Models for the Detection of Malicious Intent People in Society

Preetish Ranjan, Indian Institute of Information Technology, Allahabad, India
Vrijendra Singh, Indian Institute of Information Technology, Allahabad, India
Prabhat Kumar, National Institute of Technology, Patna, India
Satya Prakash, Indian Institute of Information Technology, Allahabad, India

ABSTRACT

This article describes how in less than two decades, internet in mobile phones has grown from a curiosity to an essential element of modern life. Although, this mind-boggling growth has no doubt facilitated international commerce, trade, and travel, it is also being used in the planning and coordination of criminal activities. These types of attacks are often referred to as socio-technical attacks. These attacks are targeted at these sensitive points to society or national security and may have a devastating impact. Often, organized, sponsored, and trained groups are involved to disguise the intelligence system, deployed for the detection of such attacks. Prior detection of such attacks may reduce its impact. In this article, the authors have developed an efficient model to detect malicious node in huge and complex corpus of data associated with call detail record (CDR). This model analyses CDRs to identify covert nodes operating within society for malicious intent.

KEYWORDS

Call Detail Record, CDR, Social Network Analysis, Socio Technical Attacks

INTRODUCTION

Society is transforming itself into e-society due to proliferation of digital technologies especially social media in mobile phones. Social media is taking different forms, involving both web and mobile technologies. It includes internet forums, instant messaging, social networking services and smart phone apps. According to Pew internet project, 95% of teen in US are online, of which 76% use social networking sites and 77% have cell phones. Facebook and Twitter report approximately 149 million and 90 million unique US visitors per month respectively. The popularity of social media grew after the emergence of smart phone. People can easily contact and communicate using various technologies available with smart phone. It provides freedom of speech and expression. We may perceive social views about particular issues which may bring a change in the perception both in positive or negative sense. There may be professional motives involved where organizations advertise their products and services.

Meanwhile, mobile phones are used in the planning and coordinating criminal activities. This is also being misused by malicious intent people to damage others for their illegal benefits. There are some people who exploit social media to access personal information or it may be used as a platform to intimidate other users. This is called socio-technical attack where technology may influence the mood of society. Socio Technical Attack is a function of virality of information in society (Huber,

DOI: 10.4018/IJDCF.2018070102

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
Mulazzani, Schrittwiener, & Weippl, 2010) which is a challenge for the investigating agencies to corroborate evidences against this. Who can say that rumors about earthquake in Andhra Pradesh were not intentional? One viral SMS triggered sudden flee of north east people from South India. How can we sure that this SMS was not made viral by some of the malicious intent people. Mobile phone technologies have played a major role during these incidents. Effect of cyber-attack is more on those who are accessing technology through internet or mobile phones. However, impact of socio technical attack is not constrained to particular section of society, but it disturbs entire society irrespective of user.

Now, people have started making their sentiments through social media recommendation in global scale, therefore, the basic challenge is to decide the ambiguity of information across social network. It is very problematic to distinguish between an authentic and unauthentic source of information in society. This motivated us to design a model which could pin-point particular set of users who are operating covertly as a source of unauthentic information. We have presented two models where first model compares the association strength of mobile phone users to find hidden correlation among nodes of social network. Second model focuses on machine learning approach where suspicious users have further been classified as malicious and non-malicious mobile phone users. These models focus on CDR analysis which may help the investigating agencies to reach near to attackers.

LITERATURE REVIEW

The emergence of smart phone has made the communication more fast and complex. Inexpensive cost of technology and corresponding service encourages users to connect with multiple motives. Service providers analyze different attributes of CDR to identify and evaluate customer base (Bianchi, dOHureuse, & Niccolini, 2011; Kianmehr & Alhajj, 2009). Marketing professionals discover shift of customers from one product to other. Seungjiae al. devised pricing strategy of product by analyzing calling pattern obtained from CDR (Shin, Park, Lee, & Lee, 1998). Due to easy availability of mobile phones and SIM cards, they are readily used to plan high profile crimes such as kidnappings. It poses a challenging risk if these are being used in secretly. This has caused a rapid growth in research in the field under study. Markus Huber et al. studied socio-technical attacks as large scale spamming on social networking sites where they explored virality of information in destructive sense (Huber, Mulazzani, Schrittwiester, & Weippl, 2010). Integrity of message may be changed and may be made viral by some malicious intent people. They were unable to identify the holistic insight within social network. Mohammad Reza et al. and Sharad Goel et al. observed that it not only the content but structure of social network is also equally responsible for the diffusion of information in network (Faghani, Saidi, & Nguyen; Goel, Anderson, Hofman, & Watts).

Power of telecommunication over ruled all the communication technology. With the abundance of smart phone application, we may connect to the whole world at a very low cost. There exist correlations among nodes of social network which need to be identified through pattern in the structure of network. Huiqi et al. observed that the higher reciprocity index value reflects closer relationship between numbers which is useful in detecting unwanted calls (Zhang & Dantu, 2010). However, CDRs analysis is proving to be helpful to mine the links among different users. Tain et al. implemented unsupervised machine learning approach to identify the clusters based on user behavior in telecommunication network using social feature instead individual feature (Zhu & Wang, 2011). There always exist some buried information embedded in raw CDR. Researcher have established time varying relationships based on dynamic graphs concatenated with link weights to identify different calling groups (Sharan & Neville, 2007). Recent researches on CDR have revealed that most calls are related to occupation (Zhou, Xu, & Huang, 2010). Mahalanobis, Euclidean and Hellinger distances have been implemented over CDRs to demonstrate the level of closeness and social bind strength among mobile phone users. Back propagation neural network, user profiling method and setting of indicators in social network were implemented over CDR to mine links within social network (Fawcett
www.igi-global.com/chapter/security-issues-in-mobile-wireless-ad-hoc-networks/131398?camid=4v1a