ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 4, July 2016

Sybil Attack in Internet of Things

Sushama Pawar, Pankaj Vanwari

Abstract*—Due to improvement in the technology the usage of social network is now days also increase. It becomes important to maintain the distribution system in several type of communication and the social network and perform their action in online social network. Internet of Thing systems is extremely vulnerable to Sybil attacks, in which a malicious user controls a large number of Sybil to act together through a secret understanding, especially with evil or harmful intent to break the system laws. The emerging Internet-of-Things (IoT) are vulnerable to Sybil attacks where attackers can manipulate fake identities to compromise the effectiveness of the Internet of Things and even disseminate spam phishing. Many security mechanisms are based on specific assumptions of identity and are vulnerable to attacks when these assumptions are violated. The Sybil Attack is fundamental problem in many systems and it has so far resisted a universally applicable solution. In this paper Survey is explorers on different types of Sybil Attack and their defense mechanism in the Internet of Things. Specifically, first define three types Sybil attacks: SA-1, SA-2, and SA-3 according to the Sybil attacker's capabilities. And then present some Sybil defence schemes, including social graph-based Sybil detection (SGSD), behaviour classification-based Sybil detection (BCSD), and mobile Sybil detection (MSD) with the comprehensive comparisons. Finally, we discuss the challenging research issues and future directions for Sybil defence in IoT.

***Index Terms*—Sybil Attack, Internet of things, Social network, SGSD, BCSD, MSD**

I. INTRODUCTION

It is easier than ever to create fake identities and user accounts in today's online communities. Despite increasing efforts from providers, existing services cannot prevent malicious entities from creating large numbers of fake accounts or Sybil's. Current defence mechanisms are largely ineffective. There are two complimentary tactics for dealing with Sybil attacks [1], [6], [7]. The first is prevention: building defences mechanisms that make it impossible for attackers to gain access to the network in the first place, usually through identity verification schemes. Here considers the second tactic: mitigation or detecting Sybil's by their abnormal characteristics. We describe a new approach to Sybil detection rooted in the fundamental behavioural patterns that separate real and Sybil users. Specifically, S the use of clickstream models as a tool to detect fake identities in online services such as social networks. Clickstreams are traces of click-through events generated by online users during each web browsing "session," and have been used in the past to model web traffic and user browsing patterns Intuitively, Sybil's and real users have very different goals in their usage of online services: where real users likely partake of numerous features in the system, Sybil's focus on specific actions (i.e. acquiring friends and disseminating spam) while trying to maximize utility per time spent. We build weighted graphs of these sequences that capture pairwise "similarity distance" between clickstreams, and apply clustering to identify groups of user behaviour patterns [1], [3]. To the best of our knowledge, first to study clickstream models as a way to detect fake accounts in online social networks. Moving forward, believing clickstream models are a valuable tool that can complement existing techniques, by not only detecting well disguised Sybil accounts, but also reducing the activity level of any remaining Sybil's to that of normal users.

A. Basic concepts

Distributed systems are vulnerable to Sybil attacks, in which an adversary creates many bogus identities, called Sybil identities, or Collaborative and recommendation-based computer systems are plagued by attackers who create fake or malicious identities to gain more influence in the system such attacks are often referred to as "Sybil attacks" and compromises the running of the system or pollutes the system with fake information. The Sybil identities can "suppress" the honest identities in a variety of tasks, including online content ranking, file sharing, reputation systems etc. Recently, there has been an increasing interest in defending against Sybil attacks in social networks. In a social network, two user identities share a link if a relationship is established between them. Each identity is represented as a node in the social graph.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 4, July 2016

B. Sybil Attack in Internet of Things

With the embedded sensors on objects, IoT can sense the information from the environments, the objects and our body (via sensor network, radio-frequency identification (RFID) technique, wearable devices, etc. With the emerging wireless communication techniques, such as short-range wireless communications and Wi-Fi, IoT can enable users to share information with others in social network and the Internet of connected vehicles. Furthermore, by integrating the sensing, communication, and computation capabilities IoT can offer diverse intelligent services to form smart home, smart grid, smart community, and smart city as shown in Fig. I.1

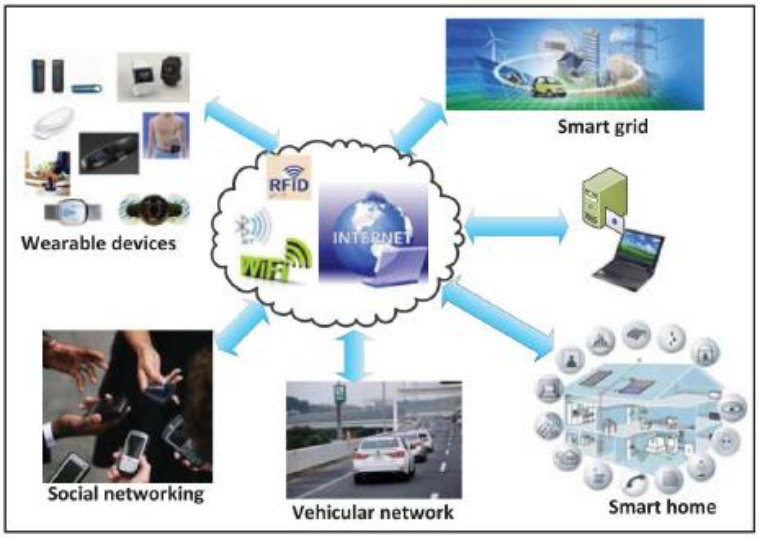


Fig.I.1 Overview of Internet of Thing

C. Introduction to Sybil Attack

The emerging IoT is vulnerable to Sybil attacks where attackers can manipulate fake identities to compromise the effectiveness of the systems. In the presence of Sybil attacks, the IoT systems may generate wrong reports, and users might receive spam and lose their privacy. These Sybil accounts not only spread spam and advertisements, but also disseminate malware and fishing websites to others to steal other users' private information. Since most Sybil attackers behave similarly to normal users, to find out whether an account is Sybil or not is extremely difficult, which makes Sybil defence of paramount importance in the IoT.

D. Categories of Sybil Attacks

James Newsome et al. have mentioned different categories of Sybil attacks [11]

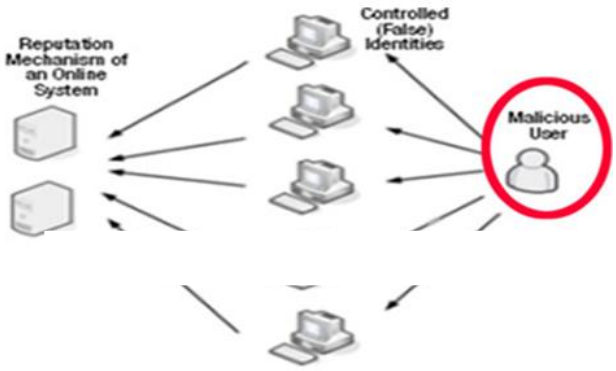


Fig I.2 Illustration of Sybil Attack

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 4, July 2016

1) Direct vs. Indirect Communications

In Direct Communication type attack, the Sybil nodes communicate directly with legitimate nodes. When a legitimate node sends a radio message to a Sybil node, there is possibility of listening message by one of the malicious devices. Similarly, messages which are sent from Sybil nodes are in reality sent from one of the malicious devices. In general, the attackers with much more direct communications are much more difficult to detect. In Indirect Communication attack, no legitimate nodes are able to communicate directly with the Sybil nodes. Instead one or more of the malicious devices claims to able to reach the Sybil nodes routed through the legitimate node.

2) Simultaneous vs. Non-Simultaneous

In Simultaneous attack, the attacker may try to have his Sybil identities all participate in the network at once. A particular hardware entity can only act as one identity at a time. In Non-Simultaneous attack, the attacker might present a large number of identities slowly over a period of time, somehow only acting as a small number of identities at any given time. The attacker can do this by having one identity seem to leave the network, and have another identity join in its place. A particular identity might leave and join multiple times, or the attacker might only use each identity once. Another possibility is that the attacker could have several physical devices in the network, and could have these devices exchange their identities.

3) Fabricated vs. Stolen Identities

In Fabricated Identities, the attacker can simply create arbitrary new Sybil identities. For instance, if each node is identified by a 32-bit integer, the attacker can simply assign each Sybil node a random 32-bit value. In Stolen Identities, an attacker cannot produce new identities. For example, suppose the name space is intentionally limited to prevent attackers from inserting new identities.

4) Insider vs. Outsider

Whether an attack is an insider or outsider directly determines the capability of the attacker. Attacker holds at least one genuine identity for an insider and claims that as if she receives certain data from the other nodes, and that is by using the fake identities. Distributed system assumes that each node is honest and therefore assumes that the false data can be easily forwarded to the whole system. However, for an outsider, she is any illegal or says dishonest entity; before launching or inducing a Sybil attack, she needs to first access the system. But, distributed systems use some kind of authentication to prevent illegal access, for example, entering a password, data encryption.

5) Selfish vs. Malicious

For security-related problems, there are two different types of attackers: either selfish or malicious. Selfish attackers manipulate the false data just for their own advantage. While malicious attackers attempt to threaten or weaken a system. For instance, in the previous critical resource accessing example, if the attacker has resource accessing rights all to her, then definitely she is a malicious attacker, because others cannot use the resource. However, if other users can also access the resource with a smaller amount of probability, then she is selfish attacker.

6) Busy vs. Idle

All Sybil identities can participate in a distributed system simultaneously, or only some of them can work, while others are in an idle state. If the attacker can very easily get ample of fake identities, some Sybil nodes that are idle could make them more real, as an honest node may leave or re-enter the system many times. However, the power of Sybil attacks results from the number of the identities. Obtaining a large number of identities is if very difficult, then the attacker must use all of them in order to launch a successful attack.

7) Discarded vs. Retained

For an attacker, managing of old Sybil identities is really necessary. After locating a Sybil node, further one can identify the others by monitoring the claimed communication between a suspect node and the detected Sybil node. Because the attacker is not aware of whether the old identities have been detected yet, once in a while, she has to determine whether or not to reject them.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 4, July 2016

II. TYPES OF SYBIL ATTACKS

This chapter focuses on detailed description of Sybil attacks along with its types and defense mechanism in Sybil attack.

A. Sybil Attack

Sybil attack is process of creating fake accounts in online social network. For example creating fake accounts on Facebook, LinkedIn etc. Here we provide the survey of Sybil attacks and their defense mechanism in Internet of Things. Specifically three types of Sybil attacks in distribution system and their defense schemes with comparisons.[1],[2],[4],[10]The different characteristics including social structure and behavior between Sybil attackers and normal users could be used to identify.In this paper, the main aim is to understand the three basic types of Sybil attack defenses[6],[7],[8]

i.e. 1. Social graph based Sybil detection
2. Behavior classification based Sybil detection
3. Mobile Sybil detection.

Problem statements of three of them in details and out of three defense mechanism on one Sybil defenses in short i.e. Social Graph based Sybil detection and briefly explain Behavior classification based Sybil detection. Sybil attacks exist in the IoT to maliciously manipulate the systems. In this section, we define three types of Sybil attacks. Following are the types of Sybil Attack.

1) SA-1 Sybil attack

The SA-1 attackers usually build connections within the Sybil community as shown in Fig. 3.1 i.e., Sybil nodes tightly connect with other Sybil nodes. In other words, the number of social connections between Sybil nodes and honest ones is limited, i.e. the number of SA-1 attack edges is limited. The SA-1 attackers usually exist in sensing domain and social domain[1]. The main goal is to manipulate the overall option or popularity. For example, in an online voting system, SA-1 can illegally forge a massive number of identities to act as normal users and submit the votes with the biased options. The final voting result might be manipulated by the SA-1 attackers, since a considerable portion of votes are from the SA-1 attackers.

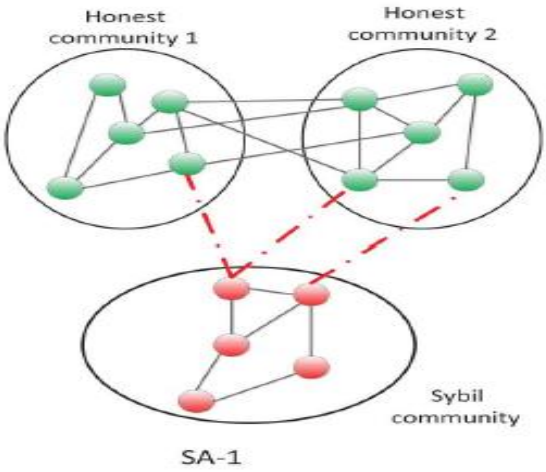


Fig.II.1 SA-1

2) SA-2 SYBIL ATTACK

SA-2 attackers usually exist in social domain. Unlike SA-1, SA-2 is able to build the social connections not only among Sybil identities but also with the normal users. In other words, the capability of SA-2 is strong to mimic the normal user's social structures from the perspective of social graph. Therefore, the number of attack edges is large as shown in fig 2. The goal of SA-2 is to disseminate spam, advertisements, and malware; steal and violate user's privacy; and maliciously manipulate the reputation system. For example, in OSNs, SA-2 can forge the profiles and friend list as normal users, but purposely spread spam, advertisements, and malware. SA-2 would focus on some specific behaviour and repeat them in the high frequency.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 4, July 2016

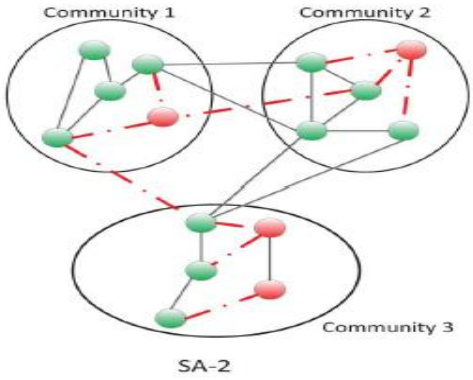
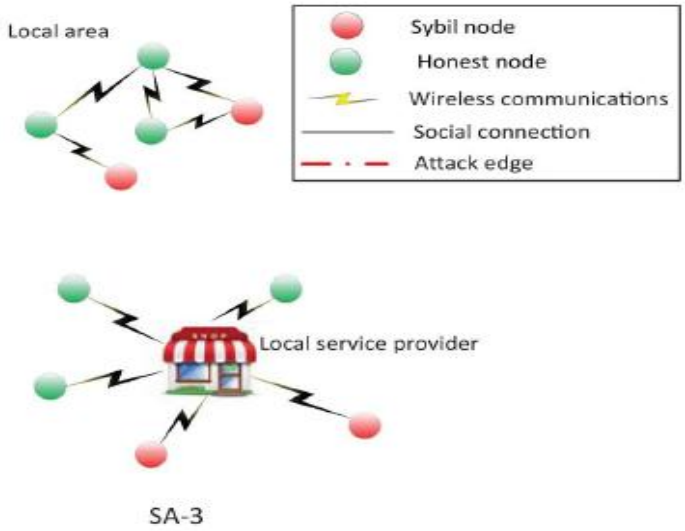


Fig. II.2 SA-2

3) SA-3 SYBIL ATTACK

SA-3 Sybil attack usually exists in mobile networks (i.e., mobile domain). The primary goal of SA-3 is similar to that of SA-2. However, the impact of SA-3 may be in a local area or within a short period. Due to the dynamics of mobile networks, mobile users cannot keep connections with others for the long time, or the connections are intermittent fig 3 shows the attack in mobile domain. Furthermore, the centralized authority cannot exist in mobile networks at all the time. Thus, unlike that in the online system, the social relationships, global social structure, topology, and historical behaviour patterns in mobile networks are not easy to obtain for Sybil defence toward SA-3. The mobility and lack of global information result in difficulties in SA-3 defence compared with the defence on SA-1 and SA-2.



B. Detection methods in Sybil Attack

To determine whether a suspect node is Sybil or not, Sybil Guard and Sybil Limit both rely on the assumption that social networks are fast mixing, and the number of attack edges is limited. To identify Sybil nodes, the schemes make use of random routes, a special kind of random walks in which each node uses a pre-computed random permutation as a one-to-one mapping from incoming edges to outgoing edges. Sybil Defender consists of three components: a Sybil identification algorithm, a Sybil community detection algorithm, and two supporting approaches to limiting the number of attack edges. The three components can be used in conjunction to best mitigate Sybil attacks.

C. Basic Detection methods in Sybil Attacks (Algorithm 1)

As shown in algorithm 1, that takes the social graph G(V,E), a known honest node h, and a suspect node u as inputs, and outputs whether u is Sybil or not. Our algorithm is based on random walks. A random walk on a graph is

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 4, July 2016

defined by the sequence of moves of a particle between nodes of G. If the particle is at node i with degree di, then the probability that the particle follows the edge (i, j) and moves to a neighbour j is 1/di. The intuition of our Sybil identification algorithm is that, as there is a small cut between the honest region and the Sybil region, the random walks originating from a Sybil node tend to get "trapped" into the Sybil region. Also, since we assume that the size of the Sybil region is not comparable to the size of the honest region, the number of nodes traversed by the random walks originating from an honest node will be larger than the number of nodes traversed by the random walks originating from a Sybil node, as long as the random walks are long enough and we perform the random walks many times [2]. For simplicity, we define the number of times one node being traversed by a set of random walks as the frequency of that node. Note that one node may be traversed by the same random walk multiple times.

Algorithm 1

Pre-processing (G, h)
1: J = {h}
2: for i = 1 to f do
3: Perform a random walk with length ls = log n originating from h
4: J = J ∪ {the ending node of the random walk}
5: end for
6: l = lmin
7: while l <= lmax do
8: for i = J.first () to J.last () do
9: Perform R random walks with length l originating from node i
10: Get ni as the number of nodes with frequency no smaller than t
11: end for
12: output hl, mean ({ni : i ∈ J}), stdDeviation({ni : i ∈ J})i
13: l = l + 100
14: end while

D. Basic Detection methods in Sybil Attacks (Algorithm 2)

Algorithm 2, to determine whether a suspect node u is Sybil, the algorithm first performs R random walks with an initial length l = l0 originating from u. l0 is larger than or equal to lmin used in Algorithm 1. The algorithm then compares the number of nodes whose frequency is no smaller than t with the mean value in tuple hl,mean, stdDeviationi outputted by Algorithm 1. If the former is smaller than the latter by an amount larger than stdDeviation we consider u is Sybil and end the algorithm[2].

Otherwise, the algorithm doubles l and repeats the process, until l is larger than lmax. If u is still not identified as Sybil when the value of l reaches lmax, we consider it honest and end the algorithm.

Given a social graph G (V, E) and a known honest node h, lmax, the maximum random walk length that decides when to end the algorithm, can be determined as follows. We do R random walks originating from h with length lmax. The number of nodes with frequency no smaller than t should be larger than |V |/2. Given that we assume the Sybil region is smaller than the honest region, lmax determined in this way is large enough for R random walks originating from a Sybil node to cover the Sybil region, so as to exhibit the difference between the random walks originating from an honest node and from a Sybil node. This algorithm adaptively tests the suspect node while doubling the random walk length each time. This guarantees that the algorithm can identify the Sybil nodes in differently sized Sybil regions: for small Sybil regions short random walks are already enough, while for large regions long random walks need to be performed.

Algorithm 2

Sybil Identification (G, u, tuples from Alg.1)
1: l = l0
2: while l <= lmax do
3: Perform R random walks with length l originating from u

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 4, July 2016

4: m = the number of nodes whose frequency is no smaller than t
5: Let the tuple corresponding to length l in the outputs of Algorithm 1
be hl,mean, stdDeviationi
6: if mean − m > stdDeviation ∗ _ then
7: output u is Sybil
8: end the algorithm
9: end if
10: l = l ∗ 2
11: end while
12: output u is honest

III. COMPARATIVE STUDY AND PROPOSED WORK

This section discuss about comparative study of four different types of defense mechanism in Sybil. We have also discussed about short falls exist in defense mechanism. Algorithm and proposed enhancements possible in each of them so that they can still perform better. Next section discuss about our proposed work.

1. Comparison of SybilGuard, SbilLimit, SybilInfer, Sum up. Sybil defender and Sybil shield

This section discuss about comparative study of four different types of defense mechanism in Sybil. During comparison, we come across with some similarities and differences exist in each type which has been highlighted in below tables. Table explores properties and evaluation of Social network-based Sybil defense schemes [2],[4],[5][10]

	Assumption	Algorithm	Ranking	Cutoff
SybilGuard (Sigcomm, 06)	**Non-Sybil region is fast mixing**	**Random walk performed by each node**	**Varying random walk length**	**Whether or not walk intersection Occurs**
SybilLimit (IEEE S & P'08)	**Non-Sybil region is fast mixing**	**Multiple random walks performed by each node**	**Varying number of random walks and walk length**	**Whether or not tails of random walks intersect**
SybilInfer (NDSS'09)	**Non-Sybil region is fast mixing, modified walks are fast mixing**	**Bayesian inference on the results of the random walks**	**Probability of node being non-Sybil from Bayesian inference**	**Threshold on the probability that a given node is non-Sybil**

While evaluating Sybil defense mechanisms we come across with certain shortfalls exist in each algorithm some of them are listed below

- It works on assumption.
- Assumption is not same for each method.
- Security etc.

By identifying shortfalls from Survey and comparative study, we propose certain enhancements which will make each of them better while detecting Sybil attack.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 4, July 2016

Proposed Enhancement

- In proposed enhancement, detection approach that groups "similar" user clickstreams into behavioural clusters, by partitioning a similarity graph that captures distances between clickstream sequences.
- This algorithm uses describe a new approach to Sybil detection rooted in the fundamental behavioural patterns that separate real and Sybil users.
- Clickstreams are traces of click-through events generated by online users during each web browsing "session," and have been used in the past to model web traffic and user browsing patterns.

Proposed Algorithm

We have given a similarity graph algorithm for Sybil attack. In the proposed algorithm, we considered certain parameters in the process of detecting Sybil user such as Normal users use many social network features, Sybil focus on a few actions (e.g. friend invite, browse profiles)

Proposed function-Computing Sequence Similarity

Having defined three models of clickstream sequences, in this it compute the distance between pairs of clickstreams.

Defining Distance Functions

Common Subsequence's [9]

It involves locating the common subsequence's of varying lengths between two clickstreams.

It formalize a clickstream as a sequence S = (s1s2...si...sn), where si is the ith element in the sequence and Tk as the set of all possible k-grams (k consequences)

$$Dk(S1,S2) = \left(\frac{|Tk(S1) \cap Tk(S2)|}{|Tk(S1) \cup Tk(S2)} \right)$$

Where

D -: Distance for locating the common subsequences of varying length between two Clickstream

K-: k consecutive elements

Tk-: as the set of all possible k-grams in sequence S

Finally, the distance between two sequences can then be computed based on the number of common subsequences shared by the two sequences.

Common Subsequence's With Counts. [9]

The common subsequence metric defined above only measures distinct common subsequences, i.e. it does not consider the frequency of common subsequences. We propose a second distance metric that rectifies this by taking the count of common subsequence's into consideration. For sequences S1, S2 and a chosen k, we first compute the set of all possible subsequence's from both sequences as T = Tk(S1) ∪ Tk(S2). Next, we count the frequency of each subsequence within each sequence i (i = 1, 2) as array [ci1,ci2, ...,cin] where n = |T|. Finally, the distance between S1 and S2 can be computed as the normalized Euclidean Distance between the two arrays:

$$D(S_1, S_2) = \frac{1}{\sqrt{2}} \sqrt{\sum_{j=1}^{n} (c_{1j} - c_{2j})^2}$$

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 4, July 2016

IV. REAL TIME EXAMPLE

Renren's[3] security team trained system using clickstreams from 10K users, of which 8K was randomly selected, and 2K was previously identified as suspicious by the security team. 500 honest users that have been manually verified by Renren's security team were used as seeds. Once trained, system was fed clickstreams from 1 million random users for classification as normal or suspicious. In total, system identified 22K potential Sybil accounts. These accounts are now being investigated by the security team.

LinkedIn[3] LinkedIn's security team used our software to analyze the clickstreams of 40K users, of which 36K was randomly sampled, and 4K was previously identified as suspicious by the security team. These clickstreams were gathered in February, 2013. Again, our feedback was very positive, but did not include precise statistics. However, we were told that our system confirmed that ≈1700 of the 4000 suspicious accounts are likely to be Sybil's. Our system also detected an additional 200 previously unknown Sybil's.

V. CHALLENGES IN SYBIL ATTACK

Some research challenges and potential solutions on Sybil defences are listed below.

A) Privacy and Sybil Defences

Since many Sybil defences, e.g., BCSD and MSD, tend to study the user's behaviours, such as clickstream, browse history, and contact, it is critical to address the privacy leakage during Sybil defence, especially in a mobile environment. For example, when the contact information is used to detect SA-3, user's contact history might be disclosed to others, including mobile users, Sybil attackers. Although it is helpful to the Sybil defence, the leakage of user's information still violates their privacy[1]. With the proper cryptographic encryption, i.e., homomorphic encryption, it is possible to hide the real information in the cipher text and enable addition or multiplication operations on the cipher texts. However, the computation and communication overheads have to be dramatically increased, especially in a mobile environment where energy consumption is also a crucial issue for mobile users. Alternatively, it is possible to explore user's common profiles and preferences, which reduce the privacy leakage, for Sybil defence. The challenging issue is how to guarantee the Sybil defence accuracy while preserving privacy.

B) Cooperative Sybil Defences

Due to the lack of sufficient knowledge or the capability of users, Sybil defence may be ineffective and inefficient in some scenarios. For example, in a mobile network, mobile user's capability is not as powerful as that on the server side, or even weak compared with online users[1]. One possible and promising approach is the cooperation among servers and mobile users for Sybil defence. The mobile users can detect the suspicious Sybil users in the early stage via cryptographic schemes, such as authentication of identities or user contacts, event signatures, and local community structure. The mobile users then report them to the servers with the corresponding contact or other information. The centralized servers would be an assistance to process the complicated operations, such as user behavior learning, social graph or community detection. The servers could take the advantages of the computation and storage capability and confirm the Sybil detection from mobile users. In addition, the cooperation among mobile users can also facilitate the Sybil defence. With the cooperation, more knowledge about Sybil attackers can be obtained for further detection. Therefore, the cooperative Sybil defence should be a promising tendency.

VI. CONCLUSION AND FUTURE WORK

A. Concluding remarks

We believe clickstream models can be a powerful technique for user profiling in contexts outside of OSNs , this study shows that how easy it would be for a potential attacker to launch automated crawling and identity theft attacks against social networking sites. Although social networking sites are useful, we believe it is important to raise awareness among users about the privacy and security risks that are involved.

B. Scope for feature work

Studying ways to extend clickstream models to detect malicious crowdsourcing workers and forged online product and travel reviews and detecting new types of image-spam attacks.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 4, July 2016

REFERENCES

[1] Kuan Zhang, Xiaohui Liang, Rongxing Lu, and Xuemin Shen, "Sybil Attack and their Defence mechanism in Internet of Things, " ," in Proc. IEEE Conf.2014.

[2] W. Wei, F. Xu, C. Tan, and Q. Li, "Sybil Defender: Defend against Sybil attacks in large social networks," in Proc. IEEE Conf. Comput. Commun.

[3] G. Wang et al., "You are how you click: Clickstream analysis for Sybil detection," in Proc. 22nd USENIX Security Symp., 2013.

[4] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, "An analysis of social network-based Sybil defenses," in SIGCOMM, 2010.

[5] J. Douceur, "The Sybil Attack," Proc. Revised Papers First Int'l Workshop Peer-to-Peer Systems, pp. 251-260, 2002.

[6] Rakesh G.V,Shanta Rangaswamy, Vinay Hegde,Shobha G ,"A survey of techniques to defend against Sybil attacks in social networks", in International Journal Of Advance Research in computer and Communication Engineering,Vol. 3,Issue 5,May 2014.

[7] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove. An analysis of social based Sybil defenses. In SIGCOMM, 2010.

[8] Neha Gahlot," Survey on Sybil Attacks and its Defensive Measures, "IJARCCE Vol. 4, Issue 6, June 2015.

[9] Information Storage and Retrieval by Robert R. Korfhage.

[10] H. Yu, M. Kaminsky, P. Gibbons, and A. Flaxman, "Sybil Guard: Defending against Sybil attacks via social networks," IEEE ACM Trans. Netw., vol. 16, no. 3, pp. 576–589, Jun. 2008.

[11] Snehal Pise, Prof. Ratnaraj Kumar "Recent Trends in Sybil Attacks and Defense Techniques in Social Networks" ISSN: 2278-0181 Vol. 3 Issue 1, January – 2014.