

# Location Authentication based on Wireless Access Point Information to Prevent Wormhole Attack in Samsung Pay

Gwonsang RYU<sup>1</sup>, Changho SEO<sup>1</sup>, Daeseon CHOI<sup>2,\*</sup>

<sup>1</sup>Department of Convergence Science, Kongju National University, Chungnam 32588, Korea

<sup>2</sup>Department of Medical Information, Kongju National University, Chungnam 32588, Korea  
ryugs2409@kongju.ac.kr

**Abstract**—This paper proposes a location authentication method to prevent wormhole payment attack in Samsung Pay. The primary feature of this method is comparing wireless Access Point (AP) information collected by the current Samsung Pay user and a wireless AP model (WM) that was created from wireless AP information (WI) sent by previous Samsung Pay users. To create the WM, an autoencoder is used. Unlike the existing location authentication techniques that use WI, our method does not require additional hardware, modification of the Point of Sale (POS) software, or any pre-requisite information such as the location coordinates of the POS. We show that the proposed location authentication technique exhibits the minimum Equal Error Rate (EER) of 2.4% in real payment environments.

**Index Terms**—artificial neural networks, authentication, authorization, learning (artificial intelligence), wireless networks.

## I. INTRODUCTION

Samsung Pay [1] is a simple pay method that is provided by Samsung Electronics. It has more users than Apple Pay [2]. In Samsung Pay, Payment Information (PI) that contains a one-time credit card number is issued to the user's smartphone. Then, the smartphone is tapped against a Point of Sale (POS) device and the PI is transmitted to the POS via Magnetic Secure Transmission (MST) channels [1]. Choi et al. [3] states that the MST signal can be eavesdropped on and the eavesdropped PI can be used by an attacker in other stores, as shown in Fig. 1.

To prevent this kind of attack, we propose a location authentication method that uses wireless Access Point (AP) information. The wireless AP information (WI) consists of the Basic Service Set Identifier (BSSID), which represents the media access control (MAC) address, and the Received Signal Strength Indication (RSSI). The proposed method collects the WI near the POS with the current Samsung Pay user's smartphone and compares it with the wireless AP model (WM) that has been built from the WI collected by previous Samsung Pay users. If the comparison fails, the relay attack might be suspected.

The main contributions of this paper are as follows:

- We propose a location authentication method that does not need additional Hardware (HW) and does not require modification of the POS's Software (SW). Therefore, it is a very simple and low-cost method.
- Unlike the methods that use GPS, our method does not require any pre-requisite information such as the location coordinates of the POS. A POS's WI model is built from WI that is collected by previous Samsung Pay users.
- The proposed method does not require additional user behavior. The additional behavior is only required when a wormhole payment attack is suspected.
- Our method takes a very short time to compare WI and the WM.

The rest of this paper is organized as follows: Section 2 describes the proposed location authentication method. Experiments are presented for evaluating our method in Section 3. Section 4 presents a discussion of the findings from the experimental results and security issues. Related work is represented in Section 5. Section 6 concludes this paper.

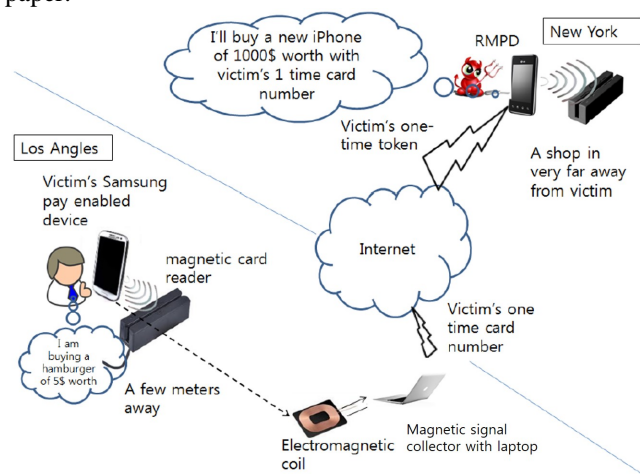


Figure 1. Wormhole payment attack against Samsung Pay [3]

## II. LOCATION AUTHENTICATION SYSTEM

The proposed location authentication system consists of a smartphone, a conventional POS, and a Samsung Pay server. The smartphone collects WI when a user pays with Samsung Pay and sends the WI to the Samsung Pay server. The POS is a conventional POS that does not change anything. The

\*Corresponding author: Daeseon Choi

This work was partly supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (B0717-16-0139, Security Technologies for Financial Fraud Prevention on Fintech) and the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (2016R1A4A1011761).

Samsung Pay server verifies the User ID (UID) and issues the PI. In addition, it builds the WM with the WI that is sent by early-stage users of the POS. The Samsung Pay server compares WI that is received from the current user and the WM that it has built. The proposed method is deduced Samsung Pay user's smartphone application and Samsung Pay server. We assume that the smartphone is secure from any active attacks. This means that an adversary cannot change the UID that is stored in the smartphone. In addition, we assume that the POS and the Samsung Pay server are also secure from any active attacks.

#### A. Location Authentication Process

The proposed location authentication process is illustrated in Fig. 2.

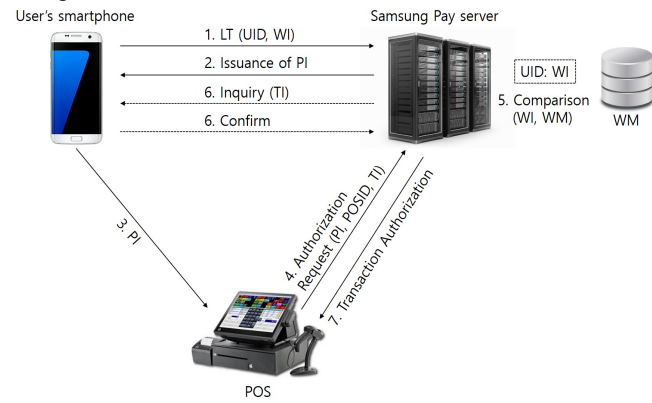


Figure 2. Proposed location authentication method

The following steps are followed when a user pays with Samsung Pay.

1. The user's smartphone collects WI near a POS when the user uses the Samsung Pay application. It then makes a Location Token (LT) that includes the WI and a UID and sends it to a Samsung Pay server. The Samsung Pay server temporarily stores the LT.
2. The Samsung Pay server issues a PI to the smartphone. The PI contains a one-time credit card number. The Samsung Pay server then stores the UID with the PI.
3. The smartphone sends the PI to the POS via the MST channel.
4. The POS sends the PI, a POSID, and current Transaction Information (TI), such as the list of purchased items and prices, to the Samsung Pay server.
5. The Samsung Pay server retrieves the UID from the PI that is stored in Step 2 and retrieves the LT that is stored in Step 1 with the UID. It then compares the WI retrieved from the LT and the WM retrieved from the POSID. If the comparison fails, the transaction is suspected to be a wormhole payment attack. Then, the Samsung Pay server will run Step 6. If the WM has not been made yet, the Samsung Pay server will run Step 6 because it does not compare the WI and the WM.
6. (Conditional) The Samsung Pay server sends an inquiry to the user. The inquiry shows the content of the TI to the user and requests confirmation. The user reviews the TI and confirms the transaction.
7. The transaction is authorized.

#### B. Collecting WI

The user's smartphone collects the WI while the user utilizes the Samsung Pay application. The smartphone should collect the WI near a POS quickly. The RSSI of the collected WI is calculated by the following equation:

$$RSSI = -(10n \log \frac{d}{d_0} - A), \quad (1)$$

where  $n$  is the signal loss coefficient factor,  $d$  is the distance between the wireless AP and smartphone,  $d_0$  is the reference distance, and  $A$  is the signal strength at the reference distance  $d_0$ . The RSSIs are collected several times to find the mean of the RSSIs for a single BSSID as follows because the measured RSSI's variance is very large:

$$x = \frac{\sum_{i=1}^m RSSI_i}{m}, \quad (2)$$

where  $m$  is the number of measurements. Every sample is then converted by the following equation because the RSSI follows the logarithmic scale:

$$x'_i = 10^{\frac{x_{mean} - x_i}{10n}}, \quad (3)$$

where  $x_{mean}$  is the average of the set of  $x$ . It is then normalized as follows:

$$x''_i = \frac{|x'_{mean} - x'_i|}{x'_{var}}, \quad (4)$$

where  $x'_{mean}$  and  $x'_{var}$  are the average and variance of the set of  $x'$ , respectively. The  $\mathbf{x}$  represents the set of  $x''$  as follows:

$$\mathbf{x} = \{x''_1, x''_2, \dots, x''_p\}, \quad (5)$$

where  $p$  is the number of collected wireless APs. The  $x$  denotes the WI of that POS.

#### C. Autoencoder

A denoising autoencoder [4] proposed by P. Vincent et al. is used to model the WM of a POS. An autoencoder is an artificial neural network used for feature learning and consists of two parts, the encoder and the decoder.

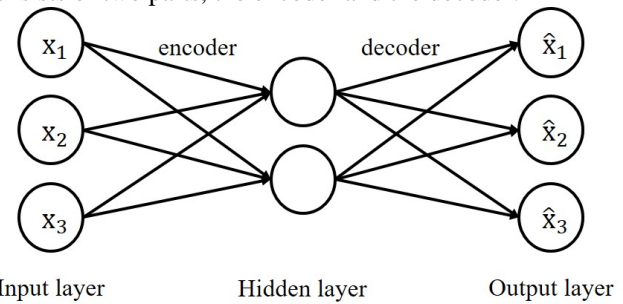


Figure 3. Basic architecture of an autoencoder

For  $\mathbf{x}$ , which is the WI of a POS, the encoder of an autoencoder can be written as follows where there is one hidden layer, as shown in Fig. 3:

$$\mathbf{y} = \sigma_1(\mathbf{W}\mathbf{x} + \mathbf{b}), \quad (6)$$

where  $\sigma$  is an element-wise activation function such as a sigmoid function or rectified linear unit,  $\mathbf{W}$  is a weight matrix, and  $\mathbf{b}$  is a bias vector. After that,  $\mathbf{y}$  is mapped onto the reconstruction  $\hat{\mathbf{x}}$  of the same shape as  $\mathbf{x}$  in the decoder as follows:

$$\hat{\mathbf{x}} = \sigma_2(\mathbf{W}'\mathbf{y} + \mathbf{b}') \quad (7)$$

The loss function is defined as follows:

$$L(\mathbf{x}, \hat{\mathbf{x}}) = \|\mathbf{x} - \hat{\mathbf{x}}\|^2 = \|\mathbf{x} - \sigma_2(\mathbf{W}'(\sigma_1(\mathbf{W}\mathbf{x} + \mathbf{b})) + \mathbf{b}')\|^2, \quad (8)$$

where function  $L$  is the loss function. Training is used to find  $\mathbf{W}$  and  $\mathbf{W}'$ , which minimize  $L(\mathbf{x}, \hat{\mathbf{x}})$ . The WM is the set of  $\mathbf{W}$  and  $\mathbf{W}'$ . The WM stores the optimum weight matrices and bias vectors.

#### D. Comparison of WI and WM

This subsection represents the method that compares the WI and the WM. WI' is a reproduction result made by inputting WI into an autoencoder that holds WM. *Diff* is obtained by comparing WI and WI' as follows:

$$Diff = (WI' - WI)^2 \quad (9)$$

If *Diff* is less than a pre-defined threshold, the collected WI is accepted as valid for the POS. If *Diff* exceeds the threshold, the WI is rejected as non-valid for the POS.

### III. EXPERIMENT

This section evaluates how well the proposed location authentication method works in a real environment. The WI was collected at seven neighboring stores in Kongju, Korea as shown in Fig. 4.



Figure 4. Wireless AP information collection place



Figure 5. Example of collection site

As shown in Fig. 5, the WI was collected from six different positions because Samsung Pay users can pay from different positions at the POS.

The WI was collected from each position. The WI was also collected for 12 different days. The Scapy library was used to collect WI on a laptop running Ubuntu 14.04 LTS. The PC that equipped Intel i7-4790 CPU built WM and compared WI and the WM. The top three wireless APs that

had a powerful RSSI were used because wireless APs with a powerful RSSI are helpful for location authentication. Wireless APs that have a weak RSSI are not helpful for location authentication because a wireless AP that has a weak RSSI shows no difference from an RSSI that is measured from other points.

The WM of a store had been made, and then the WM and the WI that was collected from the same store and other stores were compared. The False Acceptance Rate (FAR), which accepts the WI collected in other stores, was then measured, and the False Rejection Rate (FRR), which rejects the WI collected in the same store, was measured. After that, the Equal Error Rate (EER), which represents when the FAR and FRR are equal, was measured. In addition, the WM that was made using an autoencoder and the WM that was made using a Gaussian Mixture Model (GMM) [5] were compared, because the wireless APs with a strong RSSI follow the shape of Gaussian distribution, as shown in Fig. 6. In Fig. 6, x-axis means RSSI value and y-axis means the number of RSSI value. Table 1 shows the configuration of our experiments. In Table 1, "every" and "next" are compared with the WI that is collected in every store and the next store. Additionally, time difference is compared with the WI that is collected after a few days when the WM has been made. In addition, the training period is the collection period of the WI for making the WM.

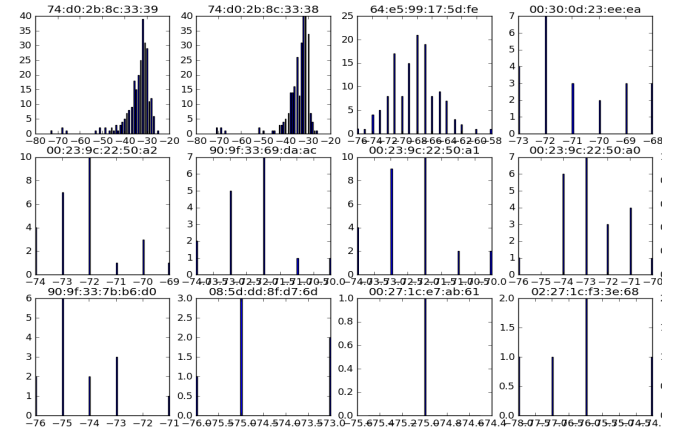


Figure 6. Example of collected wireless AP distributions

TABLE I. EXPERIMENTAL CONFIGURATIONS

	Every / Next Store	Time Difference (Days)	Training Period (Days)
Experiment 1	Every	0, 7	1
Experiment 2	Next	0	1
Experiment 3	Next	1-7	1
Experiment 4	Next	1	3-7

#### A. Experiment 1

The WI that was collected in every store on the same day was compared the WM after the WM had been made, and the WI that was collected in every store after seven days was compared the WM after the WM had been made. As shown in Fig. 7 and Table 2, the results show that EERs were measured as 2.4% and 4.1% when AE was used and EERs were measured as 5.3% and 9.0% when GMM was used.



TABLE II. RESULTS OF EXPERIMENT 1

Every store			
Same day		After 7 days	
AE	GMM	AE	GMM
2.4%	5.3%	4.1%	9.0%

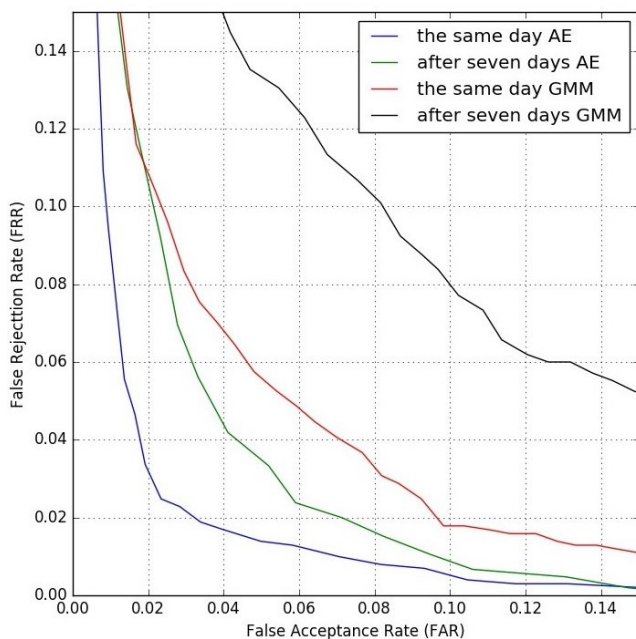


Figure 7. Comparison with data that is collected in every store

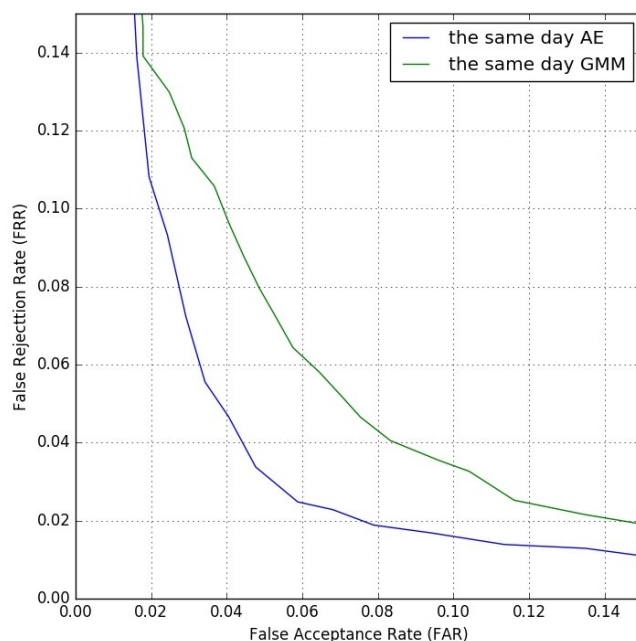


Figure 8. Comparison with data that is collected in next stores

### B. Experiment 2

In the second experiment, we compared the WM and WI collected in the next stores and the same store on the same day after the WM had been made. As shown in Fig. 8 and Table 3, the results show that EER was measured as 4.1% when AE was used and EER was measured as 6.1% when GMM was used.

TABLE III. RESULTS OF EXPERIMENT 2

Next store	
Same day	
AE	GMM
4.1%	6.1%

### C. Experiment 3

The WI that was collected in the next stores one, three, five, and seven days was compared the WM after the WM had been made. As shown in Fig. 9 and Table 4, the results

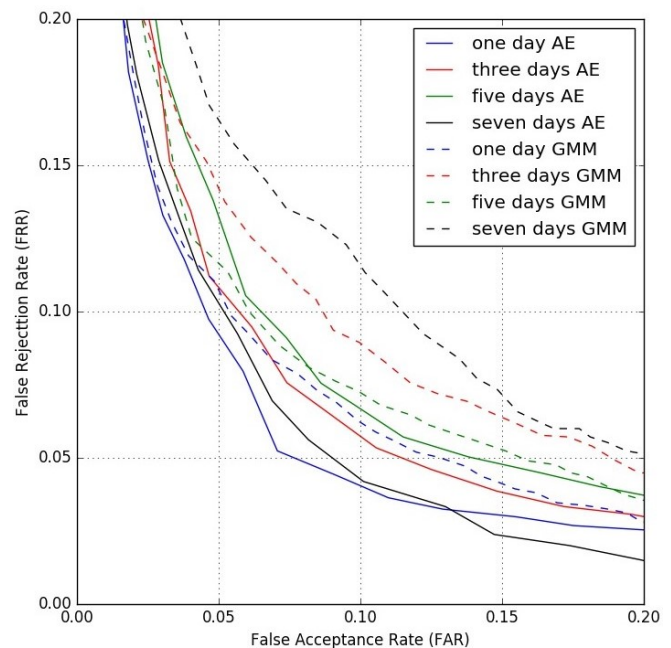


Figure 8. Comparison with data that is collected after a few days

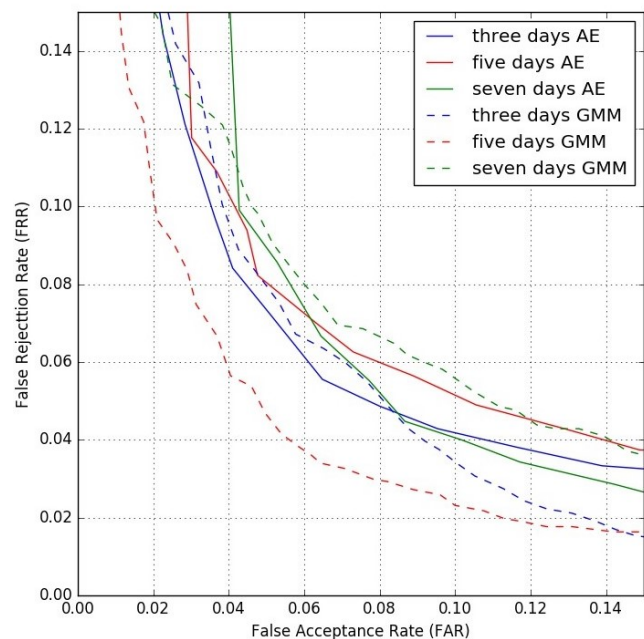


Figure 9. The WM is made from the WI that is collected over a few days

TABLE IV. RESULTS OF EXPERIMENT 3

Next store							
After n days							
1 Day		3 Days		5 Days		7 Days	
AE	GMM	AE	GMM	AE	GMM	AE	GMM
6.3%	7.8%	7.5%	9.1%	8.0%	8.1%	7.0%	10.7%

show that EERs were measured as 6.3% and 7.5% and 8.0%, and 7.0% when AE was used and EERs were measured as 7.8% and 9.1% and 8.1%, and 10.7% when GMM was used.

### D. Experiment 4

In the fourth experiment, we compared the WM that had been made by the WI that was collected over three, five, and seven days and the WI that was collected in the next stores

the next day. As shown in Fig. 10 and Table 5, the results show that EERs were measured as 6.0% and 6.6%, and 6.3% when AE was used and EERs were measured as 6.4% and 4.8%, and 6.8% when GMM was used.

TABLE V. RESULTS OF EXPERIMENT 4

Next store					
The WM is made from the WI that is collected for n days					
3 Days		5 Days		7 Days	
AE	GMM	AE	GMM	AE	GMM
6.0%	6.4%	6.6%	4.8%	6.3%	6.8%

#### IV. DISCUSSION

In this section, we provide a security analysis of the proposed method and discuss its usability and time performance.

##### A. Security Analysis

The proposed method might consider being attacked as follows:

1. The eavesdropper (Eve) tries to make a payment that uses the eavesdropped PI later. However, this attack will not succeed because the PI can only be used once
2. The attacker can make a payment that overwrites the user's LT with the attacker's LT stored in the Samsung Pay server. However, the attacker cannot overwrite the LT because the LT is stored after fingerprint authentication.
3. The Eve can send the WI that the Eve collects near the Samsung Pay user to the attacker. The attacker can then forge the LT received from the Eve and submit the LT. However, the attacker's LT cannot be referred because the wormhole payment attack uses the victim's LT. Therefore, this attack will fail.
4. When a WM has not been made for any store yet, the Eve sends the WI that is collected in another store to the Samsung Pay server. The Eve then sends their own PI to the attacker. The attacker then makes a payment in another store with the PI that has been sent by the Eve. The Samsung Pay server sends an inquiry to the Eve because a WM has not made for the store. The Eve then confirms the attacker's transaction. If this process is repeated several times, the WM of the store is made from the WI that was collected in another store. However, this attack not only incurs some costs to Eve, but can also be prevented by comparing the WI that is collected in the same store and the WI that is collected in the other store when the WM was made from the WI that was collected in the other store. If the WI that is collected in the other store is very similar to the WI that is collected in the same store, forgery might be suspected.

##### B. Accuracy of Proposed Method

The accuracy of the WI comparison is a very important issue. The results of the proposed method are measured as a minimum EER of 2.4% when the attacker uses the eavesdropped PI in a nearby store. In more extreme cases when an attack happens in the very next store, the results are measured as EERs from 4.1 to 8%. That is a very meaningful result because this is a very extreme case. If the

attacker is in a nearby store, they will be easy to catch. If the attacker is in a faraway store to avoid getting caught, the result of the proposed method will be almost 0%. Thus, a faraway attacker cannot succeed. However, if the user is rejected in a correct location, the attacker can succeed in a wormhole payment attack.

##### C. Usability and Time Performance

In this subsection, we represent the usability and time performance. For the usability, the proposed method requires minimal additional user actions. It sends the inquiry to the user only when a WM has not been made or when an attack is suspected. The user then just checks on the inquiry that has been received from the Samsung Pay server. An inquiry based on a false negative should also be considered. In this case, the service provider can choose a good answer. As shown in Figs. 7-10, the service provider can choose between usability and security by selecting the desired threshold in an inverse graph. The proposed method is deduced that the Samsung Pay user's smartphone application and Samsung Pay server.

For the time performance, if the time is sufficient, several WI samples can be collected, and this large number of samples makes the comparison more accurate. However, the average Samsung pay user spends 5 seconds in front of a POS. Therefore, we have just 5 seconds. These five seconds are a long time, but the proposed method performs various tasks, such as changing Wi-Fi channels, collecting the WI, normalizing the WI, issuing the PI. Additionally, our method does not require additional time delay. The required time is also very little compared with the WM and WI. It takes at most  $10^{-3}$  seconds on a PC with Intel i7-4790 CPU. Therefore, the proposed method does not cause any time delay in the Samsung Pay service.

#### V. RELATED WORK

Past work on location authentication can generally be grouped into two types: outdoor location authentication and indoor location authentication.

An outdoor location authentication technique that uses GPS was proposed in [6]. It compares the GPS coordinates of the smartphone and the address information of the POS. This method requires exact coordinate information for every POS, which is difficult to acquire. Moreover, the GPS cannot be used indoors because the GPS signal cannot be received indoors. The indoor location authentications were proposed techniques that use Bluetooth Low Energy (BLE) [7] and WI [8]. The technique that uses BLE [7] was a proximity detection method using the RSSI of BLE Beacon. However, it requires an additional device, which means a huge additional cost. The technique that was proposed in [8] used WI such as BSSID and RSSI. It compares the WI that was collected by the user's smartphone and the WI that was collected by the user's PC. This technique requires the user's PC to collect WI. If the technique is applied in an easy payment application, every POS should have additional HW to collect WI. This would incur huge expenses. Additionally, there is a way to input the ID of the POS when the PI is issued, but it has the disadvantage that the user has to perform additional actions. We compare our proposed method and related works in Table 6. Table 6 shows that the

proposed method is more convenient than other methods.

There are many indoor positioning techniques that utilize WI such as fingerprinting [9-12], differential Wi-Fi AP [13], and wireless indoor logical localization (WILL) [14].

TABLE VI. COMPARISON BETWEEN THE PROPOSED METHOD AND RELATED WORKS

	GPS [6]	BLE [7]	BSSID [8]	Input ID	Our method
Does not need additional user behavior	O	O	O	X	O
Does not need additional costs	O	X	X	O	O
Does not need POS modification	X	X	X	O	O
Does not need pre-requisite information	X	O	O	O	O
Indoor support	X	O	O	O	O

There are also many other techniques that use Radio Frequency Identification (RFID) [15-17], BLE [18], FM Radio [19], the acoustic background spectrum (ABS) [20], and geo-magnetism [21]. However, these techniques are not used for location authentication.

## VI. CONCLUSION

In this paper, we proposed a location authentication technique that uses WI such as BSSID and RSSI. It compares the WM that made the WI collected by previous Samsung Pay users and the WI that was collected by the current Samsung Pay user. Through very extreme experiments that compared the WI of nearby stores, we have shown that our proposed method can prevent wormhole payment attack effectively. If we had compared with faraway stores, we might have obtained better results. Furthermore, the proposed method has the advantages that it does not need additional hardware, additional costs, the modification of the POS's software, or additional user behavior, unlike other location authentication techniques. Moreover, the proposed method is not for Samsung Pay and can also applied to other easy payment applications.

Future work will study the adaptive training method. WI that is sent by an authorized Samsung Pay user will be used to update a WM. The WM should also be modified because the WI changes continuously.

## REFERENCES

- [1] Security Technology Research Team, "Analysis on Samsung Pay service and its security features," Federal Security Agency, Korea, 2015.
- [2] Apple Pay, "Apple Pay: Your wallet without the wallet," Retrieved August 22, 2015.
- [3] D. Choi and Y. Lee, "Eavesdropping One-Time Tokens Over Magnetic Secure Transmission in Samsung Pay," 10th USENIX Workshop on Offensive Technologies (WOOT 16), 2016.
- [4] P. Vincent, H. Larochelle, Y. Bengio, and P. A. Mangzagol, "Extracting and composing robust features with denoising autoencoders," in Proc. the 25th international conference on Machine learning, ACM, Jul. 2008, pp. 1096-1103. doi: 10.1145/1309156.1390294
- [5] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength," in INFOCOM 2008. The 27th Conference on Computer Communications, Apr. 2008, pp. 2441-2449. doi: 10.1109/INFOCOM.2008.239
- [6] H. Takamizawa and N. Tanaka, "Authentication system using location information on iPad or smartphone," International Journal of Computer Theory and Engineering, vol. 4, no. 2, pp. 153-157, 2012. doi: 10.7763/IJCTE.2012.V4.441
- [7] D. Kim, S. Kim, D. Choi, and S. Jin, "Accurate Indoor Proximity Zone Detection Based on Time Window and Frequency with Bluetooth Low Energy," Procedia Computer Science, vol. 56, pp. 88-95, 2015. doi: 10.1016/j.procs.2015.07.199
- [8] M. H. Chen and C. H. Chen, "Secondary user authentication based on mobile devices location," 2010 IEEE Fifth International Conference on Networking, Architecture and Storage (NAS), Jul. 2010, pp. 277-281. doi: 10.1109/NAS.2010.56
- [9] T. N. Lin, S. H. Fang, W. H. Tseng, C. W. Lee, and J. W. Hsieh, "A group-discrimination-based access point selection for WLAN fingerprinting localization," IEEE Transactions on Vehicular Technology, vol. 63, no. 8, pp. 3967-3976, Oct. 2014. doi: 10.1109/TVT.2014.2303141
- [10] K. Kaemarungsi and P. Krishnamurthy, "Analysis of WLAN's received signal strength indication for indoor location fingerprinting," Pervasive and Mobile Computing, vol. 8, no. 2, pp. 292-316, 2012. doi: 10.1016/j.pmcj.2011.09.003
- [11] N. Alsindi, Z. Chaloupka, N. AlKhanbashi, and J. Aweya, "An empirical evaluation of a probabilistic RF signature for WLAN location fingerprinting," IEEE Transactions on Wireless Communications, vol. 13, no. 6, pp. 3257-3268, Jun. 2014. doi: 10.1109/TWC.2014.041714.131113
- [12] Y. Jiang, X. Pan, K. Li, Q. Lv, R. P. Dick, M. Hannigan, and L. Shang, "Ariel: Automatic Wi-Fi based room fingerprinting for indoor localization," in Proc. the 2012 ACM Conference on Ubiquitous Computing, 2012, pp. 441-450. doi: 10.1145/2370216.2370282
- [13] N. Chang, R. Rashidzadeh, and M. Ahmadi, "Robust indoor positioning using differential Wi-Fi access points," IEEE Transactions on Consumer Electronics, vol. 53, no. 3, pp. 1860-1867, 2010. doi: 10.1109/TCE.2010.5606338
- [14] C. Wu, Z. Tang, Y. Liu, and W. Xi, "WILL: Wireless indoor localization without site survey," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 4, pp. 839-848, 2012. doi: 10.1109/TPDS.2012.179
- [15] P. Yang, W. Wu, M. Moniri, and C. C. Chibelushi, "Efficient object localization using sparsely distributed passive RFID tags," IEEE Transactions on Industrial Electronics, vol. 60, no. 12, pp. 5914-5924, Dec. 2013. doi: 10.1109/TIE.2012.2230596
- [16] E. DiGiampaolo and F. Martinelli, "Mobile robot localization using the phase of passive UHF RFID signals," IEEE Transactions on Industrial Electronics, vol. 61, no. 1, pp. 365-376, Jan. 2014. doi: 10.1109/TIE.2013.2248333
- [17] F. Seco, C. Plagemann, A. R. Jimenez, and W. Burgard, "Improving RFID-based indoor positioning accuracy using Gaussian processes," 2010 International Conference on Indoor Positioning and Indoor Navigation, Sept. 2010, pp. 1-8. doi: 10.1109/IPIN.2010.5647095
- [18] R. Faragher and R. Harle, "An analysis of the accuracy of Bluetooth low energy for indoor positioning applications," in Proc. the 27th International Technical Meeting of the Satellite Division of the Institute of Navigation, Tampa, FL, USA, Sep. 2014, pp. 201-210
- [19] V. Moghtadaiee and A. G. Dempster, "Indoor location fingerprinting using FM radio signals," IEEE Transactions on Broadcasting, vol. 60, no. 2, pp. 336-346, Jun. 2014. doi: 10.1109/TBC.2014.2322771
- [20] S. P. Tarzia, P. A. Dinda, R. P. Dick, and G. Memik, "Indoor localization without infrastructure using the acoustic background spectrum," in Proc. the 9th International Conference on Mobile Systems, Applications, and Services, New York, NY, USA: ACM, 2011, pp. 155-168. doi: 10.1145/1999995.2000011
- [21] J. Chung, M. Donahoe, C. Schmandt, I. Kim, P. Razavai, and M. Wiseman, "Indoor location sensing using geo-magnetism," in Proc. the 9th international conference on Mobile systems, applications, and services, New York, NY, USA: ACM, 2011, pp. 141-154. doi: 10.1145/1999995.2000010