International Journal of Engineering & Technology, 7 (4.19) (2018) 919-925

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Fake Profiles Types of Online Social Networks: A Survey

Rafeef Kareem*[1], Wesam Bhaya[2]

[1,2] *Information Networks Department, College of IT, University of Babylon, Iraq*
**Corresponding Author E-mail: rafeef.kareem@yahoo.com*

Abstract

Today, OSNs (Online Social Networks) considered the most platforms common on the Internet. It plays a substantial role for users of the internet to hold out their everyday actions such as news reading, content sharing, product reviews, messages posting, and events discussing etc. Unfortunately, on the OSNs some new attacks have been recognized. Different types of spammers are existing in these OSNs. These cyber-criminals containing online fraudsters, sexual predators, catfishes, social bots, and advertising campaigners etc.
OSNs abuse in different ways especially by creating fake profiles to carry out scams and spread their content. The identities of all these malicious are so damaging to the service providers and the users. From the opinion of OSNs service providers, the loss of bandwidth moreover the overall reputation of the network is affected by fake profiles. Thus, needing more complex automated methods, and tremendous effort manpower to discover and stopping these harmful users.
This paper explains different kinds of OSNs risk generators such as cloned profiles, compromised profiles, and online bots (spam-bots, chat-bots, and social-bots). In addition, it presents several classifications of features that have been used for training classifiers in order to discover fake profiles. We try to show different ways that used to detect every kind of these malicious profiles. Also, this paper trying to show what is the dangerous type of profile attacks and the most popular in OSNs.

Keywords: *Online Social Networks, OSNs, Fake Profile, Fake Account.*

1. Introduction

OSNs, such as Twitter and Facebook, have become popular increasingly in the last few years' social networks used by peoples to share news, chat with friends or to make them in touch with their families. With over time the user interactions with colleagues, friends, people they consider trustworthy. This communication formed a social graph that takes controls on how to distribute the information in the social network. Generally, the that users received distributed messages by the users they are joined to is by the form of tweets, status updates or wall posts [1].
In the last few years, the social Web was threatened by fake criminals who trying persistently to break the privacy of OSN platforms users and attack them [2].
The attractiveness of criminals for social networking sites is growing, when the popularity of social networking sites growth, such as, the worms that exploit the old ideas that are applied to a new technology, that specifically target Myspace and Facebook users. Classic worms such as worm that used to spread the contacts in a victim's Outlook address book. Many e-mail users this type of tricks have already been seen now, but on social networking sites, they are not as well-known. although such attachments email might be increasing more suspicion [3].
The huge amount of user content that generated by OSNs is always under attack of a spammer because the OSNs provided it easily. The goals of cyber criminals are stealing professional, social or financial information by exposing the users with unwanted information on the web likes, pornography, or stealing the user's personal, political, etc. so as to trick them. From the users' point of view, there is no more secure, professional, personal, and even financial data.
Nowadays the attacker discovering a lot of ways to control on the user account in a social network the purpose of them are to exploiting these accounts in all ways that they can to do. In the next section, we will discuss many types of the OSNs profile account that exploited and created by the attacker to abuse them in any way that helps his purposes. [4].

2. OSNs Profiles

In OSNs, there are several different profiles. This section provides a classification of different legal and illegal profiles, with their features and the popular way that used to detect them. Also at the end of this paper, there is table presented summary of these typed, Figure1 shows the types of social profile that we will discuss some of them here.

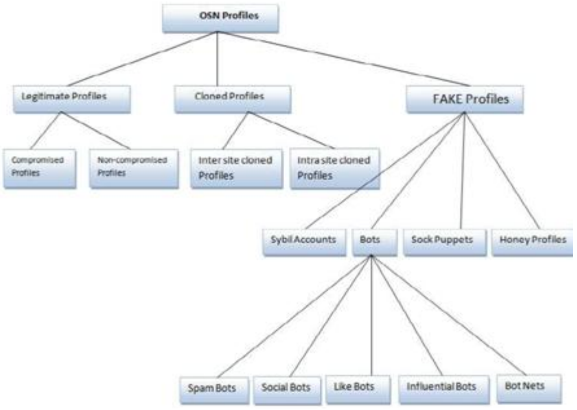

Fig. 1: Types of OSNs profiles [4]

2.1 Legitimate Profiles

It is consisting of two type of profiles:

2.1.1 Compromised Profiles

A compromised account is each legal account that has been taken over by an attacker. Because of compromised accounts are actually real accounts but the owner of them lost the controlling on them for any malware agent such as phisher, in another word the owner doesn't have complete control on their own account. So, the study considering that the Compromised accounts are the most complexes and difficult kind of accounts. Recently the studied have appeared that the spread of compromised profiles are more than 97% rather than fake profiles [4].

As a result of the previous reason, the attackers have the ability to control the owner's trusted relationships in his/her account, which has already been, so the attackers began to exploit and to compromised the legitimate accounts. There are many ways can be used to make an account from compromised type, such as, by exploiting the vulnerability of a cross-site scripting, or by stealing the user's login credentials using a phishing scam. Compromised accounts are the most valuable accounts to cybercriminals because these type of account let the attackers to spread malicious content more effectively by allowing them to have control of the trust relationship and the account history. Sensitive institutional, personal data and valuable computing resources are put at risk when accounts are compromised. Even accounts with nothing private or of value in email or personal files and limited or no access to institutional data are valuable to hackers [1].

Finally, acquaintances and intruders are two types of hackers that are used to make compromised accounts: the intruder is an unknown third party, harmful or shares misleading information is the way that an intruder work when compromises an account, Spammers are considered one of intruder's type. while an acquaintance is a relative, coworker, or friend of the original user [5].

2.1.1.1 Ways of the Accounts Are Compromised

There are several ways how accounts are compromises, which are [5]:

- **Password Stolen on Another Site.** It means that your password is Reusing on other different sites, that puts resources at risk, especially when those your (umich.edu) email is your username. Your account can be easily accessed if your account on those sites is compromised.
- **Password Sharing.** There is a time that you enforcing to sharing your password with a family member or a friend, the might exploit it to access to your account and misused it or they might not have been careful on it as you are.
- **Weak Password.** A simple or short password, can be vulnerable to brute-force techniques or guess.
- **Unsecured Network.** Remember always Use a Secure Internet Connection. because If you log in to a website like Wolverine Access while Wi-Fi network is not unprotected, your information account might be stolen.
- **Phishing.** Emails that send you asking to validate, upgrade, or verify, your account by providing your password or logging in to a webpage are most probably phishing scams.
- **Malware.** Using a computer infected with a virus or using a computer that not untrusted, or running a keyboard logger to other compromised malicious system.

2.1.1.2 Types of Compromised

Compromised accounts have four Types of them; Forced Shares, Pranks, Information Gathering, and Forced Follows, as follow [5]:

- **Forced Share:** When a hacker shares of malicious intent on the social media site or content that is false misleading. That type called a forced share compromised accounts

- **Prank:** The content that is shared by a hacker with others users for laughs that type is called a prank. It is involving random content, for example, confessions of love or song lyrics for the hacker.
- **Information Gathering:** Hacker using a user account to learn sensitive information about them, for example, spammers used their password to compromise the original user's other accounts, for instance. Bank account. hackers can share content by posts messages on social media with other users, that's for (pranks and forced shares). The Forced Follows is harder to detect than Forced Shares, because the Twitter API returns the current number of followers of a user when the tweet was collected rather than when the tweet was published to study detection of forced shares, researchers need to know which accounts will be compromised in the future, So That they need to keep track how the number of followers changes over time. The information gathering is considered as the harder one to detect, because of the hacker never change anything about the posting or account.
- **Forced Follow:** This type happened when the user account is forced by the hacker to follow other malicious or fake accounts.

2.1.2 Non Compromised Profiles

It means the account was not exploiting to be compromised profile but maybe they exploited to create another fake profile.

2.2 Cloned Profiles

The stealing process for the private information victim's so as to make one more profile that can get the private information of victim's friends, is called a cloned profile. In other words, the stealing of the existing user's profile identity and used it to create a new fake profile is also known profile cloning. They also called as (Identity Clone Attacks (ICAs)).[4]

The clone attack identity is discovered on OSNs that create fake identities of specific users. Rising the trust among mutual friends to do more tricks in the future and acquiring personal information of victim's friends' by appearing as the real user profile, that is the original aim of the adversary in this attack. There are two type of these attacks are defined already: the first one is cross-site profile cloning, and the second one is single site profile cloning. they discussed in the next subsection.[6]

2.2.1 Types of Cloned Profile

The clone profiles consisted of two types.

A. Single-Site Profile Cloning:

It also named Intra Site Profile Cloning. In the same social network, the real user profile is duplicated by the adversary and sending a friend request to users' friends by using this cloned profile. An unwitting user might believe that request is coming by a familiar user so the user will validate it, that makes the adversary accessing to user personal information very easy and starting to exploiting it in a suspicious way. Adversaries able to make one more account of an already existing user and pretend to be some real user with the same name. Figure 2 shows how it works [6].

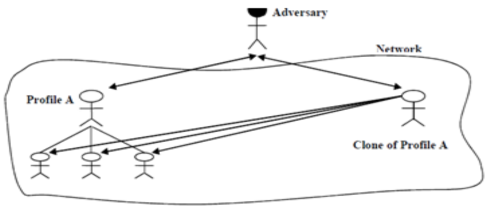

Fig. 2: Working of Single-Site Profile Cloning [4]

B. Cross-Site Cloning

In cross-site cloning (also called Intersite profile cloning), the adversary detects a user account in network A, then make a clone profile with that user account characteristics in network B which real user until now does not create an account on it (Figure 3).

Friend requests are sending by the adversary to account of the victim's friends in network B. The friends of the victim believe that they know the requests sender and validate them, when that friends validate the request, the adversary shell stealing their private information. The adversary used this to steal information to create many other clone profiles or to deceived some in the future. because of service providers think this kind of attack is a new user which is recording on these websites, so detecting it is very difficult for profiles owners and service providers. Detecting cloned profiles with more efficient methods can lead to more protection for users that using social networks, and also movement increasing for service providers to advance their level of security they provide on their platforms in the services.[6]

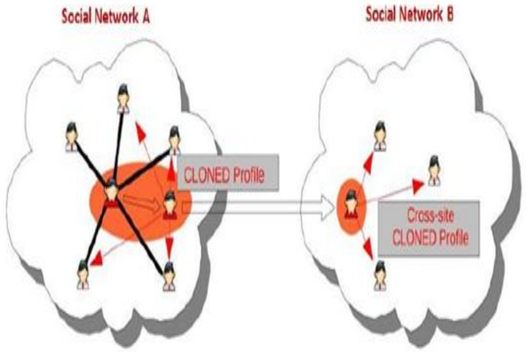

Fig. 3: Working of Cross Site Cloning [6]

It becomes very hard to discover these types of attacks, because of the Service Providers take it as a new register in these OSNs and The users handling with it as a request friend coming from a legal user. Discovering cloned profiles can improve the security level in OSNs which in turn will keep users protected from any type of illegal access.

2.3 Fake Profiles

The fake profiles are unlike of cloned profile in different ways. an adversary makes one more account of the already existing one that happens in case of cloned profiles, and that not the way of fake profiles work Cloned Profiles are usually created to take out the victim information or her/his friends but the Fake Profiles are used for different working for example advertising, Spamming, etc.,

There is various purposed make people create the fake profile e.g., just to have one more account, or just to create multiple accounts deliberately to enter into people's subgraph. The fake account has three reasons to be created, and have two ways that used to create it.: first: is created by manually creating one more account, and the other is created by writing a script.

While the three main reasons for created fake profiles is: one: to enhance the level of trust or popularity among the others. two: is to distribute the content spam among the real users. Three: OSNs service providers allow one account per email-id connection or per mobile, and to get over this limitation, users made one more account using various phone numbers or email-ids [4].

Because of Fake accounts are lack trusted connections, and they are not central nodes in the graph and They also have no history or unique data, so that they have limited virility. Because of these reasons, compromised accounts are much more valuable to attackers than fake account. The entities of the fake account are existing in anywhere on the internet like a social network, shopping sites, discussion blogs, forums, websites, online dating websites, and banking systems, etc. Fake profiles are hurtful for OSNs and can be riskier in the future if not discovering at an early time. There is a different type of fake profiles in OSNs, we are described some of the popular ones in the next subsections [7].

2.3.1 Sockpuppet

There are accounts on the Internet are created with the purpose to exploiting them in different ways to deceive Internet users, for example, used to convince people of a particular product or to convince them of a particular company or to promote a tourist destination, these accounts called Sockpuppet.

In different words, Sockpuppet is an account that is created for the purpose of deceiving or promoting a something or for someone on social networking sites, and discussion forums. Often, in the case of social sites, blogs, users create new accounts called the account sockpuppet. If There are two different accounts belonging to the same person are found on any social network or news blog or discussion forum, these accounts are called Sockpuppet pair [8].

2.3.2 Sybil Attack

Our systems today are vulnerable to Sybil attacks, in which an attacker injects multiple fake accounts into the system to compromise security and privacy. Sybil attacks are becoming pose a significant threat to online social systems because it increasingly extended. An attacker can inject in the system multiple identities colluding to compromise privacy and security. Latterly, the widespread rising of OSNs let them to be for Sybil attacks like attractive victims. In popular social networks such as Twitter and Facebook, there are tens of millions of Sybil accounts and these numbers are rising. Via propagating social malware, the Attackers can leverage Sybil accounts to compromise system security in addition to system privacy via learning users' private information [9].

In the design of distributed systems Avoiding Sybil or multiple identities, attacks are known to be an essential problem. Multiple influence and identities the working of systems that rely upon open membership can create by Malicious attackers. Certification authority provides usually the protections against the attacks Sybil rely on trusted identities. But users' demands to view and present these trusted identities are inconsistent with the open membership that is the cause of the success of the system in the first place. Latterly, there has been a study on the application of social networks in the research community to mitigate Sybil attacks.

Unlike traditional solutions, a number of schemes have been suggesting that attempt to protect against Sybil's in a social network by using the property structure of the social networks. These schemes require to rely on the trust that is embodied in existing social relationships between users and don't require central trusted identities. there are many methods, mechanisms and algorithms ‹Appear to detect Sybil nods, one approach to preventing these "Sybil attacks" is to have a trusted agency certify identities[10], However we discuss some of the method in the next subsection [11].

2.3.2.1. Sybil Community Detectors

There are algorithms that used for decentralized detection performing of Sybil nodes on social graphs, these algorithms are (Sybil Limit, Sybil Rank, Sybil Guard, and, Sybil Infer). Two assumptions of normal and Sybil user behavior that the algorithms are based on, (one) because of the friend requests from unknown strangers didn't accept by normal users, that make The numbers of edges between Sybil's and normal users will be limited. (Two) Attackers can create unlimited edges and Sybil's between them.

Because of they make Sybil's appear more legitimate to normal users, that make the edges between Sybil's are beneficial depending on these assumptions, and because of the number of edges between Sybil's is greater than the number of edges connecting to normal users, Sybils tend to form tight-knit clusters.

The edges connecting Sybil's and normal users are called attack edges, but we called the edges between Sybil's as Sybil edges. The algorithms of Sybil detection used to locate the small number of edge cuts that separate the Sybil region from the social graph to identify Sybil clusters.

The max-flow approach is used by sumup uses, while Sybil Guard, Sybil Limit, and Sybil Infer, walks for this purpose all leverage specially engineered randomly. All of these algorithms have appeared that all algorithms are generalize to the problem of communities detecting Sybil nodes, although all of these algorithms are implemented differently [12]**.**

2.3.3 Bots as Fake Profiles

We called some of the computer programs that interact with humans by producing some data, its especially interact with the persons using the internet (netizens) in order to alter their behavior, as a bot. Bots generated More than 60% of the total web data. Online bot is also called as a web robots or simply bot, these bots perform various tasks automatically and quickly that the human never do it alone. Fundamentally, the bot was designed to help humans to make their works automatic and speed up it The basic purpose of bots was work as an automatic responder to customer queries, act as a medical expert to resolve health-related issues and automatic travel guide, and automatically aggregate contents from various news sources. But in these days the bots are exploiting by the public in different domains. Bots are used in social networks, to retweet a post without validating its source so as to make it virus-related(viral). Bots are used in online multiplayer games, to gain the unfair benefits. Since the bot wants to interact with humans and create social networks, which are even more difficult to identify, so they act as automated avatars.

Bots also used to send friend requests in OSNs, posting messages and, influence users. Sybil accounts are similar to bot but the basic difference is that the bots are automated computer programs, while Sybil accounts are handled by users manually. These online computer programs used web data crawling to extracts and identify the information from web servers at a higher speed which was not possible by a human alone, and that is the main use of bots. Bots become a serious threat to the internet because they designed for malicious activities.

In a variety of ways, Bots was added to social media systems. Depending on the social media system, a new account may be created with the explicit intention of having a bot control it. This may even be possible automatically, but the platforms of most social network work to guaranty that only human can be creating new accounts. Bots may also be added as followers to accounts that the purchaser does not control. Bots can be of two kinds malignant and benign. The designers of Malignant bot might have many goals in their mind e.g. to support and spread fake, to change person thought about a product, or to misdirect people, or malicious news. So, depending on the function of them we divided the bots into 5 categories as you see in the figure below. we show three categories from them in the following subsections. Figure 4 shows the Bots types [4].

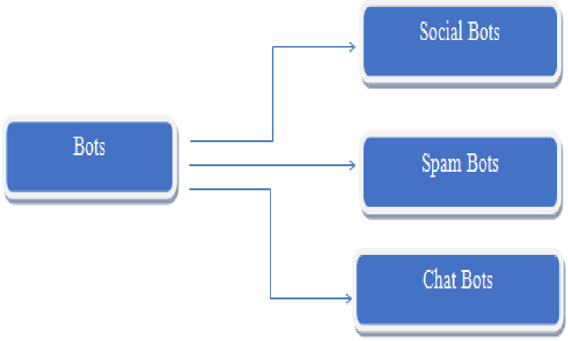

Fig. 4: type of bots

2.3.3.1 Spam Bots

It one of bot's type that is designed for the purpose of malicious activities only. The original goal of design the spam bots are to spreading harmful content such as links, to influence a particular article which is not that worthy, pornographic websites or pollutes the network by creating a huge number of unwanted relationships, paid contents, to shill for any person or organization, or advertisements.

Normal bots are used in a different form than the Spam bots are those bots which very extended unsolicited contents among users without their authorization. But the normal bots are developed for daily activities like social bots: which mimic a normal user, or weather update (e.g. Twitter bots). Social bot software was used with an OSN profile to instructed and developed a social bot perform operations such as, writing and reading the creating social interactions, social content(spam), joining the online social communities, and behaving like real users [2].

2.3.3.2 Social Bots

A social bot is a computer program that considers as a new seed that mimics real users and controls OSN accounts. social bots can be used to influence OSN. In another word, the automation software that has the ability to perform basic activities e.g. sending a connection request and posting a message and controls on a particular OSNs by an account is called as a social bot. since the social bots behave like humans and keep users busy, so they consider the higher complex computer programs. To reach and infect a maximum number of users and exposed hosts, Bots are announcing themselves like viruses.

A self-declared bots different from socialbot (for example. "Twitter bots that post up-to-date weather forecasts") and spambots is that it is designed to be stealthy the socialbot able to compromising the social graph of a targeted OSN infiltrating (i.e., connecting to) its users so as to reach an influential position, because socialbot able to passing itself as a human being. This feature can be exploited to distribute the propaganda and wrong information so as to prejudice the public opinion. As socialbots sneak a targeted OSN, they can further be gathering the data of private users' e.g. phone numbers, email addresses, etc. like this data are being valuable to an adversary, and can be large-scale phishing campaigns, spam email, and used for online profiling and. So not be shocked when that various type of socialbots are being presented to selling with prices beginning from $29 and up to $2,500 per multi-featured bot in the Internet black- market [13].

2.3.3.3 Chat Bots

We called a software that interactive to automate tasks for a human with a chat service as a Chabot. The term bot, is a point to programs automated, these programs do not need to an operator human, and The bot term is short for the robot when the engineering started to design the first-generation of Chatbots, was for chat users guesting, for example, quote bots or quiz or to help operate chat rooms. However, Chatbots are now sending chat spam that is the main enterprise of it.

Because of the commercialization of the Internet via either links user profile or links in chat messages the Chatbots deliver spam URLs. the spam links are distributed in different chat rooms to thousands of users, and the controlling on few hundred chat bots it all do by single bot operator, that made bots chat to the operator very helpful of the bot who is paid per-click through affiliate programs.

There is many other abusing used to the bots, for example, booting, similar malicious activities, spreading malware, and phishing. The abuse of chat bots is defending by A few countermeasures, but none of them are very effective. To avoid bot's chats linking rooms chat Yahoo! was use the CAPTCHA tests. This defensing becomes ineffectual as bot's chats bypass captcha tests with human-assisted. We saw that even after the deployment of CAPTCHA tests the bots continuing to join chat rooms with the majority members of a chat room or with the chat rooms. Depend on key phrases or Third-party chat clients filter out chat bots, or keywords that are well- known to use by bot's chats, it couldn't catch those unknown bots chat that do not use the known phrase or keywords, and this is the drawback with this approach [14]. Table 1 shows different OSNs profile attacks.

Table 1: Summery of various OSNs profile

	Cloned Profiles	**Sybil Accounts**	**Compromised Profiles**	**Bots**	**Sock Puppets**
Definition	Stealing the personality of a user's profile that existing before to generate a new one considered as a fake profile to the existing one to employ it in all malicious behavior such as publish immoral sites, etc.	it is the accounts created manually by malware users to attack the trusted network. The hackers can exploit these accounts to discover the security of the specific system and also the privacy of the system by studying the private information of users.	it considered the complex fake profile to discover because it actually a realistic account but its creator lose all or partial control on it to a phisher or any malicious agent.	It is a software that does different tasks automatically and quickly that the human impossible do it alone.	It created with a purpose, that is to cheat others or to support something or someone on social networking sites, blogs, etc.
Purpose	* joy and amusement * blacken or cheating a person * theft people's private information	*To compromise the privacy and security, and arrival to resources, etc. *discovering the security of any system.	* for a person blacken or trick. * To propagations malicious content by using the trusted network. * To Legal abuse	*work as a competent medical to issues health treatment. * To collect contents automatically from different sources news. * it acts to customer queries as a responder auto.	* To bypass a ban or comment from a website. *To a Public Opinion Juggle * To support or defend an organization or a person.
Target Networks	Facebook, Myspace, Twitter, LinkedIn.	LinkedIn, Twitter, Facebook.	Twitter, Facebook, Online Payment Systems, LinkedIn, etc.	Twitter, Facebook, LinkedIn.	Facebook, Wikipedia, Twitter, LinkedIn.
Effected Group	People without online, online users, accounts, etc.	Politicians, Organizations, celebrities, Netizens, etc.	user-friends, Real account owners.	Bloggers, OSNs, OSN users, etc.	Wikipedia users, Researchers, Bloggers.
Types	Intra profile cloning site, Inter profile cloning site.	______________	Complete-Compromised(CC). Partial-Compromised(PC).	Influential-bots, Social-bots, Spam-bots, and chat-bots.	Meat puppet, sock puppet, Strawman.
References	[15][6][16]	[9] [17][11]	[1][18]	[12] [19]	[8] [19] [21]

2.3 Methods Used for Fake Profile Detection

In previous sections, we describe a different kind of OSNs profiles and their properties. This section present, some of several numbers of techniques that used by different researchers to discover fake profiles.

In [6], researchers based on the similarities, divide the Facebook network into smaller communities, so as to, check whether it is a clone or not. All the profiles similar to the real profiles are gathered to calculate the strength of the relationship.

In [16], for detecting social network profile cloning, the researchers have suggested a method by system designing with three constituents called information profile verifier, profile hunter, and distiller. To uniquely identify the profile, the distiller selects attributes which can be used and extracts from real user profiles the information. Then the Profile hunter locates the profiles of the user on different OSN and processes the information passed by information distiller to generate a record profile which contains links to all the profiles returned by the result and link to the user's real profile. then the Profile verifier gathering the score that similar between all the profiles and display the result to the user.

In [15], demonstrate two profile cloning attacks type in OSN. thereafter, the study defined profile similarity and strength of relationship measures by using a new approach for detecting clone identities. It will be decided which profile is a clone and which one is genuine by a predetermined threshold, depending on similar attributes and strength of relationship among users which are computed in detection steps. Finally, to demonstrate the effectiveness of the proposed approach the experimental results are presented.

The authors of [22] avoid and stop the attack of cloning type approach of an attacking methodology, during a conversation between the clone and real profiles, Fake content is injected into the network and an ICA is carried out to collect information.

The authors in [19] discuss out of four (support vector machine, decision tree, neural networks, and K-nearest neighbor) techniques classification, and found that the best one in predicting spam bots in the Twitter network is a Bayesian classifier.

In [21], the authors display the natural language processing techniques to be using in a sock puppet detection method for Wikipedia network. they also defense of Sybil accounts and paid a vital attention towards the detection and their respective attacks.

In [23], researchers have discussed the way to identifying influential nodes in complex networks by using a semi-local measure centrality as a tradeoff between other time-consuming measures and the low relevant degree centrality.

The [24] show us a way to detect the Sybil profile by using anew, a new structure based method that called Sybil scar, to perform Sybil detection in OSNs.

The authors of [1] were used to detect compromised user accounts in social networks. They apply it in two popular social networking sites, Facebook and Twitter. They use anomaly detection to identify accounts that experience a sudden change in behavior and a composition of statistical modeling. They developed a tool, called COMPA, that Implements their approach, and we ran it on a dataset of 106 million Facebook messages as well as on a large-scale dataset of more than 1.4 billion publicly-available Twitter messages. COMPA was able to identify compromised accounts on both social networks with high precision.

The [25] show the way to detect the profiles in twitter if they fake profile or normal one by using technology called (Entropy Minimization Discretization (EMD)) on numerical features and analyzed the results of the Naïve Bayes algorithm).

The author in [26] used many type of classification algorithms to detect the fake account in twitter like decision tree, nave base, neural network, support vector machine and random forest .

Table 2 below explore the brief conclusion of the detection techniques that it has been shown in this section.

Table 2: Explore Ways to Detect The Fake Profiles

	Properties	**Reference**	**Year**
Clone Profile	Using a profile similarity algorithm to measure and detect possibly cloned identity in OSNs through the use of social links and attributes.	[22]	2011
	Designing a system that comprised three main components (Information distiller, Profile Verifier, Profile Hunter)	[16]	2011
	There are three steps to detect cloned profiles in a same social network, (Collecting Suspicious Profiles, Profile Evaluation, Attribute Similarity Measure)	[15]	2014
	Using an approach which consists of 6 steps (Discovering community the social network graph, Extraction user's attribute, Search in the community, Selecting profile, Computing strength of the relationship, Decision making)	[6]	2014
Compromised Profile	It has been using a novel approach to detect compromised user accounts in social networks, they approach uses a composition of statistical modeling and anomaly detection to identify accounts that experience a sudden change in behavior.	[1]	2012
Sybil Profiles	It has been proposing a Sybil lascar, a new structure method to perform Sybil detection in OSNs.	[24]	2017
Sock Puppet	Uses authorship attribution methods for the detection of sock puppeteering in Wikipedia	[21]	2013
Spam Bots	It has been using four techniques of classification and found that the best one in predicting spam bots in the Twitter network is a Bayesian classifier.	[19]	2010
Fake accounts	Used the nave base algorithm to detect if the accounts are fake or normal	[25]	2017
	Used five type of classification algorithms to detect the fake account in twitter .	[26]	2016

3. Conclusions

In recent years, the use of the network has increased in general and the social networking sites such as Facebook, Twitter, and Instagram in particular. People created accounts on each social network to communicate with family, friends or for scientific or entertainment purposes. But because the registered user put his private information, the attackers have started to create different types of the fake account by exploiting this personal information for cyber-criminal used. Various types of fake accounts have appeared, such as Compromise (the most difficult and dangerous type), Clone, Sybil, Bot fake account, etc. In the other site, many algorithms and technologies were appeared, to detected the fake accounts and to prevent the exploitation of real or personal information to prevent exploit them by the attackers for malicious purposes, but we couldn't tell any technologies are the best because every one of them different in the speed of execution and the rate of accuracy.

References

[1] M. Egele, C. Kruegel, and G. Vigna, "C OMPA : Detecting Compromised Accounts on Social Networks," NDSS Sympoium, 2013.

[2] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "Design and analysis of a social botnet," Comput. Networks, vol. 57, pp. 556–578, 2012.

[3] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us," Proc. 18th Int. Conf. World wide web - WWW '09, p. 551, 2009.

[4] M. A. Wani and S. Jabin, "A sneak into the Devil's Colony - Fake Profiles in Online Social Networks," eprint arXiv:1705.09929, 2017.

[5] C. VanDam, J. Tang, and P.-N. Tan, "Understanding compromised accounts on Twitter," Proc. Int. Conf. Web Intell. - WI '17, pp. 737–744, 2017.

[6] M. Y. Kharaji and F. S. Rizi, "An IAC Approach for Detecting Profile Cloning in Online Social Networks," Int. J. Netw. Secur. Its Appl. (IJNSA), vol. 6, no. 1, pp. 75–90, 2014.

[7] T. Stein, E. Chen, and K. Mangla, "Facebook immune system," Proc. 4th Work. Soc. Netw. Syst. - SNS '11, vol. m, pp. 1–8, 2011.

[8] X. Zheng, Y. M. Lai, K. P. Chow, L. C. K. Hui, and S. M. Yiu, "Sockpuppet detection in online discussion forums," Proc. - 7th Int. Conf. Intell. Inf. Hiding Multimed. Signal Process. IIHMSP 2011, pp. 374–377, 2011.

[9] P. Gao, N. Z. Gong, S. Kulkarni, K. Thomas, and P. Mittal, "SybilFrame: A Defense-in-Depth Framework for Structure-Based Sybil Detection," Comput. Res. Repos., p. 17, 2015.

[10] J. R. Douceur, "The Sybil Attack," Springer-Verlag London, UK, IPTPS '01 Revised Papers from the First International Workshop on Peer-to-Peer Systems pp. 251–260, 2002.

[11] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, "An analysis of social network-based Sybil defenses," Proc. ACM SIGCOMM 2010 Conf. SIGCOMM - SIGCOMM '10, p. 363, 2010.

[12] Z. Yang, C. Wilson, X. Wang, T. Gao, B. Y. Zhao, and Y. Dai, "Uncovering Social Network Sybils in the Wild," Internet Meas. Conf., vol. 8, no. 1, 2011.

[13] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "The socialbot network: when bots socialize for fame and money," Acm, p. 93, 2011.

[14] B. A. Shawar and E. Atwell, "Measurement and Classification of Humans and Bots in Internet Chat," Bridg. Gap Acad. Ind. Res. Dialog Technol. Work. Proc., no. August, pp. 89–96, 2007.

[15] F. Salehi Rizi et al., "A New Approach for Finding Cloned Profiles in Online Social Networks," arXiv Prepr. arXiv1406.7377, vol. 6, no. April, pp. 25–37, 2014.

[16] G. Kontaxis, I. Polakis, S. Ioannidis, and E. P. Markatos, "Detecting social network profile cloning," 2011 IEEE Int. Conf. Pervasive Comput. Commun. Work. PERCOM Work. 2011, pp. 295–300, 2011.

[17] H. Yu et al., "SybilGuard," Proc. 2006 Conf. Appl. Technol. Archit. Protoc. Comput. Commun. - SIGCOMM '06, vol. pages, no. 3, p. 267, 2006.

[18] D. Savage, X. Zhang, X. Yu, P. Chou, and Q. Wang, "Anomaly detection in online social networks," Soc. Networks, vol. 39, no. 1, pp. 62–70, 2014.

[19] A. Wang, "Detecting spam bots in online social networking sites: a machine learning approach," Data Appl. Secur. Priv. XXIV, pp. 335–342, 2010.

[20] Z. Bu, Z. Xia, and J. Wang, "A sock puppet detection algorithm on virtual spaces," Knowledge-Based Syst., vol. 37, pp. 366–377, 2013.

[21] T. Solorio, R. Hasan, and M. Mizan, "A Case Study of Sockpuppet Detection in Wikipedia," Proc. Work. Lang. Anal. Soc. Media, no. Lasm, pp. 59–68, 2013.

[22] B. Bhumiratana, "A model for automating persistent identity clone in online social network," Proc. 10th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2011, 8th IEEE Int. Conf. Embed. Softw. Syst. ICESS 2011, 6th Int. Conf. FCST 2011, pp. 681–686, 2011.

[23] D. Chen, L. Lü, M. S. Shang, Y. C. Zhang, and T. Zhou, "Identifying influential nodes in complex networks," Phys. A Stat. Mech. its Appl., vol. 391, no. 4, pp. 1777–1787, 2012.

[24] B. Wang, L. Zhang, and N. Z. Gong, "SybilSCAR: Sybil detection in online social networks via local rule based propagation," IEEE INFOCOM 2017 - IEEE Conf. Comput. Commun., no. May, pp. 1–9, 2017.

[25] B. Erşahin, Ö. Aktaş, D. Kilmç, and C. Akyol, "Twitter fake account detection," 2nd Int. Conf. Comput. Sci. Eng. UBMK 2017, pp. 388–392, 2017.

[26] A. El Azab, A. M. Idrees, M. A. Mahmoud, and H. Hefny, "Fake Account Detection in Twitter Based on Minimum Weighted Feature set," Int. J. Comput. Electr. Autom. Control Inf. Eng., vol. 10, no. 1, pp. 13–18, 2016.