One Cycle Attack: Fool Sensor-Based Personal Gait Authentication With Clustering

Tiantian Zhu, Lei Fu, Qiang Liu, Zi Lin, Yan Chen, *Fellow, IEEE*, and Tieming Chen, *Member, IEEE*

***Abstract*— Gait authentication, especially sensor-based patterns, has been studied by researchers for decades. Nowadays, gait authentication has become an important facet of biometric systems due to the so-called unique characteristics of each user. With the development of various technologies (i.e., hardware, data processing, features extraction, and learning algorithms), the performance of sensor-based authentication methods is gradually improving. But we have found that the vulnerability of most existing methods can be compromised easily. In this paper, we propose a novel attack model, called one cycle attack, to bypass existing gait authentication methods. Firstly, the gait sequence is divided into multiple gait cycles. By adopting the K-mean algorithm, we get the average distance of each feature sample (extracted from the gait cycle) to its closest cluster center, and its result confirms that independent individuals may have similar gait cycles. Secondly, using six state-of-the-art models it was found that the adversarial gait cycle found with the clustering method can bypass the victim's model rapidly. Furthermore, to improve the accuracy of sensor-based gait authentication methods to fight against attacks, we present a WPD-LSTM (Wavelet Packet Decomposition and Long Short-Term Memory) multi-cycle defense model which considers the contextual contents of the neighboring gait cycles in the gait sequence. Experimental results on two datasets (the largest public sensor-based gait database OU-ISIR and new dataset from our laboratory) show that our attack model can bypass most of the victims' models within a limited number of attempts. Specifically, we can compromise 20%-80% of users within 5 attempts by utilizing imitation. On the contrary, the success rate of attackers has been greatly mitigated by deploying our multi-cycle defense model.**

***Index Terms*— Gait authentication, motion sensor, attack and defense, adversarial gait cycle, deep learning.**

Manuscript received February 21, 2020; revised June 18, 2020 and July 16, 2020; accepted August 11, 2020. Date of publication August 14, 2020; date of current version September 3, 2020. This work was supported in part by the National Natural Science Foundation of China under Grant U1936215 and Grant 61772026, in part by the Ministry of Industry and Information Technology of China under Grant TC190H3WN, and in part by the State Grid Corporation of China under Grant 5211XT19006B. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Andrew Beng Jin Teoh. *(Corresponding authors: Lei Fu; Yan Chen.)*

Tiantian Zhu and Tieming Chen are with the College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China (e-mail: ttzhu@zjut.edu.cn; tmchen@zjut.edu.cn).

Lei Fu is with the College of Mechanical Engineering, Zhejiang University of Technology, Hangzhou 310023, China (e-mail: fulei@zjut.edu.cn).

Qiang Liu is with the College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China (e-mail: qiangliu@zju.edu.cn).

Zi Lin and Yan Chen are with the Department of Electrical Engineering and Computer Science, Northwestern University, Evanston, IL 60208 USA (e-mail: zilin2020@u.northwestern.edu; ychen@northwestern.edu).

Digital Object Identifier 10.1109/TIFS.2020.3016819

I. Introduction

THE development and popularization of mobile devices, such as smartphones, smart tablets, and smartwatches have generally benefited the public for decades. While these mobile devices store masses of private information, security was regarded as a risk by users. It is important to set up effective authentication methods to protect the security of mobile devices. A wide variety of authentication technologies are embedded in these mobile devices to protect the devices from illicit use. One well-known countermeasure is knowledge-based authentication in which PINs, passwords, and patterns were first proposed, and they also play an important role in the recent mobile device authentication scenarios. Another type of countermeasures is biometric-based authentication. The existing approaches exploit biometrics including but not limited to face [1], fingerprint [2], iris [3], voice [4] and keystroke dynamics [5] to help authenticate the real users explicitly. Although these methods can achieve higher accuracy, users are required to explicitly enter authentication information. The user's comfort is undoubtedly reduced as a side effect of improving security. To balance the accuracy and usability, dynamic biometric authentication, such as gait dynamics [6], implicitly authenticates the user based on his/her walking patterns.

Motion sensors, especially acceleration sensors and gyroscope sensors, have been widely accepted by the industry community due to their low-power requirement [7], their low impact, and for their capacity to provide data directly related to the state of motion [8]. During the sensor-based gait authentication, the mobile devices record the relevant sensor data while the user is walking and uses it for user differentiation. The device can be hung on the waist [9], ankle [10], hip [11], [12], or in the pocket [13], [14]. Most of the studies show that placing the device in these different positions will all achieve a high level of accuracy. Unlike other biometric authentication methods (face, fingerprint, etc.), sensor-based gait authentication does not require the user to follow an explicit behavior, such as placing a finger on the fingerprint sensor or aligning the face in the front camera. In daily life, users can complete authentication as long as they walk normally. Early work has shown that sensor-based gait authentication has great potential in medical [15], [16], financial [17], and military applications [18], etc. The famous product, UnifyId [19], which is the first implicit authentication platform designed for online and physical world use, authenticates different people utilizing their unique walking

1556-6013 © 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Northwestern University. Downloaded on October 10,2020 at 10:35:04 UTC from IEEE Xplore. Restrictions apply.

patterns as one of the behavioral biometrics. The recent report by FedTech [18] also shows that gait authentication is an indispensable factor for the authentication of a soldier in the field.

The safety of sensor-based gait authentication has always been a concern of the academic community. Some researches [20]–[23] have analyzed its ability to resist attacks, in which the majority of foresaid attacks employed mimicry. These studies show that even in imitation, it is difficult for attackers to reproduce the victim's complete gait. In other words, to match the sequences produced by the act of walking from person to person is difficult.

Given the proposed weaknesses regarding the above attack theory, since the complete gait sequence is difficult to be bypassed or even imitated, we propose a novel attack model which is based on the authentication mechanism of existing gait authentication methods. In our attack model, attackers aim to split a gait sequence into several independent gait cycles and then pick up adversarial gait cycles (i.e., gait cycles of others that can bypass the user's authentication model) to bypass the victim's model. Our inspiration comes from [24], in which the author assumes that there must be a significant overlap between the behavioral samples of many users. We hypothesize that the set of walk patterns of all users can be clustered into a limited and small number of cluster data, where users with similar gait behaviors belong to the same cluster. One gait cycle similar to that of a victim can be easily found by attackers using some clustering algorithms, e.g., kmeans++ [25], and then the relevant gait cycle will be exploited to bypass the victim's black-box model.

In our attack model, the attacker has no other information about the victim besides the position of the mobile device where the victim will usually carry the device in order to help with authentication. The attacker tries to bypass the black-box model by finding a gait cycle similar to that of a victim from the gait database with a minimum number of attempts. Attacks can be divided into two categories. In the first category, the attacker does not observe the victim's gait and picks up cycles directly from an existing gait database. In the second category, the attacker has the ability to observe the victim's gait and then asks other people to imitate the victim's gait to produce a large amount of suspicious data which is used to get a more elaborate gait database. The hypothesis theorizes that adversarial gait cycles similar to those of the victim are incremental in the mimicry scenario (by imitating the victim, it is easier for the attacker to find an adversarial gait cycle which can bypass the victim's black-box model within a limited number of trials). In our defense model, the contextual contents of the neighboring gait cycles in the gait sequence are considered by the defender using a WPD-LSTM network architecture with multi-cycle training. Unlike the previous works [16], [26]–[28], the single gait cycle is no longer extracted for model training. Experiments on a public dataset of 744 participants from the research community and a dataset of 20 participants collected in our laboratory have proven that ordinary attackers can compromise 15%-60% of the users within 10 attempts; likewise, mimic attackers can compromise 35%-100% of the users within 10 attempts. However, by deploying our WPD-LSTM multi-cycle defense model, the robustness of the gait authentication system improves significantly. In general, the contribution of our article is as follows:

- We present an effective sensor-based gait authentication attack and verify that the vulnerability in the state-of-the-art black-box models can be easily exploited by attackers on the largest gait authentication dataset through clustering. By deploying our heuristic adversarial gait cycle matching algorithm, the attack can compromise the victim's black-box model rapidly.
- Unlike the scope of previous work which was concerned only with the characteristics of a single gait. We propose a WPD-LSTM multi-cycle defense model which is able to consider the contextual contents of the neighboring gait cycles and inherent inter-relationships between different sub-series in the gait sequence. Our defense method observes the user's gait characteristics from a global perspective and improves the robustness of the model.
- Experiments on the largest public dataset and a laboratory dataset show that in a very small number of attempts, the attacker can bypass the victim's existing black-box model easily, and imitation will dramatically increase the probability of a victim's black-box model being bypassed. On the contrary, the WPD-LSTM multi-cycle defense model can hardly be evaded by attackers compared to the state-of-the-art LSTM-related methods.

The remainder of this paper is organized as follows. Section II surveys the relevant work, including sensor-based gait authentication and adversarial biometrics. In Section III, we introduce the preliminary background and motivation for our work. Methodology is discussed in Section IV. Section V describes the experiments and results of our attack model and defense model. We discuss and conclude our work in Section VI.

II. Related Work

A. Sensor-Based Gait Authentication

Gait authentication has been widely discussed for dozens of years [6], [29], [30]. There are multiple ways to realize gait authentication, and sensor-based gait authentication is one of the most popular approaches. Mäntyjärvi *et al.* [31] used embedded MEMS (Micro-Electro-Mechanical System) which were attached to the back belts of the test subjects. Using a signal correlation method, the authors reached their best EER of 7%. Gafurov *et al.* [32] used a 3-D accelerometer attached to the leg right above the ankle, and in two proposed methods (histogram similarity and cycle length) achieved an EER of 5% and 9% respectively. With the development of MEMS technology and mobile devices, smaller sensors are embedded into smart devices, which makes it possible to conduct and conclude authentication in the pocket. Ren *et al.* [16] deployed their framework on both the user-end (with Pearson Correlation Coefficient) and server-end (with support vector machine) with experimental results from 26 subjects with smartphones placed in a hip pouch, waist pouch or pant pocket

Authorized licensed use limited to: Northwestern University. Downloaded on October 10,2020 at 10:35:04 UTC from IEEE Xplore. Restrictions apply.

showing that their framework can effectively cope with different phone placements. Furthermore, while Ahmad *et al.* [33] allowed test subjects to place their smartphones freely in their pocket, the trained artificial neural networks (ANN) model reached an average accuracy of 95%. LSTM is mixed with other machine learning methods [28] to improve the accuracy of the gait authentication model, but such a complex network structure would introduce a huge computational overhead load, rendering it inapplicable in lightweight gait authentication. Moreover, the inherent inter-relationships between different sub-series of the gait sequence has never been considered by the existing deep learning models [27], [28]. Vision-based authentication is another important way to identify the individuals in image sequences by the way they walk [34], which is not considered by this work.

In this paper, we rebuild some state-of-the-art methods which are used for sensor-based gait authentication, and then we try to launch the attack to bypass the target model with the least tries. Moreover, we present a WPD-LSTM defense model which is able to consider the contextual contents of the neighboring gait cycles in the gait sequence, as well as the inherent inter-relationships between sub-series.

B. Adversarial Biometrics

The security of biometric systems is always a hot topic, and there have been several adversarial methods on behavioral biometrics. On the one hand, Connor and Ross *et al.* [30] noticed that when the users intentionally avoided being detected during the training phases this would result in a disaster for the biometric system. By manipulating the training data, imposters can easily bypass the weak profiles or models [35]. On the other hand, imposters can find out adversarial samples to fool the profiles or models during the testing phases. As for keystroke dynamics, Serwadda and Phoha [36] performed rigorous statistical analysis on the large scale dataset (about 3000 users for 2 years) and launched synthetic attacks to mimic target users, they found the attack can increase the mean Equal Error Rates (EERs) partly. Negi *et al.* [24] have studied how to bypass the authentication system utilizing the fake data of other users. Later, Khan *et al.* [37] put the adversarial samples into smart devices by augmented reality and audiovisual techniques. This method enables an attacker to precisely mimic multiple behavioral features at a millisecond's resolution. Touch input biometric is another popular biometric and several attacks have been proposed that have been omitted too. Serwadda and Phoha [38] showed that a robot driven by input gleaned from general population swiping statistics can significantly degrade classification performance. Khan *et al.* [39] demonstrated that shoulder surfing attacks had a high bypass success rate by observing the victim's touch behavior for less than two minutes.

As for gait biometrics, there also have been several studies done about how to hack gait authentication. Gafurov *et al.* [21] asked attackers to walk as the victim did without any feedback. Subsequently, Mjaaland *et al.* [22] trained the attackers with some feedback. Unfortunately, both of the above two types of mimicry attack failed due to the lack of sample size and the limited ability to accurately imitate by the attackers. Mimicry attacks scarcely compromised the gait authentication system, which was also verified by Ren *et al.* [16] on a dataset containing walking traces of long term patterns. With the help of a treadmill and a feedback-based mechanism, Kumar *et al.* [40] designed an attack for sensor-based gait authentication system and evaluated its impact by employing two random imitators, finally, the mean false alarm rate increased by 6 times. But in the real-world scenario, victims' samples are difficult to obtain and the feedback of the training is not viable in most cases, which makes the treadmill attack unpractical.

Unlike previous works, our method is able to compromise the gait authentication system without using the victims' samples or additional feedback. Moreover, compared to [40] which uses a small dataset (18 participants), we evaluate our method on the largest gait dataset available to show the reliability of our attack method.

Zhao *et al.* [41] showed that in machine learning-based biometric authentication systems, the acceptance region, defined as the region in feature space where the feature vectors are accepted by the classifier, is significantly larger than the true positive region. The attacker with only the knowledge of the length of the feature space can impersonate the user with less than 2 attempts on average. To mitigate it, they tried to add beta-distributed noise or feature vectors extracted from a sample of raw inputs to the training data. Different from Zhao's work [41], we also use random attack (details in Section V-B) as the baseline method and try to randomly select the gait cycle from the existing datasets instead of regenerating the gait that falls in the victim's feature space.

III. Preliminary and Motivation

In this section, we first introduce the threat model and datasets of our work. After that, we propose our motivation by explaining the gait cycle extraction algorithm, listing the popular cluster features, and analyzing the intrinsic connection amongst different human beings.

A. Threat Model

In our threat model, each mobile device has a unique owner, and attackers attempt to access the device illegally. Our system assumes that several widely used motion sensors (i.e., acceleration sensors and gyroscope sensors) are available on the device. The attacker has no other information about the victim besides the position where the mobile device is usually carried in order to help with authentication (i.e., the attacker is with little knowledge of the feature space of machine learning-based methods [41]). To compromise the device owner's black-box model, the attacker first needs to submit his/her candidate data, we consider the following three scenarios:

1) Manipulate Motion Sensors: The attacker can use SMASheD [42] to directly manipulate motion sensors on unrooted Android devices via Android debug bridge functionality. We assume that by installing an application with only the INTERNET permission (refer the threat model section in [42]), the attacker can feed false data to target sensors (i.e., three-axis data of acceleration sensors and gyroscope sensors) via the remote control without the victim's knowledge.

Authorized licensed use limited to: Northwestern University. Downloaded on October 10,2020 at 10:35:04 UTC from IEEE Xplore. Restrictions apply.

TABLE I

OVERVIEW OF OUR DATASETS; OU-ISIR, GREDO AND GREDI REPRESENT THE LARGEST SENSOR-BASED GAIT DATABASE [26], GAIT RECOGNITION EXPERIMENTAL DATASET OF OWNERS, AND GAIT RECOGNITION EXPERIMENTAL DATASET OF IMITATORS, RESPECTIVELY. ALL THESE THREE DATASETS CONTAIN LEVEL-WALK SEQUENCES FOR WALKING BACK AND FORTH

Dataset	Participants	Gender F/M	Imitation
OU-ISIR	744	355/389	No
GREDO	20	10/10	No
GREDI	20	10/10	Yes

2) Imitation Based on Human Training: The attacker use a feedback-based training mechanism [40] to train imitators for imitating selected gait pattern (i.e., when the imitator is fully trained, the imitator will carry the victim's device to bypass the target black-box model).

3) Imitation Based on Robotic Body Design: The attacker can build a robotic body, and control the movement of the robotic body to generate corresponding motion sensor signals (i.e., three-axis data of acceleration sensors and gyroscope sensors) to carry out the attack.

Note that the focus of our work is to explain the vulnerability of the existing black-box models for gait authentication. When launching the attack in the real world, the attacker will comprehensively take into account the cost and the price.

B. Datasets

In total, we obtained three datasets for the attack and defense purpose, the details of our datasets are shown in Table I.

1) OU-ISIR: The first one is the largest sensor-based gait database OU-ISIR provided by Ngo *et al.* [26]. In OU-ISIR, level-walk data of 744 subjects (389 males and 355 females) with ages ranging from 2 to 78 years was captured, and two level-walk sequences for each subject were extracted automatically by using acceleration and gyroscope sensors with a sample rate of 100HZ.

To verify the universality of our attack algorithm, we split OU-ISIR into two randomly balanced parts: OU-ISIR-A and OU-ISIR-B; each part has the same male to female ratio. OU-ISIR-A is used for learning and OU-ISIR-B is used for attack.

2) GREDO and GREDI: It was noticed that in OU-ISIR all the participants received the experiment independently and they could not observe others' walking patterns. In order to get the performance data of our attack model under a manner of mimicry, we developed an Android application which can record the data of motion sensors (especially, acceleration sensors and gyroscope sensors) at a stable sample rate of 100HZ. Then we asked 20 participants (10 female participants and 10 male participants, all of them in their twenties and of a similar figure) to help collect walking data on a level surface. All participants are full-time graduate students (graduate students familiar with the authors) in our laboratory. All participants are between 165cm and 170cm tall and weigh between 55kg and 60kg. The data collection procedure lasts for one day (from 8 a.m. to 4 p.m.). The same smartphone was used (Huawei Honor 9) in all trials and tied to the center of the back waist of each participant with the same device placement.

In the data collection phase, all participants were made to walk on a flat road 80 meters in length (walk back and forth for once). We collected the normal walking data of each participant as OU-ISIR [26] did and recorded it as GREDO (Gait Recognition Experimental Dataset of Owners). During the data collection process, one cannot observe the gait pattern of others. For each participant, we got sensor data in 2*80 meters, and 40*80 presents the complete volume of the GREDO data. Similar to OU-ISIR [26], we split GREDO into two parts. Finally, we got two normal datasets (GREDO-A with 5 females and 5 males, GREDO-B with 5 females and 5 males). To get the mimicry dataset for the 20 participants we selected the victims in turn: we first selected one participant as the victim and recorded his/her walk pattern (2*80 meters), then we asked the remaining 19 people to imitate the victim's pattern one by one (2*80 meters for each person). During the imitation process, the imitator can observe the gait pattern of the victim throughout the data collection session (see this victim in person without practice in advance). Also, we have informed all the participants in advance that we will use multiple cycles (C cycles, $C \geq 1$) for authentication, and let them learn the victim's gait behavior as much as possible. Finally, we got the dataset for GREDI (Gait Recognition Experimental Dataset of Imitators). In GREDI, for each person there exist 40*80 meters data and out of which 2*80 belong to the victim and the remaining 38*80 belong to the imitators.

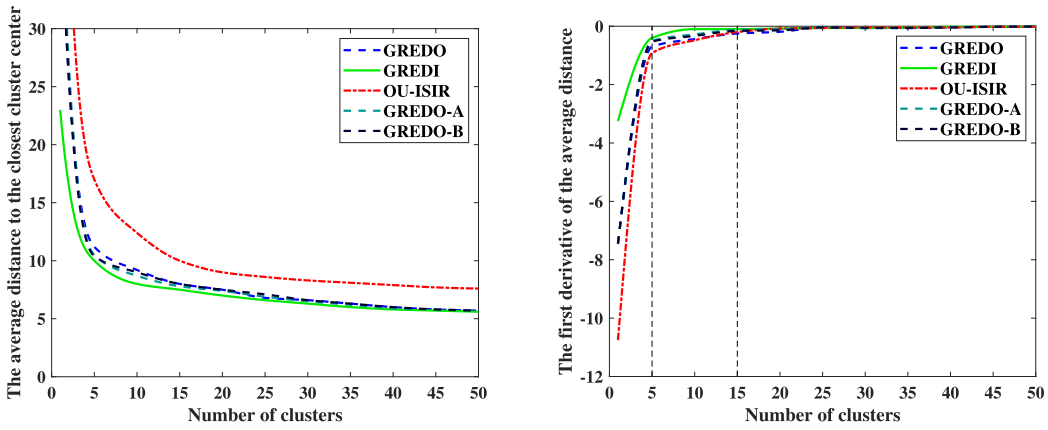
C. Motivation

Considering the sensor-based user authentication, previous work is always based on the hypothesis that each person has a unique gait pattern. Thus, the researchers build multiple classifiers or rules to distinguish a real user from an impostor. However, we hypothesize that there must be a distinct overlap among the gait cycles of some users. The gait sequence of one person can be divided into multiple gait cycles. One can imagine that there exists a big cluster in which all the gait cycles within similar user patterns will belong to. But these clustered gait cycles may come from different users. In our opinion, we can generate all such clusters and find the gait cycle which can bypass the victim's model by exploiting the data collected from the general population with the scenario similar to the victim.

To verify the feasibility of the above hypothesis, we analyze the dataset including OU-ISIR, GREDO, and GREDI. Firstly, we follow the state-of-the-art method of picking up gait cycles from the gait sequence. Secondly, we give the popular clustering features which are used for sensor-based gait authentication. Finally, we conduct clustering to verify our hypothesis.

1) Gait Cycle Extraction: Cycle extraction is the prerequisite for all the existing gait authentication methods (we will introduce these methods in Section IV-A.1) and our attack. We choose the cycle extraction algorithm (CEA) presented by [12]. CEA is automated, accurate and widely referred to

Authorized licensed use limited to: Northwestern University. Downloaded on October 10,2020 at 10:35:04 UTC from IEEE Xplore. Restrictions apply.



(a) The average distance of each feature sample to the closest cluster center v.s. the number of clusters.

(b) The first derivative of the average distance v.s. the number of clusters.

Fig. 1. Analysis results of our hypothesis on three datasets: gait cycles from different person may belong to the same cluster.

by other works [16], [43]. To verify that existing gait behavior schemes are easy to be compromised, we re-implemented the CEA algorithm. Note that acceleration sensors and gyroscope sensors are useful in gait authentication. Without loss of generality, we select accelerometer data as a basis for the partitioning task. From the data (OU-ISIR, GREDO, and GREDI) we found that one gait cycle length varies between 50 to 100 samples depending on the speed of the person. Moreover, the range for the male is 50 to 85 and that for the female is 55 to 100. To maintain consistency, all the cycles are normalized to a length of 100 observations as [12] did.

2) Clustering Features: Both acceleration and magnitude vector are key attributes in sensor-based gait authentication. Magnitude vector is usually calculated as a more invariant combination of resulting acceleration [21], [44]:

$$r(k) = \sqrt{x^2(k) + y^2(k) + z^2(k)}, \quad k = 1, \cdots, K$$

where $x(k)$, $y(k)$, $z(k)$ are the accelerations measured in the corresponding directions at time k. Finally, for each gait cycle, the following features in the time domain are used to create the adversarial clusters.

(1) Magnitude vector. The magnitude vector in one gait cycle. It has been explained previously.
(2) Mean. Mean value in one gait cycle.
(3) Standard deviation. Mean of the deviations in one gait cycle.
(4) Highest value. Maximum value in one gait cycle.
(5) Lowest value. Minimum value in one gait cycle.

We chose the above features due to the following reasons: Firstly, these features are typical and proposed by recent studies [44]–[47]. Secondly, a large number of features will increase the overhead of our clustering algorithm. A small set of representative features have been proven necessary for classification tasks in [45]. Moreover, the existing work has demonstrated that there is a value after which the performance does not significantly increase since the last features only correspond to noise [48], [49].

3) Feasibility Analysis: Under the different values of K (number of clusters), we utilize the K-mean algorithm to get the average distance of each feature sample (extracted from the gait cycle) to its closest cluster center. Fig. 1(a) represents the average distance of each feature sample to the closest cluster center. Fig. 1(b) shows the first derivative of the average distance represented by Fig. 1(a).

From Fig. 1(a), we can find that on all three datasets, the average distance is decreasing with the increment of K. Especially, when $K = 50$, the average distances of GREDO, GREDO-A and DREDO-B are all around 6. Also, our hypothesis is intuitively supported by Fig. 1(b). Fig. 1(b) shows that when K is around 5, higher values of K will not improve the clustering by much. When K is larger than 15, the curve of the first derivative will be flat. Note that the total number of the individuals of our datasets are 744 and 20 (larger than 15), respectively. It can satisfy our hypothesis that gait cycles from the different people may belong to the same cluster.

IV. Methodology

In this section, we will present two key components in our design: the attack model and the defense model. In the attack model, we introduce how an attacker can bypass the existing black-box gait authentication model easily by employing the adversarial gait cycle matching. In the defense model, we offer a WPD-LSTM multi-cycle defense model, which considers the contextual contents of the neighboring gait cycles in the gait sequence, and is thus hard to compromise.

A. Attack Model

The overview of our attack model is shown in Fig. 2. Firstly, the gait sequences from different people are collected by attackers. Secondly, adversarial gait cycles are extracted based on clustering. Finally, attackers can easily bypass the black-box model with adversarial gait cycles. It should be noted that from a practical perspective, it is relatively difficult to simulate an attack on the sensor-based gait authentication system directly. But the attacker can use some additional tools to launch an attack against the new victim in the real-world scenario, such as feeding false information to the android sensors (i.e., manipulating three-axis data of acceleration sensors

Authorized licensed use limited to: Northwestern University. Downloaded on October 10,2020 at 10:35:04 UTC from IEEE Xplore. Restrictions apply.

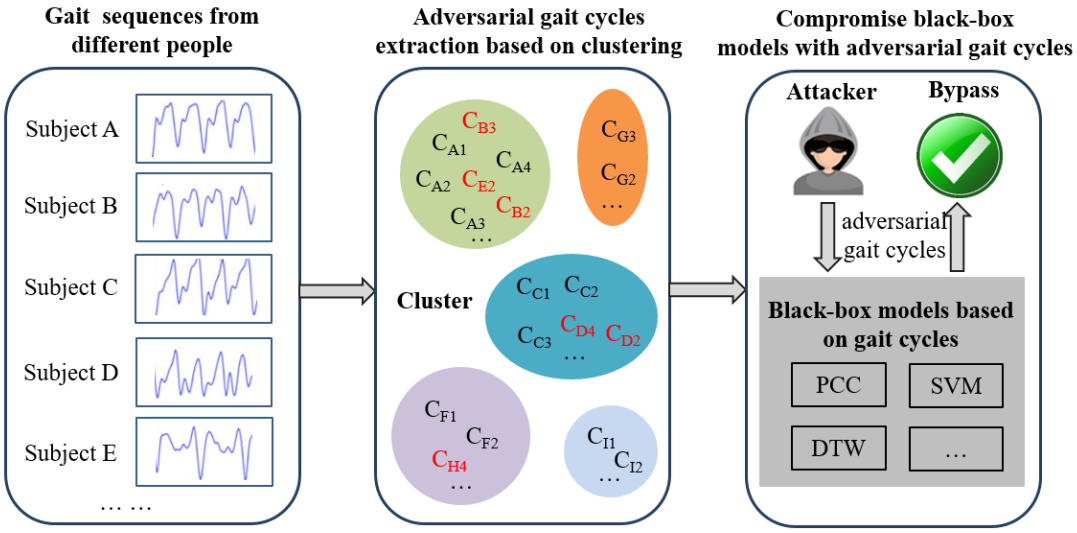


Fig. 2. The overview of attack model. Compromise starts at gait sequences data collection from different people and ends when the adversarial gait cycles are extracted by attackers followed by black-box models cracking. Here, black-box model means the attacker does not know in advance the authentication model used by the victim. C_{A1} represents the first gait cycle in the gait sequence from subject A.

and gyroscope sensors via Android debug bridge functionality as [42] did) or building a robotic body to carry out the attack [24]. In the following section, we will explain in detail how to build a black-box model and perform the adversarial gait cycle matching.

1) Black-Box Model Design and Construction: In recent years, lots of methods have been proposed for gait authentication using gait cycles. We can divide them into two main categories: One category is to construct profiles with motion sensor data directly and then to calculate the similarity score between the targeted profile and test samples. The other category is to use feature engineering and machine learning techniques to build a classifier to represent the user's walk pattern. In this article, we collectively refer to a profile or a classifier used for gait authentication as a model.

Considering the validity and reliability, we chose diverse methods from statistical classifiers to deep learning based networks. Totally, six state-of-the-art algorithms in gait authentication are chosen by us. To get an implementation as close as possible to the previous works [16], [26]–[28]. We implemented these approaches as well as their optimizations. All methods are listed as follows.

a) PCC-based black-box model: PCC [50] is the co-variance of the two variables divided by the product of their standard deviations. It can measure linear similarity between two gait cycles. As [16] did, we used a weighted PCC when computing the similarity between the extracted gait cycles and the user model. The final accuracy depends on the similarity scores and the pre-defined threshold.

b) SVM-based black-box model: SVM [51] is a kind of supervised learning classifier which can solve the non-linear classification problem utilizing kernel tricks. We used binary-class SVM as [16] did. Since standard classification methods cannot be directly applied to raw cycle data, the gait cycles will be first translated into feature vectors. In the training phase, the ratio of the number of samples from the owner (positive sample) to that of other users (negative samples) is usually experiential. Here, we chose the ratio as 13, since it was the best parameter defined in [16] via grid search. In the testing phase, we will get the accuracy returned from the SVM model for each gait cycle. The final accuracy is the average of the accuracy of all cycles in a gait sequence. Here, we utilize libsvm [52] with RBF kernel to train the model for each user.

c) DTW-based black-box model: DTW [53] can measure the similarity between two time sequences regardless of speeding up or slowing down. DTW algorithm is used as a baseline in paper [26] due to its low overhead and high accuracy. Here, we use the cumulative distances in DTW to judge the similarity between two gait cycles as [26] did.

d) CNN-based black-box model: CNN [54] is one kind of feed-forward deep neural networks. Unlike the traditional feature engineering, a number of kernels is defined to extract potential features at each convolutional layer in CNN. CNN is well designed by IDnet [27] to authenticate different users by walk cycles. Here, we rebuild a CNN network with two convolutional layers and two fully connection layers followed by a One-class Support Vector Machine (OSVM) classifier as IDNet did. One may concern that the training data is not enough for deep network [27]. To address this issue, we use wavelet decomposition for data augmentation, which will be discussed in Section IV-B.

e) LSTM-based black-box model: LSTM [55] is an improvement to RNN [56] and still has the basic structure of RNN, the basic unit of LSTM involves a cell, an input gate, an output gate and a forget gate. The previous work [28] has proposed a LSTM network to authenticate users. Furthermore, LSTM network structures mixed with other machine learning methods such as CNN are deployed in [28] to improve the accuracy of the gait authentication model, but the complex network structure will introduce huge computational overhead, rendering it not applicable in lightweight gait authentication.

Authorized licensed use limited to: Northwestern University. Downloaded on October 10,2020 at 10:35:04 UTC from IEEE Xplore. Restrictions apply.

In our black-box model design, we consider both the single LSTM network structure and the CNN+LSTM network structure which have shown good performance in [28].

For black-box model design and construction, we firstly reproduce these six benchmarks and try to achieve a good performance on our datasets. We then regard them as black-boxes with the assumption that we do not know anything about the models except the input way of testing samples. The only result we can get from these black-boxes is 'yes' or 'no'. That is to say, we just know whether we have passed the authentication model, which completely simulates the real-world scenario.

2) Adversarial Gait Cycle Matching: From the perspective of attackers, they generally want to bypass the authentication system within a limited number of attempts. Here, we assume attackers don't have gait data from the user they wish to imitate and they also know nothing about the composition of the black-box models used for authenticating. We consider the following two scenarios:

a) Scenario I: widespread attack: The attacker does not observe the victim's walk patterns but he/she has access to some public gait datasets (e.g., OU-ISIR is a public dataset which contains gait data from many other people). We call it a widespread attack. This scenario has never been studied before in the area of gait authentication attack.

Recall that our hypothesis is that there must be a distinct overlap among the gait cycles of some users. The aim of the attacker is to explore the adversarial gait cycle from various people in order to find candidates from the cluster of the victim. We take Fig. 2 as an example: In the cluster of subject A, C_{B2}, C_{B3} and C_{E2} can be considered as adversarial gait cycles. What an attacker needs to do is find these adversarial gait cycles and try to use them to bypass the black-box model of subject A. Here, the most intuitive way is that we can run the K-means algorithm under different values of K and try different centroids to pick up the adversarial gait cycles. However, it is time-consuming for attackers to choose a suitable value of K. Moreover, the clusters in the K-means algorithm may change considerably for different values of K, rendering it inapplicable in real attack scenarios.

Inspired by the K-means++ algorithm [24], [25], we present a heuristic adversarial gait cycle matching algorithm, as shown in Algorithm 1. In Algorithm 1, the first gait cycle is selected as a center of the dataset, and then each subsequent gait cycle (center of clustering) is selected with a probability proportional to its contribution to the overall distance given the previous selections. The core idea of our heuristic algorithm is that if the previously found gait cycle cannot bypass the black-box model, the newly found features of the gait cycle will be located as far away as possible from that of all previously found gait cycles to increase the probability that it is in the victim's cluster.

b) Scenario II: mimic attack: The attacker has the ability to observe the victim's walking patterns and then asks other people to imitate the victim's gait to produce a specific gait database. We call it a mimic attack. This scenario has been studied by previous work [16], [21], [22], [40], but the probabilities of successfully bypassing the black-box authentication model are quite low. We re-apply our heuristic adversarial gait cycle matching algorithm (Algorithm 1) on the GREDI directly, the preliminary results in Fig. 1 has shown the differences between gait cycles of different people become smaller on a mimicry dataset (GREDI). More results will be discussed in Section V.

Algorithm 1 Adversarial Gait Cycle Matching Algorithm

Input:
A large public or mimicry dataset $X = \{x_i \mid i = 1, 2, \ldots, M\}$
Output: Total number of attempts t
Initialize:
(1)The first cycle we selected is the center (mean) of the dataset $C_1 = x_{mean}$
(2)The number of attempts $t = 1$
(3)Adversarial gait cycle $AGC = false$

```
while !AGC do:
    D(x_i) = Distance(x_i, nearest C_t chosen so far)
    C_t = x_j with the probability D(x_j)^2 / sum_{i=1}^{M} D(x_i)^2
    if C_t can bypass the black-box model then
        AGC = true
        break
    end if
    t = t + 1
end while
```

B. Defense Model

To gain a robust model that can fight against our one cycle attack, we propose a WPD-LSTM multi-cycle defense model to consider the contextual contents of the neighboring gait cycles in the gait sequence, as well as the inherent inter-relationships between sub-series. In our defense model, the single gait cycle is no longer extracted for model training, we try to use C gait cycles to train the model for gait authentication instead of one cycle. In this section, we will introduce the key components in our multi-cycle defense model.

1) Wavelet Packet Decomposition: WPD is an efficient tool for analyzing time series signals for weak, unbalanced, instantaneous, and singular components [57], [58]. The wavelet packet transform (WPT) is usually presented through a wavelet packet complete binary tree [59], where each node is marked by order (d, n), d ($d = 0, 1, 2, \ldots$) represents the current depth of the WPT tree, and n ($n = 1, \ldots, 2^d$) represents the node number at the corresponding depth d. Each node in the decomposing level n contains a wavelet packet coefficient $P_j^n(k)$ ($k = 1, \ldots, N_d$, N_d is the length of the WPD coefficient), which can be described as follows:

$$P_j^n(k) = 2^{-j/2} \int_{-\infty}^{\infty} A(\omega, t) e^{j\omega t} \psi_d^n \left(t - 2^d k\right)^* dt dZ(\omega)$$
$$\approx \frac{1}{2^{j/2}} \int_{-\infty}^{\infty} A\left(\omega, 2^{-j}k\right) e^{j\omega k} \psi^* \left(2^{-j}\omega\right) dZ(\omega)$$

2) Long Short-Term Memory Networks: LSTM network is well-suited to learn from time series when contextual dependencies are expected to be recorded [55]. This is

Authorized licensed use limited to: Northwestern University. Downloaded on October 10,2020 at 10:35:04 UTC from IEEE Xplore. Restrictions apply.

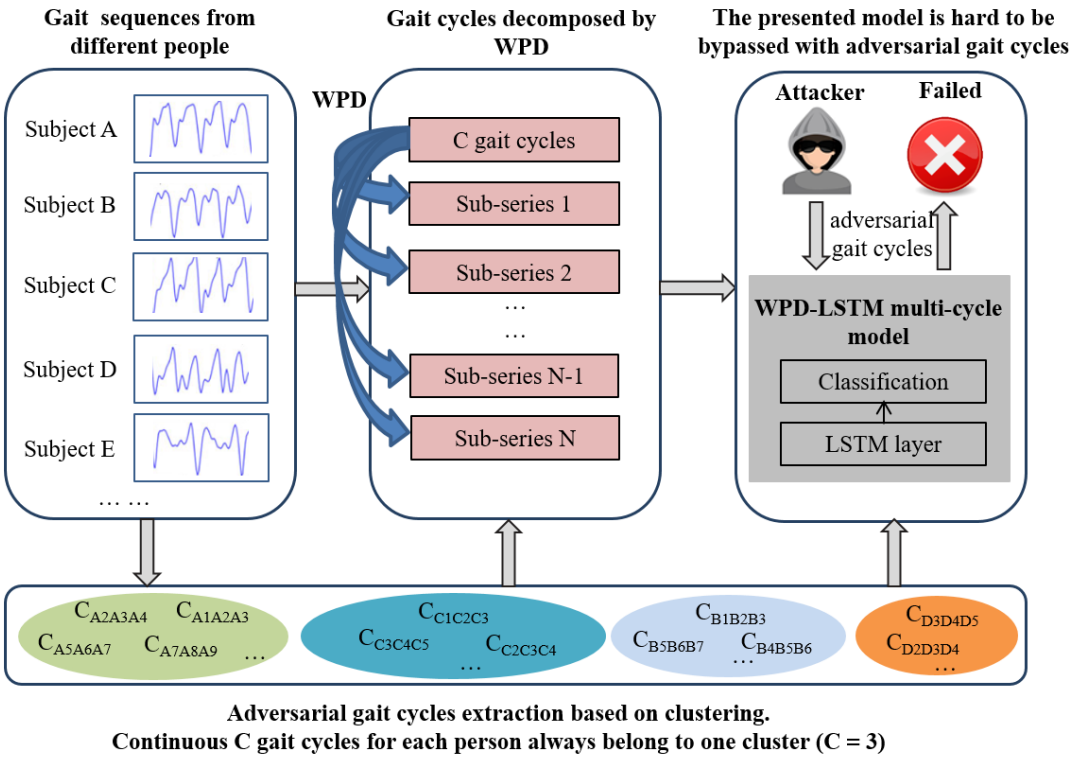


Fig. 3. The framework of WPD-LSTM multi-cycle defense model. C_{A1A2A3} represents the first continuous 3 gait cycles in the gait sequence from subject A. The continuous C gait cycles for each person always belong to one cluster ($C = 3$). By adopting WPD and LSTM, it is difficult for attackers to bypass the presented model.

one of the main reasons why we chose LSTM for gait authentication. LSTM has been combined with other machine learning methods [28] to improve the accuracy of the gait authentication model, but the complex network structure will introduce huge computational overhead, rendering it not feasible in lightweight gait authentication. Moreover, the inherent inter-relationships between different sub-series of the gait sequence has never been considered by the existing LSTM network. Next, we will introduce our hybrid VPD-LSTM defense model.

3) WPD-LSTM Multi-Cycle Defense Model: In Fig. 3, we present the framework of our WPD-LSTM multi-cycle defense model. C_{A1A2A3} represents the first continuous 3 gait cycles in the gait sequence from subject A. The continuous C gait cycles for each person always belong to one cluster ($C = 3$). By adopting WPD and LSTM, it is difficult for attackers to bypass our model, which will be evaluated in Section V. We will introduce each module below.

WPD is employed to decompose the gait sequence data. A frequently-used Dmeyer mother wavelet (dmey) is utilized as the mother wavelet. Different frequency bands usually exist simultaneously in the gait sequence, which will affect the accuracy of the final model. After decomposition via WPD, the gait sequence will be separated into several sub-series, which contain low-frequency components and high-frequency components. The key problem in WPD is how to choose the depth d of the WPT tree. If the value of d is too small (i.e., $d = 3$ in our experiment), the original time-series will not be sufficiently decomposed and components of different frequencies will be mixed together. Conversely, when the value of d is too large (i.e., $d = 5$ in our experiment), the gait sequence will be overly decomposed, rendering a component of a particular frequency to appear at multiple other decomposition products. When d is set to 4, all the decomposed sub-series are approximate sinusoidal signal with less noise. Finally, we choose $d = 4$.

Additionally, the proposed WPD-LSTM multi-cycle model uses a gait sequence with C gait cycles and all the sub-series from the gait sequence as the model input. In this way, the inherent inter-relationships between sub-series and the contextual contents of the neighboring gait cycles in the gait sequence will be considered. For each user, we utilize binary classification to distinguish authorized users from attackers and label the data of the authorized user as 1 and that of other users as 0. To construct the training set, we adopt the stratified sampling to pick up positive samples and negative samples heuristically [60]. Meanwhile, the ratio of the number of samples by the owner to that of other users is 1:5, which has been proven to be optimal in previous works [45]. Next, a 2-layer LSTM structure is presented in our WPD-LSTM model. Here, we follow the popular LSTM network for human activity recognition [61] and reuse its network structure. Finally, the output of the LSTM layer will enter into the fully connected layer (dense) as an input, followed by a softmax layer for classification.

Compared with the traditional gait authentication methods, our defense model has the following advantages: (1) Our defense model addresses the information dependence issue between the neighboring gait cycles in the gait sequence since LSTM is capable of learning long-term dependencies [55].

Authorized licensed use limited to: Northwestern University. Downloaded on October 10,2020 at 10:35:04 UTC from IEEE Xplore. Restrictions apply.

It also requires less operational time than previous models where feature engineering is badly needed. (2) Our defense model considers the inherent inter-relationships between sub-series generated via WPD. It also has the capability to capture hidden non-linear relationships of original gait sequences and sub-series. (3) The classification accuracy and robustness of our defense method are noticeably improved by decomposing the original gait sequence, and it can fight against one cycle attack effectively.

V. Evaluation

In this section, we present the experiments to evaluate the effectiveness of our attack model. And we also evaluate the robustness of our defense model against one cycle attack. Our experimental results demonstrate that our attack algorithm is effective across all different settings and our defense method is effective to fight against this kind of attack.

A. Implementation Details

In our article, a number of black-box models have been designed for attack validation. All these models are reproduced from existing works, and all of these methods take the well labeled gait cycles as training input.

For the SVM model, the kernel we chose is the radial basis function (RBF). We set the cost value as 100 and γ as 0.01. For the CNN model, the kernels of convolutional layers are 1*10, 4*10, respectively. In training the CNN, the learning rate is 0.0025, and the number of epochs for training is 200. The batch size is 128. For the LSTM model and CNN+LSTM model, the structure of LSTM has one hidden layer with 64 hidden neurons and the proposed CNN network is constructed with 4 convolution layers and 2 max-pooling layers. The learning rate is set to 0.0025, and the number of epochs for training is 300. The batch size is 128.

Unlike the above black-box models, our defense model uses C gait cycles combined with all the sub-series decomposed via WPD as input. Furthermore, we used a 2-layered LSTM structure with 32 hidden neurons in each layer. The learning rate, the number of epochs, and the batch size are 0.0025, 300, 16, respectively. All these parameters in our defense model are well-tuned though grid search.

Recall that there are two attack scenarios in our attack model: widespread attack and mimic attack. For all the datasets introduced in Section III-B, OU-ISIR-A, GREDO-A and owners' data in GREDI (for each person, there are 2*80 meters belong to the owner) are used for modeling, OU-ISIR-B and GREDO-B are used for a widespread attack, and the imitators' data in GREDI (for each person, there are 38*80 belong to the imitators) is used for a mimic attack. In OU-ISIR, each person has 10 to 15 cycles for model training. In GREDO and GREDI, each person has 70 to 78 cycles for model training.

In all the above models, the ratio of the number of gait sequences in the training set to that in the test set is 1:1 for each user since the authentication task is usually modeled as a binary-classification problem. In the training set of SVM, LSTM and WPD-LSTM, we utilized stratified sampling techniques to pick up positive and negative samples by the same way described in Section IV-B.3; the ratios of the number of gait sequences from the owner to that of other users are 1:13 (SVM) and 1:5 (LSTM and WPD-LSTM), respectively.

B. Performance Metrics and Terms Explanation

Our performance metrics are listed as follows:

- True positive (TP). The authorized owner is correctly identified.
- False positive (FP). Other users are incorrectly identified as the authorized owner.
- False negative (FN). The authorized owner is incorrectly identified as other users.
- True negative (TN). Other users are correctly identified.
- True positive rate (TPR). $TPR = TP/(TP + FN)$.
- False positive rate (FPR). $FPR = FP/(FP + TN)$.
- True negative rate (TNR). $TNR = TN/(TN + FP)$.
- False negative rate (FNR). $FNR = FN/(FN + TP)$.
- Equal error rate (EER). EER represents the point where FPR and FNR are equal. The lower EER is, the better of the gait authentication system will be.
- Prob(k). Fraction of users in the dataset whose classifiers were compromised after k attempts.

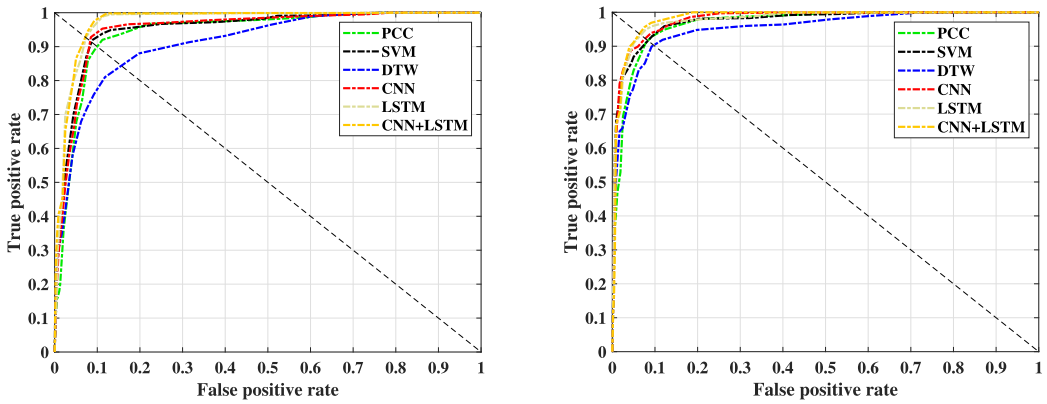
The explanation of our terms are listed as follows:

- Widespread attack. The attacker does not observe the victim's walk patterns but he/she has access to some public gait datasets (OU-ISIR-B and GREDO-B). Then the attacker utilizes adversarial gait cycle matching algorithm (Algorithm 1) to pick up the adversarial gait cycle(s).
- Mimic attack. The attacker has the ability to observe the victim's walking patterns and then asks other people to imitate the victim's gait to produce a specific gait database (GREDI). Then the attacker utilizes adversarial gait cycle matching algorithm (Algorithm 1) to pick up the adversarial gait cycle(s).
- Random attack. The attacker will randomly pick up the adversarial gait cycle from different datasets without replacement. The datasets can be either some public gait datasets (OU-ISIR-B and GREDO-B) or a special dataset (GREDI).
- One cycle attack model. Most of the previous works [16], [26]–[28] extracted single (one) gait cycle for model training. In order to verify the vulnerability of the existing methods, we propose a novel attack model which contains two attacks (widespread attack and mimic attack). Also, we use random attack as the baseline to illustrate the effectiveness of our attack model.
- Multi-cycles defense model. Unlike the previous works [16], [26]–[28], in our multi-cycle defense model, the single gait cycle is no longer extracted for model training. The contextual contents of the neighboring gait cycles in the gait sequence are considered by the defender using a WPD-LSTM network architecture with multi-cycle training.

C. Performance on Attack Model

In this section, we firstly introduce the performance of all the black-box models, then we conduct one cycle attack on

Authorized licensed use limited to: Northwestern University. Downloaded on October 10,2020 at 10:35:04 UTC from IEEE Xplore. Restrictions apply.



(a) ROC curve for OU-ISIR-A. (b) ROC curve for GREDO-A.

Fig. 4. ROC curve on different black-box models for two datasets; the decision threshold θ varies from 0 to 1 at step growth 0.01.

these models. In our experiment, OU-ISIR-B and GREDO-B are used to evaluate the ability of a widespread attack. Accordingly, GREDI is used to evaluate the rate of compromise in a mimic attack.

1) Performance of Black-Box Models: In order to launch a one cycle attack, the most important thing which should be done is to ensure that our elaborate black-box models can replicate the optimal results achieved in previous works. These models will undoubtedly fail to fight against any attacks with poor accuracy.

We first evaluate the accuracy of the black-box models. Since different methods have different threshold ranges, we utilize a ROC curve to display the overall performance of different methods intuitively. ROC curve shows the true positive rate against the false positive rate with various classification thresholds is θ. The ROC curves on different black-box models are shown in Fig. 4. Note that EER is the value of the false positive rate at the intersection of the diagonal and the ROC curve. In Fig. 4(a), we can see that the EERs of all the methods are within 10% except DTW (EER = 15.39%) on dataset OU-ISIR-A, which is consistent with the situation described in previous work [26]. Fig. 4(b) depicts the relationship between the true positive rate and the false positive rate at various thresholds θ on dataset GREDO-A. Results of overall performance on this dataset are similar to that of OU-ISIR-A. In summary, all the black-box models we reproduced have achieved a high level of accuracy as in previous works [16], [26]–[28].

2) Black-Box Models v.s. One Cycle Attack: In the authentication phase, each gait cycle extracted by our adversarial gait cycle matching algorithm will be compared with the judgment threshold θ of the corresponding model to get the final result. We recorded the EER and corresponding threshold of each model on OU-ISIR-A and GREDO-A in Table II. For different models, we can get an optimal threshold for distinguishing the user owner from others, which is logical in the real-world scenario.

After determining the evaluation criteria for each model, we attempted to study the robustness of the proposed black-box models against a one cycle attack. We summarize the results of testing our adversaries on OU-ISIR-B, GREDO-B, and DREDI in Table III. Table III shows the fraction

TABLE II

EER AND CORRESPONDING THRESHOLD OF EACH MODEL ON OU-ISIR-A AND GREDO-A

Model name	OU-ISIR-A		GREDO-A	
	EER	threshold	EER	threshold
PCC [16]	9.91%	0.75	8.87%	0.74
SVM [16]	8.93%	0.48	8.79%	0.50
DTW [26]	15.39%	0.14	9.98%	0.08
CNN [27]	8.69%	0.81	8.92%	0.78
LSTM [28]	8.09%	0.42	7.98%	0.49
CNN+LSTM [28]	8.04%	0.51	7.95%	0.48

(i.e., Prob(k)) of users on OU-ISIR-B, GREDO-B and DREDI whose models were compromised after 1, 5, 10, 20 and 50 tries of launching a widespread attack, mimic attack and random attack for each of the black-box models we used. In addition to the widespread attacks and mimic attacks discussed in Section IV-A.2, we use random attacks as our baseline method, in which the attacker will randomly pick up the adversarial gait cycle from the dataset without replacement. To be specific, we implement it with the API (Application Programming Interface) `random.sample()` in python [62]. We conclude the content of Table III as follows:

a) The vulnerability in the state-of-the-art black-box models can be easily exploited by attackers: For the widespread attack, the average fractions of compromised users on OU-ISIR-B after 50 tries are 0.87, 0.92, 1, 0.72, 0.58, and 0.57 for each black-box model. The average fractions of compromised users on GREDO-B after 50 tries are 0.95, 0.85, 1, 0.65, 0.40, and 0.40. As for mimic attacks, the values are 1, 1, 1, 0.80, 0.55 and 0.55, respectively. Attackers can compromise most of the users in gait authentication through widespread/mimic attack with a limited number of tries. Viewed from another perspective, it also means the same user can belong to different clusters (i.e., the adversarial gait cycle that can bypass the victim's black-box model belongs to the victim's cluster, and the adversarial gait cycle that cannot bypass the victim's black-box model belongs to the other cluster/clusters).

b) The attack methods proposed in this paper are much more effective than random attacks: Note that the performance of our widespread attacks and mimic attacks were higher when

Authorized licensed use limited to: Northwestern University. Downloaded on October 10,2020 at 10:35:04 UTC from IEEE Xplore. Restrictions apply.

TABLE III

FRACTION OF USERS ON OU-ISIR-B, GREDO-B AND DREDI WHOSE MODELS WERE COMPROMISED AFTER 1, 5, 10, 20 AND 50 TRIES OF WIDESPREAD ATTACK, MIMIC ATTACK AND RANDOM ATTACK FOR EACH OF THE BLACK-BOX MODELS WE USED. ALL THE RESULTS ARE THE AVERAGE BASED ON 10 EXPERIMENTS INDEPENDENTLY

Model name	The number of attempts (k)	Prob(k)					
		Widespread attack		Mimic attack	Random attack		
		OU-ISIR-B	GREDO-B	GREDI	OU-ISIR-B	GREDO-B	GREDI
PCC [16]	1	0.07	0.05	0.05	0	0.05	0.05
	5	0.23	0.20	0.35	0.01	0.05	0.05
	10	0.42	0.40	0.50	0.03	0.10	0.05
	20	0.60	0.65	0.95	0.07	0.10	0.15
	50	0.87	0.95	1	0.16	0.10	0.20
SVM [16]	1	0.10	0.10	0.10	0	0	0
	5	0.18	0.25	0.45	0	0.05	0
	10	0.35	0.30	0.60	0.01	0.05	0.10
	20	0.61	0.55	0.80	0.04	0.05	0.10
	50	0.92	0.85	1	0.12	0.10	0.15
DTW [26]	1	0.16	0.10	0.10	0	0	0.05
	5	0.34	0.45	0.80	0.02	0.05	0.10
	10	0.53	0.60	1	0.07	0.10	0.15
	20	0.70	1	1	0.14	0.10	0.20
	50	1	1	1	0.25	0.20	0.25
CNN [27]	1	0.09	0.05	0.05	0	0	0
	5	0.17	0.15	0.30	0.01	0	0.05
	10	0.32	0.30	0.45	0.02	0.05	0.05
	20	0.44	0.45	0.70	0.04	0.05	0.10
	50	0.72	0.65	0.80	0.06	0.10	0.15
LSTM [28]	1	0.08	0	0.05	0	0	0
	5	0.18	0.05	0.20	0.01	0	0.05
	10	0.28	0.15	0.35	0.02	0	0.10
	20	0.37	0.25	0.45	0.02	0.05	0.15
	50	0.58	0.40	0.55	0.03	0.05	0.15
CNN+LSTM [28]	1	0.07	0	0.05	0	0	0
	5	0.18	0.05	0.20	0.01	0	0.05
	10	0.26	0.10	0.30	0.01	0	0.10
	20	0.36	0.25	0.45	0.02	0.05	0.15
	50	0.57	0.40	0.55	0.03	0.05	0.15

bounded by the performance of the baseline method, which verifies the effectiveness of our adversarial gait cycle matching algorithm.

c) Imitation will dramatically increase the probability of a victim's black-box model being bypassed: After comparing the Prob(k) on various datasets in the experiment, a significant difference between the adversaries is that the performance of mimic attacks improves much more quickly when compared to a widespread attack. The main reason is that the sample error of possible walking patterns will be closer by imitation, and it allows our adversarial gait cycle matching algorithm to locate attack points more efficiently.

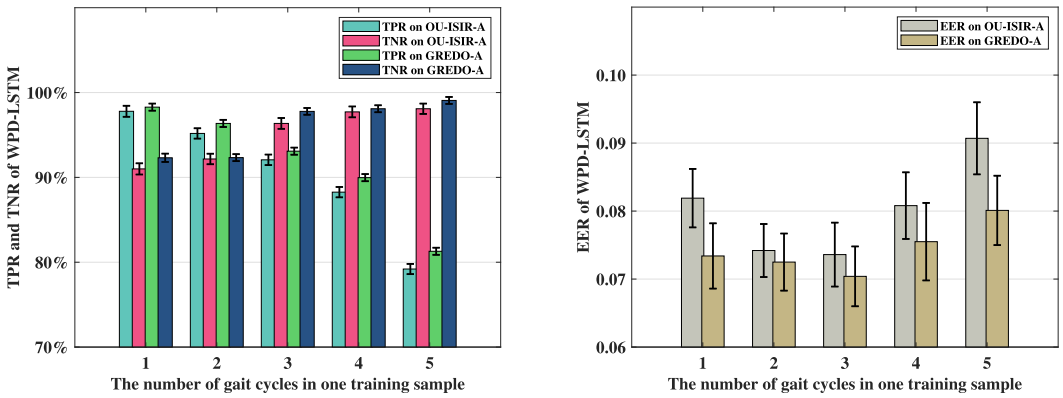
D. Performance on Multi-Cycle Defense Model

In this section, we first evaluate the performance of our WPD-LSTM multi-cycle defense model. Then we evaluate the ability of our proposed model to defend against two different types of attacks which are extended from a one cycle attack. Finally, we compare our solution with state-of-the-art work to show its superiority.

1) Performance of WPD-LSTM Multi-Cycle Model: In our WPD-LSTM multi-cycle defense model, it is important to determine the number of gait cycles in each training sample (gait sequence). That is to say, how many gait cycles C need to be included in a gait sequence. We conducted the experiment on OU-ISIR-A and GREDO-A. In the experiment, the data samples of the training set and the testing set were both sequences containing C gait cycles. In order to make full use of the data and ensure the coverage of the model, we also use the sliding window [45] to build defense model. There are $C-1$ continuous gait cycles between adjacent samples. The performance of the WPD-LSTM model under different values of C is shown in Fig. 5. Fig. 5(a) depicts the change of the true positive rate and the false negative rate under different values of C when threshold $\theta = 0.5$ and Fig. 5(b) depicts the EER under different values of C. When $C = 1$, the situation of training and testing is the same as that in the black-box model design. Therefore, when $C = 1$, we can find that the EER of the WPD-LSTM-based model is 8.12% and 7.39% on OU-ISIR-A and GREDO-A, which is similar to the results of the LSTM-based black-box model in Table II. When C is larger than 1, one gait sample for training and testing will contain C continuous gait cycles.

An interesting phenomenon occurs in Fig. 5(b) when C is smaller than 3, the final EER increases as C increases. While when C is larger than 3, the final EER decreases as C increases. We can see the reason for this from Fig. 5(a) which is as follows: In most of the authentication tasks, we should take care of the tradeoff between TPR and TNR. A high TNR means that the model has higher security, but the corresponding TPR will be reduced, making the usability of the system worse. In Fig. 5(a), we can find that C has a great impact on TPR and TNR. When C increases, the TPR

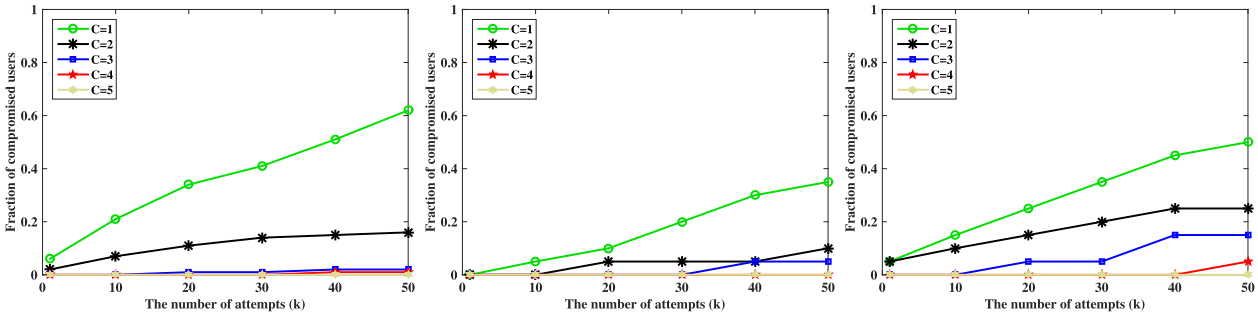
Authorized licensed use limited to: Northwestern University. Downloaded on October 10,2020 at 10:35:04 UTC from IEEE Xplore. Restrictions apply.



(a) The true positive rate and the false negative rate under different values of C when threshold $\theta = 0.5$.

(b) The average error rate under different values of C.

Fig. 5. Performance of the WPD-LSTM model under different values of C on OU-ISIR-A and GREDO-A. We use 10 independent repeat experiments to record the maximum, minimum and average.



(a) Performance of widespread attack against WPD-LSTM model on OU-ISIR-B.

(b) Performance of widespread attack against WPD-LSTM model on GREDO-B.

(c) Performance of mimic attack against WPD-LSTM model on GREDI.

Fig. 6. Fraction of compromised users over the first 50 attempts under different number of cycles C. For each attempt, the input is a gait sequence consisting of C repeated gait cycles.

will decrease but the TNR will increase. Here, C is a potential threshold as well as θ. Finally, we choose $C = 3$ as our cycle collection and design the WPD-LSTM-based 3-cycle model.

2) WPD-LSTM Model v.s. Various Attacks: Given the best value of C, we try to study the robustness of our proposed model against two different types of attacks. Since the number of gait cycles for training and testing has been changed (from 1 to C), we propose two similar attacks extended from one cycle attack.

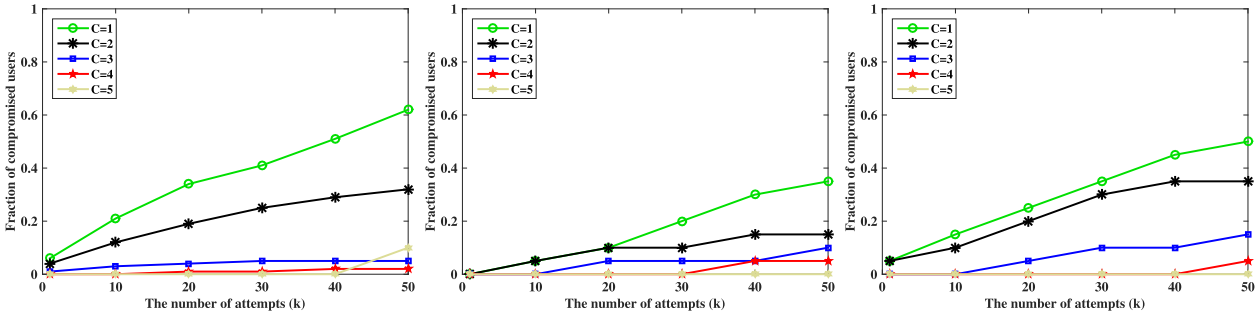
a) Extension I of one cycle attack: In each attempt, the attacker picks up one gait cycle using Algorithm 1, he/she repeats the adversarial gait cycle for C times and structures a new gait sequence for authenticating.

b) Extension II of one cycle attack: In each attempt, the attacker picks up C continuous gait cycles (here, we regard C cycles as a big "cycle") using Algorithm 1, and then puts the new sequence (C continuous gait cycles) into the authentication model. It is the same as the multi-cycle model design where the data samples of the training set and the testing set are both sequences containing C gait cycles.

We summarize the results of the above two attacks on OU-ISIR-B, GREDO-B and DREDI in Fig. 6 and Fig. 7, respectively. The performance between repeated gait cycles and continuous gait cycles does not deviate much, this is consistent with our expectations because the proposed multi-cycle defense model can effectively defend against these two attacks. When $C = 1$, the fractions of compromised users of these two attacks are the same because the gait sequences for authenticating are the same (one gait sequence only contains one gait cycle). We can see that when C is set to 3, 4, and 5, the fractions of compromised users on all the three datasets after 50 tries are still less than 0.1 using the WPD-LSTM model. It's worth noting that when C is 4 or 5, although the model has strong anti-attack capabilities, it can be seen from Fig. 5(a) that the model has a very low TPR.

3) Comparison Results of Multi-Cycle Classification: Similar to Table III, we attempted to study the robustness of our defense model and each of the proposed black-box models against a C-cycle attack ($C = 3$). We summarize the results of testing our adversaries on OU-ISIR-B, GREDO-B, and DREDI in Table IV. From Table IV, we can find that our WPD-LSTM model has the best performance, the average fractions of compromised users for the WPD-LSTM model on OU-ISIR-B, GREDO-B and GREDI after 50 tries are 0.05, 0.10, and 0.15, respectively. By using 3 gait cycles for model training, the robustness of some black-box models (SVM, CNN, LSTM, and CNN+LSTM) has increased, but the robustness of PCC and DTW has dropped. The main reason is that PCC and DTW will construct profiles with motion sensor data directly and then to calculate the

Authorized licensed use limited to: Northwestern University. Downloaded on October 10,2020 at 10:35:04 UTC from IEEE Xplore. Restrictions apply.



(a) Performance of widespread attack against WPD-LSTM model on OU-ISIR-B. (b) Performance of widespread attack against WPD-LSTM model on GREDO-B. (c) Performance of mimic attack against WPD-LSTM model on GREDI.

Fig. 7. Fraction of compromised users over the first 50 attempts under different number of cycles C. For each attempt, the input is a gait sequence consisting of consists of C continuous gait cycles.

TABLE IV

FRACTION OF USERS ON OU-ISIR-B, GREDO-B AND DREDI WHOSE MODELS WERE COMPROMISED AFTER 1, 5, 10, 20 AND 50 TRIES OF WIDESPREAD ATTACK, MIMIC ATTACK AND RANDOM ATTACK FOR OUR DEFENSE MODEL AND EACH OF THE BLACK-BOX MODELS WE USED. IN EACH ATTEMPT, THE ATTACKER PICKS UP 3 CONTINUOUS GAIT CYCLES. ALL THE RESULTS ARE THE AVERAGE BASED ON 10 EXPERIMENTS INDEPENDENTLY

Model name	The number of attempts (k)	Prob(k)					
		Widespread attack		Mimic attack	Random attack		
		OU-ISIR-B	GREDO-B	GREDI	OU-ISIR-B	GREDO-B	GREDI
WPD+LSTM	1	0.01	0	0	0	0	0
	5	0.01	0	0	0	0	0
	10	0.03	0	0	0	0	0
	20	0.04	0.05	0.05	0.01	0	0
	50	0.05	0.10	0.15	0.02	0	0.05
PCC [16]	1	0.09	0.10	0.10	0.01	0.05	0.05
	5	0.29	0.20	0.40	0.02	0.05	0.05
	10	0.47	0.45	0.60	0.04	0.10	0.05
	20	0.68	0.70	1	0.08	0.10	0.15
	50	0.93	1	1	0.17	0.15	0.20
SVM [16]	1	0.09	0.10	0.10	0	0	0
	5	0.17	0.25	0.30	0	0.05	0
	10	0.37	0.30	0.50	0.01	0.05	0.05
	20	0.63	0.50	0.85	0.05	0.05	0.10
	50	0.92	0.80	1	0.11	0.10	0.15
DTW [26]	1	0.17	0.10	0.10	0	0.05	0.05
	5	0.37	0.55	0.80	0.03	0.05	0.10
	10	0.56	0.75	1	0.09	0.10	0.15
	20	0.77	1	1	0.15	0.15	0.25
	50	1	1	1	0.27	0.25	0.30
CNN [27]	1	0.03	0.05	0.05	0	0	0
	5	0.08	0.10	0.10	0.01	0	0
	10	0.17	0.15	0.20	0.02	0	0.05
	20	0.32	0.25	0.30	0.03	0.05	0.10
	50	0.41	0.40	0.45	0.06	0.10	0.15
LSTM [28]	1	0.01	0	0	0	0	0
	5	0.03	0.05	0.05	0	0	0.05
	10	0.05	0.05	0.15	0.01	0	0.05
	20	0.08	0.10	0.20	0.01	0.05	0.10
	50	0.10	0.15	0.25	0.02	0.05	0.10
CNN+LSTM [28]	1	0	0	0	0	0	0
	5	0.02	0.05	0.05	0	0	0.05
	10	0.04	0.05	0.10	0	0	0.05
	20	0.06	0.10	0.15	0.01	0	0.05
	50	0.09	0.15	0.20	0.02	0.05	0.10

similarity score between the targeted profile and test samples without machine learning methods. More gait cycles may introduce new noise to the model of PCC and DTW. For the SVM model, the average fractions of compromised users have little change compared to the previous method in Table III since the length of the time series has little effect on the extraction of statistical features. For other black-box models, the average fractions of compromised users have dropped significantly, especially LSTM and CNN+LSTM. The main reason is the contextual contents of the neighboring gait cycles can be considered by the LSTM network structure.

Authorized licensed use limited to: Northwestern University. Downloaded on October 10,2020 at 10:35:04 UTC from IEEE Xplore. Restrictions apply.

TABLE V

COMPARISON WITH OTHER SOLUTIONS ON OU-ISIR-A AND GREDO-A. ALL THE SAMPLES FOR TRAINING AND TESTING ARE GAIT SEQUENCES WITH 3 CONTINUOUS GAIT CYCLES. THERE ARE 2 CONTINUOUS GAIT CYCLES BETWEEN ADJACENT SAMPLES

Model name	EER on OU-ISIR-A	EER on GREDO-A
WPD-LSTM	7.27%	6.99%
PCC [16]	11.42%	10.51%
SVM [16]	8.81%	8.65%
DTW [26]	19.37%	12.20%
CNN [27]	8.54%	8.70%
LSTM [28]	7.92%	7.80%
CNN+LSTM [28]	7.89%	7.73%

We also compared with the state-of-the-art black-box models and computed the corresponding EER using the WPD-LSTM 3-cycle model as shown in Table V. An observation is that PCC and DTW in our new training setting performed worse than the original black-box models, thus indicating that statistical-based methods may not be applicable in the multi-cycle scenario. Another observation is that our WPD-LSTM method performs better than LSTM and CNN+LSTM methods in the 3-cycle training scenario (EERs of WPD-LSTM are 7.27% and 6.99%, EERs of LSTM are 7.92% and 7.80%, EERs of CNN+LSTM are 7.89% and 7.73%). While in the one cycle training scenario, they are evenly matched (EERs of WPD-LSTM are 8.12% and 7.39%, EERs of LSTM are 8.09% and 7.98%, EERs of CNN+LSTM are 8.04% and 7.95%). The main reason is that the inherent inter-relationships between different sub-series of the gait sequence has been considered by our WPD-LSTM network, but this effect cannot be reflected during the one cycle training. In summary, our approach performs better than all the other solutions on OU-ISIR-A and GREDO-A, which indicates that our proposed model can better represent the gait patterns of users.

VI. CONCLUSION

In this paper, we propose a novel attack model, the one cycle attack, to compromise sensor-based gait authentication from the perspective of an attacker. With the help of an improved cycle extraction algorithm and an adversarial gait cycle matching algorithm, we have demonstrated that the vulnerability in the state-of-the-art black-box models can be easily exploited by attackers using the largest gait authentication dataset. Furthermore, to improve the robustness of sensor-based gait authentication methods to fight against attacks, we present a WPD-LSTM-based multi-cycle defense model which is able to consider the contextual contents of the neighboring gait cycles in the gait sequence.

Experimental results show that our attack model can compromise most of the victims within a limited number of attempts. In addition, we have demonstrated that with imitation our attack will be more effective. Moreover, the experiment indicates that our WPD-LSTM model can better represent the gait/walk patterns of users and greatly mitigates the success rate of attackers under two different attack scenarios.

REFERENCES

[1] R. Chellappa, C. L. Wilson, and S. Sirohey, "Human and machine recognition of faces: A survey," *Proc. IEEE*, vol. 83, no. 5, pp. 705–741, May 1995.

[2] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Springer, 2009.

[3] K. W. Bowyer, K. Hollingsworth, and P. J. Flynn, "Image understanding for iris biometrics: A survey," *Comput. Vis. Image Understand.*, vol. 110, no. 2, pp. 281–307, May 2008.

[4] T. Kinnunen and H. Li, "An overview of text-independent speaker recognition: From features to supervectors," *Speech Commun.*, vol. 52, no. 1, pp. 12–40, Jan. 2010.

[5] F. Monrose and A. Rubin, "Authentication via keystroke dynamics," in *Proc. 4th ACM Conf. Comput. Commun. Secur. (CCS)*, 1997, pp. 48–56.

[6] D. Gafurov, "A survey of biometric gait recognition: Approaches, security and challenges," in *Proc. Annu. Norwegian Comput. Sci. Conf.*, 2007, pp. 19–21.

[7] *BMA400*. Accessed: Feb. 1, 2020. [Online]. Available: https://www.bosch-sensortec.com/products/motion-sensors/accelerometers/bma400.html

[8] *Android Motion Sensor*. Accessed: Feb. 1, 2020. [Online]. Available: https://developer.android.com/guide/topics/sensors/sensors_motion

[9] L. Rong, Z. Jianzhong, L. Ming, and H. Xiangfeng, "A wearable acceleration sensor system for gait recognition," in *Proc. 2nd IEEE Conf. Ind. Electron. Appl. (ICIEA)*, May 2007, pp. 2654–2659.

[10] D. Gafurov, E. Snekkenes, and P. Bours, "Improved gait recognition performance using cycle matching," in *Proc. IEEE 24th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, 2010, pp. 836–841.

[11] C. Nickel, T. Wirtl, and C. Busch, "Authentication of smartphone users based on the way they walk using k-NN algorithm," in *Proc. 8th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP)*, Jul. 2012, pp. 16–20.

[12] M. O. Derawi, P. Bours, and K. Holien, "Improved cycle detection for accelerometer based gait authentication," in *Proc. 6th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP)*, Oct. 2010, pp. 312–317.

[13] D. Gafurov, E. Snekkenes, and P. Bours, "Gait authentication and identification using wearable accelerometer sensor," in *Proc. IEEE Workshop Automat. Identificat. Adv. Technol.*, Jun. 2007, pp. 220–225.

[14] T. Hoang, D. Choi, and T. Nguyen, "Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme," *Int. J. Inf. Secur.*, vol. 14, no. 6, pp. 549–560, Nov. 2015.

[15] W. Xu *et al.*, "KEH-Gait: Towards a mobile healthcare user authentication system by kinetic energy harvesting," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2017, pp. 1–15.

[16] Y. Ren, Y. Chen, M. C. Chuah, and J. Yang, "User verification leveraging gait recognition for smartphone enabled mobile healthcare systems," *IEEE Trans. Mobile Comput.*, vol. 14, no. 9, pp. 1961–1974, Sep. 2015.

[17] *The Way You Walk Could Be the Best Biometrics Authentication Solution as of Yet*. Accessed: Feb. 1, 2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/the-way-you-walk-could-be-the-best-biometrics-authentication-solution-as-of-yet/.

[18] *The Next Biometric Authentication Method for DISA? Your Gait*. Accessed: Feb. 1, 2020. [Online]. Available: https://fedtechmagazine.com/article/2018/01/next-biometric-authentication-method-disa-your-gait

[19] *UnifyID*. Accessed: Feb. 1, 2020. [Online]. Available: https://unify.id/

[20] D. Gafurov, E. Snekkenes, and T. E. Buvarp, "Robustness of biometric gait authentication against impersonation attack," in *Proc. Confederated Int. Conf. Move Meaningful Internet Syst.* Berlin, Germany: Springer, 2006, pp. 479–488.

[21] D. Gafurov, E. Snekkenes, and P. Bours, "Spoof attacks on gait authentication system," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 491–502, Sep. 2007.

[22] B. B. Mjaaland, P. Bours, and D. Gligoroski, "Walk the walk: Attacking gait biometrics by imitation," in *Proc. Int. Conf. Inf. Secur.* Berlin, Germany: Springer, 2010, pp. 361–380.

[23] M. Muaaz and R. Mayrhofer, "Smartphone-based gait recognition: From authentication to imitation," *IEEE Trans. Mobile Comput.*, vol. 16, no. 11, pp. 3209–3221, Nov. 2017.

[24] P. Negi, P. Sharma, V. S. Jain, and B. Bahmani, "K-means++ vs. behavioral biometrics: One loop to rule them all," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2018, pp. 1–13.

Authorized licensed use limited to: Northwestern University. Downloaded on October 10,2020 at 10:35:04 UTC from IEEE Xplore. Restrictions apply.

[25] D. Arthur and S. Vassilvitskii, "k-means++: The advantages of careful seeding," in *Proc. 18th Annu. ACM-SIAM Symp. Discrete Algorithms*. Philadelphia, PA, USA: Society for Industrial and Applied Mathematics, 2007, pp. 1027–1035.
[26] T. T. Ngo, Y. Makihara, H. Nagahara, Y. Mukaigawa, and Y. Yagi, "The largest inertial sensor-based gait database and performance evaluation of gait-based personal authentication," *Pattern Recognit.*, vol. 47, no. 1, pp. 222–231, 2014.
[27] M. Gadaleta and M. Rossi, "IDNet: Smartphone-based gait recognition with convolutional neural networks," *Pattern Recognit.*, vol. 74, pp. 25–37, Feb. 2018.
[28] Q. Zou, Y. Wang, Q. Wang, Y. Zhao, and Q. Li, "Deep learning-based gait recognition using smartphones in the wild," 2018, *arXiv:1811.00338*. [Online]. Available: http://arxiv.org/abs/1811.00338
[29] S. Sprager and M. Juric, "Inertial sensor-based gait recognition: A review," *Sensors*, vol. 15, no. 9, pp. 22089–22127, Sep. 2015.
[30] P. Connor and A. Ross, "Biometric recognition by gait: A survey of modalities and features," *Comput. Vis. Image Understand.*, vol. 167, pp. 1–27, Feb. 2018.
[31] J. Mäntyjärvi, M. Lindholm, E. Vildjiounaite, S.-M. Mäkelä, and H. Ailisto, "Identifying users of portable devices from gait pattern with accelerometers," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Mar. 2005, pp. 1–4.
[32] D. Gafurov, K. Helkala, and T. Soendrol, "Gait recognition using acceleration from MEMS," in *Proc. 1st Int. Conf. Availability, Rel. Secur. (ARES)*, 2006, pp. 1–6.
[33] M. Ahmad, A. M. Khan, J. A. Brown, S. Protasov, and A. M. Khattak, "Gait fingerprinting-based user identification on smartphones," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2016, pp. 3060–3067.
[34] H. El-Alfy, I. Mitsugami, and Y. Yagi, "A new gait-based identification method using local Gauss maps," in *Computer Vision*, vol. 9008, C. Jawahar and S. Shan, Eds. Cham, Switzerland: Springer, 2015, pp. 3–18.
[35] L. Huang, A. D. Joseph, B. Nelson, B. I. Rubinstein, and J. D. Tygar, "Adversarial machine learning," in *Proc. 4th ACM Workshop Secur. Artif. Intell. (AISec)*, New York, NY, USA, 2011, pp. 43–58.
[36] A. Serwadda and V. V. Phoha, "Examining a large keystroke biometrics dataset for statistical-attack openings," *ACM Trans. Inf. Syst. Secur.*, vol. 16, no. 2, pp. 1–30, Sep. 2013.
[37] H. Khan, U. Hengartner, and D. Vogel, "Augmented reality-based mimicry attacks on behaviour-based smartphone authentication," in *Proc. 16th Annu. Int. Conf. Mobile Syst., Appl., Services (MobiSys)*, New York, NY, USA, Jun. 2018, pp. 41–53.
[38] A. Serwadda and V. V. Phoha, "When kids' toys breach mobile phone security," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2013, pp. 599–610.
[39] H. Khan, U. Hengartner, and D. Vogel, "Targeted mimicry attacks on touch input based implicit authentication schemes," in *Proc. 14th Annu. Int. Conf. Mobile Syst., Appl., Services (MobiSys)*, 2016, pp. 387–398.
[40] R. Kumar, V. V. Phoha, and A. Jain, "Treadmill attack on gait-based authentication systems," in *Proc. IEEE 7th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Sep. 2015, pp. 1–7.
[41] B. Z. H. Zhao, H. J. Asghar, and M. A. Kaafar, "On the resilience of biometric authentication systems against random inputs," 2020, *arXiv:2001.04056*. [Online]. Available: http://arxiv.org/abs/2001.04056
[42] M. Mohamed, B. Shrestha, and N. Saxena, "SMASheD: Sniffing and manipulating Android sensor data for offensive purposes," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 4, pp. 901–913, Apr. 2017.
[43] Q. Zou, L. Ni, Q. Wang, Q. Li, and S. Wang, "Robust gait recognition by integrating inertial and RGBD sensors," *IEEE Trans. Cybern.*, vol. 48, no. 4, pp. 1136–1150, Apr. 2018.
[44] C. Nickel, H. Brandt, and C. Busch, "Classification of acceleration data for biometric gait recognition on mobile devices," in *Proc. BIOSIG*, vol. 11, 2011, pp. 57–66.
[45] T. Zhu *et al.*, "RiskCog: Unobtrusive real-time user authentication on mobile devices in the wild," *IEEE Trans. Mobile Comput.*, vol. 19, no. 2, pp. 466–483, Feb. 2020.
[46] C. Shen, Y. Chen, and X. Guan, "Performance evaluation of implicit smartphones authentication via sensor-behavior analysis," *Inf. Sci.*, vols. 430–431, pp. 538–553, Mar. 2018.
[47] T. Hoang, D. Choi, V. Vo, A. Nguyen, and T. Nguyen, "A lightweight gait authentication on mobile phone regardless of installation error," in *Proc. IFIP Int. Inf. Secur. Conf.* Berlin, Germany: Springer, 2013, pp. 83–101.
[48] M. Ghil, "Advanced spectral methods for climatic time series," *Rev. Geophys.*, vol. 40, no. 1, pp. 1–3, 2002.
[49] T. J. Harris and H. Yuan, "Filtering and frequency interpretations of singular spectrum analysis," *Phys. D, Nonlinear Phenomena*, vol. 239, nos. 20–22, pp. 1958–1967, Oct. 2010.
[50] *Pearson Correlation Coefficient*. Accessed: Jun. 10, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Pearson_correlation_coefficient
[51] *Support Vector Machine*. Accessed: Jun. 10, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Support_vector_machine
[52] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," *ACM Trans. Intell. Syst. Technol.*, vol. 2, no. 3, pp. 1–27, Apr. 2011.
[53] D. J. Berndt and J. Clifford, "Using dynamic time warping to find patterns in time series," in *Proc. KDD Workshop*, Seattle, WA, USA, 1994, vol. 10, no. 16, pp. 359–370.
[54] *Convolutional Neural Network*. Accessed: Jun. 10, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Convolutional_neural_network
[55] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, 1997.
[56] *Recurrent Neural Network*. Accessed: Jun. 10, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Recurrent_neural_network
[57] L. Fu, Y. Wei, S. Fang, X. Zhou, and J. Lou, "Condition monitoring for roller bearings of wind turbines based on health evaluation under variable operating states," *Energies*, vol. 10, no. 10, p. 1564, Oct. 2017.
[58] P. Li, K. Zhou, X. Lu, and S. Yang, "A hybrid deep learning model for short-term PV power forecasting," *Appl. Energy*, vol. 259, Feb. 2020, Art. no. 114216.
[59] P. Boškoski and Đ. Juričić, "Fault detection of mechanical drives under variable operating conditions based on wavelet packet Rényi entropy signatures," *Mech. Syst. Signal Process.*, vol. 31, pp. 369–381, Aug. 2012.
[60] J. E. Trost, "Statistically nonrepresentative stratified sampling: A sampling technique for qualitative studies," *Qualitative Sociol.*, vol. 9, no. 1, pp. 54–57, 1986.
[61] *LSTMs for Human Activity Recognition*. Accessed: Jun. 10, 2020. [Online]. Available: https://github.com/guillaume-chevalier/LSTM-Human-Activity-Recognition
[62] *Python*. Accessed: Jun. 10, 2020. [Online]. Available: https://www.python.org/

Tiantian Zhu received the Ph.D. degree in computer science from Zhejiang University, Hangzhou, China, in 2019. He is currently a Lecturer with the College of Computer Science and Technology, Zhejiang University of Technology, China. His research interests include mobile security, OSN security, and artificial intelligence.

Lei Fu received the Ph.D. degree in mechanical engineering from Zhejiang University, Hangzhou, China, in 2018. He is currently a Lecturer with the College of Mechanical Engineering, Zhejiang University of Technology, China. His research interests include fault diagnosis, signal processing, and artificial intelligence.

Authorized licensed use limited to: Northwestern University. Downloaded on October 10,2020 at 10:35:04 UTC from IEEE Xplore. Restrictions apply.

Qiang Liu received the B.Sc. degree in electronic information engineering from the Beijing Institute of Technology, Beijing, China, in 2018. He is currently pursuing the Ph.D. degree with the College of Computer Science, Zhejiang University, Hangzhou, China. His research interests include system security, software security, and firmware analysis.

Zi Lin received the B.Sc. degree in computer science and technology from Zhejiang University, Hangzhou, Zhejiang, China, in 2018. He is currently pursuing the master's degree with the College of Computer Science, Northwestern University, Evanston, IL, USA. His research interests include system design and deep learning.

Yan Chen (Fellow, IEEE) received the Ph.D. degree in computer science from the University of California at Berkeley, Berkeley, CA, USA, in 2003. He is currently a Professor with the Department of Electrical Engineering and Computer Science, Northwestern University, Evanston, IL, USA. Based on Google Scholar, his articles have been cited over 7000 times and his H-index is 34. His research interests include network security, measurement, and diagnosis for large-scale networks and distributed systems. He received the Department of Energy (DoE) Early CAREER Award in 2005, the Department of Defense (DoD) Young Investigator Award in 2007, and the Best Paper Nomination in ACM SIGCOMM 2010.

Tieming Chen (Member, IEEE) received the Ph.D. degree in computer software and theory from Beihang University, Beijing, China, in 2011. He is currently a Professor with the College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou, China. His research interests include cyberspace security and intelligence security. He is also a member of ACM.

Authorized licensed use limited to: Northwestern University. Downloaded on October 10,2020 at 10:35:04 UTC from IEEE Xplore. Restrictions apply.