Detection of spoofed identities on smartphones via sociability metrics

Conference Paper · May 2017

DOI: 10.1109/ICC.2017.7997423

4 authors, including:

Fazel Anjomshoa
Clarkson University
10 PUBLICATIONS **29** CITATIONS
SEE PROFILE

Burak Kantarci
University of Ottawa
155 PUBLICATIONS **1,131** CITATIONS
SEE PROFILE

Melike Erol Kantarci
University of Ottawa
107 PUBLICATIONS **2,194** CITATIONS
SEE PROFILE

Detection of Spoofed Identities on Smartphones via Sociability Metrics

Fazel Anjomshoa, *Student Member, IEEE,* Burak Kantarci, *Senior Member, IEEE*
Melike Erol-Kantarci, *Senior Member, IEEE* and Stephanie Schuckers, *Member, IEEE*

***Abstract*—The pervasiveness of smartphones equipped with various built-in sensors combined with the capability of serving multiple applications that could access social network information introduces next generation soft biometrics tools that could be used to verify a user's identity through their social behavior. Smart mobile devices can provide multi-modal data acquisition from various social networking applications, and when aggregated, these data can help form highly identifiable behaviometric information. Continuous identification and authentication of users through monitoring social behavior improves detection of identity spoofing. In this paper, we propose a social behaviometric framework to cope with identity spoofing on smartphones. The proposed framework consists of a front-end client module that acquires and provides social networking data to the back-end module which runs online machine learning procedures and provides analytics as a service to the front-end in order to verify user identity through social interactions. We evaluate the performance of the proposed framework by using real data collected from participants, and inject noisy behavioral patterns to simulate identity spoofing scenarios. Performance results show that under anomalous behavioral patterns, the proposed system can identify genuine users with up to 97% success ratio using an aggregated behavior pattern on five different social network applications.**

I. Introduction

Mobile social networking applications reveal significant and useful information about user behaviour. According to Ericsson's report, mobile applications for social networking produce high volumes of data that can be augmented with analytics for the betterment of various services [1]. Most users have regular behavioral patterns that are learnable which can ultimately be used for continuous recognition of behavioral signatures of users in social networks. That being said, in [2], we hypothesized that the behavioral patterns on various social network platforms can help continuously identify users and verify that the smartphones are in possession of the proper user. To this end, we proposed a mobile behaviometric framework that assesses users' social activity, and introduced sociability metrics to generate signatures of users' activities.

In this paper, we extend the previously proposed sociability assessment framework and propose a generalized framework in order to investigate the efficiency of social behaviometric identification in the presence of identity spoofing attacks on smartphones and illegitimate access to social network services. The proposed framework is built on the Track My Social Network Activity (TrackMaison) architecture proposed in [2]. We use five popular social networking applications on mobile platforms, namely Facebook, Twitter, Linkedin, Skype and WhatsApp while the contextual data is built on location (of usage), and distribution profile for uplink/downlink Wi-Fi data generation and session duration through these applications. Upon generation of the contextual data for each user, behavioral patterns of each user are clustered by using the DBSCAN algorithm, which enables learning user behavior within a week time frame. To simulate the spoofed identities, we artificially inject noisy contextual patterns into the user's data, particularly, we cloak five-day contextual data of the victim by the contextual data of another user. Thus, detection of identity spoofing is analogous to the anomaly detection problem. Through various test cases on real data, we show that the proposed social behaviometric approach can achieve up to 96% success ratio in detecting anomalous behavior (i.e., spoofed identities) on the mobile social network applications on smartphones.

Moreover, as sociability metrics that are defined through these contextual data are the key indicators for identification, we also investigate the impact of historical and recent sociability signatures on the performance of continuous social identification by assigning different weights to historical and recent sociability values. We show that while forming the sociability metrics on a running average basis, unbalanced weights of historical and recent data (e.g. 30%-70% or vice versa) in forming the running average values of sociability metrics lead to at most 80% success ratio whereas equal contribution of past and recent sociability can achieve 94% accuracy (i.e. true rejection and true acceptance) in continuous identification of the users on mobile social network platforms.

The rest of this paper is organized as follows. Section II illustrates the background of the research. In Section III, the system design and architecture are described. The results are shown in section IV followed by the conclusion in section V.

II. Related Work

The traditional identification schemes on mobile phones such as pin codes and passwords have well-known vulnerabilities [3] whereas widely used biometric identification schemes are more secure at the expense of extra hardware on devices [4], [5]. Biometric authentication schemes are categorized into two groups [6]: 1) Physiological biometrics such as fingerprint, facial recognition, iris and so on, and 2) behavioral biometrics which are based on human habitual signature including walking [7], handwriting, keystroke dynamics [8], interaction with the mobile device [9] and social networking. Continuous identification is based on behavioral patterns of users which advances existing identification mechanisms to

F. Anjomshoa and S. Schuckers are with the Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY, 13699 USA e-mail: {anjomsm,sschucke}@clarkson.edu

B. Kantarci and M. Erol-Kantarci are with the School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON, Canada, Ottawa, ON, K1N 6N5. e-mail: {burak.kantarci,melike.erolkantarci}@uottawa.ca

more secure, easier and non-intrusive fashion. Yampolskiy et al [10] categorize behavioral biometrics into five different classes of authorship based biometrics, human computer interaction (HCI)-based biometrics, indirect HCI-based biometrics, motor-skills biometrics and purely behavioral biometrics. In particular, the popularity of social networks yields users to generate a large amount of data coming from mobile wearable devices. There are various research efforts in the area of mining social network induced information. Chen et al [11] address the social network traits like scam or finding the stem of rumors [12]. The authors in [13], [14] discuss the possibility of using behavioral patterns on social platforms for user identification. Yet, verification with real traces and identification success have not been evaluated comprehensively. With the widespread adoption of Internet of Things (IoT) devices, their use as a base for user identification is expected to grow [15]. Behaviometrics is also an important part of smart homes, as user signals and interaction with the homes can be used to reconfigure a smart home [16]. For hand-held devices, usage behavior patterns such as gestures on touchscreens have been considered as continuous authentication solutions which is proposed in [17]. Although these works are relevant, they do not focus on identifying users uniquely based on contextual patterns on social networks.

Table I
DEFINITIONS

SYMBOL	DESCRIPTION
$\mathcal{A}$	Social Activity Rate
$\mathcal{SF}$	Sociability Factor
$\mathcal{D}$	data usage
τ	The number of sessions per day
T_k	$k-th$ activity rate
t	Duration of the activity
u	User u
$\mathcal{U}$	Set of users | $u \in \mathcal{U}$
p	Data point
$\mathcal{P}$	Set of Data points
ins	Instantaneous rate
sh	Short term activity
$overall$	overall activity
$normal$	Normalized activity
$\mathcal{A}_{ins_i}^{\mathcal{U}^u_{app_x}}$	Instantaneous Social activity of user u using application x in a session i
$\mathcal{A}_{sh}^{\mathcal{U}^u_{app_x}}$	Short-term Social activity of user u using application x
$\mathcal{A}_{overall}^{\mathcal{U}^u_{app_x}}$	Overall Social Activity
$\mathcal{A}_{normal}^{\mathcal{U}^u}$	Normalized Social Activity
α	Balancing coefficient to choose T_k or T_{k-1} activity rate
μ	Mean
σ	Standard Deviation

III. SYSTEM DESIGN

The front-end application collects data from five popular social network services which are; Facebook, Twitter, LinkedIn, Skype and WhatsApp. The collected data is stored as sessions, and each session presents the corresponding user's social interaction through the device. Basically each session data includes session ID, social network application identifier, the time that the session is started, the time that the session ended (i.e. the duration of that session), the amount of data consumed in the session and the initial location where the session started. The amount of data used is the amount of cellular or Wi-Fi data consumed by the social network services.

To identify the behaviometric signature of users, the following components are required:

Figure 1 system architecture includes main modules and methods, namely monitoring, data collection, normalization, training and identification modules. Below, more details on each module are provided.

1) Data Collection: Mobile user data collected from the device is uploaded to a private cloud-based server. The server stores the raw data from all users in a database. The database is queried for training and identification purposes.

2) User Characterization Model: User characterization is done by extracting a combination of features from both users' interaction over online social networks as well as the built-in sensors of the device. The details of the model are provided in the following sections.

3) Training Strategy: Training strategy builds a profile for each user based on the collected data. Training is performed continuously on a sliding window of data over time. This allows capturing naturally altering patterns of user behavior.

4) Identification Strategy: Machine learning is the core of user identification. Thus, the system is trained with feature sets collected by the front-end application, and user identification is performed based on each interaction through the device.

Once the session data is transferred to the server, the raw collected data is converted to several metrics of interest. This process is called normalization. In this study, two social identification metrics, namely the social activity rate and sociability factor are used which were initially defined in [2]. In the rest of this section, we revisit these metrics to assist the readers.

Social Activity Rate: Social activity rate corresponds to the relative amount of data that a user generates when using social networking applications. The absolute data usage of a user is normalized by the data usage of all active users. Social activity rate of a user is a function of the user's short term (daily) and instantaneous social activity rates. Instantaneous social activity rate denotes the data usage by a particular social network application in a single session. Thus, denotes the amount of data from the social network application x (app_x) in session-i and, is the duration of time that the app_x in session-i was used. Meanwhile instantaneous social activity rate ($\mathcal{A}_{ins_i}^{\mathcal{U}^u_{app_x}}$) is formulated as shown in (1).

$$\mathcal{A}_{ins_i}^{\mathcal{U}^u_{app_x}} = \mathcal{D}_i^{\mathcal{U}^u_{app_x}} / t_i^{\mathcal{U}^u_{app_x}} \tag{1}$$

It is worthwhile noting that Short term (daily) activity denotes the average data usage on the corresponding social network app in a session per day as formulated in (2). A weighted sum of consecutive short term social activity rates provide the overall social activity rate ($\mathcal{A}_{overall}^{\mathcal{U}^u_{app_x}}(T_k)$) as shown in Eq. (3).

$$\mathcal{A}_{sh}^{\mathcal{U}^u_{app_x}} = \left(\sum \mathcal{D}_i^{\mathcal{U}^u_{app_x}} / t_i^{\mathcal{U}^u_{app_x}} \right) / \tau_x \tag{2}$$

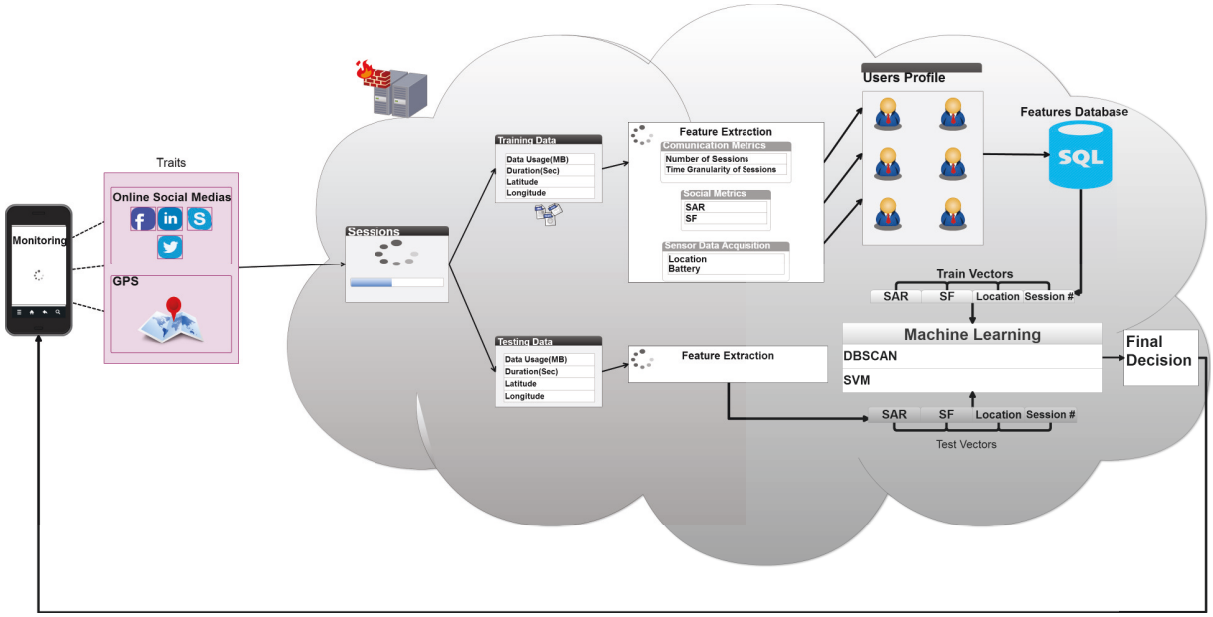

Figure 1. Minimalist overview of the system architecture.

$$\mathcal{A}^{\mathcal{U}^u_{app_x}}_{overall}(T_k) = \alpha * \mathcal{A}^{\mathcal{U}^u_{app_x}}_{sh}(T_{k-1}) + (1-\alpha) * \mathcal{A}^{\mathcal{U}^u_{app_x}}_{sh}(T_k) \quad (3)$$

The normalized social active rate ($\mathcal{A}_{normal_i}$) is aggregated overall social factors of a user averaged by the maximum social activity rate in pool of active users as shown in Eq. (4)

$$\mathcal{A}^{\mathcal{U}^u}_{normal} = \sum_{x \in \mathcal{X}} \omega_x \mathcal{A}^{\mathcal{U}^u_{app_x}}_{overall}(T_k) / \operatorname*{argmax}_{u \in \mathcal{U}} \sum_{x \in \mathcal{X}} \omega_x \mathcal{A}^{\mathcal{U}^u_{app_x}}_{overall} \quad (4)$$

Sociability Factor: Sociability of users is not limited to their data consumption but it is also a function of the time they spend on mobile social network applications. Therefore we define the sociability factor metric as another identifier. Similar to the social activity rate, the sociability factor also has instantaneous, short term and global components that ultimately lead to a normalized sociability factor value. Thus, instantaneous sociability factor per app is calculated as the total time that a user spends on a social networking app in a single session as formulated in Eq. (5). Short term sociability factor ($\mathcal{SF}^{\mathcal{U}^u_{app_x}}_{sh_i}$) is defined as the average time that a user spends on a particular social network app in a session over a short time window, e.g., a day, as formulated in (6) where $t^{\mathcal{U}^u_{app_x}}_i$ stands for duration of session-i of user-u on app_x. As formulated in eq. (7), the overall sociability factor ($\mathcal{SF}^{\mathcal{U}^u_{app_x}}_{overall_i}(T_k)$) is a weighted sum of short term sociability factors where T_k denotes the $k-th$ short term sociability factor used in the calculation, and β is a weight factor for each mobile social network app. Finally, as expected, the normalized sociability factor ($\mathcal{SF}_{normal_i}$) is the aggregated overall sociability factors of a user scaled by the maximum aggregated sociability factors in the active users pool as shown in Eq. (8).

$$\mathcal{SF}^{\mathcal{U}^u_{app_x}}_{ins_i} = t^{\mathcal{U}^u_{app_x}}_i \quad (5)$$

$$\mathcal{SF}^{\mathcal{U}^u_{app_x}}_{sh} = \left(\sum t^{\mathcal{U}^u_{app_x}}_i\right) / \tau \quad (6)$$

$$\mathcal{SF}^{\mathcal{U}^u_{app_x}}_{overall}(T_k) = \beta * \mathcal{SF}^{\mathcal{U}^u_{app_x}}_{sh}(T_{k-1}) + (1-\beta) * \mathcal{SF}^{\mathcal{U}^u_{app_x}}_{sh}(T_k) \quad (7)$$

$$\mathcal{SF}^{\mathcal{U}^u_{app_x}}_{normal} = \sum_{x \in \mathcal{X}} \omega_x \mathcal{SF}^{\mathcal{U}^u_{app_x}}_{overall}(T_k) / \operatorname*{argmax}_{u \in \mathcal{U}} \sum_{x \in \mathcal{X}} \omega_x \mathcal{SF}^{\mathcal{U}^u_{app_x}}_{overall} \quad (8)$$

IV. Performance Evaluation

The performance of machine learning-based continuous identification on mobile social network applications is evaluated by using the platform that was initially introduced in [2] which collects data usage, activity duration, location and usage frequency of project participants on five popular social network applications, namely Facebook, Twitter, LinkedIn, Skype and WhatsApp. The back-end server computes the social activity rate and sociability factor by using the data rates and session duration as formulated in (4) and (8). The identification part was done by using DBSCAN Density-based spatial clustering of applications with noise (DBSCAN) [18]. DBSCAN groups the data points that are nearest neighbors of each other, and aims at forming dense regions. The front-end connectivity of the testbed is provided by Android-based tablets that continuously push data collected from 13K sessions in a two-month window.

Six representative users out of the participant set are chosen. The raw data along with the user traits can be accessed online at [19]. It is worthwhile mentioning that the algorithm filled the missing data points with the mean value up to that point. The results are based on different set of values for α and β in (3) and (7). As mentioned before, social active rate denotes the amount of data that a user spends on social network applications whereas sociability factor is a function of the duration that a user interacts with their mobile device. It is worthwhile

noting that connected IoT devices, and mobile applications that run on those devices are prone to security vulnerabilities as a result of unauthorized access as stated in [20]. Thus, this paper does not aim to replace biometric authentication in IoT-integrated platforms or consumer devices but aims to strengthen existing password, fingerprint, face or speech recognition-based authentication by incorporating knowledge based spatiotemporal abstraction on mobile social networking applications and services. That being said, a performance metric, namely the authentication error probability is defined in order to evaluate the disruption probability in continuous authentication of users on connected mobile devices. In this paper the authentication error probability is cumulative.

Besides evaluating the performance of sociability-based identification, under identity spoofing scenarios, we also investigate the impact of the contextual parameter weights on the long term sociability signature, which is formulated by (3) and (7). To this end, various values have been set in the form of ((α)-(1-α)) for social activity rate, and in the form of ((β)-(1-β)) for sociability factor as follows: 30%-70%, 50%-50% and 70%-30% where each set respectively refers to (α) and (1- α). For example, 30%-70% means α and β are equal to 30%.

Each figure presents the authentication error probability (AEP) of the system during the 5-day period after a user's behavior has been learned (i.e., converged authentication error probability). It is worth noting that the motivation behind continuous authentication is to reduce the frequency of biometric authentication, and allow the users to keep using their devices. As formulated in (9), AEP_t denotes the disruption probability due to triggering of biometric authentication. The ratio of the cumulative value of false or true rejections (FR and TR) starting from the beginning of training moving to the end of the time of interest (t) to the cumulative value of total acceptances and rejections. Indeed, false acceptance may lead to severe consequences. In this section, we also show the false acceptance probability, and the impact of the contextual parameter weights ($\alpha - \beta$) on the number of false acceptances.

$$AEP_t = \frac{\sum_{k=0}^{t} (FR_k + TR_k)}{\sum_{k=0}^{i} (FR_k + FA_k + TR_k + TA_k)} \qquad (9)$$

By normal condition, we denote the situation where user identities are not spoofed, and a smartphone is in possession of the legitimate user. Thus, under normal condition, the system can only experience false rejections that will increase the authentication error probability (i.e. trigger biometric authentication). On the other hand, by anomalous condition, we denote artificially injected noisy patterns on each day to the contextual data of the selected users. More specifically, artificially injected noise denotes, cloaking of the contextual patterns of the genuine user by the contextual data (short term) of another randomly selected user. We inject noisy patterns to each daily pattern one by one. Thus, any spoofed identity can only be detected until the end of the day. Thus, under anomalous condition, the system may experience high authentication error probability (i.e. triggering of biometric authentication) due to true rejection or false rejection. Therefore, in Figs. 2-4, the gray bars represent the false rejections whereas the black bars represent the disruption due to any rejection.

Fig. 2 presents the situation where the weight of historical social activity rate and sociability factors is 30% whereas the weight of the recent values of these sociability metrics is 70%. As user-1 and user-3 reveal less deviation other than the points representing extreme social activity levels (0% and 100%) [19], they present better success rate under normal condition. Moreover, since user-3 has a higher social activity rate which is also correlated with its sociability factor, under normal conditions, the user can be identified with a success ratio that is close to 100%. It can also be concluded that the users with lower social activity factor (i.e. shorter session duration), such as user-2, lead to higher error rates in identification under normal condition. This conclusion also holds for the scenarios where identities are spoofed through injecting noisy patterns because under anomalous conditions, besides false rejections, true rejections will also trigger biometric authentication which is a result of an error generated by the behavioral authentication. As the sociability signature of user-3 has less fluctuations, the authentication error probability of the corresponding user is still under 4%. However, when we consider all users, the overall average continuous authentication ratio is around 74%.

Fig. 3 and Fig. 4 present the same results under (α-β) is set to (50%-50%) and (70%-70%), respectively. The former denotes the situation where past and recent sociability metrics of a user contribute to formulation of the sociability metrics equally whereas the latter denotes the situation where recent sociability metrics have higher impact on the formulation of the sociability metrics. It is worthwhile noting that the sociability metrics, namely the social activity factor and the sociability rate, along with the location data, are the inputs of the machine learning modules in the proposed framework. When the three figures (i.e. Figs. 2-4) are compared, it is clearly seen that having past and recent sociability values equally contribute to the new inputs of the machine learning component helps improve the success ratio. For most users, the AEP is below 10% which translate into a success ratio over 90%.

In addition to the observations reported above, in Figs.2-4, it is an expected phenomena under anomalous condition to have $\geq AEP$ in comparison to the normal condition. Indeed, this increase does not indicate a failure of the proposed system but indicates a disruption in continuous behavioral authentication in order verify user identity via biometrics.

Besides these values, we have also tested the False Acceptance (FA) probability under 15%-15% and 85%-85% combinations for α-β. As illustrated in Fig. 5, the system suffers from false acceptances when past sociability values are lightly valued. Moreover, 15% and 50% settings lead to the minimum number of false acceptances in detecting impostor profiles. By studying given data, the minimum number of FA for all users is experienced under $\alpha = \beta = 15\%$ setting by just one out of 30 noisy instances which translates into ≈97% success in identification. This rate decreased to ≈74% by eight FA occurrences out of thirty noisy instances when $\alpha = \beta = 30\%$. The performance of the system under $\alpha = \beta = 50\%$ improves by reporting only two FA occurrences which translates into ≈94% accuracy.

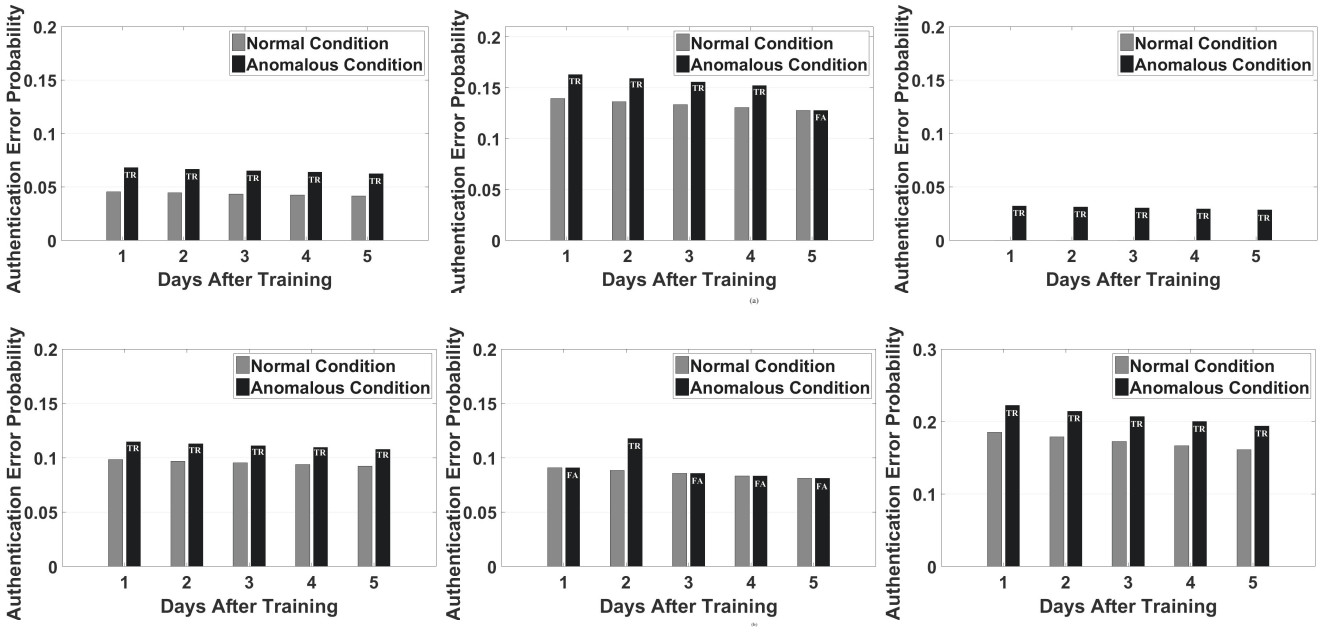

Figure 2. Biometric authentication probability(TR + FR) under DBSCAN with spoofing identities when α and β equal to 30%

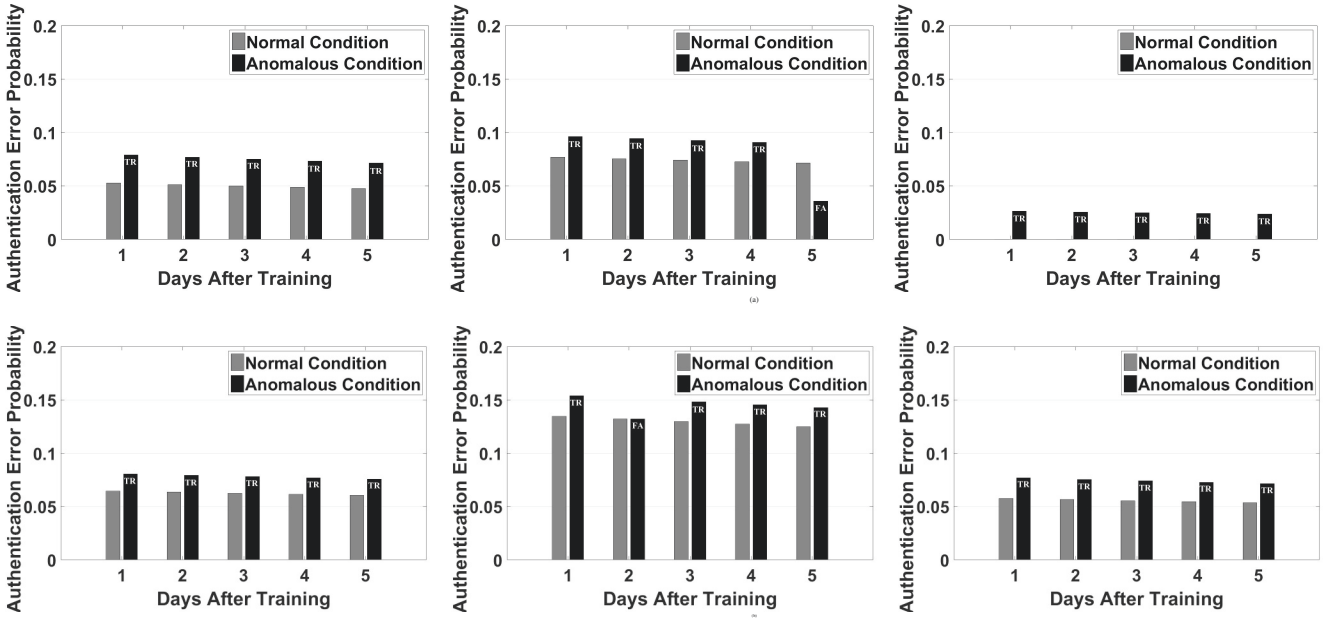

Figure 3. Biometric authentication probability(TR + FR) under DBSCAN with spoofing identities when α and β equal to 50%

V. Conclusion

We have proposed integration of machine learning-based continuous identification of users with smartphones by using contextual data generated by mobile social networking applications. We have particularly considered five popular social networking applications, namely Facebook, LinkedIn, Twitter, WhatsApp and Skype. Furthermore, we have augmented social contextual data with location information obtained from the built-in GPS sensors of smartphones. As the system is proposed against identity spoofing on mobile platforms, we have tested the performance of the proposed framework under scenarios where artificial noisy patterns have been injected to the regular contextual data of the users. Our results on real collected data show that the users with high social activity and sociability factor (i.e. longer session duration on social networks) are highly identifiable (up to 100%) under normal condition whereas the users that are less active can be identified with a success ratio between 80%-95% depending on various factors including the correlation between their sociability factor (i.e. session duration) and social activity rate (data usage). We have further shown that in the presence of noisy patterns (i.e. spoofed identities), when past and recent sociability metrics contribute equally to the current sociability metrics (i.e., inputs of machine learning procedures), user identification can still be as accurate as 94%.

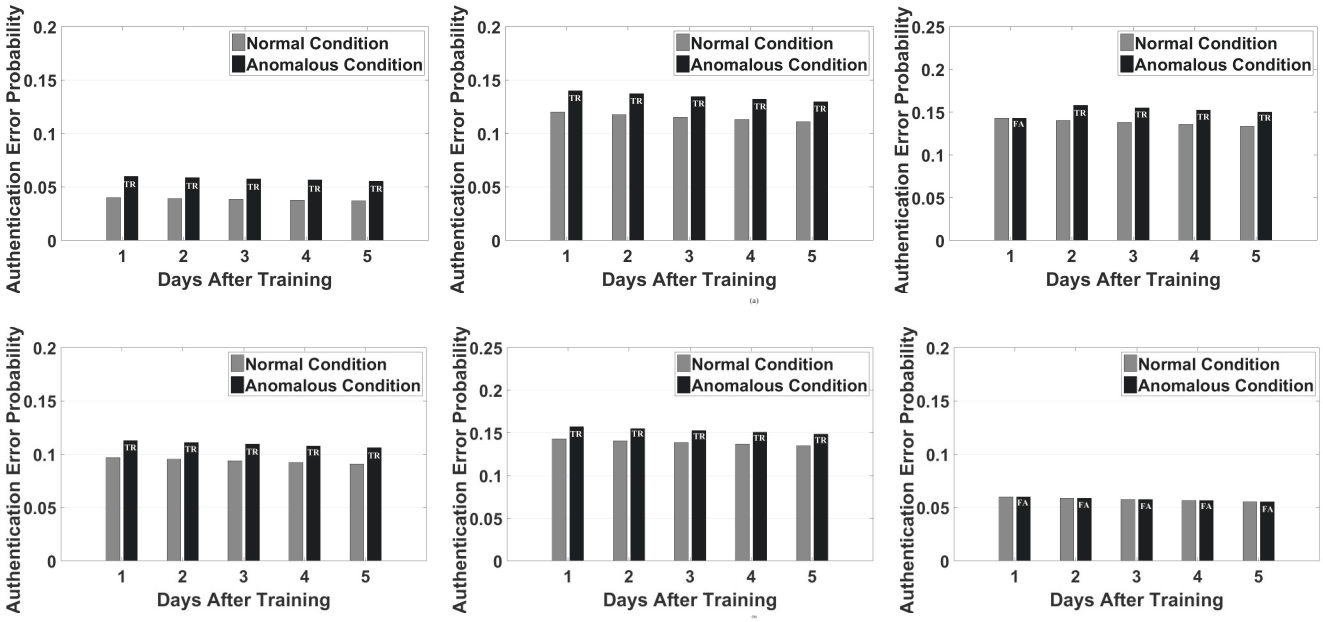

Figure 4. Biometric authentication probability(TR + FR) under DBSCAN with spoofing identities when α and β equal to 70%

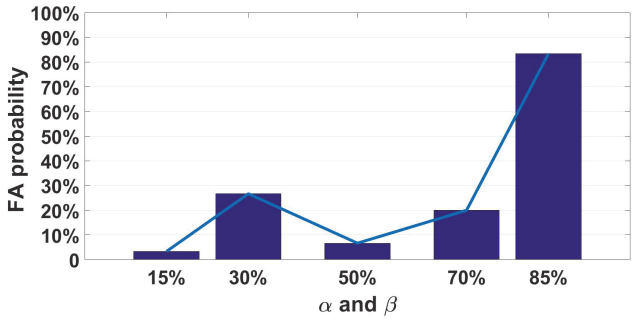

Figure 5. System performance for different settings for α and β over all users under 30 noisy instances.

ACKNOWLEDGMENT

This material is based upon works supported by the Center for Identification Technology and Research (CITeR) and the U.S. National Science Foundation (NSF) under Grant Numbers IIP-1068055 and CNS-1464273, and a gift from Qualcomm.

REFERENCES

[1] "Ericsson mobility report," ITU, 2016. [Online]. Available: http://www.ericsson.com/res/docs/2015/ericsson-mobility-report-june-2015.pdf

[2] F. Anjomshoa, M. Catalfamo, D. Hecker, N. Helgeland, A. Rasch, B. Kantarci, M. Erol-Kantarci, and S. Schuckers, "Mobile behaviometric framework for sociability assessment and identification of smartphone users," in *IEEE Symp. on Computers and Communications*, 2016, pp. 1084–1089.

[3] H. Zhang and M. Li, "Security vulnerabilities of an remote password authentication scheme with smart card," in *Intl. Conf. on Consumer Electronics, Communications and Networks*, 2011, pp. 698–701.

[4] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," *IEEE Communications Surveys & Tutorials*, vol. 17/3, pp. 1268–1293, 2015.

[5] A. Dantcheva, P. Elia, and A. Ross, "What else does your biometric data reveal? a survey on soft biometrics," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 3, pp. 441–467, 2016.

[6] M. Sultana, P. P. Paul, and M. Gavrilova, "A concept of social behavioral biometrics: Motivation, current developments, and future trends," in *Intl. Conf. on Cyberworlds*. IEEE, 2014, pp. 271–278.

[7] S.-W. Lee and K. Mase, "Recognition of walking behaviors for pedestrian navigation," in *Control Applications, 2001.(CCA'01). Proceedings of the 2001 IEEE International Conference on*. IEEE, 2001, pp. 1152–1155.

[8] H. Lv and W.-Y. Wang, "Biologic verification based on pressure sensor keyboards and classifier fusion techniques," *IEEE Transactions on Consumer Electronics*, vol. 52, no. 3, pp. 1057–1063, 2006.

[9] F. Al-Turjman, "Impact of user's habits on smartphones' sensors: An overview," in *HONET-ICT International IEEE Symp.*, 2016, pp. 70–74.

[10] R. V. Yampolskiy and V. Govindaraju, "Behavioural biometrics: a survey and classification," *Intl. J. of Biometrics*, vol. 1/1, pp. 81–113, 2008.

[11] X. Chen, R. Chandramouli, and K. P. Subbalakshmi, "Scam detection in twitter," in *Data Mining for Service*. Springer, 2014, pp. 133–150.

[12] A. Louni, A. Santhanakrishnan, and K. Subbalakshmi, "Identification of source of rumors in social networks with incomplete information," *arXiv preprint arXiv:1509.00557*, 2015.

[13] M. Sultana, P. P. Paul, and M. L. Gavrilova, "Online user interaction traits in web-based social biometrics," *Comput Vis Image Process Intell Syst Multimedia Technol*, pp. 177–190, 2014.

[14] M. Sultana, P. P. Paul, and M. Gavrilova, "Social behavioral biometrics: An emerging trend," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 29, no. 08, p. 1556013, 2015.

[15] B. Kantarci, M. Erol-Kantarci, and S. Schuckers, "Towards secure cloud-centric internet of biometric things," in *IEEE 4th Intl. Conf. on Cloud Networking*, 2015, pp. 81–83.

[16] A. S. Crandall and D. J. Cook, "Behaviometrics for identifying smart home residents," in *Human Aspects in Ambient Intelligence*. Springer, 2013, pp. 55–71.

[17] A. B. Budurusubmi and S. S. Yau, "An effective approach to continuous user authentication for touch screen smart devices," in *IEEE Intl. Conf. on Software Quality, Reliability and Security*, Aug 2015, pp. 219–226.

[18] N. Vaswani, A. R. Chowdhury, and R. Chellappa, "Activity recognition using the dynamics of the configuration of interacting objects," in *IEEE Computer Soc. Conf. on Computer Vision and Pattern Recognition*, vol. 2, June 2003, pp. 633–640.

[19] "Trackmaison data set and user traits," Online, 2016. [Online]. Available: http://nextconlab.academy/CITER/

[20] D.-G. Shin and M.-S. Jun, "Home iot device certification through speaker recognition," in *2015 17th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2015, pp. 600–603.