

Forgery Resistance of User Authentication Methods Using Location, Wi-Fi and Their Correlation

Ryosuke Kobayashi^a and Rie Shigetomi Yamaguchi^b

The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, Japan

Keywords: Behavioral Authentication, Impersonation, Location, Wi-Fi, Correlation.

Abstract: In recent years, much research has been conducted on user authentication methods utilizing human behavioral information. It is known that human behavioral information represents their characteristics and can be utilized in user authentication as well as biometric information such as facial or fingerprints. Particularly, location information representing a person's stay and movement history strongly reflects his/her characteristic and can achieve high accuracy in user authentication within behavioral authentication methods. On the other hand, location information is easily inferable by others and there is a concern that the inferred information could be exploited for impersonation. In user authentication methods utilizing location information, it is essential to enhance resistance to impersonation even when the location is inferred. However, there has been no research conducted on this aspect. In this paper, we aim to enhance forgery resistance by utilizing not only the location information collected by smartphones but also Wi-Fi information and the correlation between location and Wi-Fi data in the context of user authentication methods. These three modality were combined through the score fusion method. As a result, this approach successfully improved authentication accuracy and resistance to impersonation.


1 INTRODUCTION


In recent years, user authentication methods utilizing behavioral information, known as behavioral authentication, have been proposed and are sometimes referred to as the fourth authentication method (Yamaguchi et al., 2020a). One of the distinctive features of behavioral authentication is that users are authenticated without conscious input of information, which sets it apart when compared to conventional authentication methods. With the advancement of IoT (Internet of Things) technology, it has become easy and automatic to collect human behavioral information. By utilizing such collected behavioral information, it becomes possible to implement user authentication methods that users are not consciously aware of.

One of the advantages of the method of being authenticated without the user's awareness is that it can be utilized as continuous authentication (Traore, 2011). Continuous authentication is a method of authenticating not only when logging into a service but also continuously during the usage of the service. As

the usage opportunities of mobile devices increase, the possibility of someone else stealing the device during the usage of the service has also increased. The conventional authentication system cannot detect the change of users during the usage of the service with authentication only at login, but continuous authentication can detect this change. However, continuous authentication is a method that places a significant burden on users. If users are asked to enter authentication information repeatedly during the usage of the service, the burden on users will be significant. By utilizing behavioral authentication, we can achieve continuous authentication without increasing the user's burden.

The utilization of behavioral information for user authentication implies that this information represents an individual's characteristics like biometric data such as face and fingerprints. In particular, location information has a strong characteristic and it can achieve high accuracy within behavioral authentication when utilized for authentication (Fridman et al., 2016). Location information can be collected using GPS embedded in smartphones, and it becomes possible to estimate an individual's residence or workplace by analyzing the history of this information (Liao et al.,

^a  <https://orcid.org/0000-0001-8001-2367>

^b  <https://orcid.org/0000-0002-6359-2221>

2007). These analytical results indicate that location information strongly represents an individual's characteristics.

However, location information can also be easily known or inferred by others since it is physically exposed like fingerprints and faces. For example, it is natural to be able to know the location information of a person present in front of you at the time. Furthermore, if you know where a person works, it's possible to infer that they are likely to be at their office during the day. In this way, location information is easily inferable by others, and it can lead to easy inference of authentication information when utilized in user authentication. In other words, using location information in authentication methods carries the risk of being easily impersonated by others.

In user authentication methods utilizing location information, there is existing research (Miyazawa et al., 2022) that utilizes the correlation with Wi-Fi information to reduce the risk of impersonation. Wi-Fi data can be automatically collected using sensors in smartphones like location data, and combining it with location information is straightforward. In this method, the assumption is that even if location information alone is inferred, Wi-Fi information is not easily inferred, thus enhancing resistance to impersonation. However, from the perspective of authentication accuracy, there is a challenge where this correlation-based authentication method achieves lower accuracy than authentication methods utilizing only location information. In this paper, we propose a method that combines authentication methods utilizing location information, authentication methods utilizing Wi-Fi information, and authentication methods utilizing the correlation between location and Wi-Fi information to maintain both improved resistance to impersonation and reduced authentication accuracy.

The rest of this paper is structured as follows. In section 2, we introduce related research on behavioral authentication methods and combinations of authentication methods. In section 3, we explain the proposed method in this study. In section 4, we describe the experiments conducted in this study, including the dataset used, experimental scenarios, and results. Finally, in section 5, we conclude this paper and discuss future works.

2 RELATED WORK

In this section, we introduce some existing researches on user authentication methods utilizing behavioral information and attack models against these authentication techniques.

2.1 Behavioral Authentication

There are some types of behavioral information utilized for authentication. Abuhamad et al. (Abuhamad et al., 2020) categorized behavioral authentication methods based on the modalities they utilize for behavioral authentication and classified them into two types. One is referred to as behavioral biometrics. Behavioral biometrics is known as traditional behavioral authentication and is a method that leverages human's habits when performing specific actions for user authentication. This includes authentication methods utilizing keystroke dynamics (Raul et al., 2020), touch gestures (Chen et al., 2020), motion (Sufyan et al., 2023), and so on.

Another is user profiling which utilizes behavioral profiles. User profiling is a relatively new technology when compared to behavioral biometrics. The behavioral profiles can be obtained by analyzing information such as location (Thao et al., 2020), Wi-Fi (Kobayashi and Yamaguchi, 2015), activity (Zeng et al., 2017), app usage (Yamaguchi et al., 2020b), and so on. We focus on location-based authentication and Wi-Fi based authentication in this research, which is included in user profiling.

2.2 Attack Model

Rayani et al. (Rayani and Changder, 2023) presented some existing researches on behavioral authentication and attack methods for them. They introduced both behavioral biometrics and user profiling regarding behavioral authentication methods. However, they only presented attack methods related to behavioral biometrics such as gait (Kumar et al., 2015), touch-screen (Khan et al., 2016), keystroke (Khan et al., 2018), and so on. This implies the absence of research on attack methods for user profiling. Therefore, we focused on attacks against location-based and Wi-Fi based authentication in this study.

3 PROPOSED METHOD

A typical user biometric authentication system operates in two distinct phases: enrollment and verification (Rattani et al., 2009). In enrollment phase, user's biometric information is captured, processed, features extracted and labels are assigned to him/her to establish identity, representing the template of the user. Verification phase compares query biometric samples of the respective user with the enrolled template to verify an identity. In this comparison process, a score is calculated to determine how well the input query

represents the legitimate user. If the score is higher than a given threshold, then the authentication system verifies the authentication is success. The behavioral authentication scheme is similar to that of biometric authentication mentioned above, and our proposed method also utilizes this scheme.

We utilize the location information and Wi-Fi information collected from smartphones in this proposed method. From the location information, we calculate a score using a location-based authentication method, and from the Wi-Fi information, we calculate a score using a Wi-Fi-based authentication method. Additionally, we calculate a score using a correlation-based authentication method that utilizes the correlation between location and Wi-Fi. These three types of scores are combined to calculate the final score and make an authentication decision. Fig. 1 illustrate the proposed method. In this section, we explain these three scoring methods and the method of combining the scores.

3.1 Location-Based and Wi-Fi-Based Authentication Method

The scoring methods for location-based authentication and Wi-Fi-based authentication utilize the approach proposed by Kobayashi et al. (Kobayashi and Yamaguchi, 2017). This section provides an explanation of these methods.

3.1.1 Notation for Location Information and Wi-Fi Information

A user u is assumed to be at a location l at a specific time t . For the user u , l is uniquely determined when t is determined. This l is referred to as location information, denoted as $L_u(t) = l$.

Furthermore, it is assumed that there are wireless LAN access points w around a user u at a specific time t . We refer to the information of these wireless LAN access points as Wi-Fi information in this paper. Generally, the number of wireless LAN access points around u is not limited to one. When there are wireless LAN access points w_1, w_2, \dots around u at a given time t , Wi-Fi information is represented as $W_u(t) = \mathbf{w} = \{w_1, w_2, \dots\}$. The Wi-Fi information obtained by radio sensors in devices like smartphones includes the SSID (Service Set Identifier) and BSSID (Basic Service Set Identifier) of the wireless LAN access points as well as signal strength. The BSSID and SSID have a 1-to-N relationship, so we utilized only the BSSID of the wireless LAN access points in this Wi-Fi-based authentication method. Therefore, when referring to Wi-Fi information, we specifically mean

the BSSIDs of the wireless LAN access points in this paper.

3.1.2 Preprocessing

Human daily behavior follow rhythmic patterns with a periodicity of one day. However, when we say that human behaves periodically, it does not mean that the same behavior are carried out at the same time every day. Even for the same behavior, the timing may vary, and there are instances where activities unique to that day are performed. This variation is referred to as the fluctuation of behavior, and processing must be conducted to absorb this fluctuation of behavior to utilize behavioral information for authentication. In this section, we explain preprocessing in the context of location and Wi-Fi information to absorb these fluctuations.

There are three types of fluctuation which are time fluctuation, location fluctuation, and Wi-Fi fluctuation. We describe each of these below.

- Time Fluctuation.

For example, we consider the case of taking the same train every day to commute. Even if you take the same train, the time of boarding may not be the same when the train is delayed. This is the time fluctuation. To absorb the time fluctuation, it is necessary to consider slightly shifted times as the same information. In this study, we attempt to absorb the time fluctuation by rounding the location and Wi-Fi information to every hour. Namely, let $t = (d, time)$ (where d represents the day, $time$ represents the hour and below). With d fixed, for h o'clock $\leq time < (h + 1)$ o'clock ($h = 0, 1, \dots, 23$), $L_u(d, time)$ and $W_u(d, time)$ are considered constant.

- Location Fluctuation.

To absorb the location fluctuation, it is sufficient to consider the same information even if the stay location is slightly shifted. In this study, we adopt the quadkey (Corporation,) as a tool to represent the location to absorb the location fluctuation, considering location information not as specific points but as areas with a certain extent. Namely, we denote l as the area where the user stayed the longest at a given time h o'clock $\leq time < (h + 1)$ o'clock. Thus, we express $L_u(d, time) = l$ for (h o'clock $\leq time < (h + 1)$ o'clock).

- Wi-Fi Fluctuation.

To absorb the Wi-Fi fluctuation, we discard Wi-Fi information with a low number of detections and select a maximum of five Wi-Fi information with the highest detection counts in this study. In other words, at a given time h

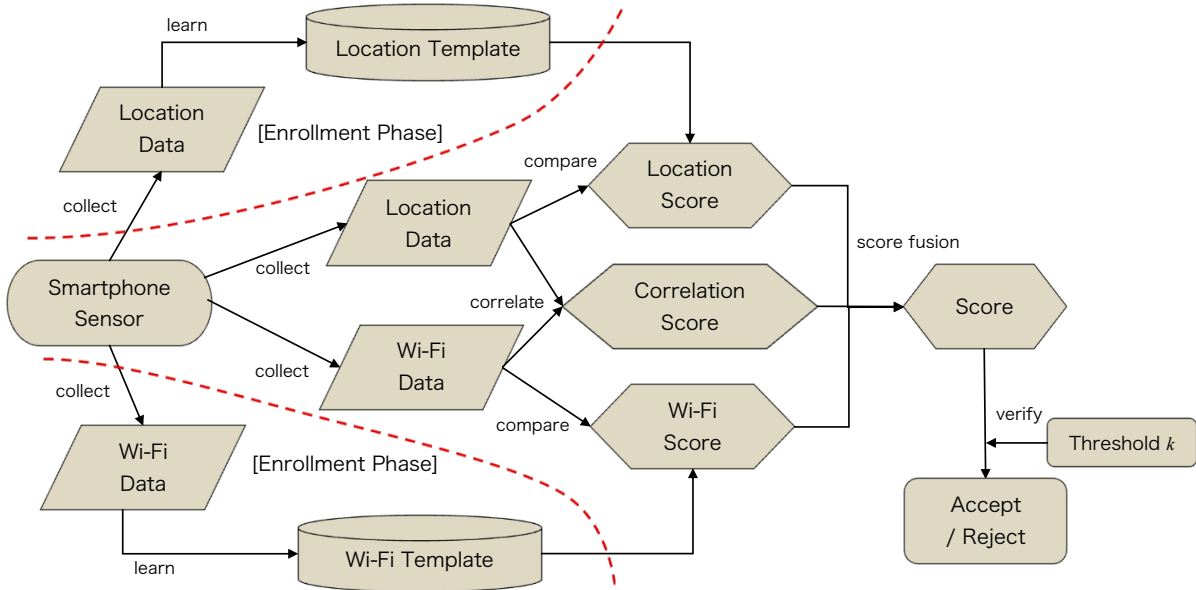


Figure 1: Overview of Proposed Method.

o'clock \leq time $<$ $(h + 1)$ hour, if the top five Wi-Fi information with the highest detection counts are denoted as w_1, w_2, \dots, w_5 , then we express $W_u(d, time) = w_1, w_2, \dots, w_5$ (h o'clock \leq time $<$ $(h + 1)$ o'clock).

In the following sections of this paper, concerning these authentication methods, we will denote $L_u(d, time)$ and $W_u(d, time)$ as $L_u(d, h)$ and $W_u(d, h)$ respectively due to their constancy for h o'clock \leq time $<$ $(h + 1)$ o'clock.

3.1.3 Template Making

User authentication methods generally consist of two main phases which are the enrollment phase and the verification phase. In the enrollment phase, information representing an individual's authenticity is pre-registered. This information is commonly referred to as a template. In the verification phase, the pre-registered template is compared with authentication information to make an authentication decision. In this section, we describe the algorithm for creating the template registered in the enrollment phase.

When referring to the location and Wi-Fi template for a user u , denoted as $T_u^{loc}(h)$ and $T_u^{wifi}(h)$ respectively, these templates can be obtained from Algorithm 1 and 2.

3.1.4 Similarity Score Calculation

The similarity score for verification can be calculated by comparing the authentication information with a

Algorithm 1: Template Making Algorithm for Location.

Require: Behavioral data

D : Learning period

$L_u(d, h)$: Location information of user u at date d and time h

Ensure: $T_u^{loc}(h)$: Location template

function MAKE_LOCTEMPLATE($D, L_u(d, h)$)

$T_u^{loc}(h) \leftarrow \{\}$

$c \leftarrow 0$

for d in D **do**

if $L_u(d, h)$ in $T_u^{loc}(h)$ **then**

$T_u^{loc}(h)[L_u(d, h)] += 1$

else

$T_u^{loc}(h)[L_u(d, h)] \leftarrow 1$

end if

$c += 1$

end for

for t_{loc} in $T_u^{loc}(h)$ **do**

$T_u^{loc}(h)[t_{loc}] \leftarrow T_u^{loc}(h)[t_{loc}] / c$

end for

return $T_u^{loc}(h)$

end function

template. This section describes the method of calculating the score.

Let the score for user u at day d and time h be denoted as $S_u^{loc}(d, h)$ and $S_u^{wifi}(d, h)$. These values are calculated using the algorithm shown in Algorithm 3 and 4.

Algorithm 2: Template Making Algorithm for Wi-Fi.

Require: Behavioral data
 D : Learning period
 $W_u(d, h)$: Wi-Fi information of user u at date d and time h
Ensure: $T_u^{wifi}(h)$: Wi-Fi template
function MAKE_WIFITEMPLATE($D, W_u(d, h)$)
 $T_u^{wifi}(h) \leftarrow \{\}$
 $c \leftarrow 0$
for d **in** D **do**
 for w **in** $W_u(d, h)$ **do**
 if w **in** $T_u^{wifi}(h)$ **then**
 $T_u^{wifi}(h)[w] += 1$
 else
 $T_u^{wifi}(h)[w] \leftarrow 1$
 end if
 end for
 $c += 1$
end for
for t_{wifi} **in** $T_u^{wifi}(h)$ **do**
 $T_u^{wifi}(h)[t_{wifi}] \leftarrow T_u^{wifi}(h)[t_{wifi}] / c$
end for
return $T_u^{wifi}(h)$
end function

Algorithm 3: Similarity Score Calculating Algorithm for Location.

Require: Behavioral data
 $L_u(d, h)$: Location information of user u at date d and time h
 $T_u^{loc}(h)$: Location template of user u at time h
Ensure: $S_u^{loc}(d, h)$ Similarity score for location
function COMPARE_LOC($L_u(d, h), T_u^{loc}(h)$)
 $S_u^{loc}(d, h) \leftarrow 0$
if $L_u(d, h)$ **in** $T_u^{loc}(h)$ **then**
 $S_u^{loc}(d, h) \leftarrow T_u^{loc}(h)[L_u(d, h)]$
end if
return $S_u^{loc}(d, h)$
end function

3.2 Correlation-Based Authentication Method

Regarding the authentication method utilizing the correlation between location and Wi-Fi information, we employ the approach by Miyazawa et al. (Miyazawa et al., 2022). In this section, we will confine the explanation to the principles and notation of this method.

This approach asserts that when the user's location changes, information related to Wi-Fi, such as the access points connected to his/her smartphone and the

Algorithm 4: Similarity Score Calculating Algorithm for Wi-Fi.

Require: Behavioral data
 $W_u(d, h)$: Wi-Fi information of user u at date d and time h
 $T_u^{wifi}(h)$: Wi-Fi template of user u at time h
Ensure: $S_u^{wifi}(d, h)$ Similarity score for Wi-Fi
function COMPARE_WIFI($W_u(d, h), T_u^{wifi}(h)$)
 $S_u^{wifi}(d, h) \leftarrow 0$
for w **in** $W_u(d, h)$ **do**
 if w **in** $T_u^{wifi}(h)$ **then**
 $S_u^{wifi}(d, h) \leftarrow T_u^{wifi}(h)[w]$
 end if
end for
return $S_u^{wifi}(d, h)$
end function

number of access points around the smartphone, also changes. They utilized this characteristic and proposed an correlation-based authentication method by assigning a positive score when both location information and Wi-Fi information change, and a negative score when only one of them changes.

The correlation between location and Wi-Fi refers to the correlation between changes in location information and changes in Wi-Fi information in Miyazawa's method. In other words, based on the assumption that when the location of a smartphone changes, the surrounding Wi-Fi devices also change, they quantitatively represent this relationship with scores and utilize it for authentication.

In this paper, the score of this correlation-based authentication method is denoted as $S_u^{corr}(d)$ for user u at a specific day d . Note that $S_u^{corr}(d)$ can take value in the range of $-1 \leq S_u^{corr}(d) \leq 1$.

3.3 Fusion Method

In this research, the final score for verification is obtained by taking the average of the three types of scores calculated so far. It should be noted that while $0 \leq S_u^{loc}(d), S_u^{wifi}(d) \leq 1$, the scores for correlation have a range of $-1 \leq S_u^{corr}(d) \leq 1$. Therefore, normalization is performed on the correlation score before taking the average. In other words, the final score $S_u(d)$ is expressed as following.

$$S_u(d) = \frac{S_u^{loc}(d) + S_u^{wifi}(d) + \frac{S_u^{corr}(d)+1}{2}}{3}$$

4 EXPERIMENT

In this section, we will describe the experiments conducted in this research.

4.1 Dataset

In this research, we utilized the dataset obtained from a demonstration experiment for data collection conducted prior to this experiment by us. The data collection experiment was conducted from February 1 to March 31, 2021. We managed to collect the location and Wi-Fi data of 3,088 participants. This demonstration experiment was conducted under the ethical review of the Ethics Review Committee of our organization.

We utilized the data from 85 participants who were Android users and had data collected for 50 days or more from this dataset for this experiment.

4.2 Experimental Scenario

In this research, we aimed to investigate the impersonation resistance of behavioral authentication considering cases where location information is inferred by others. Based on this objective, we conducted the following experiments.

- **Authentication Performance.**
This experiment aims to evaluate the performance of the authentication system using *TAR* (True Acceptance Rate) as the evaluation metric. The authentication system is as shown in the Figure 1, and it adopts four types of combinations which are location and Wi-Fi, location and correlation, Wi-Fi and correlation, and location, Wi-Fi, and correlation. Furthermore, we apply our data to methods that utilize only single-factor among location, Wi-Fi, and correlation, and evaluate their performance in a similar manner for comparison with fusion methods.
- **Location Estimation Attack.**
The purpose of this experiment is to calculate the attack success rate on the authentication system when the user's location is completely known to others. The authentication system for this experiment is the same as above.

In this section, we will provide detailed explanations of these experimental scenarios.

4.2.1 Authentication Performance

It is necessary to set the template making period for authentication experiments utilizing location or Wi-Fi

information. Therefore, in this experiment, the template making period for authentication experiments on day d was set from day 1 to day $(d - 1)$ ($2 \leq d \leq$ (number of experiment days)). For example, for a user who collected data for 60 days, for the authentication experiment on the 2nd day, the template was created using only the data from the 1st day. For the authentication experiment on the 60th day, the template was created using data from day 1 to day 59, covering a period of 59 days.

In this scenario, we conducted seven cases as following including authentication experiments using only location, Wi-Fi, and correlation individually, as well as four cases combining these three factors.

- (g): Location
- (w): Wi-Fi
- (c): Correlation
- (gw): Fusion of location and Wi-Fi
- (gc): Fusion of location and correlation
- (wc): Fusion of Wi-Fi and correlation
- (gwc): Fusion of location, Wi-Fi, and correlation

4.2.2 Location Estimation Attack

In this experiment, we calculate the success rate of an attack when an attacker a attempts to impersonate a legitimate user u by conducting a location estimation attack. We assume that the attacker has knowledge of the legitimate user location information in this attack. On the other hand, the attacker is unable to access the legitimate user's Wi-Fi information. Instead, the attacker uses their own Wi-Fi information as authentication information. In other words, the attacker uses $\{L_u(t), W_a(t)\}$ as authentication information. This authentication information is compared with the legitimate user's template, and the final score is calculated from each score to verify the authentication decision. The target authentication systems are (gw), (gc), (wc), and (gwc). The False Acceptance Rate (*FAR*) is used as a metric to calculate the attack success rate.

4.3 Evaluation Metrics

We use *TAR* and *FAR* as evaluation metrics in this experiment. *TAR* is used to evaluate the accuracy of the authentication system, while *FAR* is used to evaluate resistance against impersonation from others. A higher *TAR* indicates a higher accuracy in the authentication method, and a lower *FAR* indicates a higher resistance to impersonation when the location information is estimated.

When the score S calculated from the provided authentication information satisfies $S \geq k$ under a given threshold k , it is considered the authentication system accepts the authentication information, while when $S \leq k$, it is considered the authentication system rejects it. TAR and FAR are defined as follows.

$$TAR = \frac{\text{(Number of acceptance)}}{\text{(Total genuin tests)}}$$

$$FAR = \frac{\text{(Number of acceptance)}}{\text{(Total imposter tests)}}$$

Note that the genuine test refers to an authentication test that compares a template of a legitimate user u with the user’s authentication information, while the imposter test refers to an authentication test that compares a template of a legitimate user u with the authentication information of an attacker a .

Both TAR and FAR change accordingly by varying the threshold k as defined above. Simply enhancing resistance to impersonation, that means reducing FAR , can be achieved by increasing k . However, increasing k results in a lower TAR which makes the authentication method less user-friendly. TAR and FAR are in a trade-off relationship.

4.4 Experimental Result

In this section, we describe the experimental results.

4.4.1 Authentication Performance

We varied the threshold k in the range $[0, 1]$ for the seven cases and calculated TAR . The trend is that the fusion methods with other information have higher TAR compared to the results from single-factor in the small k range. On the other hand, in the large k range, the TAR for single-factor like location and correlation is higher compared to the fusion methods. Kobayashi et al. claimed that Wi-Fi-based authentication method achieved very small FAR and they set the threshold k to a very small value in their research (Kobayashi and Yamaguchi, 2017). It is possible to set the threshold to a small value in this research from the result of Kobayashi et al., and we can say the fusion methods perform better than the single-factor methods. The actual TAR for each method is as Table 1.

4.4.2 Location Estimation Attack

The FAR values indicate the attack success rate when the attacker conducting a location estimation attack on the authentication systems. A low value for k is sufficient as mentioned in the previous section, and Table 2 shows the FAR values for each methods at

Table 1: TAR at $k = 0.2, 0.4, 0.6$ and 0.8 .

k	0.2	0.4	0.6	0.8
g	0.878	0.774	0.573	0.241
w	0.850	0.559	0.187	0.024
c	0.814	0.742	0.645	0.489
gw	0.933	0.796	0.393	0.051
gc	0.921	0.787	0.599	0.273
wc	0.870	0.690	0.476	0.054
gwc	0.936	0.792	0.482	0.068

$k = 0.2$. Since wc is the method that least incorporates location information, its FAR value is smaller than others.

TAR of location-based authentication method is equivalent to the success rate of impersonation when the location information is known by an attacker. The FAR values in Table 2 seem large, but when compared to TAR for location-based authentication method in Table 1, it is evident that they are smaller. In other words, it is possible to reduce the attack success rate even when the location information is inferred by others by combining multiple factors.

Table 2: FAR under Location Estimation Attack at $k = 0.2$.

$(k = 0.2)$	gw	gc	wc	gwc
FAR	0.847	0.886	0.172	0.755

5 CONCLUSION

While location information strongly represents human’s characteristics, it can be easily inferred by others, posing a risk of impersonation in authentication methods utilizing it. Therefore, we assumed cases where location information is inferred and conducted experiments to enhance resistance to impersonation by combining it with other authentication methods in this paper. We conducted some experiments by combining authentication methods utilizing location, Wi-Fi, and correlation information to enhance both authentication accuracy and resistance to impersonation. As a result, the approach combining Wi-Fi and correlation yielded the best results. This aligns with our study’s assumption of considering cases where location information is inferred, and not incorporating location authentication led to superior outcomes.

5.1 Future Work

In this paper, we conducted experiments assuming that all location information is inferred. However, it is not guaranteed that the location information for all

times throughout the day can be accurately inferred in reality. Even if places like home or workplace are known, only parts of the day might be inferred. Therefore, it is a challenge to examine which methods are suitable for cases where only certain location information is inferred in future work. Additionally, we focused on inferring only location information in this research, but it is conceivable that certain Wi-Fi information can also be inferred. Exploring scenarios where partial information of both location and Wi-Fi is inferred is another future research direction.

REFERENCES

- Abuhamad, M., Abusnaina, A., Nyang, D., and Mohaisen, D. (2020). Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey. *IEEE Internet of Things Journal*, 8(1):65–84.
- Chen, H., Li, F., Du, W., Yang, S., Conn, M., and Wang, Y. (2020). Listen to your fingers: User authentication based on geometry biometrics of touch gesture. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 4(3):1–23.
- Corporation, M. Bing maps tile system. <https://learn.microsoft.com/en-us/bingmaps/articles/bing-maps-tile-system>. Accessed:2023-05-21.
- Fridman, L., Weber, S., Greenstadt, R., and Kam, M. (2016). Active authentication on mobile devices via stylometry, application usage, web browsing, and gps location. *IEEE Systems Journal*, 11(2):513–521.
- Khan, H., Hengartner, U., and Vogel, D. (2016). Targeted mimicry attacks on touch input based implicit authentication schemes. In *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*, pages 387–398.
- Khan, H., Hengartner, U., and Vogel, D. (2018). Augmented reality-based mimicry attacks on behaviour-based smartphone authentication. In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*, pages 41–53.
- Kobayashi, R. and Yamaguchi, R. S. (2015). A behavior authentication method using wi-fi bssids around smartphone carried by a user. In *2015 Third International Symposium on Computing and Networking (CANDAR)*, pages 463–469. IEEE.
- Kobayashi, R. and Yamaguchi, R. S. (2017). Behavioral authentication method utilizing wi-fi history information captured by iot device. In *2017 International Workshop on Secure Internet of Things (SIoT)*, pages 20–29. IEEE.
- Kumar, R., Phoha, V. V., and Jain, A. (2015). Treadmill attack on gait-based authentication systems. In *2015 IEEE 7th international conference on biometrics theory, applications and systems (BTAS)*, pages 1–7. IEEE.
- Liao, L., Fox, D., and Kautz, H. (2007). Extracting places and activities from gps traces using hierarchical conditional random fields. *The International Journal of Robotics Research*, 26(1):119–134.
- Miyazawa, A., Thao, T. P., and Yamaguchi, R. S. (2022). Multi-factor behavioral authentication using correlations enhanced by neural network-based score fusion. In *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, pages 569–577. IEEE.
- Rattani, A., Freni, B., Marcialis, G. L., and Roli, F. (2009). Template update methods in adaptive biometric systems: A critical review. In *Advances in Biometrics: Third International Conference, ICB 2009, Alghero, Italy, June 2-5, 2009. Proceedings 3*, pages 847–856. Springer.
- Raul, N., Shankarmani, R., and Joshi, P. (2020). A comprehensive review of keystroke dynamics-based authentication mechanism. In *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2019, Volume 2*, pages 149–162. Springer.
- Rayani, P. K. and Changder, S. (2023). Continuous user authentication on smartphone via behavioral biometrics: a survey. *Multimedia Tools and Applications*, 82(2):1633–1667.
- Sufyan, F., Sagar, S., Nayel, S., Chishti, M. S., Ashraf, Z., and Banerjee, A. (2023). A novel and lightweight real-time continuous motion gesture recognition algorithm for smartphones. *IEEE Access*.
- Thao, T. P., Irvan, M., Kobayashi, R., Yamaguchi, R. S., and Nakata, T. (2020). Self-enhancing gps-based authentication using corresponding address. In *Data and Applications Security and Privacy XXXIV: 34th Annual IFIP WG 11.3 Conference, DBSec 2020, Regensburg, Germany, June 25–26, 2020, Proceedings 34*, pages 333–344. Springer.
- Traore, I. (2011). *Continuous Authentication Using Biometrics: Data, Models, and Metrics: Data, Models, and Metrics*. Igi Global.
- Yamaguchi, R. S., Nakata, T., and Kobayashi, R. (2020a). Redefine and organize, 4th authentication factor, behavior. *International Journal of Networking and Computing*, 10(2):189–199.
- Yamaguchi, S., Gomi, H., Kobayashi, R., Thao, T. P., Irvan, M., and Yamaguchi, R. S. (2020b). Effective classification for multi-modal behavioral authentication on large-scale data. In *2020 15th Asia Joint Conference on Information Security (AsiaJCIS)*, pages 101–109. IEEE.
- Zeng, Y., Pande, A., Zhu, J., and Mohapatra, P. (2017). Wearia: Wearable device implicit authentication based on activity information. In *2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pages 1–9. IEEE.