Journal of Organizational and End User Computing
Volume 33 • Issue 1 • January-February 2021

A Bio-Inspired Defensive Rumor Confinement Strategy in Online Social Networks

Santhoshkumar Srinivasan, Vellore Institute of Technology, Vellore, India
Dhinesh Babu L. D., Vellore Institute of Technology, Vellore, India

ABSTRACT

Online social networks (OSNs) are used to connect people and propagate information around the globe. Along with information propagation, rumors also penetrate across the OSNs in a massive order. Controlling the rumor propagation is utmost important to reduce the damage it causes to society. Educating the individual participants of OSNs is one of the effective ways to control the rumor faster. To educate people in OSNs, this paper proposes a defensive rumor control approach that spreads anti-rumors by the inspiration from the immunization strategies of social insects. In this approach, a new information propagation model is defined to study the defensive nature of true information against rumors. Then, an anti-rumor propagation method with a set of influential spreaders is employed to defend against the rumor. The proposed approach is compared with the existing rumor containment approaches and the results indicate that the proposed approach works well in controlling the rumors.

KEYWORDS

Anti-Rumor Spreading, Cybersecurity, Defensive Rumor Control, Influence Maximization, Online Social Networks, Protective Mechanism, Rumor Control

1. INTRODUCTION

The proliferation of internet-enabled devices such as smartphones has led to the increased usage of Online Social Networks (OSNs) for real-time information sharing (Leskovec, Backstrom, & Kleinberg, 2009; Guille, Hacid, Favre, & Zighed, 2013). This kind of information sharing helps the society in dissemination of the useful information on a large scale in a shorter duration (Bakshy, Rosenn, Marlow, & Adamic, 2012). Also, OSNs are helping for the growth of organizational businesses by finding new customer bases/marketing medium (Pham, Tran, Thipwong, & Huang, 2019) and OSNs serve as organization's crucial decision propagation platform during disastrous events (Ngamassi, Ramakrishnan, & Rahman, 2016; Subramaniyaswamy, et al., 2017). However, along with useful information propagation and increasing the business prospects, OSNs also serve as fertile land for false information or rumor propagation on an unprecedented scale (Wen, et al., 2015). For example, in 2013, there was a rumor initiated at OSNs related to Barack Obama's injury in an explosion at the White House. This rumor has made a major crackdown on the U.S stock market amounted to U.S

DOI: 10.4018/JOEUC.2021010103

dollar 136.5 billion within three minutes of propagation (Domm, 2013) (Foster, 2013). This shows that the rumor spreads faster than normal information in online mediums like OSNs (Doerr, Fouz, & Friedrich, 2011). Such an exacerbated propagation causes irreversible damage to society during emergency events as a negative effect. Consequently, researches on identifying and controlling the rumors have been a rising recent interest among industry experts and academicians.

Rumor in OSNs can be defined as an information/story that is unverified or authenticity source is unknown during its circulation in the network (DiFonzo & Bordia, 2007). There have been various research works to protect the OSNs from rumors through different methodologies such as: blocking rumor spread through node blocking (Hu, Pan, Hou, & He, 2018) and link blocking (Kimura, Saito, & Motoda, 2009), defeating rumor spread through 'anti-rumor' information as a protective mechanism (Li, Zhu, Li, Kim, & Huang, 2013; Afassinou, 2014; Tong, et al., 2017). In a real-world situation, blocking the individuals has privacy and user agreement issues in large scale networks like OSNs (Ahn, Shehab, & Squicciarini, 2011; Huber, Weippl, Kitzler, & Goluch, 2011). So, the protective mechanism through anti-rumor information is a widely accepted and more focused solution domain for rumor containment problems (Tripathy, Bagchi, & Mehta, 2010).

When a rumor spreads in OSNs, the authorities or individuals in the network identify true information against the rumor and propagate it in the network (Ji, Liu, & Xiang, 2014). This act of defending against rumors through anti-rumor propagation protects the OSNs by breaking the rumor in the network. This defensive mechanism to protect OSNs can be studied from the defensive mechanism of social insects to protect against the pathogen in the real-world. The defensive mechanism of both possesses the same behavior such as one-to-one contact, fast-spreading of epidemics in the system of social insects (Naug & Camazine, 2002) and OSNs (Doerr, Fouz, & Friedrich, 2011), and defending protection using the set of individuals against the epidemics in social insects (Myles, 2002) as well as OSNs (Li, Zhu, Li, Kim, & Huang, 2013). Hence, the defending protection mechanism of social insects is employed in the proposed approach to control the rumors in OSNs.

Social insects lead a group living in colonies. The defensive systems of these insects have evolved as a co-operative immune protection system against the parasite infection. The disease transmission in such colonies is controlled or removed using the co-operative actions of individual insects as a group defensive protection at the colony level. In this work, the defensive protection act of insects such as 'Dampwood termites' (Rosengaus, Jordan, Lefebvre, & Traniello, 1999; Myles, 2002) has inspired this study to control rumor propagation in OSNs. The infected termites create vibration in response to pathogen infection. This defensive action from nestmates is identified by other termites to escape from the infection. These termites transmit the immunization through the contact. Such behavioral response of termites against the pathogen effectively removes the infection from the colony in a short time.

The main objective of this work is to spread anti-rumors against rumor propagation with the help of the most influential spreaders in the network. To enable faster anti-rumor propagation in the network, this paper defines two new sets of most influencers called flocking and gushing influencers to initiate the anti-rumor propagation. Flocking and gushing influencers spread the information as a co-operative approach among the participants in the network. When the information initiated from flocking and gushing influencers, all other participants try to communicate with neighbors as a contagious effect. This sort of behavior is same as the co-operative behavior of social insects. Previous works on rumor containment through 'anti-rumor' propagation consider various optimization factors in identifying the initial spreaders, propagating true information, and competing against rumor propagation (He, Song, Chen, & Jiang, 2012; Liu, et al., 2016). But, none of these discuss the co-operative rumor containment approach that handles rumors through flocking and gushing information propagation.

In this work, a novel rumor containment approach called Rumor Control via Defensive Protection (RC-DP) is proposed to spread 'anti-rumor' as defensive protection against the rumors. This approach tries to combat rumors using a co-operative rumor containing behavior. First, the proposed work models the propagation of anti-rumor as a defensive act against the rumor propagation. This propagation