *Computer-Aided Civil and Infrastructure Engineering*, vol. 26, no. 5, pp. 368–380, 2011.

[3] L. Xie, B. Sheng, C. C. Tan, H. Han, Q. Li, and D. Chen, "Efficient tag identification in mobile RFID systems," in *IEEE INFOCOM*. IEEE, 2010, pp. 1–9.

[4] J. Wang, J. Xiong, X. Chen, H. Jiang, R. K. Balan, and D. Fang, "TagScan: Simultaneous target imaging and material identification with commodity RFID devices," in *23rd Annual International Conference on Mobile Computing and Networking*. ACM, 2017, pp. 288–300.

[5] H.-S. Yeo, G. Flamich, P. Schrempf, D. Harris-Birtill, and A. Quigley, "Radarcat: Radar categorization for input & interaction," in *29th Annual Symposium on User Interface Software and Technology*. ACM, 2016, pp. 833–841.

[6] D. Turcsany, A. Mouton, and T. P. Breckon, "Improving feature-based object recognition for X-ray baggage security screening using primed visual words," in *IEEE International Conference on Industrial Technology (ICIT)*. IEEE, 2013, pp. 1140–1145.

[7] G. T. Flitton, T. P. Breckon, and N. M. Bouallagu, "Object recognition using 3D SIFT in complex CT volumes." in *BMVC*, no. 1, 2010, pp. 1–12.

[8] C. Lin, J. Hu, Y. Sun, F. Ma, L. Wang, and G. Wu, "WiAU: An accurate device-free authentication system with ResNet," in *15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 2018, pp. 1–9.

[9] H. Liu, Y. Wang, J. Liu, J. Yang, Y. Chen, and H. V. Poor, "Authenticating users through fine-grained channel information," *IEEE Transactions on Mobile Computing*, vol. 17, no. 2, pp. 251–264, 2018.

[10] W. Wang, A. X. Liu, M. Shahzad, K. Ling, and S. Lu, "Understanding and modeling of wifi signal based human activity recognition," in *21st annual international conference on mobile computing and networking*. ACM, 2015, pp. 65–76.

[11] Z. Chen, L. Zhang, C. Jiang, Z. Cao, and W. Cui, "WiFi CSI based passive human activity recognition using attention based BLSTM," *IEEE Transactions on Mobile Computing*, 2018.

[12] X. Wang, L. Gao, S. Mao, and S. Pandey, "CSI-based fingerprinting for indoor localization: A deep learning approach," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 1, pp. 763–776, 2017.

[13] Z. Wu, Q. Xu, J. Li, C. Fu, Q. Xuan, and Y. Xiang, "Passive indoor localization based on csi and naive bayes classification," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1566–1577, 2018.

[14] Y. Zou, Y. Wang, S. Ye, K. Wu, and L. M. Ni, "TagFree: Passive object differentiation via physical layer radiometric signatures," in *IEEE PerCom*. IEEE, 2017, pp. 237–246.

[15] C. Wang, J. Liu, Y. Chen, H. Liu, and Y. Wang, "Towards in-baggage suspicious object detection using commodity WiFi," in *IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2018, pp. 1–9.

[16] K. Wu, "Wi-Metal: Detecting metal by using wireless networks," in *IEEE ICC*. IEEE, 2016, pp. 1–6.

[17] A. Hanif, M. S. Chughtai, A. A. Qureshi, A. Aleem, F. Munir, M. Tahir, and M. Uppal, "Non-obtrusive detection of concealed metallic objects using commodity WiFi radios," in *IEEE GLOBECOM*. IEEE, 2018, pp. 1–6.

[18] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Predictable 802.11 packet delivery from wireless channel measurements," in *2010 ACM SIGCOMM*. ACM, 2010, pp. 159–170.

[19] M. M. Breunig, H.-P. Kriegel, R. Ng, and J. Sander, "LOF: Identifying density-based local outliers." vol. 29, 06 2000, pp. 93–104.