Indonesian Journal of Electrical Engineering and Computer Science
Vol. 16, No. 1, October 2019, pp. 473~481
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v16.i1.pp473-481

Fast surveillance video indexing & retrieval with WiFi MAC address tagging

K.L. Tan, K.C. Lim
Faculty of Electronic and Computer Engineering, Universiti Teknikal Malaysia Melaka, Malaysia

Article Info

Article history:

Received Nov 1, 2018
Revised Feb 6, 2019
Accepted Mar 15, 2019

Keywords:

RSSI
Surveillance video
Video indexing
WiFi MAC address
WiFi sniffer

ABSTRACT

Conventional public safety surveillance video camera systems required 24/7 monitoring of security officers with video wall display installed in the control room. When a crime or incident is reported, all the recorded surveillance video streams nearby the incident area are playback simultaneously on video wall to help locate the target person. The security officers can fast forward the video playback to speed up the video search, but it requires massive manpower if there are hundreds of video streams required to be examined on the video wall. One of the possible solutions is through a suitable video indexing and retrieval technique to prioritize the video frames that need to be processed. This paper presents a WiFi sniffer enabled surveillance camera, with 3-stage WiFi frame inspection filter and the use of collected WiFi signal strength for filtering, to tag the collected WiFi MAC addresses to the surveillance video frames according to the time of the MAC address is sniffed. Additional metadata (WiFi MAC address of smartphone) collected during the occurrence of the incident can be used to prioritize the retrieving of surveillance video frames for subsequent image processing.

Corresponding Author:

Lim Kim Chuan,
Faculty of Electronic and Computer Engineering,
Universiti Teknikal Malaysia Melaka,
Hang Tuah Jaya, 76100, Durian Tunggal, Melaka, Malaysia.
Email: kimchuan@utem.edu.my

1. INTRODUCTION

In the old days, human beings needed extensive time and intensive man-power to retrieve surveillance camera video frames that contained target person from a large video database [1-5]. When an incident occurred, all the recorded surveillance video streams nearby the incident area were playback simultaneously to help locate the target person. The security officers would fast forward the video playback to speed up the video search, but it required massive manpower if there were hundreds of video streams that needed to be monitored. The situation became more challenging to the security officers if there were multiple targets being tracked at the same time [6-9]. Even today with the Graphics Processing Unit (GPU) that can run the person search deep neural network model to automatic search for the target person from a large video database, it can take hours or even days to complete the search. The video processing time can be reduced by using multiple desktop GPUs or a more powerful server grade GPU to run the person search deep neural network model, but this requires more investment on GPU and it is not cost-effective to allocate the GPU for every available camera. This has become an issue when only finite computing power is available and huge amounts of video frames need to be processed. One of the possible solutions is through a suitable video indexing and retrieval technique to prioritize the video frames that need to be processed by the person search deep neural network model [10-12.

Nowadays, people carry their smartphone with WiFi turned on wherever they go for their smartphone to automatically connect to Internet when there is WiFi service available [13-15]. When the WiFi of the

smartphone is turned on, the smartphone will broadcast management frames known as probe request to discover all nearby access point [16-19]. The probe request contains WiFi media access control (MAC) address which is a unique identifier assigned to the network interface card of the smartphone [20]. The length of WiFi MAC address is six bytes and separated by colons. The MAC address is generated by using OUI (Organizationally Unique Identifier) number provided by IANA (Internet Assigned Numbers Authority). The MAC address is never encrypted even though the WiFi devices are connected to a WiFi network with security encryption enabled [21]. Besides probe request, there are other WiFi frames broadcast by smartphone that contain WiFi MAC address for example: disassociation, authentication, deauthentication, etc. Since each smartphone has a unique WiFi MAC address, it can be used to track a person who carries a smartphone with WiFi turned on. Research work has been carried out using WiFi MAC address for WiFi tracking. Scheuner et al. developed a generic and passive WiFi tracking system named Probr which can be used to predict room utilization, indoor localization, and person tracking [16]. Andreea et al. proposed a WiFi tracking systems that collect WiFi MAC addresses of smartphones to monitor pedestrian behaviour [22]. Julien carried out an experiment to study how frequent the smartphones broadcast probe request that can be used for WiFi tracking purpose [23]. Xu et al. proposed a pedestrian monitoring system by using WiFi MAC addresses and RSSI for localization [24]. Musa et al. proposed a trajectory estimation method by process the sniffed WiFi MAC addresses with Viterbi's algorithm [25]. Kim et al. proposed a method to predict the real location of users by using smartphone MAC addresses and access point [26]. Fukuzaki et al. designed Anonymous MAC Address Probe Sensor (AMP sensor), which can sniffs MAC addresses from transmitted packets and then upload to server for pedestrian flow analysis [27].

This paper presents a fast surveillance video indexing & retrieval with WiFi MAC address tagging. A WiFi sniffer enabled surveillance camera, with 3-stage WiFi frame inspection filter and the use of collected WiFi signal strength for filtering, is developed to tag the collected WiFi MAC addresses to the surveillance video frames according to the time of the MAC address is sniffed. The sniffed WiFi MAC address is used as a search index to retrieve the surveillance camera video frames tagged with WiFi MAC address of searching from the video database. The proposed RSSI thresholding technique is used to discard the sniffed WiFi MAC address that are not within the surveillance camera viewing distance.

2. RESEARCH METHOD

The proposed design of WiFi sniffer for metadata tagging on surveillance camera video frame is first discussed in this section. A 3-stage WiFi frame inspection filter is designed to remove unwanted WiFi frames and only certain frames that contain source MAC address and RSSI can pass the filters. The final section discusses applying the RSSI thresholding for Wifi MAC address tagging during the recording of surveillance camera video frame.

2.1. Wifi Sniffer Setup

The WiFi sniffer is built by using the Raspberry Pi 3 Model B V1.2 on board WiFi chipset (BCM43430a1). The operating system is Raspbian Stretch version March 2018. The WiFi sniffer only monitors 2.4GHz band. Nexmon firmware patch is applied to enable the monitor mode. A monitor interface named *mon0* is created by using the command "*sudo iw phy phy0 interface add mon0 type monitor*". The *mon0* interface is enabled by using the command "*sudo ifconfig mon0 up*". The WiFi sniffer used the Python raw socket to capture WiFi frames broadcasted by nearby WiFi devices.

A 3-stage WiFi frame inspection filter is designed to preserve the network bandwidth by discarding irrelevant frames and only relevant information (source MAC address and timestamp) are extracted and sent to metadata server.The first stage of filter removes subtypes that do not contain source MAC address. It checks the type and subtype of the frame and only subtypes from Table 1 can pass the filter. The first stage of filter also removes all beacon frames and probe response but keeps a list (*AP_address_list*) with their source MAC addresses.

The second stage of filter uses IEEE 802.11 addressing mechanism to remove frames that are not broadcast from the client device. Only case 1 (*To DS* = 0, *From DS* = 0) and case 3 (*To DS* = 1, *From DS* = 0) are the possible cases when a frame is broadcast from the client device. Case 1 is used to broadcast management frame and control frame while case 3 is used to broadcast data frame. For case 1, the source MAC address can belong to either client device or access point because there are few subtypes under management frame and control frame (as highlighted in Table 1) that are broadcast by client device and access point. For case 3, the source MAC address of data frame is definite belonging to client device because the frame must have *To DS* set to 1 and *From DS* set to 0.

The third stage of filter is designed to identify the source MAC address belongs to client device or access point in case 1 by comparing the source MAC address with *AP_address_list*. The source MAC address that matches with the MAC address in the *AP_address_list* will be removed.

Table 1. WiFi frames sniffed by WiFi sniffer

Type	Management frames	Control frames	Data frames
Subtypes	• Probe request • Disassociation • Authentication • Deauthentication	• Block ACK request • Block ACK • PS-Poll • RTS	• Null data • QoS data • QoS null

2.2. Smartphones Setting for Different Wifi Connection Status

The smartphones used in this research is Samsung Galaxy Note 4 with Android 6.0 and Huawei P10 with Android 8.0. These mobile devices are selected because the Android 6.0 has the highest market share (25.5%) while the Android 8.0 is the latest Android version available on smartphone according to Android developer statistics. Since different Android versions have different WiFi frame broadcast behaviour, the smartphones used in this experiment are always screen on and the WiFi is turned on. The WiFi frame broadcast behaviour is also affected by the WiFi connection status. An experiment is designed and conducted for 5 minutes duration to measure the WiFi frame broadcast behaviour of smartphones for each scenario.

2.2.1. Scenario 1: WiFi is turned on but not connected to an access point

Scenario 1 represents a situation where a smartphone user comes to a place that has never visited before with the smartphone's WiFi turned on. All the Service Set Identifiers (SSID) nearby the testbed are deleted from the smartphone's SSID history list to prevent the smartphone auto reconnect to any one of these access points. Five SSIDs that are not within the smartphone's WiFi coverage are stored in the smartphone's SSID history list to identify if there is any directed probe request broadcast from the smartphone. The smartphone's WiFi is turned on through the quick setting menu and remains screen on at home page.

2.2.2. Scenario 2: WiFi is turned on and connected to an access point

Scenario 2 represents a situation where the smartphone is connected to an access point. Before the experiment starts, all the apps running in background are stopped. The smartphone's WiFi is turned on through the quick setting menu and auto connect to the access point that is placed in FKEKK Research Lab 3. After the connection is established, one social media app (YouTube) is started and running in the background throughout the experiment.

2.3. Applying RSSI thresholding for Wifi MAC address tagging during the recording of surveillance camera video frame

The sniffed WiFi MAC address is tagged to the surveillance camera video frames by using timestamp. The combination of MAC address and timestamp is known as metadata and is sent to the metadata database during the live surveillance camera video recording. Since the WiFi sniffer will sniff all the surrounding WiFi frames within its antenna coverage regardless the camera viewing distance, there are two conditions that will cause the proposed video retrieval system to return unrelated video frames as shown in Figure 1. The first condition is the person A is outside the camera viewing distance but the smartphone's WiFi MAC address is sniffed by WiFi sniffer (see Figure 1(a)). This will cause the proposed video retrieval system to return video frames that do not contain person A.

The second condition is the person A is within the camera viewing distance but the smartphone's MAC address of person A and other person (B, C, and D) are sniffed Figure 1(b)). The proposed video retrieval system will process all the sniffed smartphone's WiFi MAC addresses (see because all the sniffed WiFi MAC addresses have equal probability to belong to person A. The person search time will increase when the number of sniffed WiFi MAC addresses is increased.

The camera viewing distance is set to 5 meters in this research. To remove the WiFi MAC address that is not within camera viewing distance, the RSSI value of the sniffed WiFi frame is used to predict the distance between WiFi sniffer and the sniffed WiFi frame. An experiment is carried out at outdoor environment to measure the RSSI value of sniffed WiFi frame when the smartphone is placed at different distances (1.5m, 3m, 5m, 10m) from the WiFi sniffer for five minutes. Any sniffed WiFi MAC address with RSSI value less than the RSSI threshold is discarded. Only sniffed WiFi MAC address with RSSI value greater than or equal to the RSSI threshold is tagged to surveillance camera video frames.

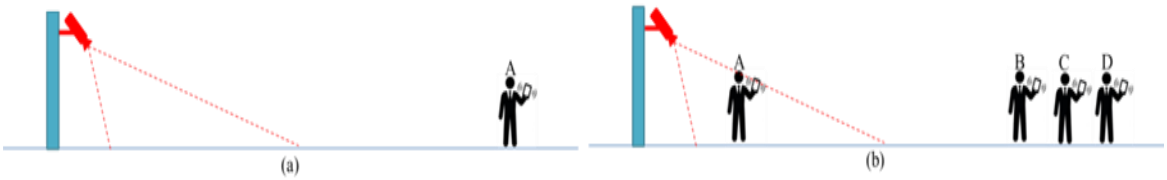

Figure 1. (a) Person A is out of camera viewing distance, but the smartphone's MAC address is sniffed. (b) Only person A is within the camera viewing distance but the smartphone's MAC address of person A and other persons (B, C, and D) are sniffed.

There are two situations where the distance between the sniffed WiFi MAC address and WiFi sniffer is misidentified due to overlapping of two RSSI distributions. The first situation is where the sniffed WiFi MAC address is within camera viewing distance (e.g., smartphone is nearby the camera up to 5 meters) but misidentified as outside camera viewing distance (5 meters and further from the camera) (see Figure 2(a)). The probability of WiFi frames within camera viewing distance but misidentified as outside camera viewing distance is calculated as follows:

$$P_{wrong\ discard} = \frac{N_{<threshold}}{N_{total}} \quad (1)$$

where $N_{<threshold}$ = Number of WiFi frames with RSSI value less than RSSI threshold

N_{total} = Total number of sniffed WiFi frames

The second situation is where the sniffed WiFi MAC address is outside camera viewing distance but misidentified as broadcasted within camera viewing distance (because the sniffed WiFi frame's RSSI is greater than RSSI threshold) (see Figure 2(b)). The probability of WiFi frames outside camera viewing distance but misidentified as broadcasted within camera viewing distance is calculated as follows:

$$P_{wrong\ tag} = \frac{N_{>threshold}}{N_{total}} \quad (2)$$

where $N_{>threshold}$ = Number of WiFi frames with RSSI value greater than RSSI threshold

N_{total} = Total number of sniffed WiFi frames

An RSSI threshold is selected based on the collected RSSI values when the difference between the probability of misidentify the smartphone is outside or within camera viewing distance is minimum. The difference between the probability of misidentify the smartphone is outside or within camera viewing distance is calculated as follows:

$$Difference = \left| P_{wrong\ discard} - P_{wrong\ tag} \right| \times 100\% \quad (3)$$

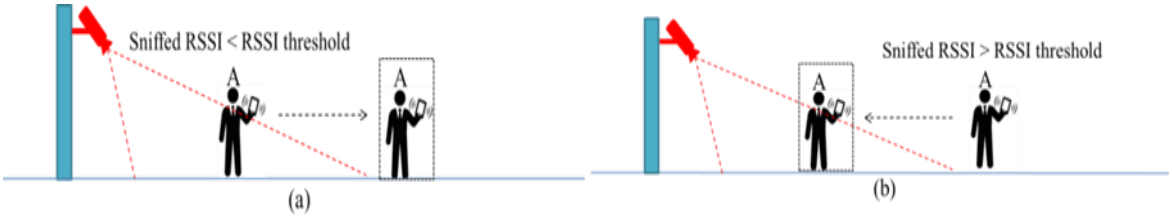

Figure 2. (a) The sniffed WiFi MAC address is within camera viewing distance but misidentify as outside camera viewing distance (b) The sniffed WiFi MAC address is outside camera viewing distance but misidentify as within camera viewing distance

3. RESULTS AND ANALYSIS

The analysis on the type of WiFi traffic frame under two scenarios is first discussed in this section. Next, the RSSI distribution of WiFi frames at different distances are analysed to identify a RSSI threshold for specific camera viewing distance. Lastly, the effect of RSSI thresholding on the probability of misidentify the distance between smartphone and WiFi sniffer is discussed.

3.1. Analysis on broadcast frequency of WiFi frame types under different scenario

3.1.1. Scenario 1: WiFi is turned on but not connected to access point

Since the smartphones are not connected to any access point, only probe request is sniffed in this scenario. Figure 3 shows the Huawei P10 did not broadcast any probe request while the Samsung Galaxy Note 4 stop broadcast null probe request after the WiFi is turned on for one minute. No directed probe request is observed for both smartphones in this scenario. The Huawei P10 only broadcast null probe request when the user open WiFi setting page to view the list of available WiFi network. It is predicted the chances to sniff probe request for scenario 1 in the future is getting less as the newer Android version keeps improving user privacy.

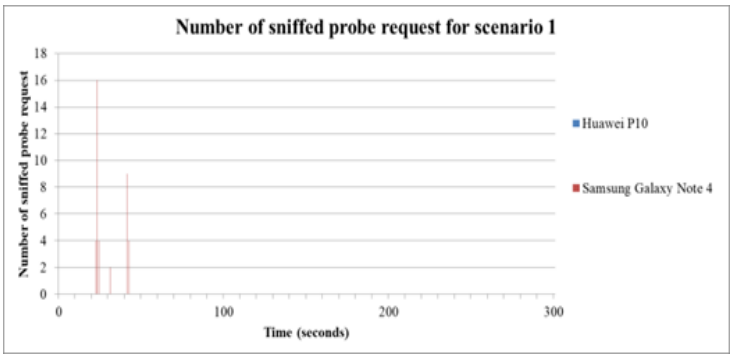

Figure 3. Number of sniffed probe request in five minutes for scenario 1

3.1.2. Scenario 2: WiFi is turned on and connected to an access point

After connected to access point, Huawei P10 Android 8.0.0 broadcast probe request in random pattern (see Figure 4(a)) but Samsung Galaxy Note 4 Android 6.0.1 stop broadcast probe request (see Figure 4(b)). The Huawei P10 broadcast null probe request after connected to access point is to discover nearby access point that can provide better link quality. The Samsung Galaxy Note 4 stop broadcast probe request after connected to access point is to preserve smartphone's battery life. Since the broadcast pattern of probe request is inconsistent across different Android version due to different purposes, other frame types such as control frame and data frame is used to increase the chances to sniff the MAC address of the smartphones. The control frame shows the highest broadcast frequency compared to the other frame types because before QoS data frame transmission to the access point, the smartphone needs to transmit an RTS frame to the access point. After the QoS data frame transmission is completed, the smartphones transmit Block_ACK_Request to request the access point to acknowledge the frames that the smartphone has sent.

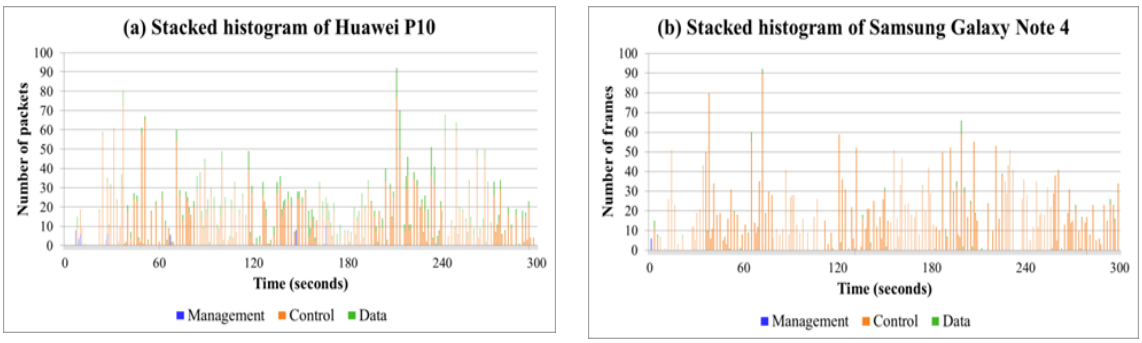

Figure 4. Number of sniffed WiFi frames for (a) Huawei P10 (b) Samsung Galaxy Note 4 in 5 minutes duration

3.2. Comparison of RSSI values at different distance from the WiFi sniffer

The RSSI distribution and statistical analysis of both smartphones at different distances from the camera are as shown in Figure 5. The mean, median, and mode of the RSSI distribution are closed to one another in this experiment as shown in Figure 5. This implies that the collected RSSI data has a fairly symmetrical distribution from 1.5 meters up to 10 meters. From Figure 5, the distribution of RSSI values shifted to negative side when the distance between smartphones and WiFi sniffer is increased.

In this test bed setting, the person search deep neural network model works well when the camera viewing distance is set to maximize the view at 5 meters. The number of pixels in an image that contain person features can be increased by using a higher megapixel camera (camera resolution used in this research is 720p only) but this requires more investment on the camera. Alternative way to increase the number of pixels in an image that contains person features is to adjust the camera viewing distance to 3 meters or even 1.5 meters, but the camera surveillance region will be reduced significantly. However, the WiFi sniffer will sniff all the surrounding WiFi frames within its antenna coverage regardless of the camera viewing distance. Since the camera viewing distance is set to 5 meters, any sniffed WiFi MAC address that is 5 meters and further from the WiFi sniffer should not be tagged to surveillance camera video frames. The WiFi MAC address that is 10 meters away from the WiFi sniffer has weaker RSSI value as compared to the WiFi MAC address that is 5 meters away from the WiFi sniffer. Therefore, RSSI thresholding is applied in the WiFi sniffer to filter the WiFi MAC address that is not within 5 meters coverage, but there is an overlapping between the distribution of RSSI at 5 meters and 10 meters, which will cause some of the WiFi MAC addresses broadcasted at 10 meters misclassified broadcasted within 5 meters. The effect of RSSI thresholding on the probability of misclassified the distance between smartphone and WiFi sniffer will be discussed in the next section.

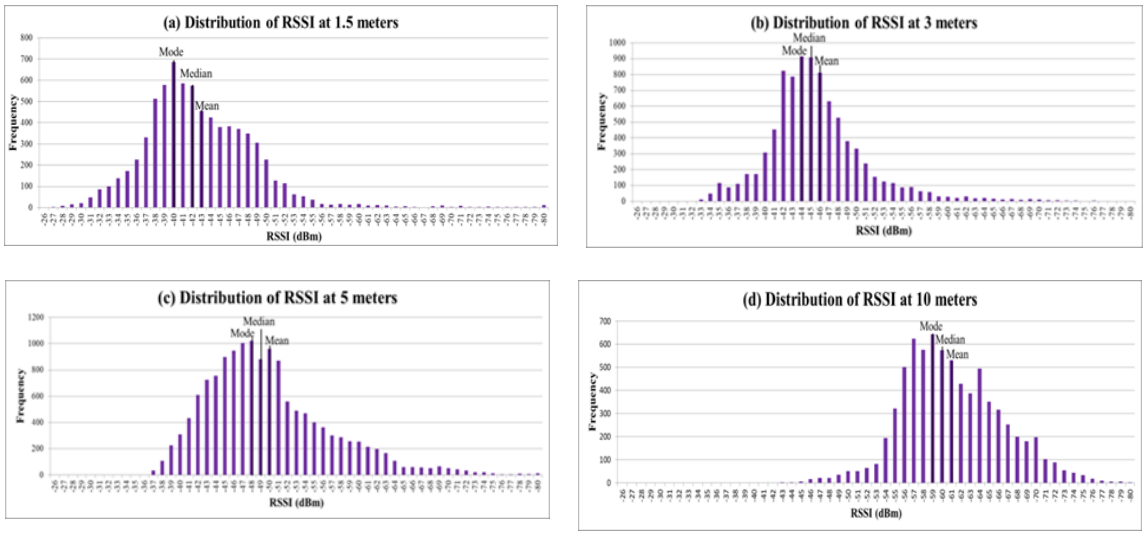

Figure 5. The RSSI distribution of both smartphones at (a) 1.5 meters, (b) 3 meters, (c) 5 meters, and (d) 10 meters

3.3. The effect of RSSI thresholding on the probability of misidentify the distance between the sniffed WiFi MAC address and WiFi sniffer

With the RSSI thresholding, any sniffed WiFi MAC address with an RSSI value less than the RSSI threshold is discarded. However, there are two situations, as discussed in Section 2.1.3 (see Figure 1), where the distance between the sniffed WiFi MAC address and WiFi sniffer is misidentified due to overlapping of two RSSI distributions.

When the camera viewing distance is set to 5 meters, the RSSI threshold is set to -59 dBm if 90% of the sniffed WiFi MAC addresses at 5 meters (indicated by green distribution) are required to be tagged to surveillance camera video frames as shown in Figure 6(a). However, there is 43% of the sniffed WiFi MAC addresses (calculated by using (2)) at 10 meters (indicated by blue distribution) will be tagged to camera video frames as shown in Figure 6(b). When the smartphone is placed at 3 meters or 1.5 meters (within 5 meters range of camera viewing distance), the probability of misidentify the smartphone is outside camera viewing distance is very low (less than 3%) and can be ignored as shown in Figure 6(c) and (d). The WiFi MAC

addresses correctly discarded are indicated by grey distribution. The WiFi MAC addresses that should not be discarded are indicated by red distribution.

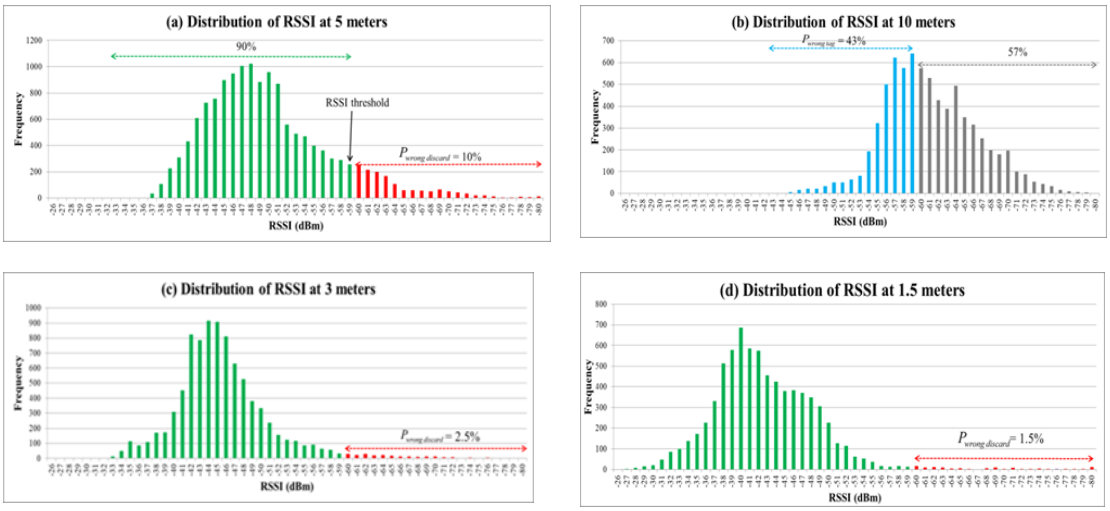

Figure 6. (a) The RSSI threshold is set to -59 dBm if 90% of the MAC addresses at 5 meters are required to be tagged to surveillance camera video frames (b) Applying threshold value of -59dBm to the collected RSSI values of WiFi MAC address at distance of 10 meters resulting in 43% of the MAC addresses wrongly tagged as 5 meters (c) & (d) The probability of misidentify the smartphone is outside camera viewing distance is very low (less than 3%) and can be ignored

There is a trade-off between the probability of misidentify the smartphone is outside or within camera viewing distance when applying RSSI threshold. If the RSSI threshold at 5 meters is reduced, the probability of misidentify the smartphone is outside camera viewing distance (when the smartphone is placed at 1.5 meters, 3 meters or 5 meters) will be reduced but at the same time the probability of misidentify the smartphone is within camera viewing distance (when the smartphone is placed at 10 meters) will be increased. The trade-off is unavoidable because the distribution of RSSI for 1.5 meters, 3 meters, 5 meters and 10 meters are overlapped. However, there is a 'balance point' in the overlapping region of the RSSI distribution of 5 meters and 10 meters where the difference in $P_{wrong\ discard}$ and $P_{wrong\ tag}$ are minimum as shown in

Figure *1*.

The corresponding RSSI value at minimum point is -56 dBm (see

Figure *1*). This RSSI value (-56 dBm) is selected to be the RSSI threshold. The probability of misidentify the smartphone outside or within camera viewing distance is almost the same when the RSSI threshold is -56 dBm, $P_{wrong\ discard}$ of 16% and $P_{wrong\ tag}$ of 18.3%, as shown in Figure 8.

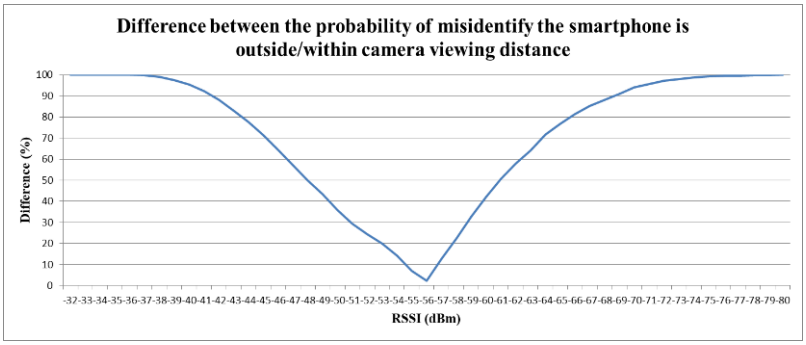

Figure 1. Difference between the probability of misidentify the smartphone is outside or within camera viewing distance. The minimum point is located at -56 dBm

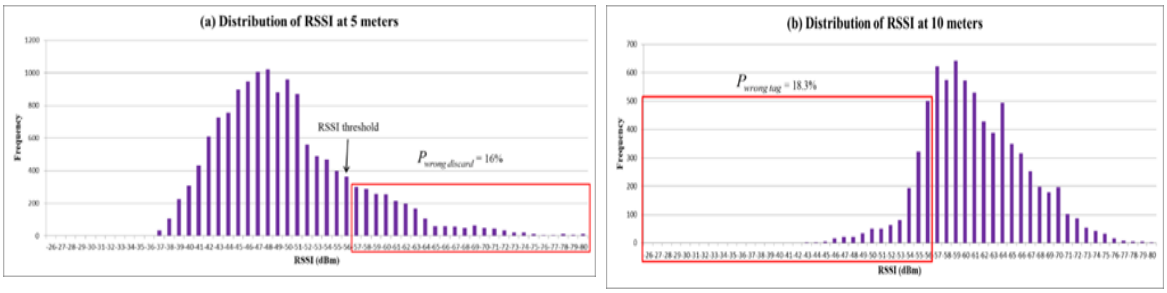

Figure 8. The probability of misidentify the smartphone is outside or within camera viewing distance are almost the same when the RSSI threshold is -56 dBm (a) $P_{wrong\ discard}$ of 16% and (b) $P_{wrong\ tag}$ of 18.3%

4. CONCLUSION

A WiFi sniffer enabled surveillance camera, with 3-stage WiFi frame inspection filter and the use of collected WiFi signal strength for filtering, is designed and developed in this project. The WiFi sniffer inside the proposed camera sniffs the smartphone WiFi MAC addresses within the radio vicinity of the sniffer and tags it to the on-going recording camera video frames the moment the MAC address is picked up by the sniffer. The sniffed WiFi MAC address is subsequently used as search index to quickly retrieve the surveillance camera video frames across all the cameras of the surveillance system video recording database that is tagged with the MAC address. Therefore, the proposed WiFi MAC address tagging technique for fast video retrieval system can prioritizes the surveillance camera video frames processing to speed up the person search process.

ACKNOWLEDGEMENTS

This work was funded by the Center for Research and Innovation Management (CRIM), UTeM under project code Gluar/CREST/2015/FKEKK/100005.

REFERENCES

[1] J. S. C. Yuk, *et al.*, "Object-based surveillance video retrieval system with real-time indexing methodology," *International Conference Image Analysis and Recognition(ICIAR'07)*, pp. 626–637, September 2007.
[2] J. Dai, *et al.*, "The Architecture and Task Scheduling Design forthe Video Analysis Center," *2016 International Conference on Progress in Informatics and Computing (PIC)*, December 2016.
[3] H. Lin, "Crowd Scene Analysis in Video Surveillance," *University of Otago*, 2016.
[4] V. K. Harihar, *et al.*, "Multi-layer Perceptron Based Video Surveillance System," *2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, December 2017.
[5] K. Akila, *et al.*, "Managing Interclass Variation In Human Action Recognition," *Proceedings of the International Conference for Phoenixes on Emerging Current Trends in Engineering and Management*, February 2018.
[6] S. Tang, *et al.*, "Multiple People Tracking by Lifted Multicut and Person Re-identification," *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 3539-3548, 2017.
[7] W. Liu, *et al.*, "Leveraging Long-Term Predictions andOnline Learning in Agent-BasedMultiple Person Tracking," *IEEE Transactions On Circuits And Systems For Video Technology*, vol. 25, no. 3, March 2015.
[8] H. Kieritz, *et al.*, "Online Multi-Person Tracking using Integral Channel Features," *2016 13th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, August 2016.
[9] A. Milan, *et al.*, "Online Multi-Target Tracking Using Recurrent Neural Networks," *AAAI Conference on Artificial Intelligence*, 2016.
[10] X. Men, *et al.*, "A deep learned method for video indexing and retrieval," *18 Proceedings of the 26th Pacific Conference on Computer Graphics and Applications*, pp. 85-88, October 2018.
[11] F. F. Chamasemani, *et al.*, "A Framework for Automatic Video Surveillance Indexing and Retrieval," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 10, no. 11, August 2015.
[12] A. Podlesnaya, *et al.*, "Deep learning based semantic video indexing and retrieval," *Proceedings of SAI Intelligent Systems Conference, Springer*, pp. 359-372, 2016.
[13] G. M. Weiss, *et al.*, "Actitracker: A Smartphone-based Activity Recognition System for Improving Health and Well-Being," *2016 IEEE International Conference on Data Science and Advanced Analytics*, October 2016.
[14] T. Dingler, *et al.*, "uCanvas: A Web Framework for Spontaneous Smartphone Interaction with Ubiquitous Displays," *IFIP Conference on Human-Computer Interaction*, pp. 402-409, August 2015.
[15] D. Wang, *et al.*, "Smartphone Use in Everyday Life and Travel," *Journal of Travel Research*, vol. 55, no. 1, 2016.
[16] J. Scheuner, *et al.*, "Probr – A Generic and Passive WiFi Tracking System," *2016 IEEE 41st Conference on Local Computer Networks (LCN)*, November 2016.

[17] G. Wilkinson, "Digital Terrestrial Tracking: The Future of Surveillance," *DEFCON 22*, 2014.
[18] S. Jamil, *et al.*, "Classifying Smartphone Screen ON/OFF State Based On WiFi Probe Patterns," *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pp. 301-304, September 2016.
[19] A. D. Luzio, *et al.*, "Mind your probes: De-anonymization of large crowds through smartphone WiFi probe requests," *Proc. IEEE INFOCOM*, pp. 1-9, 2016.
[20] V. Acuna, *et al*., "Localization of WiFi Devices Using Probe Requests Captured at Unmanned Aerial Vehicles," *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1-6, 2017
[21] M. Cunche, "I know your MAC Address: Targeted tracking of individual using Wi-Fi," *Journal of Computer Virology and Hacking Techniques*, pp. 1-9, 2014.
[22] A. C. Petre, *et al.*, "WiFi Tracking of Pedestrian Behaviour," *Smart Sensors Networks: Communication Technologies and Intelligent Applications*, pp. 309-337, June 2017.
[23] J. Freudiger, "Short: How Talkative is your Mobile Device? An Experimental Study of Wi-Fi Probe Requests," *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, June 2015.
[24] Z. L. Xu, *et al*., "Pedestrain Monitoring System using Wi-Fi Technology and RSSI Based Localization," *International Journal of Wireless & Mobile Networks (IJWMN)*, vol. 5, no. 4, August 2013.
[25] A. B. M. Musa, *et al.*, "Tracking Unmodified Smartphones Using Wi-Fi Monitors," *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems*, November 2012.
[26] M. Kim, *et al.*, "Extracting a Mobility Model from Real User Traces, " *25th IEEE International Conference on Computer Communications (INFOCOM'06)*, pp. 1-13, April 2016.
[27] Y. Fukuzaki, *et al.*, "A Pedestrian Flow Analysis System Using Wi-Fi Packet Sensors to a Real Environment," *ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pp. 721-730, 2014.

BIOGRAPHIES OF AUTHORS

Tan Kien Leong is currently a Master student at the Faculty of Electronic and Computer Engineering in Universiti Teknikal Malaysia Melaka. He received his bachelor's degree (Telecommunications) in 2015 from Universiti Teknikal Malaysia Melaka. His research interest covers deep learning, computer networking and IoT.

Lim Kim Chuan is currently a Associate Professor at the Faculty of Electronic and Computer Engineering in Universiti Teknikal Malaysia Melaka. He obtained the Ph.D degree in Machine Vision and Image Processing at Sheffied Hallam University, UK in 2010. His research interest covers 2D & 3D computer vision, image processing, embedded operating systems, WLAN/WIFI resources management