Indoor Crowd Estimation Scheme Using the Number of Wi-Fi Probe Requests under MAC Address Randomization

Yuki Furuya[1], Hiromu Asahina[1], Masashi Yoshida[1]and Iwao Sasase[1]

Abstract – **As smartphones have become widespread in the past decade, Wi-Fi signal-based crowd estimation schemes are receiving increased attention. These estimation schemes count the number of unique MAC addresses in Wi-Fi signals, hereafter called probe requests (PRs), instead of counting the number of people. However, these estimation schemes have low accuracy of crowd estimation under MAC address randomization that replaces a unique MAC address with various dummy MAC addresses. To solve this problem, in this paper, we propose an indoor crowd estimation scheme using the number of PRs under MAC address randomization. The main idea of the proposed scheme is to leverage the fact that the number of PRs per a unit of time changes in proportion to the number of smartphones. Since a smartphone tends to send a constant number of PRs per a unit of time, the proposed scheme can estimate the accurate number of smartphones. Various experiment results show that the proposed scheme reduces estimation error by at most 75% compared to the conventional Wi-Fi signal-based crowd estimation scheme in an indoor environment.**

Keywords – **Wi-Fi, MAC address randomization, PRs, bursts.**

I. INTRODUCTION

The ability to estimate the total number of people is important to improve the convenience of when utilizing facilities [1]. For example, by counting people in queues, airports, restaurants and shopping malls attempt to improve their services, and also prepare for an effective evacuation guidance during times of emergency [2]. Most of the existing works have realized such estimations by leveraging either image recognition techniques [3] or Wi-Fi signals [4]. Since Wi-Fi signal based approaches are less affected by light intensity or high congestion degree than image recognition based approaches, we focus on the Wi-Fi signal based approaches.

The Wi-Fi signal based approaches estimate the number of people inside the facility based on the fact that smartphones periodically send Wi-Fi control frame, called probe request (PR), with their unique MAC addresses [4]. Nowadays, since more and more people have Wi-Fi embeded smartphones, the Wi-Fi signal based approaches can easily estimate the number of people by counting the number of unique MAC addresses in PRs.

However, a single smartphone might have more than one MAC address when MAC address randomization is implemented in the smartphone [5]. To be more specific, an original MAC address is replaced by various dummy MAC addresses to prevent attackers from tracking locations of people [6]. This results in a larger number of unique MAC addresses than the actual number of people.

In order to solve this problem, Matte et al. [7] proposed a scheme to estimate the number of people based on the fact that PRs which are sent from the same smartphone record the same values in their subfields. Since some subfields, such as the number of antennas, should be the same in every PR, this scheme can identify dummy MAC addresses which are sent from the same smartphone by using the subfields. To our knowledge, only [7] have dealt with the MAC address randomization and thus is considered as the conventional scheme for this paper. However, since values of the subfields depend on the smartphone model, this scheme estimates a smaller number of people than the actual number of people when multiple people have the same smartphone model. Thus, to accurately estimate the number of people in a facility, it is necessary to estimate the number of the same smartphone models.

In this paper, we propose an indoor crowd estimation scheme using the number of PRs under MAC address randomization. The main idea of the proposed scheme is to leverage the fact that the number of PRs per a unit of time changes in proportion to the number of the same smartphone model. Since the number of PRs per a unit of time tends to be similar among the same smartphone models, the number of a specific smartphone model can be estimated from the number of PRs which are sent from the same smartphone model. We have clarified this fact by collecting datasets of PRs from 57 smartphones. Experimental evaluation results show that the proposed scheme improves estimation accuracy of the number of people by at most 75% compared to [7].

The following is the paper structure. Section II describes the system model. Section III explains the conventional scheme and the shortcoming of it. Section IV presents proposal to the problem. Section V shows evaluation results. Section VI concludes the paper.

II. SYSTEM MODEL

Fig.1 shows a model of an indoor crowd estimation system. We assume that the system is implemented in an area inside a facility, hereafter referred to as a target area. It is assumed that the target area is a line-of-sight environment, and up to 20 people stay in the target area for several minutes. This system consists of four elements: people, a wireless monitor, i.e. a Wi-Fi monitor, and a server. The people have their own smartphones, and it periodically sends PRs which record randomized MAC addresses. The Wi-Fi monitor continuously collects the PRs

[1]Yuki Furuya, Hiromu Asahina, Masashi Yoshida, and Iwao Sasase is with Keio University , Dept. of Information and Computer Science, 3-14-1 Hiyoshi, Kohoku, Yokohama, Kanagawa 223-8522 Japan,
E-mail: {furuya, asahina, sasase}@sasase.ics.keio.ac.jp,
yoshida@mos.ics.keio.ac.jp

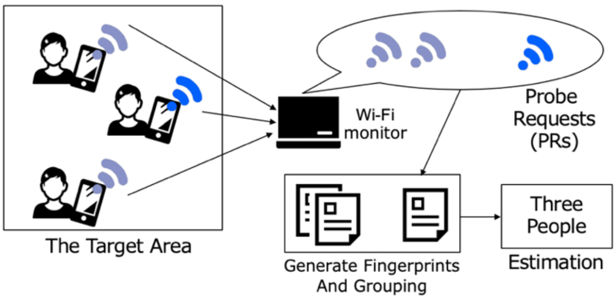

Fig. 1. System model of indoor crowd estimation.

and sends them to a server. The server estimates the number of people with a crowd estimation scheme that is not affected by MAC address randomization.

III. Conventional Scheme

The main idea of the conventional scheme [7] is to utilize the trait that PRs record the same subfields in a header even if they record randomized MAC addresses. Since subfields have to record some immutable and unique values for performing wireless communication, such as the number of antennas, the conventional scheme can identify dummy MAC addresses corresponding to the same smartphone.

A. Algorithm of the conventional scheme

The algorithm of the conventional scheme consists of the two following steps: (1) filtering PRs, and (2) estimating the number of people in a target area. When a Wi-Fi monitor receives a PR, it filters the PRs that are sent from a smartphone in the target area by selecting PRs of which Received Signal Strength Indicator (RSSI) exceeds a predetermined threshold. The threshold is experimentally determined by measuring minimum RSSI of PRs which are sent from smartphones in the target area. After this filtering, the algorithm estimates the number of people by using subfields of PRs. In particular, the algorithm creates lists of names and values of subfields as a FingerPrint (FP) of each smartphone. Finally, the algorithm counts the number of unique FPs of smartphones as the number of people in a target area.

B. Shortcoming of the conventional scheme

The conventional scheme tends to estimate a smaller number of people when multiple same model smartphones exist within a target area. In general, since same model smartphones use the same values in the subfields of their PRs, the number of unique FPs does not change even if the number of smartphones of the same model changes. This shortcoming might become a problem for improving services in a facility, since the most major model accounts for 11.73% of all smartphones as of 2019 in Japan.

Therefore, to improve the accuracy of the estimation, it is important to estimate the number of smartphones of the same model.

Table I
Average and standard deviation of bursts.

Device - OS Version	Ave.	Stdev.
Google Pixel 3 - 9.0	10.9	2.13
Google Pixel 3 XL - 9.0	6.2	0.42
iPhone6S - 11.1.1	7.6	1.78
iPhone6S - 11.1.2	9.6	2.12
iPhone6S - 11.2.6	4.6	0.7
SH-04H - 8.0.0	10.9	2.08
SH-04H - 8.0.0	13	0.82
SO-01K - 8.0.0	7.5	0.85
SO-01K - 8.0.0	7	0
SO-02K - 8.0.0	7.2	0.63
SO-03K - 8.0.0	7.3	0.48

IV. Proposed Scheme

In this paper, we propose an indoor crowd estimation scheme using the number of PRs under MAC address randomization. The main idea of the proposed scheme is to leverage the fact that the number of PRs with the same FP increases linearly with the number of the smartphones with the same model. We have collected a real-world dataset of PRs and clarified that a specific smartphone model tends to send a constant number of PRs per unit time. Based on this property, the number of smartphones of a specific model can be estimated by dividing the number of observed PRs by the number of PRs that the smartphones of a specific model sends per unit of time. To realize this, a Wi-Fi monitor has to collect all PRs without omission. However, a Wi-Fi monitor may fail to collect PRs with low RSSI since smartphones send a bunch of PRs with various transmission power levels within a small time interval. In order to deal with this problem, the proposed scheme aggregates a bunch of PRs within a small time interval into a single group, hereafter called bursts, and uses the number of bursts for the estimation. Since smartphones send at least one PR with their maximum transmission power, the number of bursts is hardly changed even if a Wi-Fi monitor fails to collect some PRs. In the following sections, we explain details of our dataset and proposed algorithm for crowd estimation.

A. Datasets

Our dataset is composed of bursts that are collected from 57 smartphones with 32 models. We use Wireshark, which is an open-source packet analyzer, to collect bursts [8]. We collect bursts for ten minutes by each model of a smartphone in an environment where there are no strong interference signals. Table I shows the average number of bursts per minute and its standard deviation of each model. As shown in Table I, the standard deviation of each model is between 0 and 2.13. This result indicates that each smartphone model tends to send an almost constant number of PRs per a unit of time. Since the same smartphone model tends to create the same FP, the number of bursts with the same FP increases linearly with the number of smartphones with the same model.

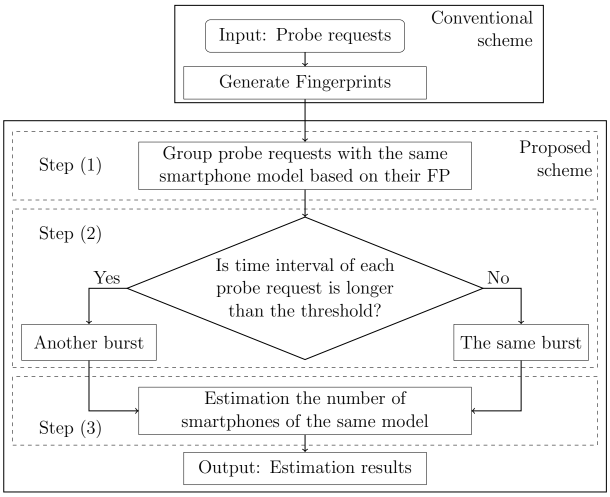

Fig. 2. Flowchart of proposed algorithm.

The aforementioned average number of bursts of each FP is stored in a server to be used in the proposed crowd estimation.

B. Algorithm

The proposed algorithm estimates the number of people from the PRs every *M* minutes. Fig.2 shows a flowchart of the proposed algorithm. The algorithm consists of the following three steps: (1) creating groups of PRs for the same smartphone model, (2) converting PRs to bursts, and (3) estimating the number of people by counting the number of smartphones with the same model in each group. Firstly, the algorithm creates groups of PRs for the same smartphone model. To be more specific, FPs of PRs are created by the conventional scheme, and the PRs are grouped by FPs. Secondly, the algorithm converts PRs in each group into bursts based on their time stamp. By analyzing bursts in our dataset, we have found that every time interval of a burst is below 0.5 (sec). Based on this fact, the algorithm merges a series of PRs into a single burst if the difference of arrival times among them is less than 0.5 (sec). Finally, the algorithm estimates the number of people by counting the number of smartphones with the same model in each group. In particular, the algorithm first accesses to the server to get the average number of bursts that the smartphone model sends per *M* minutes. Then, the algorithm divides the number of bursts in a group with the number of bursts per *M* minutes. By performing the procedures above for all groups, the number of smartphones in each group can be estimated. Finally, the algorithm outputs the total number of smartphones in all groups as an estimation result of the number of people.

V. Evaluation

In order to show effectiveness of the proposed scheme, we implement crowd estimation scheme in an indoor environment, i.e. target area. In particular, we use Wireshark as a Wi-Fi monitor, and MacBook Pro (13-inch, 2017, Two Thunderbolt 3 ports) as a server. The number of smartphones are 7, 14 and 21. In each case, an environment is repeated 4 times with different sets of smartphones, and average values of the estimation are used as estimation results. The predetermined threshold of RSSI for filtering outside PRs is -70dB and $M = 1$.

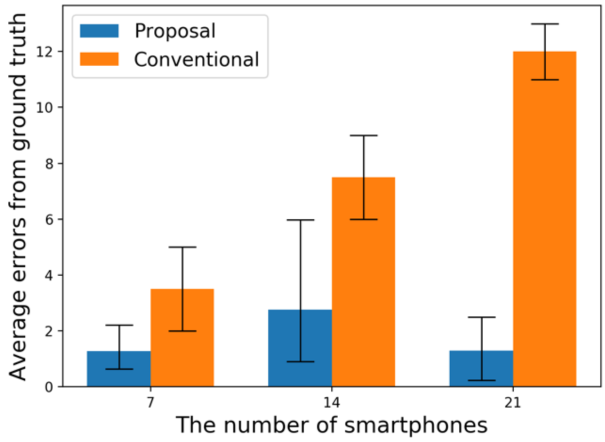

Fig. 3. Average errors from ground truth.

A. Average errors of crowd estimation

In this section, estimation accuracy of the proposed scheme and that of the conventional scheme are presented. Fig.3 shows average estimation errors from the ground truth, i.e., the actual number of smartphones, versus the number of smartphones. The error bars indicate the minimum and maximum errors. In Fig.3, we can observe that average errors of the proposed scheme are lower than those of the conventional scheme. In particular, the average error of the proposed scheme among all experiments is 1.58, and that of the conventional scheme is 6.41. In other words, the proposed scheme successfully reduces the estimation error by 75% compared to the conventional scheme. The reason behind this is that the results of the proposed scheme reflect the actual number of smartphones while those of the conventional scheme reflect only the number of unique FPs, i.e., the number of smartphone models. In fact, the errors in the conventional schemes are almost equal to the difference between the number of unique FPs and the actual number of smartphones. In this experiment, the average numbers of models of smartphones are 3, 7.5, and 13 while the actual numbers of smartphones are 7, 14, and 21 respectively. Thus, the differences between the number of models of smartphones and ground truth are 3, 7.5, 13. These differences are almost the same as average errors of the conventional scheme. On the other hand, the proposed scheme also has estimation errors at most 5.98 when the number of smartphones is 14. By analyzing our dataset, we have clarified that this error is caused by the common FP among several different smartphone models. Due to such a common FP, the proposed scheme might not correctly estimate the number of smartphones with the same FP. In order to clarify the reason for the error of the proposed scheme, we will analyze the observed PRs in the next section.

B. FPs of models of smartphones

TABLE II
RELATIONSHIP FPS AND MODELS.

OS	Android																iOS									
FPs \ Models	SCV42 9.0.0	SCV41 9	Nova Lite 2 8.0.0	Nova Lite 2 704HW 8.0.0	P10 8.0.0	SCV43 9.0	Google Pixel 3 XL 9.0	SO-03L 9.0	Google Pixel 3 9.0	SO-02K 8.0.0	SO-01K 8.0.0	SO-01K 8.0.0	701SH 8.0.0	Mate20Pro 9.0	Mate10Pro 703HW 8.0.0	HMV32 8.0.0	iPhone6 11.4	iPhone6Plus 12.1	iPhone6S 11.1.1	iPhone6S 11.2.6	iPhone6S 11.1.2	iPhone7 11.0.3	iPhone6S 12.1.4	iPhone6SPlus 12.2	iPhone7Plus 12.0.1	iPhone8 12.3.1
A	119	119							16																	
AG			668	794																						
AH2				674	1081																					
B2						1294																				
E							813		1087																	
F								2332	233																	
M										1102	124															
N1											1187	1396														
P													710													
U1														984	1023											
U2														162	173	1149										
V2																	628									
V3																	551	498								
Y																			622	576	609	416	581	699	334	152
AD1																										436

Table II shows correspondence between models of smartphones and FPs. Particularly, columns, rows, and each number in Table II show smartphone models, identifiers of FPs, and the number of observed PRs, respectively. Although almost all models of smartphone have unique FPs, several smartphone models have common FPs. For example, FPs of iPhone6S, Nova lite 2, and HMV32 are common with that of iPhone7, P10, and Mate10Pro, respectively. Since the proposed scheme relies on the unique FPs to get the unique fixed numbers of bursts, the proposed scheme cannot determine the appropriate number of bursts per a unit time of these models. Due to this reason, the estimation error of the proposed scheme slightly increases when a smartphone model has a common FP among other models. It is also observed that iOS tends to have common FPs among them in comparison with Android. One reason behind this might be the diversity of smartphones. iOS devices are made by a single company, i.e., Apple, and have similar specifications. In contrast, Android devices are characterized by their diversity. There are various models with different specifications even if they are products of the same company. Thus, different models might use a different Wi-Fi chip that creates different FPs. Based on the above, the proposed scheme might have a limitation that it can estimate accurate number of people only in the case where almost all OS of smartphones are Android. However, since the world market share of Android in 2020 March is 73.0%, we argue that the influence of the common FP of iOS on the estimation is not a serious problem in real environment.

VI. CONCLUSION

We have proposed an indoor crowd estimation scheme using the number of PRs under MAC address randomization. To improve the estimation accuracy of the Wi-Fi signal-based crowd estimation under the MAC address randomization, we leverage the fact that the number of bursts per a unit time changes in proportion to the number of the same smartphone model. Evaluation results show that the proposed scheme reduces estimation error by at most 75% compared to the conventional scheme. We have also clarified that smartphones with similar specifications or ultra power-saving mode might degrade the estimation accuracy. In future extensions, we will investigate other factors to improve the accuracy of crowd estimation.

REFERENCES

[1] S. Depatla and Y. Mostofi, "Crowd counting through walls using WiFi," in Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom), Athens, Greece, pp. 1-10, Mar. 2018.

[2] H. Zou et al., "FreeCount: Device-free crowd counting with commodity WiFi," in Proc. IEEE Glob. Commun. Conf. (GLOBECOM), Singapore, pp. 1-6, Dec. 2017.

[3] D. Figueira, M. Taiana, J. C. Nascimento, and A. Bernardino, "A window-based classifier for automatic video-based reidentification," IEEE Trans. Syst., Man, Cybern., Syst., vol. 46, no. 12, pp. 1736-1747, Dec. 2016.

[4] J. Wannenburg and R. Malekian, "Physical activity recognition from smartphone accelerometer data for user context awareness sensing," IEEE Trans. Syst., Man, Cybern., Syst., vol. 47, no. 12, pp. 3142-3149, Dec. 2017.

[5] J. Martin, T. Mayberry, C. Donahue, L. Foppe, L. Brown, C. Riggins, E. C. Rye, and D. Brown, "A study of MAC address randomization in mobile devices and when it fails," Proceedings on Privacy Enhancing Technologies, Minnesota, vol. 2017, no. 4, pp.365-383, July. 2017.

[6] J. Freudiger, "How talkative is your mobile device?: An experimental study of Wi-Fi probe requests," in Proc. 8th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec), New York City, p. 8, Jun. 2015.

[7] M. Vanhoef, C. Matte, M. Cunche, L. S. Cardoso, and F. Piessens, "Why MAC address randomization is not enough: An analysis of Wi-Fi network discovery mechanisms," in Proc. 11th ACM Asia Conf. Comput. Commun. Secur. (ASIA CCS), pp. 413–424, May. 2016.

[8] Angela Orebaugh, Gilbert Ramirez, Jay Beale, and JoshuaWright, Wireshark & Ethereal Network Protocol Analyzer Toolkit. Syngress Publishing, 2007.