I. J. Computer Network and Information Security, **2017, 1, 31-39**
Published Online January 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.01.04

Identity Verification Mechanism for Detecting Fake Profiles in Online Social Networks

Ali M. Meligy
Menoufyia University/Department of Computer Science, Shebien EL Koom, Egypt
E-mail: meligyali@hotmail.com.

Hani M. Ibrahim, and Mohamed F. Torky
Menoufyia University/Department of Computer Science, Shebien EL Koom, Egypt
E-mail: hanimir78@yahoo.com, mtorky86@gmail.com.

Abstract—Impersonating users' identity in Online Social Networks (OSNs) is one of the open dilemmas from security and privacy point of view. Scammers and adversaries seek to create set of fake profiles to carry out malicious behaviors and online social crimes in social media. Recognizing the identity of Fake Profiles is an urgent issue of concern to the attention of researchers. In this paper, we propose a detection technique called *Fake Profile Recognizer (FPR)* for verifying the identity of profiles, and detecting the fake profiles in OSNs. The detection method in our proposed technique is based on utilizing *Regular Expression (RE)* and *Deterministic Finite Automaton (DFA)* approaches. We evaluated our proposed detection technique on three datasets types of OSNs: Facebook, Google+, and Twitter. The results explored high Precision, Recall, accuracy, and low False Positive Rates (FPR) of detecting Fake Profiles in the three datasets.

Index Terms—Online Social Networks (OSNs), Security and Privacy, Fake Profiles.

I. Introduction

Online Social Media such as Facebook, Twitter, or LinkedIn, allow for users to present themselves as an online profile, using these profiles, users are able to setup variety online social relationships in a popular way [1]. Due to the open nature of OSNs, users can appear in redundant identities. Hence, verifying users' identities is one of the critical issues from the security and privacy point of view [2]. To set up any social relationships in an authenticated fashion, the users must authenticate their identities to each other in order to prevent building fake communications on a large scale. The current way of authenticating users' identities in OSNs is not enough to prevent fake profile creation, such that the single user can represent his identity with multiple profiles without any effective identity verification process. This vulnerability enables the attackers to create a variety of fake profiles for attacking the online social System. For example, Profile Hijacking [3] by which the intruder can obtain the control of some existing profiles within OSN platform. Profiling Attack [4] through which the adversary try to gather information about OSN activities. Retrieval and Analysis attack [5] is another malicious behavior, which targets multimedia information such as images, videos, audios, etc. This attack is followed by subsequent analysis as a Reverse Engineering Attack (RSE) [6], by which the attacker seeks to trick the victim into contacting with the hacker freely. Sybil attacks are one of the most prevalent and practical attacks against OSNs platforms [7], in this attack, the adversary seeks to impersonate the real users' identities across OSN via creating several fake accounts known as Sybil accounts to obtain the trust of a specific user or a specific community unfairly. Unfortunately, OSNs platforms have not strong authentication mechanisms for protecting users' profiles against Sybil profile attack except for the traditional mechanisms, such as CAPTCHA, which is routinely solved by dedicated workers for pennies per request [8].

Although the researchers introduced several methodologies and approaches for detecting Fake profiles, but it is still a hard challenge. For example, some machine learning algorithms are proposed, but they do not provide the desired effectiveness and accuracy to detect fake profiles [9]. Other researchers tried to solve this problem using Social Graph Topology and its properties [10], but there is a little evidence for depending on these approaches for detecting fake profiles in OSNs. Crowdsourcing [11], is a different approach for identifying Fake profiles but also it doesn't provide the effective and accurate solutions as it depends on a human-based account verification scheme.

In this study, we present a novel detection technique called *Fake Profile Recognizer (FPR)*. The detection methodology is based on two key approaches: *Regular Expression* and *Deterministic Finite Automaton (DFA).* Regular Expression (RE) is used for representing and authenticating the identities of profiles as set patterns, and the DFA machine is used for recognizing the identities in a trusted manner. The proposed detection technique is the real experimental work, which based on our initial study in [12].

We could design and implement the proposed technique, as well as, we simulated the detection functionality into three datasets of OSNs. Our findings

explored promising results based on *Precision, Recall, Accuracy, and False Positive Rate (FPR)* metrics.

The rest of this paper is organized as Section II presents the related work. Section III presents the major features of the proposed FPR technique. Section IV presents our evaluation and the experimental results. Section V Discusses our findings. Section VI formulates the conclusion of this work.

II. Related Work

Creating bogus accounts in OSNs become attractive strategies for criminals who target OSNs Security and privacy. For example, Phishing techniques are popular ways for scammers to entice users to accept fake friend requests [11]. The OSN Criminals can create fake profiles using either duplicating the existence of a specific account or by creating fake accounts from non-existence to perform spy and eavesdropping activities [13]. In a statistical study, Facebook says that; fake profiles ranges from 5.5% to 11.2% from all created accounts [14]. The literature introduced some approaches for handling this problem. In [2], a new algorithm is developed for computing trusted relations and distrusted relations in OSNs based on combining an inference algorithm with modified spring embedding algorithm. Some algorithms also tried to solve this problem based on a social graph segmentation among user identities [15][16].

Sybil Infer and *Sybil Rank* is another approach that returns the probability based on ranking each node in the social graph according to their perceived probabilities of being fake nodes [9][17]. Zhi Yang et al in [7], described a detection scheme for Sybil accounts in Renren OSN by monitoring the behavior of Sybils in the wild, the authors could identify several behavioral attributes that are unique to sybils and leverage them to create a measurement-based real time Sybil detector.

Other approaches are introduced to detect fake profiles based on profiles' feature and behaviors , for example in [18] an Automated Feature-based fake profile detection algorithm is introduced that depends on machine learning considerations, and in [19], a new approach is introduced to detect profile cloning based on profile's attributes similarity and friend network similarity. In paper [20], the author designed and implemented five steps based automated technique for detecting malicious users and social spam campaign. In [21], the authors described how to use Exclusive Shared Knowledge approach between the friends for identifying their close friends in an OSN. In [8], a novel approach presented for Sybil detection based on the fundamental behavioral patterns of Click-Stream models, the proposed methodology is validated using ground truth traces of 16.000 real and Sybil users from Renren social network. Crowdsourcing [22] is a standalone approach for detecting Sybil accounts in OSNs, in this paper, the authors explored the feasibility of outsourcing the Sybil detection to online human experts and they evaluated the approach on three OSNs; Renren, Facebook US, and Facebook IN.

III. Fake Profiles Recognizer

In this section, we design *Fake Profile Recognizer (FPR)* mechanism in order to detect fake profiles in OSNs. The major functionality of FPR technique is based on two important software components; *User Identity Generator (UIG)*, and *Identity Profile Recognizer (IPR)*. We can describe each component as in the following two subsections A, and B.

A. User Identity Generator (UIG)

UIG is a software component, which is responsible for creating and generating the identities of users' profiles. In addition, User Identity Generator is used for authenticating the friends in the friend list of each ego-profile. The major functionality of UIG mechanism is based on representing the identities of the created profiles using the *Regular Expression* approach (RE). RE is an effective tool for representing a variety of patterns based on a specific alphabet of symbols. Since OSNs allow for creating a lot of profiles in a redundant scheme, it is necessary to represent the identities of created profiles using a unique pattern for each one; in addition, the instances that are derived from each pattern represent the identities of friends in the friend list of each ego-profile. For more clearing, suppose we have an online social network system that involves four profiles P_1, P_2, P_3, P_4. The UIG mechanism represents the identities of these profiles by assigning a unique pattern (i.e. regular expression) for each one as in equations 1, 2, 3, and 4 respectively.

$$\sum(a,b) \rightarrow P_1 \equiv (a|b*) \quad (1)$$

$$\sum(k,l) \rightarrow P_2 \equiv (k|l)^* \quad (2)$$

$$\sum(a,b,c) \rightarrow P_3 \equiv (\text{ab}*|\ (\text{c}|\varepsilon)) \quad (3)$$

$$\sum(0,1) \rightarrow P_4 \equiv (0|\ 1^*) \quad (4)$$

The generated instances (i.e. Regular Set) that authenticate the friend list of each profile can be described as in equations 5, 6, 7, and 8 respectively.

$$P_1 \equiv (a|b^*) \rightarrow (\varepsilon, a, b, bb, bbb, \dots\dots) \quad (5)$$

$$P_2 \equiv (k|\ l)* \rightarrow (\varepsilon, k, l, kk, kl, lk, ll, \dots) \quad (6)$$

$$P_3 \equiv (ab^*(c|\varepsilon) \rightarrow (a, ac, ab, abc, abb, \dots) \quad (7)$$

$$P_4 \equiv (0|\ 1^*) \rightarrow (\varepsilon, 0, 1, 11, 111, \dots\dots) \quad (8)$$

Each instance in the regular set, which corresponding to a specific pattern of a specific profile is used to represent the identity of a specific friend in the friend list. The transition from the symmetric classical way of representing the identity of profiles and its friend lists in OSNs to our asymmetric way is depicted in Fig. 1.

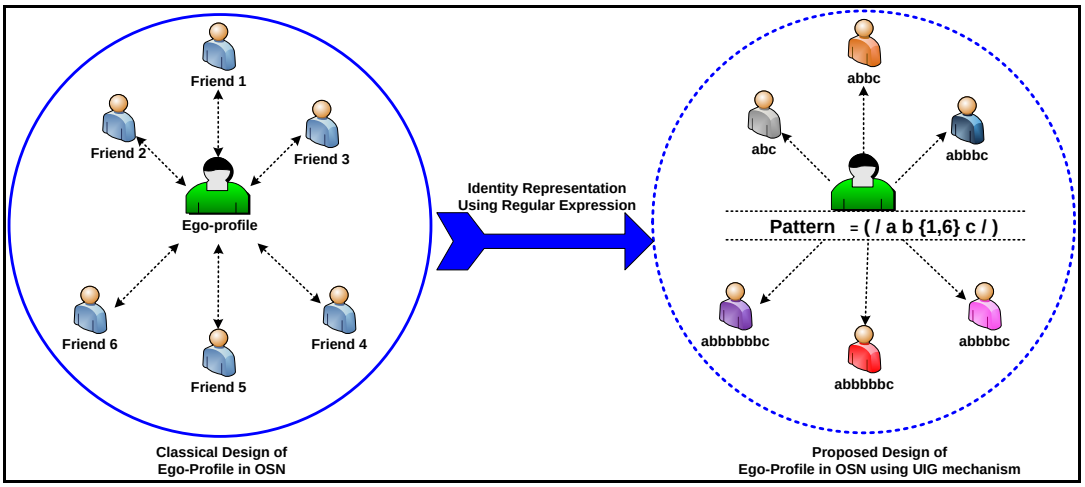

Fig.1. A proposed Scheme for Representing the Identities of Profiles using a Regular Expression.

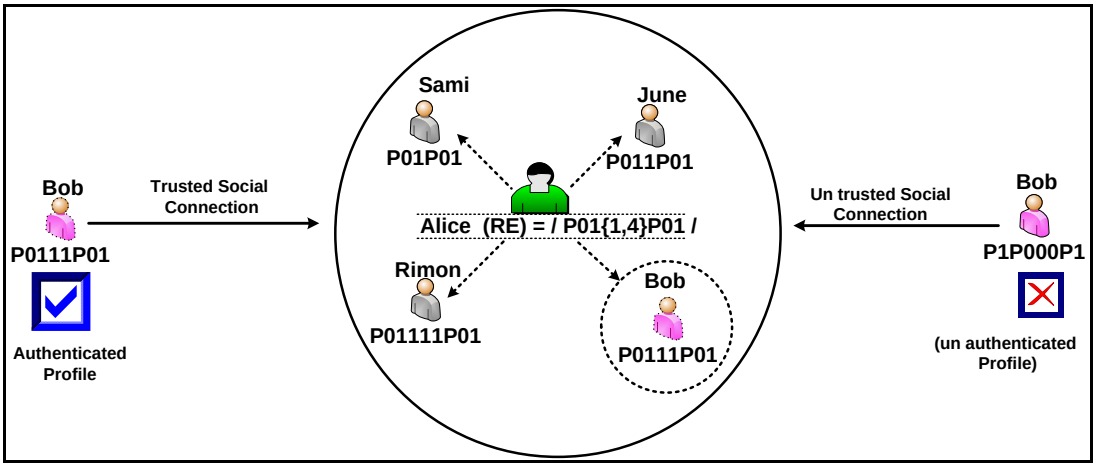

Fig.2. Modeling the Trusted/ Distrusted Connection based on UIG Functionality.

According to the symmetric way of creating profiles and their friend lists in OSNs, there is no way to verify the identities of profiles between users except some of the layout features such as profiles names, and profiles photos, this weakness allow intruders to duplicate a large amounts of fake profiles that share the same layout features without an effective way to differentiate the genuine profiles than fake ones, but with the novel asymmetric view, the UIG mechanism creates the identities of profiles based on a unique Pattern for each one and authenticate the friend list of each one based on a unique set of derived instances (i.e. Regular Set) of this pattern as depicted on the right side of Fig 1. Based on the proposed methodology of UIG mechanism, it becomes clear that the duplication of profile existence problem is solved. the identity of each profile is represented using a unique Pattern (i.e. Regular Expression) which authenticate its friends in the friend list according to the derived instances (i.e. Regular Set) of this pattern. For example, Fig 2 explores that the identity of 'Alice' in OSN can be represented using the pattern */P01{1,4}P01/*, which can derive the instances *P01P01, P011P01, P0111P01, P01111P01* , such that each instance is used to authenticate a specific friend in Alice's friend list, this way prevent to duplicate the identity of Bob's profile. we have three scenarios to receive a friend request from another profile. The first one is from a new profile that doesn't exist in the friend list before. The second one is from a duplicated profile that has the same layout features of an existed profile in the friend list. The third scenario is a friend request from a social bot which may appear as a new friend or a duplicated friend, but this scenario is combined with breaking CAPTCHA system firstly. The first scenario is verified using the User Identity Generator (UIG) as described in Fig 3**.** it explores that the new profiles , whicht send a new friend request to a specific profile should answer on some of security questions that proof the social communication in the real world, if the answer is correct, then the UIG generate an instance of the pattern for this profiles and add it to the friend list, else, the UIG rejects these profiles. The second and third scenarios will be verified using *Identity Profile Recognizer (IPR)* in subsection B.

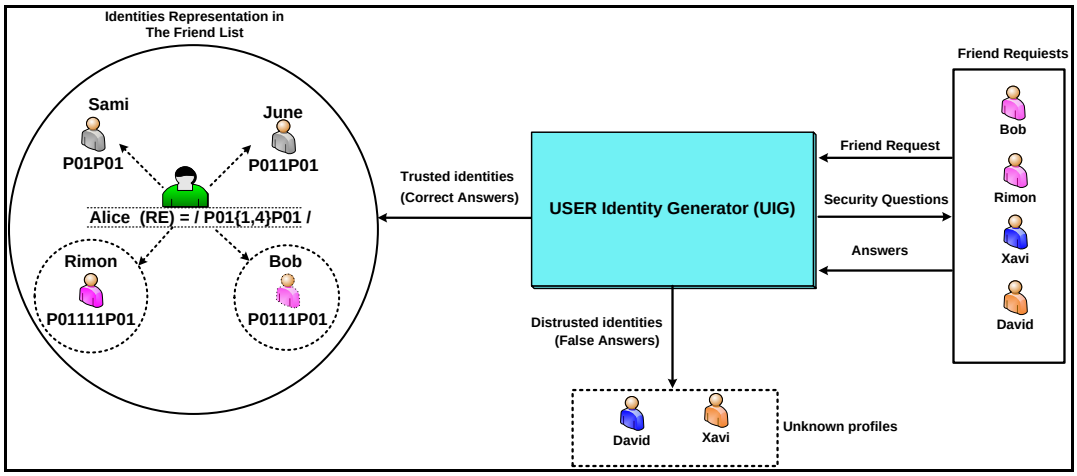

Fig.3. Verifying Friend Requests using User Identity Generator (UIG).

Algorithm 1: Identities Generation

Input: $SN = \{P_1, P_2, P_3, \dots \dots P_n\}$
Output: $I = \{I_1, I_2, I_3, \dots \dots \dots I_n\}$
Output: $FL = \{FL_1, FL_2, FL_3, \dots . FL_n\}$

Procedure: *Users Identities Generator*
for each $P_k \in SN$ do
  $I_k = generate\_Regular_{Expression}(P_k, \Sigma_k)$
  $P_k \leftarrow I_k$
end for
for each $I_k \in I$ do
  $FL_k = generate\_Regular\_Set(I_k)$
  $FL_k \leftarrow I_k$
end for
for each $P_k \in SN$ do
  return $P_k.I_k \wedge P_k.FL_k$
end for
end Procedure

The automation of *User Identity Generator (UIG)* for generating the identity of profiles and friend lists in an authenticated manner is depicted in the **Algorithm 1**.

B. Identity Profiles Recognizer (IPR)

IPR is the second software component in the proposed FPR system, which is used for recognizing the identities of profiles, and differentiating the genuine profiles than fake ones in an automated fashion. The recognition methodology in *IPR* mechanism is modeled as a *Deterministic Finite Automaton (DFA)* machine. such that, for each ego-profile in the OSN, which identified by a unique pattern (i.e. regular expression), there exist the corresponding IPR machine (i.e. DFA machine) that accept all instances (i.e. Regular Set) that can be derived from this pattern. These instances authenticate the genuine profiles in the friend list. the second and third friend requests scenarios are verified using the *Identity Profile Recognizer (IPR)* as depicted in Fig. 4. When a cloned profile sends a friend request to a specific profile, The system asks to clear the instance that represents its identity in the friend list, then, the IPR machine verifies this instance, if it accepted this instance, this means that the friend request is from a genuine profile, but the system will automatically drop the old identity of this profile, remove it from the friend list, and represent it again with a new identity by generating a new instance from the pattern . on the other hand, if the cloned profile cleared false instance of its identity , the IPR machine rejects it, and this profile is detected as a fake one.

The major functionality of IPR component is depicted in the **Algorithm 2** .

Algorithm 2: Identity Recognition

Input: Instances $I = [I_1, I_2, I_3, \dots \dots I_n]$
Output: Genuine Profiles G=[P1, P2, P2,.....Pn1]
Output: Fake Profiles F=[P1, P2, P2,.....Pn2]
Procedure: Identity Recognition
for each $I_k \in I$ do
  S← S0
  C ← NextChar (Char(x))
  While (C ≠ eof) do
    S← Move (S, C)
    C ← NextChar (Char(x))
  end While
  if S ∈ Final States F then
    G← Add (I_k)
  else
    F← Add (I_k)
  end if
end for
end for
return Genuine Profiles G=[P1, P2, P2,.....Pn1]
return Fake Profiles F=[P1, P2, P2,.....Pn2]
end Procedure

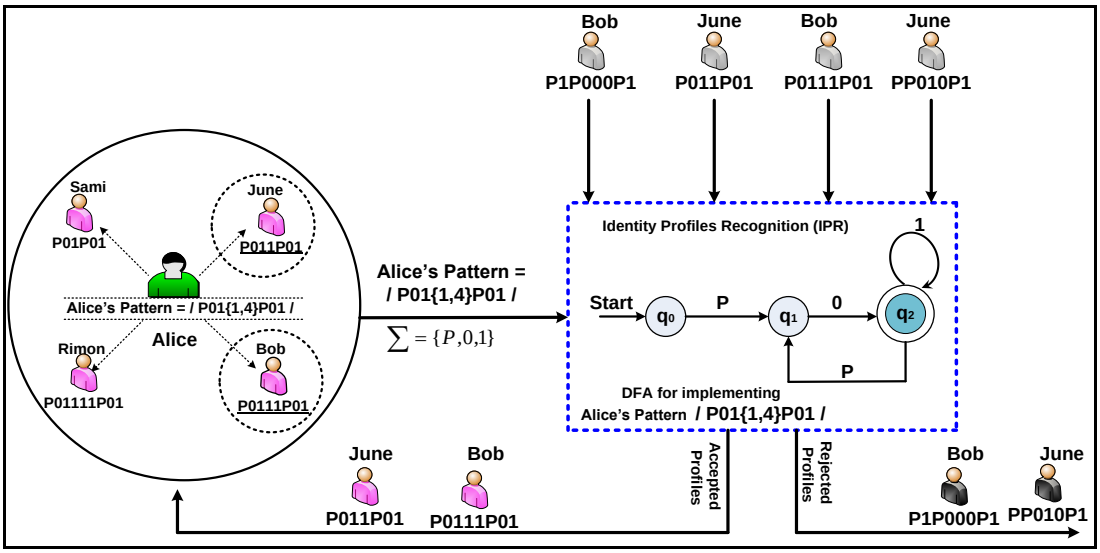

Fig.4. The identity Recognition Method for Cloned Profiles using IPR Mechanism

IV. Evaluation and Experimental Results

To assess the recognition methodology of our proposed technique, we conducted a simulation experiment on three types of social networks datasets: Ego- Facebook , Ego-Google+, and Ego-Twitter. We downloaded the source file of these datasets from SNAB library [23]. Each dataset is described as an ego profile that involves a set of circles , each circle includes set of profiles of this ego profile. The general description of the data sets is depicted in Table 1 and visualized in Fig. 5. In each dataset, we simulated the identity of the ego-profile using a specific pattern (i.e. Regular Expression), then we applied the Algorithm 1 to generate the right derived instances of this pattern that represent the identities of genuine profiles in each dataset. The pattern $/(a|b)^*a\#/$ is used for representing the identity of ego-profile in the Facebook dataset. The pattern $/(a|\varepsilon)bc^*\#/$ is used for representing the identity of ego-profile in the Google+ dataset. The pattern $/(1|0)^*100\#/$ is used for representing the identity of ego-profile in the Twitter dataset.

In each dataset, we represented the identity of fake profiles as derived instances of the pattern $/(a^*|b)(b|ab^*a)\#/$. We designed the corresponding Identy Profile Recognizer IPR(i.e. DFA machine) for each pattern, then, wee apllied the Algorithm 2 to investigate the effectivness of our *FPR* technique to detect fake profiles in each dataset.

Table 1. Datasets Description.

	Facebook	Google+	Twitter
#Profiles	4039	107614	81306
#Edges	88234	13673453	1768149
#Genuine	1399	1225	1445
#Fake	2640	1820	2555
SUM	**4039**	**3045**	**4000**

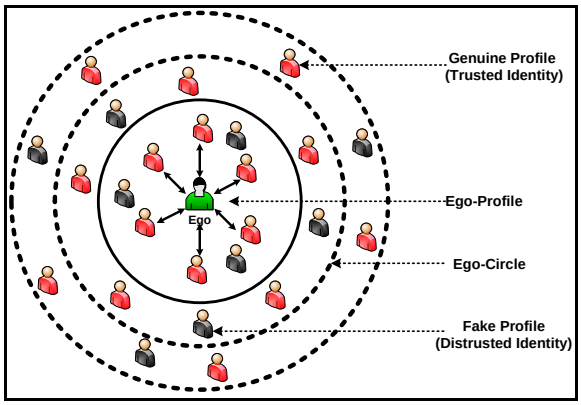

Fig.5. Datasets Representation.

We implemented the methodology of *Fake Profile Recognizer (FPR)* into Visual C++ IDE. The recognition method for detecting fake profiles is evaluated against *Precision* (in Equation 1), *Recall* (in Equation 2), *F-Measure (or F1-Score)* (in Equation 3), *Accuracy* (in Equation 4), *Specificity* (in Equation 5), *Fall-Out (or False Positive Rate FPR)* (in Equation 6), *False Negative Rate (FNR)* (in Equation 7), and *Area Under the Curve (AUC)* (in Equation 8) [24]. Our obtained results of calculating the percentage of Precision, Recall, F1-Score, and Accuracy in the three datasets are depicted in Table 2. Calculating the percentage of Specificity, Fall-Out (i.e. False Positive Rate (FPR)), False Negative Rate (FNR), and Area Under the Curve (AUC) is depicted in Table 3.

$$Precision = \frac{TP}{TP+FP} \quad (9)$$

Such that *TP* is a number of True Positive instances and *FP* is a number of False Positive instances.

$$Recall = \frac{TP}{TP+FN} \quad (10)$$

Such that TP is a number of True Positive instances and FN is a number of False Negative instances.

$$F1 - Score = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (11)$$

$$Accuracy = \frac{TP+TN}{P+N} \quad (12)$$

Such that TP is the True Positive value and TN is the True Negative value. P = (TP + FN), and N = (FP + TN) such that FN is the False Negative and TN is the True Negative.

$$Specificity = \frac{TN}{FP+TN} \quad (13)$$

Such that, TN is the True Negatives, and FP is the False Positives

$$Fall - Out = 1 - Specificity \quad (14)$$

$$False\ Negative\ Rate\ (FNR) = \frac{FN}{FN+TP} \quad (15)$$

$$AUC = 1 - \frac{FPR+FNR}{2} \quad (16)$$

Such that FPR = Fall-Out, and FNR is the False Negative Rate where FNR= FN/(FN+TP).

Fig. 6 compares the obtained results of evaluating the Precision, and Recall in the three datasets, the FPR mechanism achieved high percentage of precision and recall in Facebook dataset. Fig.7 compares the results of evaluating F1-Score and Accuracy in the three datasets, the proposed mechanism achieved outstanding accuracy of detecting fake profiles in Facebook dataset.

Table 2. Calculating Precision, Recall, F1-Score, and Accuracy for the three Datasets.

Dataset	Precision	Recall	F1-Score	Accuracy
Facebook	88.97	88.97	88.97	89.73
Google+	77.41	77.41	77.41	76.94
Twitter	81.81	81.81	81.81	81.98
AVG	82.73	82.73	82.73	82.88

Table 3. Calculating Specificity, FPR(i.e. Fall-Out), False Negative Rate (FNR), and Area Under the Curve (AUC) for the three Datasets.

Dataset	Specificity	FPR	FNR	AUC
Facebook	88.34	11.66	11.04	88.66
Google+	73.82	26.18	22.60	75.61
Twitter	79.14	20.86	18.20	80.48
AVG	80.43	19.57	17.28	81.58

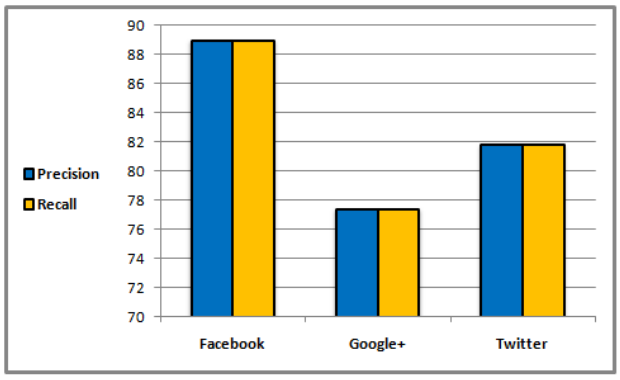

Fig.6. The Obtained Result of Evaluating FPR Mechanism Against Precision and Recall in the Three Datasets.

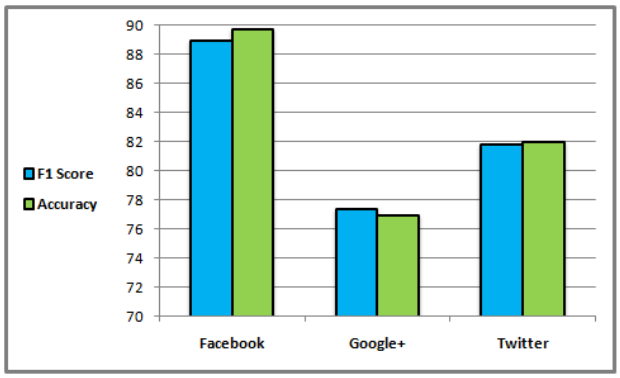

Fig.7. The Obtained Result of Evaluating Our Mechanism Against the F1-Score, and Accuracy in the Three Datasets.

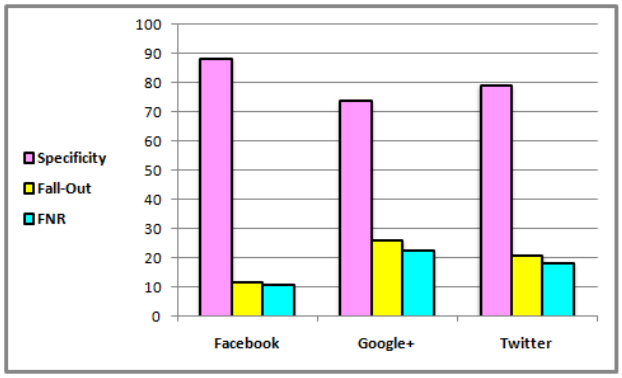

Fig.8. The Obtained Result of Evaluating FPR Mechanism Against Specificity, Fall-Out, and False Negative Rate (FNR) in the Three Datasets.

Fig.8 provides the comparison results of evaluating the FPR mechanism against the Specificity, False Positive Rate (FPR), and False Negative Rate (FNR) in the three datasets. These results also clear high specificity percentage value and low false positive rates of FPR mechanism in the Facebook dataset. In addition, Fig.9 presents the result of evaluating the FPR mechanism against the AUC metric in the three datasets. These results explore a high performance of FPR mechanism in Facebook rather that its performance in Google+ and Twitter.

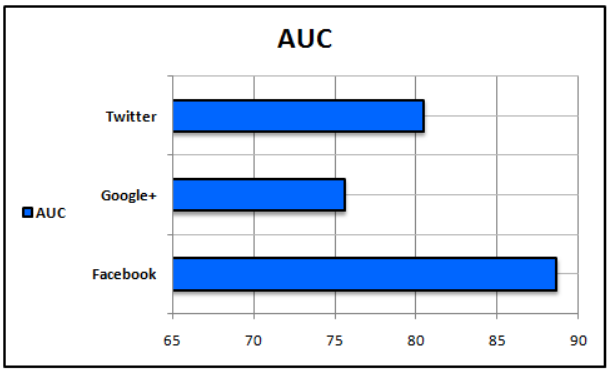

Fig.9.The Obtained Result of Evaluating FPR Mechanism Against Area under the Curve (AUC) Metric in the Three Datasets.

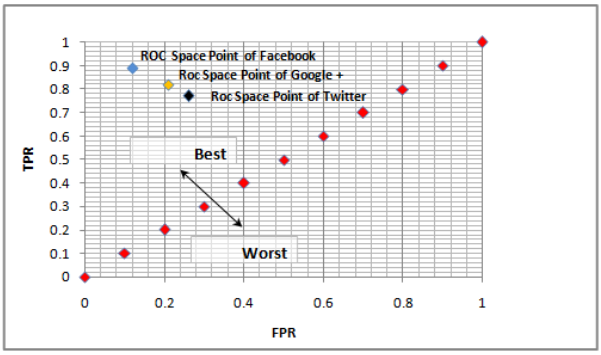

Fig.10. The Roc Space of FPR Mechanism of the Three Datasets.

Fig.10 provides the *Roc Space* Plot which clears the relation between *True Positive Rate TPR* (i.e. Recall), and *False Positive Rate (FPR)* of our proposed mechanism in the three datasets. The performance of the proposed mechanism in detecting fake profiles in the three datasets is placed on the best space, which reflects the effectiveness of the proposed technique in detecting fake profiles especially in the Facebook dataset.

V. Discussion

The presenting study was designed to solve the problem of the identity verification for detecting the fake profiles in online social networks. The functionality of our proposed mechanism (i.e. Fake Profile Recognizer (FPR)) was simulated on three datasets (i.e. Facebook, Google+, and Twitter) in order to test its effectiveness in verifying profiles' identities, and detecting fake profiles in each dataset. The most interesting finding is that the FPR mechanism achieved a Precision value 82.73% in average, this results mean that the exactness in recognizing the identities of profiles (Fake and Genuine Profiles) is 82.43% in average, in addition, evaluating the completeness and the quantity (i.e. Recall) of FPR mechanism achieved also an equivalent value. In addition, the proposed

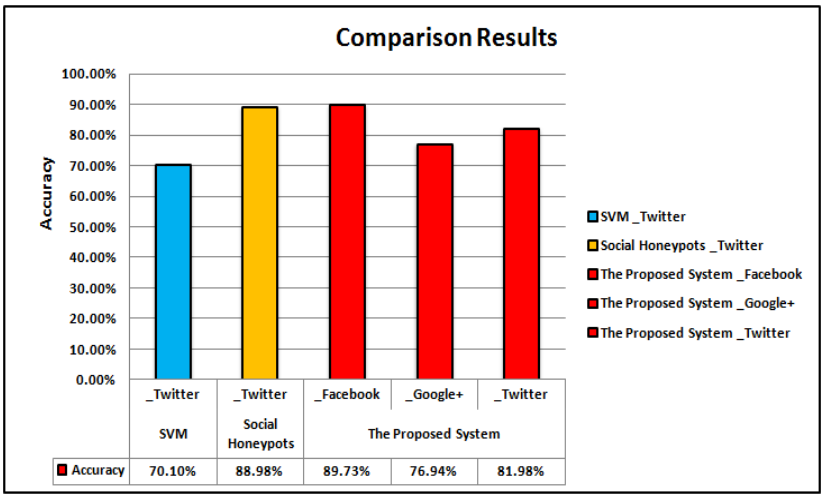

Fig.11 Comparing FPR Mechanism with SVM [24] and Social HoneyBot [25] Against Accuracy Metric.

mechanism achieved an Accuracy score 82.88% in average. Another important finding was that the proportion of negative identities that are correctly recognized by FPR mechanism (i.e. Specificity or True Negative Rate (TNR)) is 80.43% in average. Regarding measuring the False Positive Rate (FPR), and the False Negative Rate (FNR) of the recognition process, the study found that the proposed FPR mechanism achieved False Positive Rate 19.57%, and 17.28% in average respectively. Another important finding was that, the proposed FPR technique achieved good positions in the Roc Space regarding the performance in the three datasets as depicted in Fig 10, which clears that the Roc Space points of the FPR on the three datasets are placed within the best space between 0.75 to 0.90. This result means that the proposed mechanism achieved good performance in verifying, and recognizing the identity of profiles when it applied on the three datasets.

Comparing our proposed technique with other mechanisms in the literature cleared an interesting, and unexpected results in detecting fake profiles in OSNs. The interesting one is the outperforming of our technique than the Support Vector Machine (SVM), which is applied on Twitter dataset [24**]**, the unexpected result is that our system fails to achieve more accuracy than Social HoneyPot that applied also on Twitter dataset [25].

Although this distinguishing with the two mechanisms, but it is calculated for our proposed mechanism that it is applied on three different datasets (Facebook, Google+, Twitter) instead of one dataset (i.e. Twitter) as in SVM and Social HoneyPot, and our results proved a good performance of the proposed technique in the three datasets. Fig.11 compares our proposed mechanism with SVM and Social HoneyPot against the accuracy metric.

VI. Conclusion

The main objective of the current study was to verify the identity of profiles in order to detect the fake profiles in Online Social Networks (OSNs). In this paper, we introduced a detection technique called Fake Profile Recognizer (FPR) for verifying the identity of profiles and recognizing the fake ones. The performance of our proposed technique is experimentally evaluated on three types of OSNs (i.e. Facebook, Google+, and Twitter), the study found that FPR technique achieved an accuracy score 82.88% in average and a good performance point (between 0.75 and 0.90) in the ROC Space. The study has gone some way towards enhancing our understanding of verifying the identity of profiles in order to decontaminate OSNs from fake profiles. The high False Positive Rate (19.57%) of our mechanism makes these findings less generalizable to be the best mechanism for detecting fake profiles although the strong competitive accuracy results. More research using more controlled trials is needed in order to improve the performance of the proposed technique in recognizing the identity of fake profiles in OSNs.

References

[1] Ellison, Nicole B., "Social network sites: Definition, history, and scholarship", Journal of Computer-Mediated Communication, 13(1) , PP: 210-223, (2007)

[2] Thomas, G. Jennifer, and S. Aravind, "Predicting Trust and Distrust in Social Networks", SocialCom/PASSAT, (2011).

[3] L.C.Cutillo., M. Manulis and T. Strufe, "Security and Privacy in Online Social Networks", PP: 512-513. Springer, New York (2010).

[4] M. Balduzzi, C. Platzer, T. Holz, E. Kirda, D. Balzorotti, and C. Kruegel, "Abusing Social Networks for Automated User Profiling", Research Report RR-10-233,EURECOM,http://www.iseclab.org/papers/socialabuse-TR.pdf, (2012).Accessed 10 Oct 2014.

[5] Hasib, Abdullah, "Threats of online social networks", International Journal of Computer Science and Network Security (IJCSNS), 9(11), PP: 288-293, (2009).

[6] Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C. Pu, "Reverse Social Engineering Attacks in Online Social Networks", Detection of intrusions and malware, and vulnerability assessment. Springer, 6739, PP: 55-74. (2011).

[7] Z. Yang, C. Wilson, X. Wang, T. Gao, B.Y.Zhao, and Y.Dai," Uncovering Social Network Sybils in the Wild" ACM Transactions on Knowledge Discovery from Data (TKDD), 8(1), (2014).

[8] G. Wang, T. Konolige, C. Wilson, X. Wang, H. zheng, and Y. Zhao, "You are How You Click: ClickStream Analysis for Sybil Detection", In Usenix Security, PP: 241-256, (2013).

[9] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro," Aiding the Detection of Fake Accounts in Large Scale Social Online Services", Proceedings of 9th USENIX Conference on Networked Systems Design and Implementation, PP: 15-15, (2012).

[10] B. Viswanath, A. Post, K P. Gummadi, and A. Mislove," An Analysis of Social Networks-Based Sybil Defenses", SIGOMM 10, Proceedings of the ACM SIGCOMM Conference, New York, USA, PP: 363: 374, (2010).

[11] Kovacs, "Fake" Facebook Friend Request Confirmation",http://news.softpedia.com/news/Fake-Facebook-Friend-Request-Confirmation-Emails-Lead-to-Adobe-Reader-Exploit-375836.shtml,Accessed 23 Oct 2014.

[12] Meligy, H. M. Ibrahim, and M. Torky. "A Framework for Detecting Cloning Attacks in OSN Based on a Novel Social Graph Topology." MECS, International Journal of Intelligent System and Application, 7(3), PP: 13-20, (2015).

[13] T. Jean, Y. Feh, " How to Create a Fake Facebook Profile",http://www.wikihow.com/Create-a-Fake-Facebook-Profile,Accessed 23 Oct 2014.

[14] Protalinski, "Facebook Estimates that Between 5.5% and 11.2% of accounts are fake", http://thenextweb.com/facebook/2014/02/03/facebook-estimates-5-5-11.2-accounts-fake/,Accessed 24 Oct 2014.

[15] Yu, M. Kaminsky, P B. Gibbons, and A. Flaxman, " SybilGuard: Defending Against Sybil Attacks Via Social Networks", Networking, IEEE/ACM Transactions on, 16(3), PP: 576-589, (2008).

[16] Yu, P. B. Gibbons, M. Kaminiski, X.Feng, " SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks", IEEE Symposium on Security and Privacy, 18(22), PP: 2-17, (2008).

[17] G. Danezis, and P. Mittall, " SybillInfer: Detecting Sybil Nodes Using Social Networks", Network and Distributed System Security Symposium - NDSS, http://libra.msra.cn/Publication/4727139/sybilinfer detecting-Sybil-nodes-using-social-networks, (2009), Accessed 25 Oct 2014.

[18] M. Fire, G. Katz, and Y. Elovici," Strangers Intrusion Detection Detecting Spammers and Fake Profiles in Social Networks Based on Topology Anomalies", HUMAN, 1(1), pp: 26-39, (2012).

[19] M.R. Khayyambashi, and F.S. Rizzi, "An Approach for Detecting Profile Cloning in Online Social Networks", 7th International Conference on e-Commerce in Developing Countries with Focus on e-Security (ECDC), IEEE, (2013).

[20] Gao, J. Hu, and C. Wilson, "Detecting and Characterizing Social Spam Campaigns "Proceedings of the 10th ACM SIGCOMM conference on Internet measurement. ACM, PP: 35-47, (2010).

[21] R. Baden, N. Spring, and B. Bhattacharjee, "Identifying Close Friends on the Internet", 8th ACM Workshop on Hot Topics in Networks , HotNets, New York, NY, USA,(2009).

[22] G. Wang, M. Mohanlal, C. Wilson, X. Wang, M. Metzger, H. Zheng, and B.Y. Zhao, "Social Turning Tests: Crowdsourcing Sybil Detection", The 20th Network & Distributed System Security Symposium, NDSS, (2013).

[23] Lescovec, and A.J. Krevel, "SNAP Datasets: Stanford Large Network Dataset Collection ", http://snap.stanford.edu/data,Accessed 2 Nov 2014.

[24] Benevenuto F, Magno, G, Rodriguez,T, and Almedia,

V, ”etecting Spammers on Twitter”, In 7th annual Collaboration, Electronic Messaging, Anti-Abuse and, Spam Conference (CEAS) Vol. 6, Redmond, Washington, US, (2010).

[25] Lee, K, Caverlee, J, and Webb,S. ”Uncovering social spammers: social honeypots+ machine learning.” Proceedings of the 33rd international ACM SIGIR conference on Research and development in information retrieval. ACM, Geneva Switzerland July 19 - 23, 2010.

Authors’ Profiles

Ali M. Meligy, A Professor of Computer Science, Department of Mathematics, Faculty of Science, Menoufyia University, Egypt. He worked as a Professor of Computer Science, faculty of Information Technology, Middle East University for Graduate Studies, Amman, Jordan from September 2006 to August 2009. He worked as a chair of the Department of Computer Science and Information Technology at Hussein Bin Talal University, Jordan. In 2002, he was a visiting Research Professor, Institute of Computer Sconce, Humboldt University, Berlin, Germany. In 2009, he was a visiting Research Professor, LRZ Computer Center, Munich University, Germany. His research interests involve Software Engineering, Parallel and Distributed Systems, Computer Networks, Information Security, Petri Nets, and Social Networks.

Hani M. Ibrahim, Lecturer of Computer Science, Department. of Mathematics, Faculty of Science, Menoufyia University, Egypt. In 2008, he obtained his Ph.D. degree in Computer Science, Department of Mathematics, Faculty of Science, Menoufyia University, Egypt. In 2004, he obtained his Master degree in Computer Science, Department of Mathematics, Faculty of Science, Menoufyia University, Egypt. His research interests include Image Processing, Pattern Recognition, Biometric, Neural Networks, Artificial Intelligence, and Social Networks.

Mohamed F. Torky, Born in Egypt in August 1986. He is a Ph.D. Candidate in Computer Science at Faculty of Science, Menoufyia University, Egypt. He obtained his Master degree in Computer Science, Department of Mathematics, Menoufyia University, Egypt, 2013. He works as an Assistant Lecturer in the department of Computer Science, MUST University, 6 October city, Egypt. His research interests include Computers and Information Security, Cryptography, and Social Networks Security and Privacy, Petri Nets Applications, Automata Applications.

How to cite this paper: Ali M. Meligy, Hani M. Ibrahim, Mohamed F. Torky,"Identity Verification Mechanism for Detecting Fake Profiles in Online Social Networks", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.1, pp.31-39, 2017.DOI: 10.5815/ijcnis.2017.01.04

