Your MAC Address Can Be Detected Easily when Your Smartphone Connected to the Wi-Fi

https://doi.org/10.3991/ijim.v15i07.17169

Syifaul Fuada (✉), Raihan Fakhri Rabbani, Nuur Wachid Abdul Majid
Universitas Pendidikan Indonesia, Bandung, Indonesia
syifaulfuada@upi.edu

Prasetiyo
Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea

Rahmat Muttaqin, Trio Adiono
Institut Teknologi Bandung, Bandung, Indonesia

Shorful Islam
Stream Intelligence Ltd., London, United Kingdom

Abstract—In this short paper, we prove that the smartphones connected to the Wi-Fi can be detected (scanned) easily with the help of a Raspberry Pi. To capture the packet which is sent by smartphone for some distance, we used Tshark. According to the observation, the smartphone eventually broadcast some packets data containing MAC layers data, in which the period of broadcasting data depends on the smartphone's state (active scanning/sleep). Besides MAC layers data, we also detect/capture other parameters, i.e., wireless signature data transmitted by smartphone (RSSI) and Time-stamp. The RSSI value measured in this test has a range from –30 dBm to –80 dBm. The result proves in the same distance; different smartphones give different RSSI values (each smartphone emits different power strength). The RSSI value has more significant changes in a short distance (in this test result, 1 to 10 meters) and less significant change in a long distance (above 20 meters). The MAC address, time-stamp, and RSSI that scanned/captured successfully through Raspberry Pi from the smartphones can be used as a reference for various purposes/applications in future work, such as Wi-Fi scanning/tracking system.

Keywords—MAC layer data, Time-stamp, RSSI, Smartphone, Wi-Fi tracking system

1 Introduction

Nowadays, almost all people at every economic level, from the lower–middle to upper–middle-class (adults and children), already have smartphones. In the world, smartphone users continue to increase [1]. On the other hand, the update of internet technology has completed smartphone functions. Smartphones that utilize internet

access offer various capabilities to download various sources, such as music, games, applications, videos online (streaming), and many other things. Through smartphones and adequate internet support, the necessities of life can be enjoyed. Wi-Fi network as an internet source is almost available in every office and has become a primary utility at this time. Wi-Fi is more practical than LAN cables in terms of connectivity between the internet source to gadgets (e.g., laptops, tablets, smartphones, and so on). Therefore, users are more comfortable because they just activate the Wi-Fi mode on their smartphone, and the smartphone will be connected directly to the internet. However, free Wi-Fi shared to the public has a serious risk because the connected smartphones are effortless to detect/identify [2] and have a high potential to be identified/hacked. The behavior of smartphone users can be tracked [3] [4] [5].

The admin of the Wi-Fi provider can easily detect essential data such as Media Access Control (MAC) frames [6]; this issue has been elaborated on [7-8]. Even though it has been proven in [7] [8], we still want to ensure and explore again that smartphones emit not only the MAC frames but also other relevant information. The obtained data, including MAC frames, will be processed for various purposes (for example, a Wi-Fi user detector/smartphone localization system). Tracking with Wi-Fi references is considered more optimal than the Global Positioning System (GPS) for small-scale applications [9].

In this paper, we report the preliminary study to design a Wi-Fi scanner system. A tracker-node prototype based on Raspberry Pi that can scan and collect the main data from the smartphones is provided. These required data in the form of systematic log-data (i.e., MAC address) following with the RSSI can be used as a reference for a Wi-Fi scanner system or smartphone localization in an indoor environment. On the other hand, we also collect Time-stamp data from smartphones connected to Wi-Fi. The following are the main objectives of this paper: 1) to scan the wireless signature that smartphone emits; 2) to measure the RSSI in a node that associated with the smartphone MAC address, and 3) to observe the change in RSSI while the distance between smartphone and node changes. The data obtained in this work is then analyzed further and improved by using various techniques, e.g., Intersection Density, Nonlinear Least Square (NLS), Linear Kalman Filter (KF), as presented in [10], and Unscented Kalman Filter (UKF) [12]. The captured smartphone data are then encrypted, transmitted, and stored to the server. Finally, we develop a Wi-Fi scanning system's hardware to detect the smartphones' position that will be published in the future [13].

To recognize the smartphones' position connected to the Wi-Fi, we need to set an indoor localizer environment by using a minimum of three tracker-nodes. The use of three units is the minimum requirement; it is recommended to use at least four tracker-nodes then placed in the four corners of the room. Therefore, it will form a coordinate function (x-axis vs. y-axis). To perform the smartphone localization system, we need a proper algorithm, ex. Intersection density algorithm. It can map the set of node location and distance ratio into a set of circles with center and radius; the circles will intersect each other. Finally, the smartphone location (x, y) can be estimated in the location that has the most intersection point [10]. The RSSI value obtained in each node has an essential role in the intersection density that the set of circles produce, so

the misreading in one node can significantly reduce accuracy. On the other hand, position detection will not be precise due to unstable RSSI. To improve the performance, we can use further advanced algorithms, as UKF [12].

Since this work focuses on recognizing the distance variable (RSSI), MAC address, and Timestamp, we will only employ a single tracker-node. The RSSI variable will be used as a distance parameter, while the MAC address will be used to accurately detect which gadget is connected to Wi-Fi [13]. To identify when a smartphone is connected to the Wi-Fi includes the date and time data, we will use the Timestamp variable [13].

2 Methods

Several tools were used to perform the test, i.e., 1) Raspberry Pi 2.0B as an initial node prototype. To supply the Raspberry, an AC Adapter 5V/3A was used; 2) Wi-Fi module Access Point (AP) with TP-Link TL-WN722N model; 3) Three different Smartphones (Sony Xperia Z3, Xiaomi RedM3, & ASUS Padfone S); and 4) Tshark software for traffic data monitoring. Since this research is an initial study, we only select three smartphones with a random type – three smartphones owned by researchers. The specifications of each smartphone are not specified in advance.

Fig. 1 depicts the experimental setup to scan MAC layer data, smartphone power strength (RSSI), and Time-stamp from the smartphones. The test procedure is as follows: firstly, we set monitoring mode the Wi-Fi module inserted in the Raspberry Pi. Later, the smartphone Wi-Fi is turned into active scanning (one smartphone is in "connecting-mode" with AP, the others are in "discovery-mode"). Afterward, the Tshark is set in Raspberry Pi to monitor and observe the traffic data. Filter other packet data except for the data-request that our smartphone's Wi-Fi emits. The last step is to capture those packet data and observe the RSSI value from several distances and locations. The data was collected at the IC Design Laboratory, Pusat Mikroelektronika, Institut Teknologi Bandung (ITB), dated April 2017.

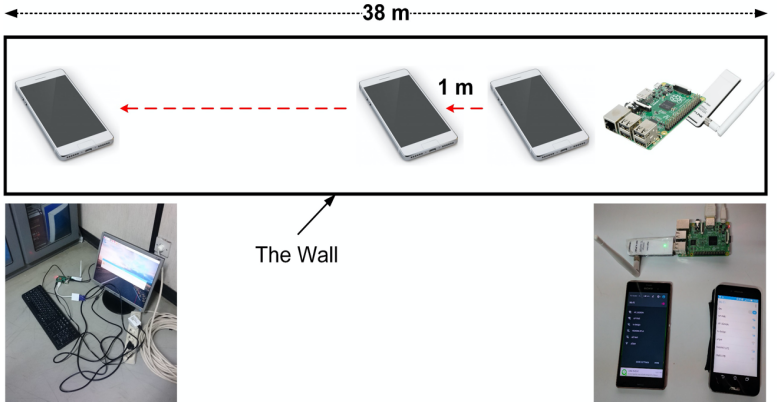

Fig. 1. Experimental set-up for the 1st scenario, containing initial tracker node (Raspberry Pi + Wi-Fi AP) and three different Smartphones

3 Results and Analysis

3.1 First scenario

As stated in Section 2, the smartphone is set to discovery-mode and connecting-mode. According to the test result, for the smartphone that is set to discovery-mode, three types of packets data are associated with the smartphone: 1) Payload data: data transfer when the smartphone has connected to existing AP; 2) Packet data response: packet data that were surrounding AP emit to response the smartphone device (associated with surrounding AP location); and 3) Packet data request: packet data that smartphone emits (associated with smartphone location). In this work, we select this mode because we want to measure the signal strength that smartphone emits. That is why we are only interested in the packet data requests. While for the smartphone sets to connecting-mode, there are several packets of data related to data transfer between smartphones and AP. The RSSI should be measured from the packet that has a source address from the associated smartphone. In this test, Fig. 1 is used as a test scenario.

In case that the smartphone has already connected to other AP, we still ensure which packet data should have been observed. Sometimes, the smartphone no longer sends the packet request data. The data captured in the node is mostly the payload data transfer between the smartphone and AP. For this reason, we need further research about the Wi-Fi communications protocol.

The RSSI was measured from several distances between node to smartphone (from 1 meter to 38 meters). In the same distance, we observed that the RSSI value was changing for each packet-data request. Hence, we measured the RSSI for 5 minutes in each distance, then took the average value to represent the RSSI value in this distance. Based on the result, as captured in Fig. 2, we can conclude that the smartphone eventually broadcasts the packet request data. This result confirms the study which is conducted by [7-8].

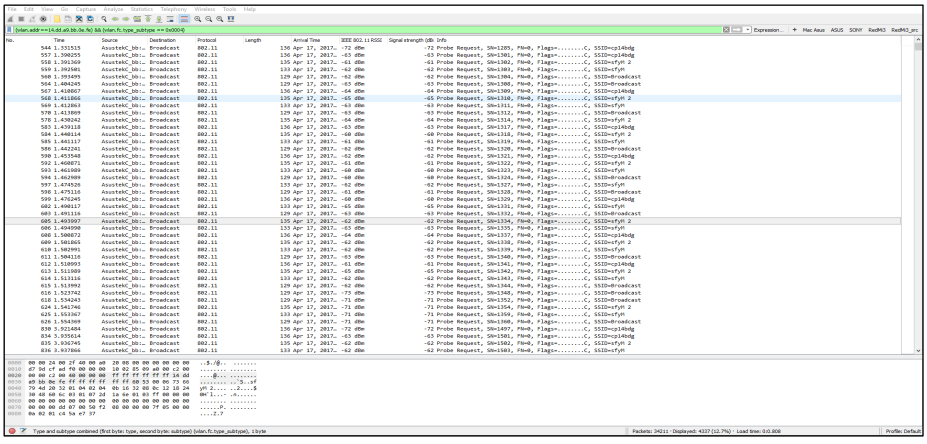

Fig. 2. Detected MAC address and Time-stamp of the smartphone

The data contain some information in MAC frame data (MAC address) and Time stamp. We can see several items in the monitoring system: Time, Source, Destination, Protocol, Arrival time, RSSI, and main related information. The broadcasting period of the packet request data from the smartphone depends on the state of smartphone (ex. the smartphone that uses power-saving mode will broadcast the packet request data slower; sleep mode; active scanning). To observe the packet request data that smartphone emits, the nodes have to be set in monitoring mode.

Fig. 3 shows the relation between measured RSSI in the change of node – smartphone distance. The RSSI value measured in this test has a range from –30 dBm to –80 dBm. The RSSI value below -90 dBm is the noise floor. To interpret the obtained RSSI value, we used Fig. 4 [11], which is adequate signal strength in Wi-Fi communication. The significant change of RSSI happens in the small distance (0 – 10 meters), whereas a small change in RSSI happens in long distance (above 20 meters). The RSSI value in the node is measured from the packet request data associated with the smartphone's MAC address.

As depicted in Fig. 3, the different smartphone in the same distance (in this test is Sony Xperia Z3, Xiaomi RedM3, & ASUS Padfone S) gives different RSSI value. The RSSI depends on the initial power that the smartphone emits, and each smartphone emits different power strength emits by phone. Other factors, e.g., a) path-loss, b) node's antenna gain, and c) the smartphone's distance to the node, can also affect the RSSI values.

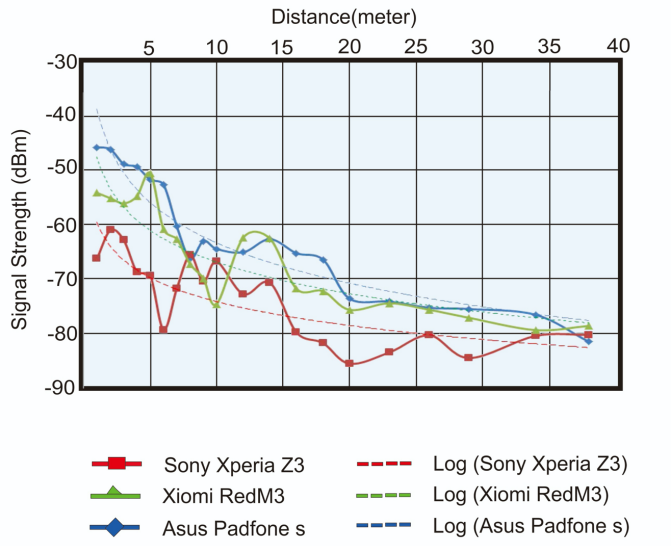

Fig. 3. A graph of RSSI (dBm) vs. Distance (meter)

RSSI	Quality	Description
–30 dBm	Amazing	Max achievable signal strength. The client can only be a few feet from the AP to achieve this. Not typical or desirable in the real world
–67 dBm	Very Good	Minimum signal strength for applications that require very reliable, timely delivery of data packets
–70 dBm	Ok	Minimum signal strength for reliable packet delivery
–80 dBm	Not Good	Minimum signal strength for basic connectivity. Packet delivery may be unreliable
–90 dBm	Unusable	Approaching or drowning in the noise floor. Any functionality is highly unlikely

Fig. 4. Wi-Fi signal strength classification, reproduced from [11]

3.2 Second scenario

This test aims to ensure the statement, as in the First scenario, that each smartphone transmits a different RSSI is correct. The results of this experiment are expected to support Fig. 3. For this reason, we use three Tracker-node units, where the nodes are constructed by the Raspberry Pi built-in Wi-Fi AP. Two smartphones are selected (ASUS Padfone S & Sony Xperia Z3) because it took first and third place in the previous test. The scenario for this experiment is depicted in Fig. 5.

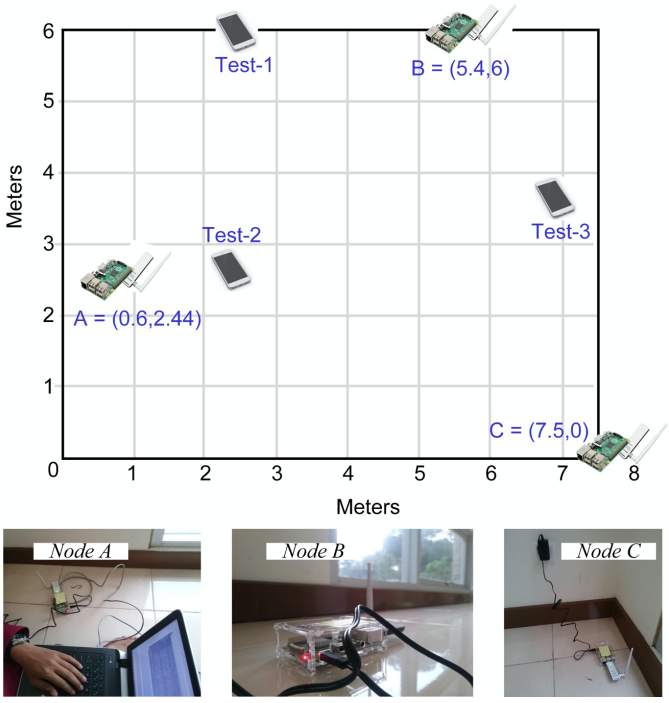

Fig. 5. Experimental set-up for the 2nd scenario

Three nodes are then denoted as A, B, and C. These nodes are placed separately with the following coordinates (0.6,2.5), (5.4,6), and (7.5,0), respectively. Smartphone 1 is placed randomly between nodes A, B, and C then positioned at three different places. The smartphone's position is later denoted as Test-1, Test-2, and Test-3. To obtain a valid result in measuring the RSSI, the position of smartphone 2 is set the same as the Smartphone 1.

The data collection procedure (RSSI measurement) follows the first scenario. Table 1 exhibits the test result of the second scenario. The average RSSI value on Test-2 is the highest when measured by Node A because it is the closest distance to Node A. The lowest RSSI value when measured by Node C because it is the farthest distance from Node C. The average RSSI value on Test-3 is slightly higher when measured by Node B compared to Node C because the distance is closer to Node B than Node C, and the lowest when measured by Node A because it is the farthest distance from Node A. The average RSSI value on Test-1 is the highest when measured by Node B because it is the closest distance to Node B. The lowest value in Node C because it is the farthest distance from Node C.

In conclusion, the average RSSI value of Smartphone 2 was higher than the Smartphone 1 for all test scenarios. This is consistent with the results in Fig. 3.

Table 1. Test results of the 2nd scenario

Node	Coordinate		Power average (dBm)					
			Smartphone 1 (Sony Xperia Z3)			***Smartphone 2 (ASUS Padfone)***		
	X	Y	Test-1	Test-2	Test-3	Test-1	Test-2	Test-3
A	0.6	2.5	-63.9811	-60.2059	-68.375	-51.3333	-50.2647	-64.3125
B	5.4	6	-63.3684	-71	-61.5897	-62.5625	-63.8333	-58.3333
C	7.5	0	-74.3902	-73.9773	-61.725	-72.5263	-67.2564	-62.2333

4 Conclusion

Based on the report received, we can conclude that the Tracker-Node (in this case, Raspberry Pi built-in Wi-Fi) is capable of scanning the wireless signature data emitted by the smartphone. Therefore, we can collect MAC addresses, RSSI, time-stamp from a smartphone connected to the Wi-Fi. According to the test associated with the RSSI value, the significant change of RSSI happens in the small distance (0 to 10 meters) and small change in RSSI happens in the long distance (above 20 meters). Thus, on this range operation, the RSSI technically can be used as a reliable parameter for further application, i.e., to determine the smartphone location. As a note, to find out the position of the smartphones, we need more than two tracker-nodes. It works based on the distance measured from the position between nodes which forms the coordinates (x, y) within the room. In future work, the localization algorithm will be performed by putting the node for each 20 – 30 meters distance. With a proper algorithm, we can observe the smartphone location accurately. The Raspberry Pi allows programing/embedding these algorithms through Phyton script. It will be considered the hy-

pothesis in the next phase of research. The use of GUI in the form of map and analyzed data (graph, chart, heat pattern, etc.) is mandatory for a monitoring purpose.

5 References

[1] 'How Many People Have Smartphones Worldwide (July 2020)'. https://www.bankmycell.com/blog/how-many-phones-are-in-the-world (accessed Jul. 20, 2020).
[2] B. Alotaibi and K. Elleithy, 'A New MAC Address Spoofing Detection Technique Based on Random Forests', Sensors, vol. 16, no. 3, p. 281, Feb. 2016, https://doi.org/10.3390/s16030281.
[3] 'How stores use your phone's WiFi to track your shopping habits - The Washington Post'. https://www.washingtonpost.com/news/the-switch/wp/2013/10/19/how-stores-use-your-phones-wifi-to-track-your-shopping-habits/ (accessed Jul. 20, 2020). https://doi.org/10.2966/scrip.140217.381
[4] A. B. M. Musa and J. Eriksson, 'Tracking unmodified smartphones using wi-fi monitors', in Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems - SenSys '12, Toronto, Ontario, Canada, 2012, p. 281, https://doi.org/10.1145/2426656.2426685.
[5] J. Freudiger, 'Short: How Talkative is your Mobile Device? An Experimental Study of Wi-Fi Probe Requests', p. 6. https://doi.org/10.1145/2766498.2766517
[6] N. Abedi, A. Bhaskar, and E. Chung, 'Bluetooth and Wi-Fi MAC Address Based Crowd Data Collection and Monitoring: Benefits, Challenges and Enhancement', p. 17.
[7] C. Matte, M. Cunche, and V. Toubiana, 'Does disabling Wi-Fi prevent my Android phone from sending Wi-Fi frames?', p. 15.
[8] M. Cunche, 'I know your MAC address: targeted tracking of individual using Wi-Fi', J. Comput. Virol. Hacking Tech., vol. 10, no. 4, pp. 219–227, Nov. 2014, https://doi.org/10.1007/s11416-013-0196-1.
[9] C. Eom, S. Jung, C. Im, and C. Lee, 'Fingerprint- and Kalman Filter-based Localization Exploiting Reference Signal Received Power Calibration', IEIE Trans. Smart Process. Comput., vol. 9, no. 3, pp. 238–243, Jun. 2020, https://doi.org/10.5573/ieiespc.2020.9.3.238.
[10] S. Fuada, T. Adiono, P. -, and H. Widhanto, 'Modelling an Indoor Crowd Monitoring System based on RSSI-based Distance', Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 1, 2020, https://doi.org/10.14569/ijacsa.2020.0110181.
[11] 'inSSIDer Office -WiFi Troubleshooting and Optimisation from MetaGeek'. https://www.network-testers.com/inssider.html(accessed Jul. 20, 2020).
[12] S. Fuada, et.al., "Accuracy improvement of RSSI-based distance localization using Unscented Kalman Filter (UKF) algorithm for Wi-Fi tracking application," iJIM, 2020. https://doi.org/10.3991/ijim.v14i16.14077
[13] T. Adiono, et al., "Prototyping the Wi-Fi Tracker System using RSSI-based Distance for Indoor Crowd Monitoring," Unpublished.

6 Authors

Syifaul Fuada is with the Program Studi Sistem Telekomunikasi UPI as a Lecturer. His research interests include analog circuit design and instrumentation, circuit

simulation, engineering education, IoT, wireless communication (e.g., VLC, Li-Fi, etc.)

Raihan Fakhri Rabbani is a student of Program Studi Sistem Telekomunikasi UPI. Jln. Dr. Setiabudhi Nomor 229 Bandung 40154. Email: raihanfakhri36@gmail.com

Nuur Wachid Abdul Majid received a S.Pd. in Informatics Engineering of Education and a M.Pd. in Technology and Vocational Education, UNY. Now, he is a lecturer in PSTI, UPI. His research interests include related to informatic education and system.

Prasetiyo received the B.S. degree in electrical engineering from ITB, Indonesia, in 2015 and Master Degree in KAIST, South Korea, in 2019. Currently, he is pursuing Ph.D. degree in KAIST. His research interests include Wireless communication, VLSI, analog integrated circuits design, and CMOS technology. Email: prasetiyo@kaist.ac.kr

Rahmat Muttaqin is a received the B.S. degree and M.Sc. degree in electrical engineering from ITB, Indonesia, in 2014 and 2020, respectively. Office address: Gd. Labtek VIII Lt. IV, Jln. Ganesha No. 10 (40116), Bandung, West Java, Indonesia

Trio Adiono is a Full professor and a senior lecturer at the School of Electrical Engineering and Informatics, and formerly serves as the Head of the Microelectronics Center, ITB. His research interests include VLSI design, signal and image processing, VLC, smart cards, and electronics solution design and integration. Email: tadiono@stei.itb.ac.id

Shorful Islam received the B.Sc. degree in University of Hertfordshire in 1995, M.Sc. degree in the University of Kent in 1996, and Ph.D. degree in the University of Lincoln in 1999. He serves an advisor of Stream Intelligence. Currently, he is working with a Cyber Security startup, building out their product and analytical capabilities and also running an analytics consultancy. His interest related to analysts, strategists, creatives, techies, and brainstorming solutions.

Article submitted 2020-07-20. Resubmitted 2020-12-03. Final acceptance 2020-12-05. Final version published as submitted by the authors.