A responsiveness model for privacy conservation against antagonist and fake user in cyber-physical and online social networks

A Vanitha and N Balakrishnan
Department of MCA, Sona College of Technology, Salem, Tamilnadu, India
E-mail: vanitarget@gmail.com and nbkkar29@gmail.com

Abstract. The enormous numbers of users are interacted with Social networking sites throughout the world. They are consistently engaging with Social Medias are Twitter, Instagram and Facebook have an incredible impression and rarely objectionable consequences for daily life. Recently, the detection of spammers and identification of fake users on Twitter has become a common area of research in contemporary online social Networks (OSNs). This paper proposes to perform a review of techniques used for detecting spammers on social media like Twitter, Facebook, Instagram, etc. Furthermore, a taxonomy of alerting spam message methodologies is presented that classifies the techniques based on their ability to detect: fake content, spam message or junk mail depends on either url or trendy news, and identifying unauthenticated users. The proposed techniques are also compared based on historical features that comprise the characteristics of user profile, wish-list, content usage, methodology used, and physical context, logging activities. This research paper contributes the study on identifying appropriate users against fake users and spam or junk mail detection using Adversary-Privacy evaluation model that helpful to preserving private data in Cyber-Physical Social Systems.

1. Introduction
The spammers are choosing the most possible environment to make harmful. They are easily influencing in social networking sites to observe the users’ physical records and tried to harm with massive quantity of inappropriate and deleterious information. Fake users [1] can send undesired tweets, messages, chats and junk mails to unleash their services in websites that affects authenticate users in additionally intrude to abuse the resource consumption. Moreover, the possibility of expanding invalid information to users through fake identities has increased that result in the unrolling of harmful content.

The various threats [4] are highlighted below table 1 in which is jeopardized in privacy and security that disrupt the social media users’ daily life activities.
Table 1. Online Social Network (OSN) users types of threats

| Types of Threats          | Attacks                                             |
|---------------------------|-----------------------------------------------------|
| Classic Threats           | Malware Phishing                                    |
|                           | Attacks Spammers                                    |
|                           | Cross-site scripting                                |
|                           | Internet Fraud                                      |
| Modern Threats            | Click-jagging                                       |
|                           | De-anonymization Face                               |
|                           | Recognition Fake                                    |
|                           | Fake Profiles                                       |
|                           | Social bots                                         |
|                           | Clone attacks                                       |
|                           | Inference attacks                                   |
|                           | Information/location leakage                        |
|                           | Socware                                             |
| Combination Threats       | Combination of both classic and modern threats, example spammer can use any modern threat make influences in social network |
| Threats to children       | Online Predators                                    |
|                           | Risky Behaviors                                     |
|                           | Cyberbullying                                       |

1.1. Online Social Network (OSN)
It enhances the metrics of safety measurement to protect users’ activities via high authentication mechanism with advanced privacy schemes.

- **A mechanism for authentication**: An OSN operator follows with stringent identification processes that confirm the users by using captcha code, multi-features framed in profile, secret keywords, one time generation code associated registered mobile number or Email, face/finger recognition pattern and photos. It prevents from malicious hackers attempt like password cracking, false profile creation, clone user account creation, etc. It highlights the hacked accounts are attacked to influence the concern user’ information or profile.

- **Advanced profile settings**: It improves high privacy and security services to the OSN users with greater protection scheme included in their personal profile, data from the fraudulent users. Also it is upgraded with securable portal whereas permit them to do safe browsing, trackers alert and notification and implements remaining safety features.

- **Improvised interface level schemes**: It helps the user to get to know the people are visited, watched closely and they can improve their users’ account privacy and security settings.

Consider the above figure on n number of users is actively participated on social networks with n number of fraudulent users. It focuses to propose a new model that devise the technique into significant phases are (i) spam messages or junk mails identification (ii) identifying flooded/forwarded routing devices that detects the entry level point of fraudulent users are connected in the network (iii) an authenticate users conformity by assigning with weightage parameters at edge level in which exponential distribution applied with respect to parameter value at randomly.
In this study, K vertices [5] are assumed with minimum weight in the formation of tree called, Steiner tree shown in figure 2. A Steiner tree of Graph G has k number of vertices and calculates the weight of a tree T by sum of weight.

It is a proven algorithm to abstract high probability of minimum weigh of vertices k in a graph G in given formula,

\[(1 + o(1))(k - 1)(\log n - \log k)/n \text{ when } k = o(n) \text{ and } n \rightarrow \infty\]  

1.2 Key generation scheme

Key establishment in sensor networks is a challenging problem because asymmetric key cryptosystems are unsuitable for use in resource constrained sensor nodes, and also because the nodes could be physically compromised by an adversary. This technique emerges into three levels of components for generating keys in the framework of pre-distributing a random set of keys to each node [9]. First, in the q-composite keys scheme, a trade off the unlikeliness of a high scalability of comprehensive network rise spontaneous attacks with respect to weak range of keys. It is needed to be strengthening the key values and generate random key in order to pre-distribution's approach in contrast to possible attacks happened in short range networks. Then, multipath- reinforcement scheme offer the services of tight security that is enhanced in between the two nodes are participated for communication process in wireless networks [17] by following from other network’s leveraging security schemes. Finally, it integrates with random pair-wise algorithm provides preserving facilities for secrecy maintained after the entire network is formed. Also it is preferably the whole network is tightly deployed and protected during the time of any other node is entered, and ensure the concern user identification rather than fraudulent users by strictly proceed node-to-node authentication and quorum-based revocation mechanism.

A new generalization principle m-variance [10] was proposed to limit the risk factor on the privacy disclosure in re-publication. An algorithm was proposed to compute the privacy-guarded relations which permit the retrieval of accurate aggregate information. Data distortion method for achieving privacy protection association rule mining [11] and privacy protection data was proposed to
classify the data and analyse based on the association rule mining. Further, the performance, data utility, privacy protection degree and data mining difficulty was evaluated based on the criteria.

2. Spammer detection and fake user identification on social networks
This proposes a hybrid classification technique that utilizes user-based, content-based, and graph-based characteristics for spammer profiles detection. A model depicted in figure 3(a) is proposed to differentiate between the non-spam and spam profiles using three characteristics. Further, it identifies different approaches of spam detection on social network to take on taxonomy by classifying these approaches into several categories. For this classification and hybrid approach, it is abstracted the spammers are roamed and participated with authenticate users in the network by the result of defined features metrics measured for fraudulent users. The model is classified into separate the identification of fake users by, (i) checking content originality and separating fake contents are flooded in the network (ii) detecting spam source like major spammer in specific URL (iii) Justifying the topics are becoming trendy in prior (iv) analysing the features to ensure the authenticate users in terms of protecting their profile and communication, and enrich the privacy schemes (v) exhausting fake users.

![Figure 3(a). Fake user node identification model.](image1)

![Figure 3(b). Data collection model.](image2)

2.1. Fraudulent user detection model
This model facilitate to store the features of mobile nodes [18] other than text characteristics especially tracking map route information in Google map using GPS service in wireless sensor network, identifying user by three level identification set up including password. In WSN, sensors are sensing the circumstances with the parameter of temperature, movements, undefined activities captured in the security needed area in which helps to improve high security against attackers and evaluates exact attacks happened location and timings. This fruitful information is encompassed for further required analysis similarly supported in figure 3(b). It clearly describes the securable data sharing and the activities to the trusted network. The attacker analysis model is thoroughly analysed with the help of elected one head node usually described as cluster head [5], a leader and another node is Hunter who finds attacker from the network. Additionally, authenticated users are also can actively participate without hesitance in this secured network. The elected leader becomes as commander commanding the concern users to adhere the privacy settings and the hunter ultimate goal is to detect the attackers before they are influencing the network.

3. Preservation techniques for privacy settings
The framework of PrivacyGrid [1], beneficial method for an anonymous user that extract the mobile authenticated user information by executing geolocation related queries during the process of GPS based delivery transactions. Hence, it directs the further research into reducing anonymous time to become high success rate in terms of strengthening the protection mechanism to enhance the privacy and security mechanism in user dashboard of social network. In the first phase, it offers a highly protectable site where the user opt their preferable profile model, named as location [3] P3P. The ad-
hoc users are permitted to store their preferred location with respect to defined privacy requirements. The locomotion metrics and measures are highly securable, it is noted in table 2 that location k-anonymity and l-diversity users and quality attributes for offering locality services, example the resolution rate of maximum spatial and maximum temporal attributes. At the second phase, it proposes an algorithm named location-based cloaking algorithms for tracking k-anonymity and l-diversity mobility users [3].

Table 2. Privacy preservation techniques

| Privacy Techniques | Advantages | Disadvantages |
|--------------------|------------|---------------|
| k-anonymity        | Proven maximum numbers of correlation are found among number of key values. | Limited parameters are used |
| l-diversity        | The same frequency level of sensitive features are extracted | Lacking of subjective knowledge in Attacks and homogenous attributes. |
| t-closeness        | Find exact match in terms of distance formulated using distribution probability values. | Lack of clarity found in obtaining information |
| Km-Anonymity       | Evaluates similarity among k tuples. | Unavailability of utility functionalities. |

A dynamic integrated grid cloaking algorithms is a combination of top-down and bottom-up approach attains great successive rate of anonymization, efficacy with minimum of complexity times and affordable cost. This hybrid approach utilizes the benefits of combination of bottom-up and top-down cloaking algorithm focusing to minimize the average duration of anonymization is proposed. PrivacyGrid includes historical cloaking that maximizes the location anonymization successive rate. Also, it ensures the queries are highly concentrated on anonymous location. It depicts an Investigational estimation of PrivacyGrid approach proves an optimal solution of location k-anonymity user as per P3P model devoid of familiarizing major performance consequences.

3.1 Privacy-preserving routing techniques

The model of integrated grid model prefers two distinguishable approaches for routing the information mentioned figure 4 (a) and (b) is for privacy preservation in online social networks, mobile node are synced or sensed via a periodic data source collection and simulation method. This repeated periodic data source collection accomplishes the optimal solution for identifying location privacy with minimal data rate but not consideration of latency rate. The data source simulation give the experimental trade-offs involving privacy, security, communication and latency. This work assures that the communication [13,14,15] is held between involving nodes in the network are secured by following the two-tier keys are called random pair-wise keys generated and passed to the user through right router devices. It supports to prevent the adversary network from the correlated data packets. In figure 4 (a) shows that the authenticated user go through formal guidelines to take securable process to do their activities in either Online or Cyber-Physical Social Network by following three level integration identification model. It senses and separated fraudulent or fake users from the network [2]. Hence it is sensed the nodes are fake by classifying their content, user, url, trendy news, tweets, spams and junk mails. Similarly figure 4(b) expresses a high confidential routing path to allow the authenticated users and neglect fake users’ access to allow taking their malicious attempts in well-structured online or cyber-physical social network [7]. This model to capture spammer and direct them to store in repository to prevent future attacks.
3.2 Adversary model for phishing and spammer detection

The wireless sensor networks [6] are highly induced way whereas the purpose of attackers’ focal point is to get perceptive key-hole point based on location. This information set has resided event-location at desired network. The Panda-Hunter application was proposed to describe a sensor network is formed to track the movements of endangered giant pandas in a bamboo forest. An every panda has tied with electronic gadget which produces a signal are capture via mounted sensors in the defined network. A poacher communicates in the network to pass the message of identifying locations of pandas [12] are movable around the forest in the fastest manner rather than traditional tracking techniques. An attacker gains this knowledge to compose threats to break privacy in public networks; hence it is required to focus next attention to detect these types of attackers.

This adversary models takes the essence of cyber security schemes in wireless sensor networks, monitors the activities with respect to classified features mention in data set [11]. The deviation can be found based comparative results of active users in terms of user profile, content, tweets and chats, photos with fake users’ content, profile, content and tweets. It ensures the genuinity of user measured with timeline. Hence, it tags spammer to break their logging activities in network.

3.3 Security analysis model

The encryption technique is emerged into end-to-end, link-to-link, and node-to-node [16] level that pass number of a packet in hidden template with secured routing schemes. The attackers are failed to find the route and number of a packets are sent. The routing paths are established while an every session is started in stipulate period instead of repeating regeneration process. The following figure is experimented the same for analyzing security assurances.
In figure 5 indicates that green text are original users and red text are fake users by analyzing security schemes utilized in the wireless sensor network. The two different nodes are sensed based on their features and distinguished in repository.

3.4 Privacy evaluation model
The formulation model considers the location based privacy issues in which deploy an adversary model against attacker to monitor the activities of the target network. An efficient adversary model includes eavesdrop [6, 12] the communication of each node i in defined network is a focal point, gives an observation of set (i, t, d) transmits a packet d in defined network at the time of t. It is supposed to be the attackers are closely tracked via the wireless medium has the n number of data packets generated randomly. Figure 6 (a) and (b) are described the evaluation model for privacy preservation.

![Figure 6(a). Privacy evaluation report-1.](image1)

![Figure 6(b). Privacy evaluation report-2.](image2)

In those above two figures are clearly describes that fake user are observed by their logging activities and are evaluated with privacy and security techniques in the assumed network.

4. Results and discussion
In addition to reviewing the techniques, the study also provides the comparison of features in miscellaneous social network for spammer detection. Those features are mined from user repository and extracted the phishing, spam messages that improves the detection model. Those features are classified into five classes are user, content, graph, structure, and time. The features are identifying concern users distinguishable from fake users by incorporating the usage, activities, major following and followers, age groups, reputation, FF ratio, and number of tweets. The content- based features contain number of retweets, number of URLs, number of replies and propagation of bidirectional, number of characters and digits, and spam words. The graph-based features include in/out degree and centrality whereas the structure-based features include average tweet length, thread life time (number of times between first and last tweets), tweet frequency, and depth of conversion tree. On the other hand, time-based features include idle time [13] in days and tweet sent in specific time interval. Therefore, the survey is assembled by the classes that are categorized according to different features that are used for analyzing and detecting Twitter spams in various groups. Further, it is carried out a comparative study on the existing techniques and methods that mainly capture the detection of spams on social network. This study includes the comparison of various previous methodologies proposed using different datasets and with different characteristics and accomplishments.

5. Conclusion
Few standard techniques have been done on the anti- eavesdropping to overcome the issues arisen in WSN. This base anti-model to detect location leads the research into identifying spammer detection on
social network with less service schemes. Then it steps into online social media network, the operator use a classification model where separating fake user, URL, content with help to improve privacy settings. It requires adding multi-features with two levels of permission to find spammer. The future direction is advance analytical model with leveraging technique can help to detect data leaks in privacy mechanism.

References
[1] Masood F, Almogren A et. al, 2019 Spammer Detection and Fake User Identification on Social Network IEEE 7 68140
[2] Zhang L, Li Y, Wang L, Lu J, Li P and Wng X 2017 An efficient context-aware privacy preserving approach for smartphones Hindawi Security and Communication Networks ID 4842694, 11 pages.
[3] Bamba L, Liu L, Pesti P and Wang T 2008 Supporting anonymous location queries in mobile environments with PrivacyGrid WWW ACM 978-1-60558-085-2/08/04.
[4] Fire M, Goldschmidt R, and Elovici Y 2014 online Social Networks: Threats and Solutions IEEE Communication Surveys & Tutorials 16 2019.
[5] Zhang J, Zhao B, Song G, Ni L and Yu J 2018 Maximum delay anonymous clustering feature tree based privacy-preserving data publishing in social networks Procedia Computer Science Elsevier 147 643-646.
[6] Fan X and Huo Y 2020 Cooperative secure transmission against collusive eavesdroppers in Internet of Things Sage international Journal of Distributed Sensor Networks 16 1.
[7] Rahman M 2018 Cyber-Physical-Social System Between a Humanoid Robot and a Virtual Human Through a Shared Platform for Adaptive Agent Ecology IEEE/CAA Journal Of Automatica Sinica 5 190.
[8] Bollobas B, Gamarnik D, Riordan O, and Sudakov B 2004 On the Value of a Random Minimum Weight Steiner Tree Combinatorica 24 187.
[9] Chan H, Perrig A, and Song D 2003 Security and Privacy Random Key Predistribution Schemes for Sensor Networks 17 10.1109/SECPRI.2003.1199337.
[10] Xiao X and Tao Y 2007 m-Invariance: Towards Privacy Preserving Re-publication of Dynamic Datasets InSIGMOD 689.
[11] Qi X and Zong M 2012 An overview of privacy preserving Data Mining Procedia Environmental Sciences Elsevier 2 1341.
[12] Zhao N, Yu F R, Li M, and Leung V C M 2016 Secure transmission in interference alignment (IA)-based networks with artificial noise Proc. IEEE VTC-Spring’16 1.
[13] Pau N S J, Taylor D P and Martin P A 2008 Robust high throughput space time block codes using parallel interference cancellation IEEE Trans. Wireless Commun. 7 1603.
[14] Zhang S, Liew S C, and Chen J 2015 The capacity of known interference channel IEEE J. Sel. Areas Commun. 33 1241.
[15] Hossain E, Rasti M, Tabassum M and Abdelnasser A 2014 Evolution towards 5G multi-tier cellular wireless networks: An interference management perspective IEEE Wireless Commun. 21 118.
[16] Cadambe V R and Jafar S A 2018 Interference alignment and degrees of freedom of the K-user interference channel IEEE Trans. Inf. Theory 54 342.
[17] Gomadam K, Cadambe V R and Jafar S A 2011 A distributed numerical approach to interference alignment and applications to wireless interference networks IEEE Trans. Inf. Theory 57 3309.
[18] Razaviyayn M, Sanjabi M, and Luo Z Q 2012 Linear transceiver design for interference alignment: Complexity and computation IEEE Trans. Inf. Theory 58 2896.