User Recognition From Social Behavior in Computer-Mediated Social Context

Madeena Sultana, *Student Member, IEEE*, Padma Polash Paul, and Marina L. Gavrilova, *Member, IEEE*

***Abstract*—Social interactions are integral part of human behavior. Although social interactions are likely to possess unique behavioral patterns, their significance for automated user recognition has been noted in the scientific community only recently. This paper demonstrated that it is possible to generate a set of unique features, called social behavioral (SB) features, from the social interactions of individuals' via an online social network (OSN). Specifically, this research identified a set of SB features from the online social interactions of 241 Twitter users and proposed a framework to utilize these features for an automated user recognition. Extensive experimentation demonstrated high recognition performance as well as distinctiveness of the proposed SB features. The most striking finding was that only ten recent tweets are enough to recognize 58% of users in our database at rank-1. The rank-1 recognition rate dramatically increased to 93% when 60 tweets were used as a probe set. Experimental results also demonstrated the stability of the proposed SB feature set over time and ability to recognize both frequent and nonfrequent OSN users. This confirms that human social behavior expressed through an OSN can provide a unique insight into user behavior recognition.**

***Index Terms*—Biometric security, human–machine interaction, information fusion, nonverbal behavior analysis, situation aware authentication, social behavioral (SB) biometrics, social context, user recognition.**

I. Introduction

SOCIAL interactions of human beings have expanded from a face-to-face communication to computer-mediated format, signifying the era of online social networks (OSNs). The growing population of social media users is in excess of 2 billion, which is more than two-thirds of the global online population [1]. According to ComScore report, Internet users spend approximately 1 of every 5 online minutes on social networking sites [2]. The unprecedented rise of the social networks and interactive human–machine environments provides a massive platform for analyzing human behavior in a computer-mediated context. This research aims to study the behavioral pattern of social interactions expressed via OSNs for user behavior recognition.

Behavioral patterns are unique credentials of a user's identity [3]. Over the last decade, patterns of human behavior, expressed through human–computer interactions (keyboard, mouse, touchscreen, smartboards, etc.), received enormous attention from researchers who study an individual identification [4], [5], [6]. The latest research revealed that even the aesthetic preferences such as favorite set of photographs can help to recognize a user [7]. And yet an essential aspect of human behavior remained the social interactions remained largely unexplored from the biometric point of view. The finding presented in this paper fills the gap by conducting a thorough study of human social interactions from a point of view of behavioral biometrics. In other words, "how humans socially interact" in a given social context is dictated by personal behavioral characteristics that can distinguish a user from another. This paper demonstrates uniqueness, permanence, and accuracy of human social interaction-based features in a given social context. This research also exploits these features for user authentication in the framework of a behavioral biometric research.

Individuals' social contacts, interactions, interests, emotions, perceptions, and connections may exhibit habitual patterns as well as behavioral characteristics. Human brain can also exploit social cues to recognize familiar people [8]. The incorporation of social intelligence and awareness in computing machines has been identified as the ultimate need of the next-generation intelligent systems [9], [10]. The recent inventions of social robots and humanoid virtual assistants [11], [12] are paving the way toward socially intelligent computing systems. In a biometric research domain, Jain *et al.* [13] recently conceptualized the future biometric system utilizing ubiquitous sources of information for decision making. In accordance with this trend, the next-generation biometric systems should be equipped with an ability to analyze social behavior and context, acquiring new knowledge, and incorporating the inference of social knowledge during the human-assisted intelligent decision-making process. Fig. 1 shows a possible authentication scenario of an intelligent biometric system, which incorporates human behavior analysis and behavioral change detection to make the system more aware and attuned to the current situation. Therefore, the aim of this research is to move one step closer to the next-generation situation aware biometric system by analyzing human social behavior in a given context as a source of authentication information. Socially intelligent biometric systems can be further integrated with interactive human–machine systems (HMS), such as humanoid

Manuscript received February 28, 2016; revised September 8, 2016; accepted January 9, 2017. Date of publication April 3, 2017; date of current version May 15, 2017. This work was supported in part by the NSERC DISCOVERY program under Grant RT731064, in part by the URGC, in part by the NSERC ENGAGE, in part by the NSERC Vanier CGS, and in part by Alberta Ingenuity. This paper was recommended by Guest Editor L. Chen.

M. Sultana and M. L. Gavrilova are with the Department of Computer Science, University of Calgary, Calgary, AB T2N 1N4, Canada (e-mail: msdeena@ucalgary.ca; mgavrilo@ucalgary.ca).

P. P. Paul is with the University of Oxford, Oxford, OX1 3PA, U.K. (e-mail: pppaul@ucalgary.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/THMS.2017.2681673

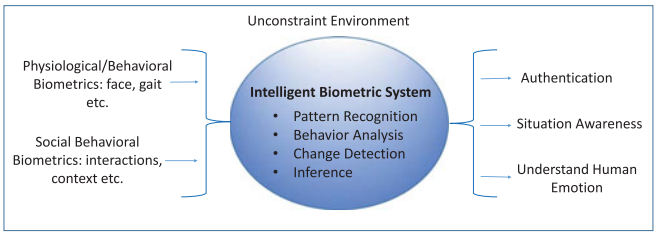

Fig. 1. Conceptual representation of a future-generation intelligent biometric system based on the traditional biometrics as well as the social behavior analysis for user authentication, situation awareness, and emotion interpretation.

virtual assistants [14], nursing robots [15], companion robots, smart homes [11], as well as with the traditional biometric-based access control systems [16], [17].

As an emerging research direction, integrating social behavior with the traditional security systems has a unique set of challenges. Unlike well-established traditional biometrics (e.g., face, fingerprint, signature), the social behavioral (SB) patterns of social interactions are not well understood. The crucial challenge is to identify a set of SB features that exhibits repeated pattern over certain period of time and is differentiating enough for user behavior recognition. Our preliminary study identified a subset of SB features and applied them for user recognition on a small dataset of 50 Twitter users [18], [19]. While the initial result was encouraging, the primary feature set used in these works was unweighted and not very distinctive. An initial dataset of 50 users was sparse (users were not socially connected) and contained only prolific users who produced more than 100 tweets per week. The applicability of SB features to nonprolific OSN users was not addressed. In addition, some critical questions such as how much social data is needed to be collected to recognize a user, how long such behavior will remain stable, what if the users are densely connected, and whether the temporal information exhibits behavioral characteristics were to be addressed as well. This paper answers the above questions by establishing the properties of uniqueness, stability, and accuracy of an enhanced set of features on a new, diverse (includes prolific and nonprolific users), and dense (socially connected) database (DB) of 250 OSN users. The following research questions are at the focus of our investigation.

1) Can a user be recognized or verified from their social interactions/activities via an OSN?

2) Do SB features obtained from an OSN possess uniqueness and stability?

3) Can this methodology be applied to nonfrequent OSN users?

4) How does the amount of collected social data affect discriminating behavior of SB features?

The contributions of this research are

1) an enhanced SB feature set incorporating weights and temporal information to model SB biometrics of users;
2) a new framework can profile a social behavior of users by creating large social network and a new matching method for user recognition;
3) evaluation of three biometric properties (accuracy, uniqueness, and stability) of the proposed SB features is supported by extensive; and
4) a data quality study is performed on a dataset with nonfrequent OSN users and a limited amount of information in a probe set.

To the best of our knowledge, this is the first comprehensive study of social interactions via OSN as a behavioral biometric, paving the way toward socially intelligent situation aware human-computing systems.

II. Relevant Work

Behavior biometric authentication is a rapidly evolving and a diverse field of research. It considers dynamic behavioral patterns instead of more permanent physiological characteristics [13], [20]. Behavioral biometrics are also quite sensitive to changes one undergoes through the lifetime [21]. On a positive side, the dynamic nature of behavioral biometrics can make them more difficult to forge [22]. In addition, acquisition of behavioral biometric is often passive (does not require co-operation from the user) and no extra sensors are typically needed to be deployed [22]. Naturally, some behavioral biometrics are more suitable for being applied in specialized domains, such as virtual worlds [23]. As a result, the focus of behavioral biometrics is rapidly expanding—comprising a wide variety of human behaviors ranging from muscle-actions to human–computer interactions. Diverse examples of contemporary behavioral biometrics are motion direction in an office environment [24], handshaking style [25], mobile device pick-up motion [26], singing sounds [27], spatio-temporal logs [28], etc. Among the latest additions to the behavioral biometrics are the personality-based traits that incorporate habits, communication, and even aesthetic preferences [3], [7], [18]. This emerging trend is the focus of interest of this paper, where users' preferences, habits, and communication patterns are being used to distinguish users from each other in the context of biometric research.

We now provide a brief review of some key works in the emerging personality-based behavioral biometrics domain. Jiang *et al.* [29] studied habitual patterns of decorating and typing styles of 225 people in a virtual game environment. This research reports that players have unique and steady habitual patterns in choosing style, color, position, and order of objects, which make them suitable to serve as a behavioral biometric trait. Another study by Olejnik and Castelluccia on 4578 users [23] demonstrates that the browsing history of a user exhibits personal preference and is unique enough to reveal the identity of the user. A similar research by Lovato *et al.* [7] on 200 subjects shows that every user has his very own preference in choosing and appreciating photographic images. The behavioral patterns of nonverbal communications (i.e., emoticons, word counts, word lengths, answer time, speed, etc.) during chat conversations have been studied by Roffo *et al.* [30]. This research on 94 individuals demonstrated that using such nonverbal communication as behavioral biometrics results in the high accuracy of recognition. And in 2015, researchers showed that fusing

social context can enhance the performance of facial recognition [31].

From the aforementioned works, it is evident that researchers are aiming at capturing individuals' personality traits and to analyze those as promising candidates for behavioral biometrics. This paper takes this research direction one step further by studying computer-mediated social interactions as a new behavioral biometric.

III. Concept of Social Behavioral Biometrics

Human social interactions are of interest for researchers from domains as diverse as social science, psychology, neuroscience, organizational behavior, and marketing. There is a rapidly increasing demand for social behavior profiling, expressed via online social media, in order to determine purchasing capabilities and preferences of users for various business applications (targeted advertisement [32], recommendation systems [33], [34]). Social signal processing recently emerged as a domain studying the nonlinguistic social cues extracted from body posture, intonation, facial expression, and gestures [10], [35]. In addition, other forms of human communications, such as voice, eye movement, head tilt, actions, and interactions with HMS as well as spatio-temporal information have been studied for the purpose of the development of intelligent equipment and sensors [36], [37]. Despite the growing interest, the use of social behaviors for biometric authentication remained largely unexplored. In order to investigate users' social behavior as a potential behavioral biometric, the concept of SB biometric was introduced in [38]. The idea is to model social behavior of individuals based on their idiosyncratic social interactions in a given social setting or social context. The definitions of SB biometrics and corresponding social settings are presented below.

1) *Definition of SB biometrics* [38]: SB biometrics are the social interactions and communication of an actor (user or avatar) in different social contexts that exhibit idiosyncratic characteristics of the actor's social behavior.
2) *Definition of social context* [38]: Social contexts for studying SB biometrics are environments and their properties that dictate the manner of communication as well as interactions between actors.

The social context is divided into two categories: offline and online [38]. Offline social context may include a focus group, a meeting room, or any physical place of social gatherings. The offline social interactions may take place during the process of collaborative activities on a project or a creative art piece. In [38], Sultana *et al.* proposed to analyze such collaborative datasets from the perspective of SB biometrics with the aim of discovering idiosyncratic behaviors of users. For instance, a user's intonation during conversations can be analyzed with the goal of recognizing users' emotions or a state of mind from the audio signals acquired during meetings. Such social cues may act as an SB biometric trait to authenticate the user's identity in a known social context, even under challenging (noisy, low data quality) environment.

Online social contexts are the web-based platforms that allow social interactions among users, such as blogs, posts, discussion forums, online games, social networks, multimedia sharing sites, etc. It is possible to observe repetitive patterns in a user's social interactions via online context since they are driven by repeatable human behaviors and habits. Furthermore, the analysis of social data may reveal valuable information, such as personal interests, preferences, communication patterns, spatio-temporal information, etc. The research presented in this paper demonstrates that a systematic analysis of the social interactions of individuals in a popular online social networking platform can be used for user authentication as a SB biometric.

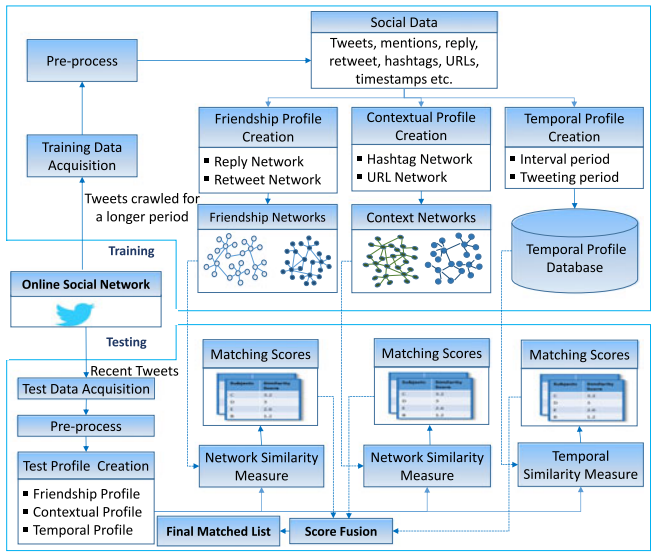

Fig. 2. Proposed framework of SB biometric system: the training features are generated from social data collected over longer periods, the test features are created from the recent tweets, and the final matched list is obtained by fusing all similarity scores of training and testing features at score level.

IV. Methodology

In this section, a methodology for modeling social interactions of users via OSN is presented. Twitter is chosen as the source of social interaction-based data. Twitter is a popular online social networking platform, which enables users to interact with their acquaintances by posting real-time microblogs called tweets. Unlike other mediums, tweets are restricted to 140 characters of length. Despite limitation on size, tweets act as a rich source of information about users and their interpersonal communicative behavior. Usually, one can extract four types of information from microblogs or tweets: content of the text (vocabulary, lexicons, capitalization, punctuations, structure of sentences, etc.), context of the text (hashtag, shared weblinks or URLs, images, etc.), interpersonal interactions (reply, retweet, etc.), and spatio-temporal information (timestamp, geolocation, etc.). Though recent study shows that content-based information of the microblogs can be useful to identify an author from a small set of twitter users [39], the contextual, interpersonal communications, and spatio-temporal social data remained under investigated from a biometric perspective. This paper presents a methodology for utilizing selected twitter features as social behavior for biometric user recognition. Fig. 2 shows a flow

TABLE I
TWITTER TERMINOLOGIES

Term	Description
Tweet	Real-time microblogs posted by users in Twitter.
Reply	Tweets posted by the user of interest in reply to another user's tweets (e.g., @user_abc) [41].
Mention	Tweets where other usernames are mentioned (e.g., @user_abc).
Retweet	Tweets, originally written by a user but posted or shared by other users in their timelines (e.g., RT@user_abc) [38].
Hashtag	Shorthand convention, preceded by # symbol, adopted by Twitter users for assigning their posts to a wider corpus of messages on the same topic [38].
URL	Weblinks shared by users in timelines. A user can direct his followers to a news article, blog post, website, video, or photograph by sharing a URL.
Timestamp	The time of posting a tweet in DD:MM:YY HH:MM:SS AM/PM format.

diagram of the proposed method. Following sections contain detailed descriptions of the major building blocks of the proposed method: data collection, social profile creation, and similarity matching.

A. Data Collection and Preprocessing

Initially, there are ten randomly selected Twitter users. Considering these ten users as an initial seed, the method randomly selects four more users for each of the initial seed users' acquaintances (from the list of following and followers). Next, considering the resulting group of 40 users as a new seed set, the method randomly selected additional 200 users who are the seed set acquaintances. The reason for seeding is to create a dataset where users have many mutual acquaintances in their followings and followers. The resulting dataset contains 250 users. Only publicly available user profiles are being selected to be crawled; therefore, no privacy considerations exist for this collection. In addition, the dataset is stored in an anonymous form without any identifying information of the users. Tweets are then crawled from each of the 250 users' timelines. An open source social network analyzing tool NodeXL [40] has been used to crawl data from Twitter. The data collection process was continued in four separate sessions over a period of four months, with elapsed time between two successive sessions of 4–6 weeks. The intervals allow us to reduce the amount of overlapped data in two successive sessions. Every session contains approximately 200 recent tweets per user. In this paper, we denote sessions as S_i, where $i = 1, 2, 3, 4$. The sessions are numbered according to the sequence of data acquisition. Therefore, session 4 contains the newest 200 tweets of each user, whereas session 1 comprises of the oldest 200 tweets per user. The 200 tweets per user in each session contain the most recent social interactions of each user via Twitter, such as mentions, replies, shared hashtags, shared URLs, and timestamps. Table I contains brief descriptions of these terminologies. After crawling, we preprocess tweets as follows.

1) For every user in each session, parse the list of replied, mentioned, retweeted acquaintances, hashtags, and URLs along with the corresponding frequency of occurrences and timestamps.
2) For each user, extract timestamps of the posts in every session.
3) Discard all other identity-related information, such as location, date of birth, time zone, personal weblink, etc.
4) Remove overlapped data from the four sessions.

B. SBB Profile Creation

The crucial task after data collection is to identify a set of content-independent or nonverbal features that contains behavioral characteristics of users. We consider three types of information to create the feature set: interpersonal interactions (replied, retweeted, and mentioned acquaintances), contextual information (shared hashtags and URLs), and temporal information (timestamps of posts). From the aforementioned information, the following three types of profiles are created for each user.

1) Friendship Profile: The biological constrains on human cognition suggest that a user can maintain stable social relationships with only 100–250 acquaintances, which is known as Dunbar's number [42]. Research shows that this theoretical cognitive limit holds for OSN users as well, even though OSNs allow users to have few thousands of social connections [43]. This provides the basis for an assumption that the smaller set of acquaintances with whom a user maintains stable relationships may possess behavioral characteristic of the user. We propose to create profile of users based on their active interactions, such as reply, mention, and retweet. Next, we mine the small set of acquaintances from the active interactions of users in Twitter and assign a relationship between them. The proposed friendship profile consists of two features: reply/mention network and retweet network.

Reply Network: The acquaintances, whom the user replies and mentions frequently as well as regularly, are added to the weighted network called a reply network. In this network, the nodes are the set of users and their replied acquaintances; the edges are created based on the "reply" relationship. For instance, if user A replies to user B, an edge between A and B is created and assigned "reply" relationship. Next, log-frequency weights are assigned to the edges calculated from the occurrences of the relationship in the corpus (profile). Algorithm 1 outlines the process of creating the reply network. The log-frequency weight is calculated using [44] the following equation:

$$W_t = 1 + \log(\mathrm{TF}_{t,d}) \tag{1}$$

where TF is the term frequency of edge *t* in profile *d*.

Retweet Network: A user also retweets a small set of acquaintances in his timeline. A weighted network has been created containing retweeted acquaintances of users. The network creation process is similar to that for a reply network. Here, the nodes are the set of users and their retweeted acquaintances; edges represent "retweet" relationship and edge weights are the log frequencies (1) of the occurrences of each relationship in the corpus.

Fig. 3(a) and (b) show the visual representations of a portion of the generated reply network and retweet network, respectively, created from session 1. The color-coded clusters

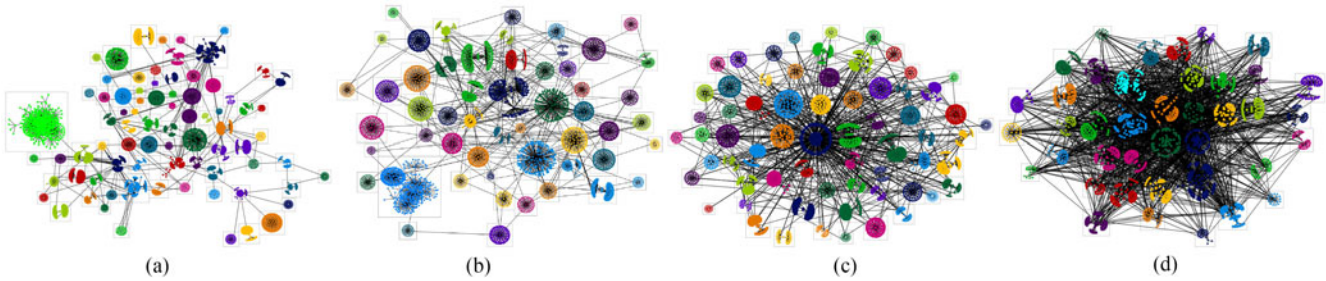

Fig. 3. Visual representation of a portion of (a) reply network, (b) retweet network, (c) hashtag network, and (d) URL network created from session 1; clusters in different colors show densely connected components (community) representing "reply," "retweet," "hashtag," and "URL" relationships of users, respectively; edges between clusters show the common replied acquaintances, retweeted acquaintances, hashtags, or URLs between two communities of the respective network; graphs are created using Harel–Koren fast multiscale layout and clustered using Wakita Tsurumi clustering tool of NodeXL.

Algorithm 1: $Creating\_Friendship\_Profile(S, U, arg)$; $arg = \{Reply, Retweet\}$.

Input: Preprocessed dataset S_{ij}, where $i = 1, 2, .., M$, $j = 1, 2, ., N$, S_{ij} contains list of replied (R) or retweeted (RT) acquaintances of user j from session i and U_j is a list of subjects in dataset.
Output: Weighted network $G_i(V, E, W)$ of arg, where V is a set of nodes, E is a set of edges, and W is a set of corresponding edge weights.
Iterate: $i = 1\,to\,M$
1) Initialize empty graph $G_i(V, E, W)$ and $k \leftarrow 1$
2) Iterate: $j = 1\,to\,N$
   a) $G(V_k) \leftarrow U_j$, assign user U_j as a node in network G
   b) $k \leftarrow k + 1$
   c) $S_y \leftarrow unique(S_{ij})$, find S_y, a set of unique elements in S_{ij}
   d) Iterate: $z = 1\,to\,length(S_y)$
      i) If S_{yz} does not exists in $GG(V_k) \leftarrow S_{yz}$, assign each S_{yz} as a node in network G, $k \leftarrow k + 1$
      ii) $E(V_{jz}) \leftarrow 1$, create an edge between U_j and S_{yz} in G
      iii) $TF_z \leftarrow count(S_{yz})$, count the number of occurrences of S_{yz} in S_{ij}
      iv) $Y_j \leftarrow unique(U_j)$, find Y_j, a set of unique elements in U_j
      v) $Sd \leftarrow S_d \cup Y_j$, find S_d, a set of unique elements in whole dataset
      vi) $W(E_{jz}) \leftarrow 1 + log(TF_z)$, assign log frequency weight to edge Ejz
   End iteration
End iteration
End iteration

in Fig. 3(a) and (b) represent densely connected components (community) in the corresponding graphs showing the density of the "reply" and "retweet" relationships of users, respectively, whereas the edges between clusters show the common replied and retweeted acquaintances between two communities in the respective networks.

2) Contextual Profile: The contextual information from tweets, such as shared hashtags and weblinks often, represents a user's interest and preferences. We propose to create contextual profiles of users based on the shared hashtags and URLs in order to explore their sharing patterns and interests. Therefore, the proposed contextual profile consists of the following features.

Hashtag Network: We propose to explore users' hashtag sharing behavior, a small set of hashtags frequently shared by a user, by creating a hashtag network. Four hashtag networks have been created by accumulating all hashtags shared by all users in our DB for four sessions. The nodes of this network are the users and shared hashtags; the edges are created based on "hashtag" relationship. For instance, if user A shares a hashtag #h1, we create an edge between A and h1. However, along with self-created hashtags, people use popular hashtags as well. Therefore, we apply TF-IDF weights in order to assign more weights to uncommon hashtags, while reducing the weights of common hashtags. The process of creating hashtag network is outlined in Algorithm 2. The TF-IDF weight is calculated using the following equation [44]:

$$W_t = (1 + \log(\mathrm{TF}_{t,d}))\log(N/\mathrm{DF}_t) \quad (2)$$

where TF is the term frequency of each edge *t* in profile *d*, *N* is the number of users' profiles in dataset, and DF is the document frequency, i.e., number of occurrences of edge *t* in *N* users' profiles.

URL Network: Similar to the hashtag network, we propose to create URL network for each session to reveal users' preferred domains and sharing patterns. However, some domains such as YouTube, Facebook, Instagram, Google, etc. are very common and shared by many users frequently. Therefore, similar to hashtag network, TF-IDF weights are applied to edges of URL network. The network creation process is outlined in Algorithm 2.

Fig. 3(c) and (d) show visual representations of a portion of the generated hashtag and URL networks, created from session 1. The color-coded clusters shown in Fig. 3(c) and (d) represent densely connected components (community) showing the density of "hashtag" and "URL" relationships of users in the respective networks. An edge between two clusters in Fig. 3(c)

Algorithm 2: $Creating\_Contextual\_Profile(S, U, arg)$; $arg = \{Hashtag, URL\}$.

Input: Preprocessed dataset S_{ij}, where $i = 1, 2, .., M$, $j = 1, 2, ., N$, S_{ij} contains list of shared hashtags (H) or URLs of user j from session i and U_j is a list of subjects in dataset.
Output: Weighted network $G_i(V, E, W)$ of arg, where V is a set of nodes, E is a set of edges, and W is a set of corresponding edge weights.
Iterate: $i = 1\,to\,M$
1) $Y_i \leftarrow unique(S_i)$, find Y_i, a set of unique elements in session S_i
2) Iterate $z = 1\,to\,length(Y_i)$
   a) $DF_z \leftarrow count(Y_z)$, count the number of occurrences of Y_z in S_i
End iteration
End iteration Iterate: $i = 1\,to\,M$
1) Initialize graph $G_i(V, E, W)$ where $V \leftarrow U \cup Y_i$
2) Iterate: $j = 1\,to\,N$
   a) $S_y \leftarrow unique(S_{ij})$, find S_y, a set of unique elements in S_{ij}
   b) Iterate: $z = 1\,to\,length(S_y)$
      i) $E(V_{jz}) \leftarrow 1$, create an edge between U_j and S_{yz} in G
      ii) $TF_z \leftarrow count(S_{yz})$, count the number of occurrences of S_{yz} in S_{ij}
      iii) $W(E_{jz}) \leftarrow (1 + log(TF_z)) \times \log(\frac{N}{DF_z})$, assign TF-IDF weight to edge Ejz
      End iteration
   End iteration
End iteration

or (d) shows that both communities share the same hashtag or URL in the respective network. Fig. 3(c) also shows that the communities of hashtag network are densely connected, i.e., share a number of common hashtags, which justifies the use of TF-IDF weights. As shown in Fig. 3(d), the communities of URL networks are more densely connected than hashtag network, justifying the use of TF-IDF weights.

3) Temporal Profile (TP): We propose to create TP of users to explore their posting patterns in the social network. The collected four sessions contain data of few consecutive days of each user. However, the number of weeks or days in different users' data vary based on users' frequencies of posts. The tweeting and interval periods of users' microblogging can be extracted by analyzing the temporal data as follows.

Seven Days Interval Period: Twitter users may have different interval patterns on weekdays and weekends as well as during days and nights. We calculate a (7×1440) feature matrix (I) to capture the regular interval pattern of each user as follows:

$$I_{lq} = \begin{cases} 1, & \text{interval} \\ 0, & \text{Tweet} \end{cases} \tag{3}$$

where $l = 1, 2, 3, \ldots, 7$ (7 days) and $q = 1, 2, 3, \ldots, 1440$ (min/day). Initially for each user, we create matrix (H) of size

Algorithm 3: $Get\_Interval\_Time(Hj)$.

Input: N number of histogram matrices $H_j | j = \{1, 2, .., N\}$ of size $(7 \times 1440 \times P)$.
Output: Boolean I_j matrix of size (7×1440).
Iterate: $j = 1\,to\,N$ //N=total number of users
1) Initialize T of size (7×1440), where $T_{lq} \leftarrow 1$
2) Iterate: $z = 1\,to\,P$ //P=total number of weeks in H_j
   a) Iterate: $l = 1\,to\,7$
      i) Iterate: $q = 1\,to\,1440$
         A) If $H_j(l, q, z) = 0$, $Temp(l, q) \leftarrow 1$
         B) Else $Temp(l, q) \leftarrow 0$
      End iteration
      End iteration
   b) $T \leftarrow T \wedge Temp$ //logical AND operation
      End iteration
3) $I_j \leftarrow T$
End iteration

$(7 \times 1440 \times P)$, where *P* is the total number of weeks present in each user's session S_{ij} and *H* is the histogram of the number of tweets in 1440 min per 7 days per *P* weeks. Next, we create I_j using H_j as input, where the value I_{lq}=1 indicates that the jth user never tweeted at lth day qth minute for *P* weeks and vice versa. The process is outlined in Algorithm 3.

Seven Days Tweeting Period: Twitter users may have different posting (tweeting) times during weekdays, weekends, days, and nights. However, the tweeting pattern is not as consistent as an interval pattern. The reason is probably the massive use of smart phones and portable devices to access the social media, which allows users to tweet anytime from anywhere. Therefore, we considered the time periods when the tweeting probability is greater than a threshold (Th) to reduce overlap in tweeting time of different users. The calculation of the feature vector *T* of size (7×1440) to capture regular tweeting pattern of each user is as follows:

$$T_{lq} = \begin{cases} 1, & \#\text{Tweet} \geq \text{Th} \\ 0, & \text{interval} \end{cases} \tag{4}$$

where $l = 1, 2, 3, \ldots, 7$ (7 days) and $q = 1, 2, 3, \ldots, 1440$ (min/day). The threshold value has been chosen empirically as $\text{Th} = P/3$, where *P* is the total number of weeks in S_{ij}. T_j is calculated using H_j as input, where the value T_{lq}=1 indicates that the jth user tweeted at lth day qth minute for at least 1/3 of *P* weeks. The process is outlined in Algorithm 4.

C. Similarity Measure

Similarity measure techniques are applied to each type of features in order to find similarities between testing and training profiles of users. For the similarity matching of friendship and contextual profiles, the method performs lookup of the nodes in the corresponding training network and extracts a small set of candidates that have common edges with the lookup nodes. Then, the similarity score (S_{Tr}) between each candidate's train

Algorithm 4: $Get\_Tweeting\_Time(Hj)$.

Input: N number of histogram matrices $H_j|j = \{1, 2, .., N\}$ of size $(7 \times 1440 \times P)$.
Output: Boolean T_j matrix of size (7×1440).
Iterate: $j = 1\,to\,N$ //N=total number of users
1) Initialize variable $Temp$ of size (7×1440), where $Temp_{lq} \leftarrow 0$
2) $Th = P/3$
3) Iterate: $l = 1\,to\,7$
   a) Iterate: $q = 1\,to\,1440$
      i) sum=0 // summation of Tweets at l^{th} day and q^{th} minute for P weeks
      ii) Iterate: $z = 1\,to\,P$
         A) $sum \leftarrow sum + H_j(l, q, z)$
            End iteration
      iii) If $sum > Th$, $Temp(l, q) \leftarrow 1$
      End iteration
   End iteration
4) $T_j \leftarrow Temp$
End iteration

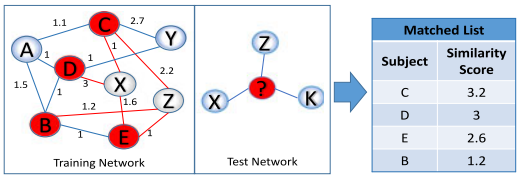

Fig. 4. Example of similarity matching of network-based profiles. The lookup nodes (X and Z) are depicted in gray color in training network. The red nodes in training network are the possible candidates of the correct match. Finally, matched candidates are ranked based on the similarity score of the relationships (edges) of the lookup nodes.

network (N_{Tr}) and test network (N_T) is calculated as follows:

$$S_{Tr} = \sum_{e \in E\{N_T \cap N_{Tr}\}} W_e \tag{5}$$

where $E\{N_T \cap N_{Tr}\}$ is the set of edges (relationship) between the common nodes of the test network and each candidate's train network, where W_e denotes the corresponding weight. Fig. 4 shows a simple example of this similarity matching process.

Equation (6) is used to calculate the similarity scores (S_p) between training (P_{Tr}) and testing (P_T) profiles of seven days interval period and tweeting period

$$S_P = \frac{\sum(P_T \cap P_{Tr})}{\sum P_{Tr}}. \tag{6}$$

Next, the similarity scores of the TP of users are calculated by taking the average scores of the interval and tweeting periods. Finally, the normalized similarity scores of retweet (RT), reply (R), hashtag (HT), URL, and TP are fused at score level for enhanced performance. Thus, the final similarity score S_f is the average score of all similarity values S_c, where $c \in$ {RT, R, HT, URL, TP}

$$S_f = \frac{\sum S_c}{\sum c}. \tag{7}$$

TABLE II
SUMMARY OF TWITTER DATABASE (DB)

Subset (DB_k)	Average number of tweets/week	Number of users	Percentage of total user (%)
DB_0	0–9	09	03.6%
DB_1	10–30	51	20.4%
DB_2	31–50	50	20.0%
DB_3	51–100	57	22.8%
DB_4	101–200	83	33.2%
Total (DB)	0–200	250	100%

V. EXPERIMENTAL RESULTS

This section presents the evaluation process for the performance of the proposed biometric user recognition system using SB features and answers the four research questions posed in the Section I. All experiments were carried out on Windows 7 operating system, 2.7 GHz Quad-Core Intel Core i7 processor with 16 GB RAM. MATLAB version R2015a was used for the implementation and experiments of the proposed method.

The DB contains 4 sessions of 250 Twitter users' data, where S_{ij} session ($S_{ij}|i = 1, 2, 3, 4; j = 1, 2, \ldots, 250$) denotes ith session containing approximately 200 tweets of user j. The average number of tweets per week of the 250 users is in the range of 0–200. Therefore, the DB contains frequent (prolific) as well as nonfrequent (nonprolific) Twitter users. One of the research questions is to investigate the applicability of the proposed SB features to nonfrequent OSN users. In order to do it, each session's data is separated into five subsets according to the average number of tweets per week in session 1. This allows us to distinguish between prolific and nonprolific users based on their weekly average interactions/posts in Twitter. The distribution of 250 users in 5 subsets (DB_0, DB_1, DB_2, DB_3, DB_4) is summarized in Table II.

The number of weeks or days in a session varies with the amount of weekly or daily interactions of the users. Fig. 5 shows a bar diagram of the range of weeks present in ith session S_i of kth subset ($DB_k|k = 0, 1, \ldots, 4$). Fig. 5 shows that DB_0 has the maximum amount of overlap (nearly 100%) between successive sessions, whereas DB_4 has the least overlap (0%). The reason for this is that the average number of weekly tweets of DB_0 dataset's users vary from 0 to 9. As a result, some users have no tweets over some weeks, which increases the amount of overlapped data between successive sessions. On the other hand, the average number of weekly tweets of DB_4 dataset's users vary from 101 to 200. Since the data collection period had intervals of four to six weeks, none of the four sessions of DB_4 has any overlap. In Fig. 5, one can see that the number of overlaps of the successive sessions of the database DB_k was reduced significantly with the increasing number of average weekly tweets of users. For instance, in Fig. 5, the amount of overlaps of the consecutive sessions of DB_1, DB_2, DB_3 have decreasing trend compared with DB_0 since the ranges of the average number of weekly tweets increased to 10–30, 31–50, and 51–100, respectively. We excluded DB_0 during experiment since majority of the users' sessions of this dataset overlap more

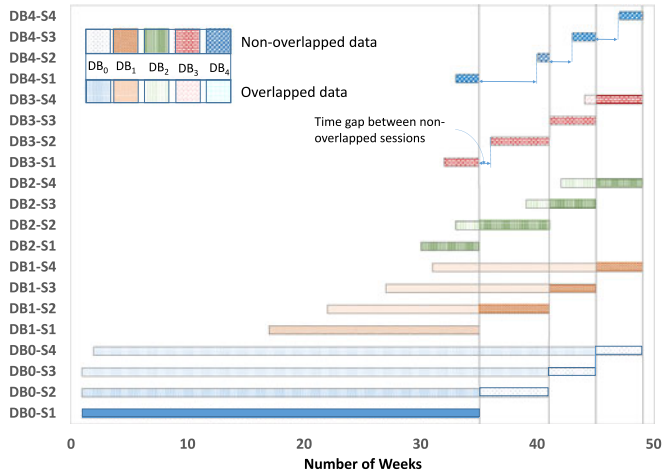

Fig. 5. Total number of weeks in session (S_i) of subdataset (DB_k), where each session contains on average 200 tweets per user; the darker region of each bar shows the amount of information/tweets present in each session (S_i) after removing overlapped data/tweets between two successive sessions (S_i, S_{i+1}); vertical lines show the end of each session S_i.

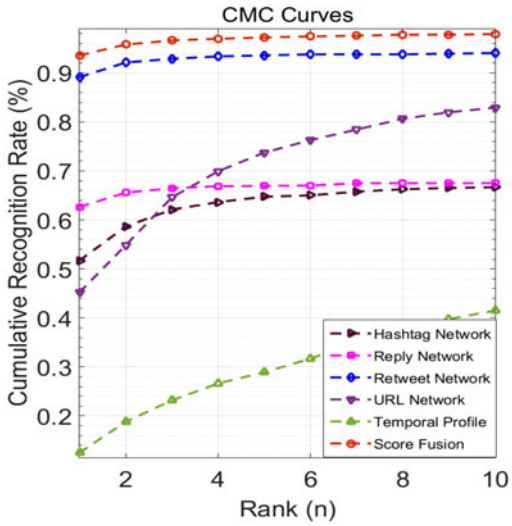

Fig. 6. CMC curves of hashtag, URL, retweet, reply, temporal features, and score fusion of all SB features on 241 users' of DB_5, where the average tweets of the users vary from 10 to 200; the curves are obtained by averaging all CMC curves of the cross validation of 4 sessions by 12 experiments. The six train and test set combinations are: S_1 versus S_2, S_1 versus S_3, S_1 versus S_4, S_2 versus S_3, S_2 versus S_4, and S_3 versus S_4.

than 95%, which made it inappropriate for creating separate training and testing sets. On the other hand, exclusion of DB_0 have nominal effect on the size of the total DB since it consists of only nine users which is only 3.6% of the whole DB. Finally, we created a dataset (DB_5=DB_1+DB_2+DB_3+DB_4) containing 241 users with 4 nonoverlapping sessions (S_1, S_2, S_3, S_4), where users' average tweets per week vary from 10 to 200. All user behavior recognition experiments are conducted in closed-set scenario, where the users are known in the DB [14].

A. *Experiment-1*

The first set of experiments is intended to evaluate the verification and identification performance in a closed-set scenario and the applicability of the proposed SB features to frequent and nonfrequent Twitter users. The closed-set identification rate will demonstrate the uniqueness of SB features in terms of distinguishing one user from another. We conduct the first set of experiments on our DB_5 dataset of 241 users. We cross validate the four sessions of data by creating six combinations of train and test sets: S_1 versus S_2, S_1 versus S_3, S_1 versus S_4, S_2 versus S_3, S_2 versus S_4, and S_3 versus S_4. The different combinations of train and test sets allow us to verify the persistence or stability of the features as well. For instance, the S_1 versus S_4 train and test set combination has at least 10 weeks of time interval and a high recognition performance on this set demonstrates persistence over 10 weeks. In total, 12 experiments are conducted with the 6 combinations of train–test sets on DB_5 to measure the closed-set identification and verification performance of the friendship, contextual, and temporal features as well as their score level fusion.

The closed-set identification performance of each feature and their fused form are analyzed by plotting cumulative match characteristics (CMC) curves. CMC curves plot the cumulative probability of obtaining the correct match in the top n positions, where $n \in N$. The average CMC curves obtained from 12 experiments on DB_5 are shown in Fig. 6.

In Fig. 6, the retweet network obtained 89% closed-set identification rate at rank-1 on DB_5, which demonstrates high level of uniqueness of retweeting behavior of users. As shown in Fig. 6, the rank-1 identification performance of the reply, hashtag, and URL networks are 62%, 52%, and 45%, respectively, which have increased to 68%, 67%, 83% at rank-10. The temporal features obtained the lowest performance during experiment. The TP obtained 13% recognition rate at rank-1 and 42% recognition rate at rank-10 on DB_5. A possible reason for the low performance of the temporal features is that many users have similar interval patterns, i.e., sleep at night, which can cause a decline of uniqueness in a large dataset. Finally, the score level fusion of all features obtained identification rate of 94% at rank-1 and 98% at rank-10, respectively, on DB_5.

The experimental results of closed-set verification of the proposed SB features and their fused form are represented by plotting detection error tradeoff (DET) curves in Fig. 7. DET curve plots false rejection rate (FRR) and false acceptance rate (FAR) with respect to different threshold values. Biometric verification is a two-class classification: genuine user versus impostor. During DET computation, we considered each user j in DB_5, where $j = 1, 2, 3, \ldots, N$ and $N = 241$, as a legitimate user and all other users $(N-1)$ as impostors. The final DET curves shown in Fig. 7 are the average of all DET curves obtained by 12 experiments on 6 train and test sets. The equal error rate (EER), an optimal point on DET where FAR (type-I error) is equal to FRR (type-II error), is commonly used as a measure of biometric verification performance. As shown in Fig. 7, the fused SB features obtained EER as low as 0.04 on DB_5. Although the FARs of hashtag and reply networks are higher than retweet and URL networks, they can be substantially reduced

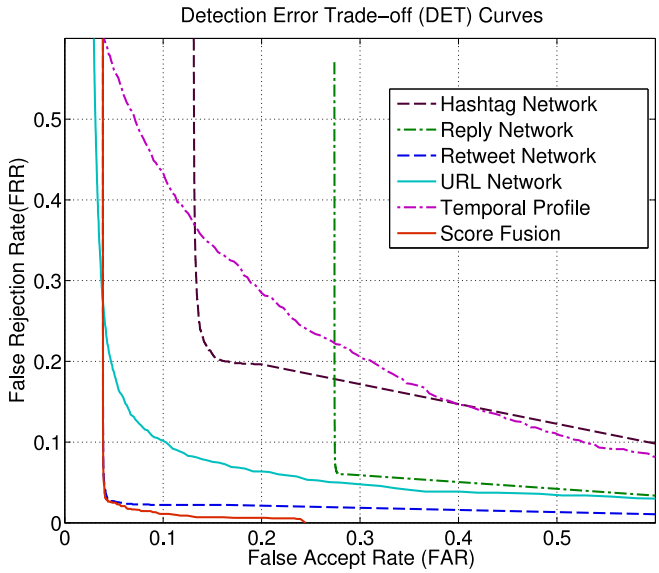

Fig. 7. DET curves of hashtag, URL, retweet, reply, temporal features, and score fusion of all SB features on 241 users' DB; each curve has been obtained by averaging over all the DET curves for each user on six train and test sets of DB_5.

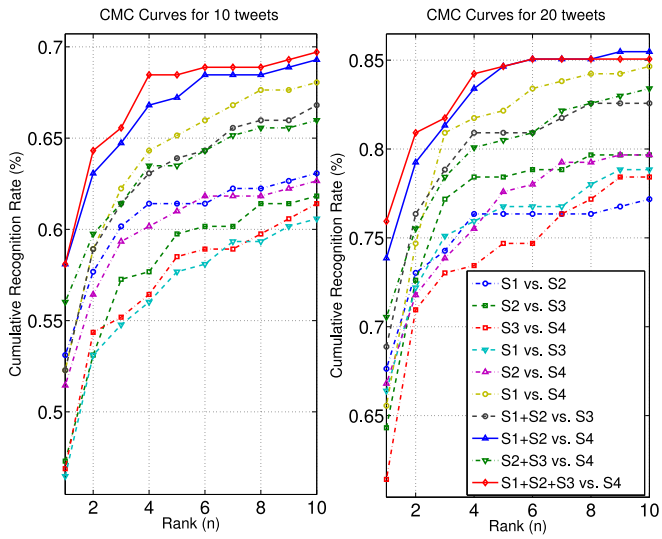

Fig. 8. CMC curves for 10 probe tweets (on left) and 20 probe tweets (on right) of the score fusion all SB features obtained on 241 users (DB_5) with 10 train and test set combinations: S_1 versus S_2, S_1 versus S_3, S_1 versus S_4, S_2 versus S_3, S_2 versus S_4, S_3 versus S_4, S_1+S_2 versus S_3, S_1+S_3 versus S_4, S_2+S_3 versus S_4, and S_1+S_2+S_3 versus S_4; the highest performance is obtained with concatenated three training sessions ($S_1 + S_2 + S_3$) versus testing session S_4.

by fusing with other three features. As shown in Fig. 7, the low EER demonstrates the applicability of the fused SB features for identity verification in a closed-set scenario.

Following are the three important findings from the first set of experiments.

1) Fusion of SB features can be utilized for user identification as well as verification in a closed-set scenario as it obtained high identification rate (94% at rank-1) and low EER (0.04) on a DB of 241 users.
2) The high identification (closed-set) rate also validates the uniqueness of the fused SB features.
3) The proposed method is applicable to prolific and non-prolific users as it obtained high recognition performance on a DB containing both frequent and nonfrequent users.

B. Experiment-2

The second set of experiments is intended to evaluate the performance of the proposed SB-based user recognition method with the presence of a small amount of information during the test phase, i.e., small length test session. We also want to evaluate the impact of the length of the training session on recognition performance. During the second set of experiments, we only evaluate the performance of the score fusion of all SB features on DB_5 with four sessions. Experiments are conducted on 10 different train and test set combinations, where the probe data comprise of 10, 20, 30, 40, 50, and 60 recent tweets from the corresponding test session. The ten different train versus test set combinations are S_1 versus S_2, S_1 versus S_3, S_1 versus S_4, S_2 versus S_3, S_2 versus S_4, S_3 versus S_4, S_1+S_2 versus S_3, S_1+S_3 versus S_4, S_2+S_3 versus S_4, and S_1+S_2+S_3 versus S_4, where + denotes the concatenation of training sessions. We train the proposed system using single session, concatenated two sessions and three sessions, where the older sessions have been used for training and the later session has been utilized for testing. Usually, a test session contains 200 recent tweets of a user. Therefore, 10, 20, 30, 40, 50, and 60 tweets contain only 5%, 10%, 15%, 20%, 25%, and 30% data, respectively, from the test session. The successive training and testing sessions may have some overlaps depending on the amount of tweets used for testing.

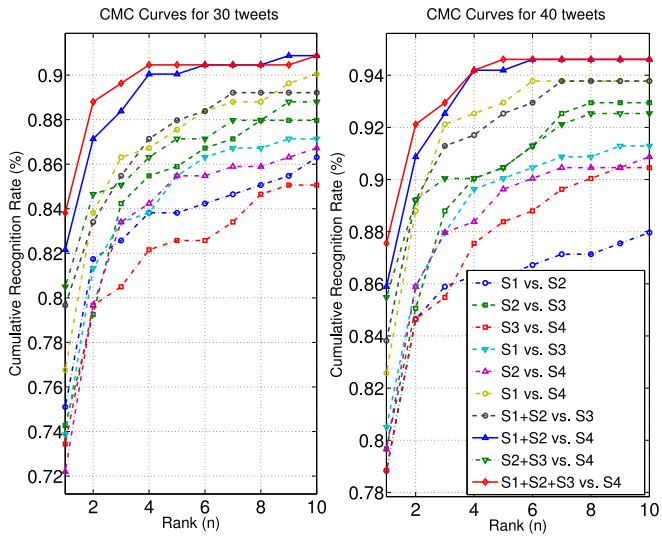

Fig. 9. CMC curves for 30 probe tweets (on left) and 40 probe tweets (on right) of the score fusion all SB features obtained on 241 users (DB_5) with 10 train and test set combinations: S_1 versus S_2, S_1 versus S_3, S_1 versus S_4, S_2 versus S_3, S_2 versus S_4, S_3 versus S_4, S_1+S_2 versus S_3, S_1+S_3 versus S_4, S_2+S_3 versus S_4, and S_1+S_2+S_3 versus S_4; the highest performance is obtained with concatenated 3 training sessions ($S_1 + S_2 + S_3$) versus testing session S_4.

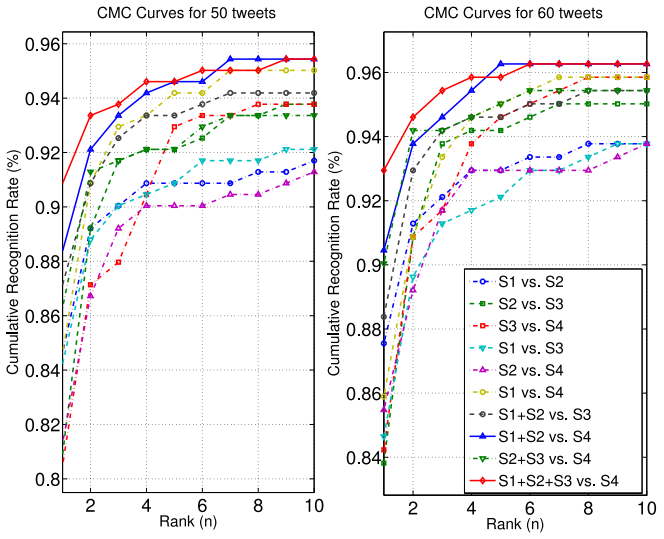

Fig. 10. CMC curves for 50 probe tweets (on left) and 60 probe tweets (on right) of the score fusion all SB features obtained on 241 users (DB_5) with10 train and test set combinations: S_1 versus S_2, S_1 versus S_3, S_1 versus S_4, S_2 versus S_3, S_2 versus S_4, S_3 versus S_4, S_1+S_2 versus S_3, S_1+S_3 versus S_4, S_2+S_3 versus S_4, and S_1+S_2+S_3 versus S_4; the highest performance is obtained with concatenated three training sessions ($S_1 + S_2 + S_3$) versus testing session S_4.

Figs. 8–10 plot the CMC curves obtained from the second set of experiments on the above-mentioned 10 train and test set combinations using 10, 20, 30, 40, 50, and 60 recent tweets from the corresponding test sessions. CMC curves on the left of Fig. 8 show that a maximum recognition rate of 52.2% at rank-1 is obtained using only ten recent tweets as a probe set with a single training session. Interestingly, this maximum recognition rate with single training session is obtained on S_1 versus S_4 train–test set combination, where the time interval between the testing session S_4 and the training session S_1 is at least 10 weeks. Therefore, this result not only demonstrates the recognition performance but also validates the stability of the fused SB features over certain period. The rank-1 recognition rate with ten tweets during testing has been improved to 58% by concatenating more than one training sessions. The left part of Fig. 8 shows that the training set consisting of the concatenated three sessions ($S_1 + S_2 + S_3$) obtained the highest recognition performance (58%) for ten tweets from test session S_4, whereas the cumulative recognition rate has increased to 70% at rank-10. For this same train and test set combination, the rank-1 recognition performance climbed up to 76% with 20 tweets as a probe set, which is shown in the right part of Fig. 8. Figs. 9 and 10 demonstrate incremental recognition performances with the growing number of tweets in probe sets. In every case, the highest recognition rate at rank-1 has been obtained with ($S_1 + S_2 + S_3$) versus S_4 train and test set combination. The CMC curves shown in Figs. 8–Fig. 10 show that longer (concatenated) training sessions enhance the recognition rate from 8% to 15% over shorter (single) training session. From Figs. 9 and 10, we can see that the highest rank-1 recognition rates using 30, 40, 50, and 60 most recent tweets from test sessions are as high as 84%, 87.6%, 91%, and 93%, respectively, whereas the corresponding cumulative recognition rates boost up to 91%, 94.6%, 95.5%, and 96.2% at rank-10.

TABLE III
STATISTICAL *T*-TEST RESULTS: *T*-VALUE, *P*-VALUE, DEGREE OF FREEDOM (DF) FOR INCREMENTAL SB FEATURE COMBINATIONS

Comparison ($F_j - F_i$)	*T*-value (df = 9)	*P*-value	Significant improvement (Yes/No)
$F_2 - F_1$	41.25	0.0000	Yes
$F_3 - F_2$	26.43	0.0000	Yes
$F_4 - F_3$	19.23	0.0000	Yes
$F_5 - F_4$	3.29	0.0047	Yes

Following are the three important findings from the second set of experiments.

1) A reasonably high recognition rate can be obtained using as little as ten recent tweets as a probe.
2) A longer training period enhances recognition performance of SB features.
3) Fused SB features remain stable over certain period of time (10–15 weeks).

C. Experiment-3

In the third set of experiments, the statistical significance of different SB feature combinations for closed-set user identification has been evaluated by *T*-test. We conduct one-tailed paired *T*-tests on the six train and test sets of DB_5 to test the statistical significance of the recognition performance of fusing SB features in an incremental way. The feature combinations are: F_1= temporal profile, F_2=F_1 + hashtag network, F_3=F_2 + reply network, F_4=F_3 + URL network, F_5=F_4 + retweet network. We test the significance of the differences between $F_2 - F_1$, $F_3 - F_2$, $F_4 - F_3$, and $F_5 - F_4$ pairs with a significance level $\alpha = 0.05$. In a hypothesis test, the *P*-values less than or equal to significance level (α) is considered statistically significant. Table III summarizes the *T*-values and *P*-values obtained for each pair. The *T*-test results show that the incremental fusion of SB features is statistically significant since in all cases $p < .01$.

D. Discussion

Our experimental results support the finding reported in [43] that OSN users hold Dunbar's number maintaining stable relationship with only a small number of acquaintances. This research further extends the idea showing that cognition driven social connections and preferences of users' via OSN possess unique behavioral characteristics.

We validated the three important biometric properties of the proposed SB features: accuracy, uniqueness, and stability over certain period of time. The 94% rank-1 identification rate (see Fig. 6) on a DB of 241 users in a closed-set scenario validates that the proposed SB features are unique enough to distinguish one user from another. The experimental results on different sessions showed that the proposed SB features do not change overnight and remain stable over a certain period. For instance, as shown in Fig. 10, the rank-1 closed-set identification rate of the proposed fused SB features in session 1 versus session 4,

which has time separation of more than 10 weeks, is 86% with 60 tweets only. It can be improved even further with more than 60 tweets in a test session or a longer training session. Therefore, we observed a certain level of permanence of SB features from the experimental results. However, similar to other behavioral biometrics, social behavior can change over time. Thus, the biometric template might needed to be updated periodically. This requirement should not pose any problems, since social behavior can be extracted and updated from the OSN accounts of the users. Another finding from our experiments is that the proposed SB features are effective even for nonfrequent Twitter users green who produce as little as ten tweets per week (less than two tweets per day). Experimental results also show that an OSN user is likely to be identified with a small set of recent tweets (i.e., ten tweets) from his timeline in a closed-set scenario. In addition, the proposed SB feature set is generic and can be adopted and extended to other social networks. Therefore, a larger community of OSN users can be accumulated under the umbrella of SB biometrics.

The proposed SB features are more suitable for identity verification (1:1) or a closed-set identification in its present form. However, they can be useful for user identification from a large population in a multimodal scenario. For example, a small suspect list can be identified by a stronger biometric such as face, then SB biometric information can be used to identify the user from the small set of candidates. Other potential security applications of the proposed SB biometric include author recognition, access control in cyberspace/OSN, anomaly detection, situation awareness, and forensic.

VI. Conclusion and Future Work

The concept of exploring social behavior for user authentication emerged only recently. This paper has presented the first comprehensive analysis of using social interactions in a given online social context as a behavioral biometric. It establishes the key properties of SB biometric features, such as uniqueness, stability, and recognition accuracy for a set of frequent and nonfrequent OSN users. The results obtained from the extensive experiments demonstrate the potential of the proposed SB biometric to be used alongside traditional behavioral biometrics in finding more discriminating SB-based features. The dataset (DB) is not yet publicly available. Further work includes validation of the data as a tool for behavior recognition, which will further reinforce presented findings.

In the future, SB-based biometric system can be used as a stand-alone application or as a part of a multimodal system incorporating other biometric modalities. The proposed SB profiles can be used as an input to other interactive HMS, such as recommendation system for social network [34], targeted marketing [32], serendipitous social interactions [45], personalized services [46], etc. A recent research [14] identified the lack of information as a significant challenge for the open-set biometric authentication and proposed to integrate authentication machines ("A-machine") with social infrastructure to accumulate information from different sources. The proposed social biometric framework can be applied in the future to such A-machine during creation of e-profiles in an open-set authentication scenario. Finally, the proposed SB biometric-based authentication system can be integrated with interactive robots [12], [15] or smart homes [11] to provide the right service to the right user.

As a future work, we will conduct a more detailed study on the spatio-temporal data to explore more temporal features. We will also consider integrating the developed SB system with an interactive web-based platform to enable real-time collection and processing of the social biometric features. Our future research includes the investigation of SB features in other online social settings as well as in offline settings in the context of interactive situation awareness systems.

References

[1] [Online]. Available: http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/, Accessed on: Aug. 20, 2016.

[2] [Online]. Available: www.comscore.com/content/download/13029/267601/, Accessed on: Aug. 20, 2016.

[3] R. V. Yampolskiy and V. Govindaraju, "Behavioural biometrics: A survey and classification," *Int. J. Biometrics*, vol. 1, no. 1, pp. 81–113, 2008.

[4] M. Karnan, M. Akila, and N. Krishnaraj, "Biometric personal authentication using keystroke dynamics: A review," *Appl. Soft Comput.*, vol. 11, no. 2, pp. 1565–1573, 2011.

[5] Z. Shen, Z. Cai, X. Guan, Y. Du, and R. A. Maxion, "User authentication through mouse dynamics," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 16–30, Jan. 2013.

[6] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 136–148, Jan. 2013.

[7] P. Lovato, M. Bicego, C. Segalin, A. Perina, N. Sebe, and M. Cristani, "Faved! biometrics: Tell me which image you like and i'll tell you who you are," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 3, pp. 364–374, Mar. 2014.

[8] M. I. Gobbini and J. V. Haxby, "Neural systems for recognition of familiar faces," *Neuropsychologia*, vol. 45, no. 1, pp. 32–41, 2007.

[9] A. Vinciarelli *et al.*,"Bridging the gap between social animal and unsocial machine: A survey of social signal processing," *IEEE Trans. Affect. Comput.*, vol. 3, no. 1, pp. 69–87, Jan.–Mar. 2012.

[10] A. Pentland, "Socially aware, computation and communication," *Computer*, vol. 38, no. 3, pp. 33–40, 2005.

[11] J. Saunders, D. S. Syrdal, K. L. Koay, N. Burke, and K. Dautenhahn, ""teach me—show me" — end–user personalization of a smart home and companion robot," *IEEE Trans. Human-Mach. Syst.*, vol. 46, no. 1, pp. 27–40, Feb. 2016.

[12] N. Magnenat-Thalmann and Z. Zhang, "Social robots and virtual humans as assistive tools for improving our quality of life," in *Proc. Intl. Conf. Digit. Home*, 2014, pp. 1–7.

[13] A. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognit. Lett.*, vol. 79, pp. 88–105, 2016.

[14] S. C. Eastwood, V. P. Shmerko, S. N. Yanushkevich, M. Drahansky, and D. O. Gorodnichy, "Biometric-enabled authentication machines: A survey of open-set real-world applications," *IEEE Trans. Human-Mach. Syst*, vol. 46, no. 2, pp. 231–242, Apr. 2016.

[15] M. Swangnetr and D. B. Kaber, "Emotional state classification in patient-robot interaction using wavelet analysis and statistics-based feature selection," *IEEE Trans. Human-Mach. Syst.*, vol. 43, no. 1, pp. 63–75, Jan. 2013.

[16] M. D. Samad and K. M. Iftekharuddin, "Frenet frame-based generalized space curve representation for pose-invariant classification and recognition of 3-d face," *IEEE Trans. Human-Mach. Syst.*, vol. 46, no. 4, pp. 522–533, Aug. 2016.

[17] B. P. Nguyen, W. L. Tay, and C. K. Chui, "Robust biometric recognition from palm depth images for gloved hands," *IEEE Trans. Human-Mach. Syst.*, vol. 45, no. 6, pp. 799–804, Dec. 2015.

[18] M. Sultana, P. P. Paul, and M. Gavrilova, "Social behavioral biometrics: An emerging trend," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 29, no. 8, 2015, Art. no. 1556013.

[19] M. Sultana, P. P. Paul, and M. Gavrilova, "Identifying users from online interactions in twitter," in *Transactions on Computational Science XXVI: Special Issue on Cyberworlds and Cybersecurity*. Berlin, Germany: Springer, 2016, pp. 111–124.
[20] A. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 125–143, Jun. 2006.
[21] A. A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics*. Berlin, Germany: Springer-Verlag, 2006.
[22] P. Campisi and D. La Rocca , "Brain waves for automatic biometric-based user recognition," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 782–800, May 2014.
[23] L. Olejnik and C. Castelluccia, "Towards web-based biometric systems using personal browsing interests," in *Proc. Eighth Int. Conf. Availability, Rel. Security.*, 2013, pp. 274–280.
[24] S. Tao, M. Kudo, H. Nonaka, and J. Toyama, "Person authentication and activities analysis in an office environment using a sensor network," in *Constructing Ambient Intelligence*. Berlin, Germany: Springer, 2012.
[25] Y. Guo, L. Yang, X. Ding, J. Han, and Y. Liu, "Opensesame: Unlocking smart phone through handshaking biometrics," in *Proc. IEEE INFOCOM*, 2013, pp. 365–369.
[26] T. Feng, X. Zhao, and W. Shi, "Investigating mobile device picking-up motion as a novel biometric modality," in *Proc. IEEE Sixth Int. Conf. Biometrics, Theory, Appl. Syst.*, 2013, pp. 1–6.
[27] D. Khazaei, K. Maghooli, F. Afdideh, and H. Azimi, "A unimodal person authentication system based on signing sound," in *Proc. Biomed. Health Informat.*, 2012, pp. 152–154.
[28] Y. Albayram, S. Kentros, R. Jiang, and A. Bamis, "A method for improving mobile authentication using human spatio-temporal behavior," in *Proc. IEEE Symp. Comput. Commun.*, 2013, pp. 000 305–000 311.
[29] W. Jiang, J. Xiang, L. Liu, D. Zha, and L. Wang, "From mini house game to hobby-driven behavioral biometrics-based password," in *Proc. 12th IEEE Int. Conf. Trust, Security Privacy Comput. Commun.*, 2013, pp. 712–719.
[30] G. Roffo, C. Segalin, A. Vinciarelli, V. Murino, and M. Cristani, "Reading between the turns: Statistical modeling for identity recognition and verification in chats," in *Proc. Int. Conf. Adv. Video Signal Based Surveillance*, 2013, pp. 99–104.
[31] R. Bhardwaj, G. Goswami, R. Singh, and M. Vatsa, "Harnessing social context for improved face recognition," in *Proc. Int. Conf. Biometrics*, 2015, pp. 121–126.
[32] Y. Zhang, Z. Wang, and C. Xia, "Identifying key users for targeted marketing by mining online social network," in *Proc. IEEE 24th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, 2010, pp. 644–649.
[33] X. Zhou, Y. Xu, Y. Li, A. Josang, and C. Cox, "The state-of-the-art in personalized recommender systems for social networking," *Artif. Intell. Rev.*, vol. 37, no. 2, pp. 119–132, 2012.
[34] Z. Wang, J. Liao, Q. Cao, H. Qi, and Z. Wang, "Friendbook: A semantic-based friend recommendation system for social networks," *IEEE Trans. Mobile Comput.*, vol. 14, no. 3, pp. 538–551, Mar. 2015.
[35] A. Vinciarelli, M. Pantic, and H. Bourlard, "Social signal processing: Survey of an emerging domain," *Image Vis. Comput.*, vol. 27, no. 12, pp. 1743–1759, 2009.
[36] N. Oliver, B. Rosario, and A. Pentland, "A Bayesian computer vision system for modeling human interactions," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, no. 8, pp. 831–843, Aug. 2000.
[37] I. McCowan *et al.*, "Modeling human interaction in meetings," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, 2003, vol. 4, pp. IV:748–751.
[38] M. Sultana, P. P. Paul, and M. Gavrilova, "A concept of social behavioral biometrics: Motivation, current developments, and future trends," in *Proc. Int. Conf. Cyberworlds*, 2014, pp. 271–278.
[39] R. M. Green and J. W. Sheppard, "Comparing frequency- and style-based features for twitter author identification," in *Proc. 26th Int. FLAIRS Conf.*, 2013, pp. 64–69.
[40] [Online]. Available: http://nodexl.codeplex.com/. Accessed on: Aug. 22, 2016.
[41] [Online]. Available: https://support.twitter.com/articles/166337-the-twitter-glossary, Accessed on: Aug. 22, 2016.
[42] R. I. M. Dunbar, *How Many Friends Does One Person Need? Dunbar's Number and Other Evolutionary Quirks*. London, U.K.: Faber & Faber, 2010.
[43] B. Gonalves, N. Perra, and A. Vespignani, "Modeling users' activity on twitter networks: Validation of dunbar's number," *PLoS ONE*, vol. 6, no. 8, 2011, Art. no. e22656.
[44] M. Lan and H.-b Low, "A comprehensive comparative study on term weighting schemes for text categorization with support vector machines," in *Proc. 14th Int. World Wide Web Conf.*, 2005, pp. 1032–1033.
[45] Z. Yu, H. Wang, B. Guo, T. Gu, and T. Mei, "Supporting serendipitous social interaction using human mobility prediction," *IEEE Trans. Human-Mach. Syst.*, vol. 45, no. 6, pp. 811–818, Dec. 2015.
[46] X. Chen, Z. Zheng, Q. Yu, and M. R. Lyu, "Web service recommendation via exploiting location and QoS information," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1913–1924, Jul. 2014.

Madeena Sultana (S'13) received the B.Sc. and M.Sc. degrees in computer science and engineering from Jahangirnagar University, Dhaka, Bangladesh, in 2008 and 2011, respectively. She is currently working toward the Ph.D. degree in computer science at the University of Calgary, Calgary, AB, Canada.

She has coauthored more than 30 publications in refereed journals and IEEE/ACM conference proceedings. Her research interests include biometric security, social behavior analysis, and digital image processing.

Ms. Sultana received the most prestigious Vanier Canada Graduate Scholarship in 2014. She also received the prestigious provincial scholarship—Alberta Innovates Technology Futures.

Padma Polash Paul received the B.Sc. degree in computer science and engineering from the University of Rajshahi, Rajshahi, Bangladesh, in 2006, the M.Phil. degree in computer science from the City University of Hong Kong, Hong Kong, in 2010, and the Ph.D. degree in computer science from the University of Calgary, Calgary, AB, Canada, in 2016.

He is currently a Postdoctoral Fellow with Oxford Computational Neuroscience, University of Oxford, Oxford, U.K. He has more than 12 years of teaching and research experience. His research interests include brain big data mining, big data analytics, computational neuroscience, machine learning, and pattern recognition. He has authored more than 70 international journal and conference papers.

Dr. Paul received a Fellowship from the Brain Science Foundation, USA.

Marina L. Gavrilova (S'96–A'98–M'03) received the Diploma with honors, specialization in computer software, from Lomonosov Moscow State University, Moscow, Russia, in 1993, and the Ph.D. degree from the University of Calgary, Calgary, AB, Canada, in 1998.

She is a Full Professor in the Department of Computer Science, University of Calgary, and Co-Director of two research laboratories: the Biometric Technologies Laboratory and the SPARCS Laboratory. She published more than 150 journal and conference papers, special issues, and book chapters. Her current research interests include information security and machine learning for biometric modeling.

Dr. Gavrilova currently serves as a Founding Editor-in-Chief of the *Springer Transactions on Computational Sciences Journal*, and on the editorial boards of the *Visual Computer*, *International Journal of Biometrics*, *Journal of Supercomputing*, and seven other journals. Her research was featured in Science Digest, Live Sciences Exhibit at the National Museum of Civilization, Canada, and on Discovery Channel, Canada.