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 model is called the Protective Propagation model. Next, this work utilizes the opinion dynamics and strength of rumor to identify the influencers who can initiate the anti-rumor propagation. Finally, an anti-rumor propagation approach is proposed as co-operative, defensive protection against rumor. The novelty of the proposed approach lies in 1. Proposing a new information propagation model that mimics the defensive protection of anti-rumors against rumors. 2. Utilizing the opinion dynamics in identifying the initial spreaders. 3. A co-operative rumor defending approach as a protective measure using ‘anti-rumors’.

The contributions of this paper are as follows.

a. This work proposes a new information propagation model called Protective Propagation (PP) model to mimic the real-world rumor and anti-rumor propagation in OSNs. The defensive nature of anti-rumor propagation is exhibited using different user states in this model.
b. The interaction influence of participants and the strength of rumors in the network are utilized to identify influential spreaders such as flocking influencers and gushing influencers. This helps in identifying the force of anti-rumor to be spread in the network.
c. A defensive protection approach is proposed in this work to propagate anti-rumor information against rumors by having initial spreaders from flocking and gushing influencers.
d. This paper validates the proposed work with six social network datasets to demonstrate the effectiveness of the proposed approach. It also compares the proposed work with recent and well-known state-of-the-art rumor control approaches. The evaluation shows the significance of the proposed work when compared with the existing works.

The rest of this paper is organized as follows: section 2 elaborately studies the related works on rumor propagation and control in social networks. Then in section 3, the defensive protection approach of the social insect, dampwood termite, is discussed with a flow chart. Section 4 explains the PP model and interactive influence update method of this work. The same section formally defines the problem of rumor control. In section 5, the paper extensively elaborates the proposed work of identifying influencers and spreading anti-rumors. Experimental evaluation, in section 6, discusses the experimental details and the results of the evaluation. In continues to that in section 7, the paper discusses the significance of the proposed work in light of the results obtained in section 6. Section 8 concludes this paper with future enhancements.

2. RELATED WORKS

Rumor propagation in OSNs plays a significant negative role in social communications. Studying such rumor propagation and controlling rumors has been trending research interest in recent days. This section discusses the major recent works in rumor propagation and control.

In social networking environments, the rumor propagation study helps to identify (Srinivasan & LD, 2019) and control the rumors (Li, Zhu, Li, Kim, & Huang, 2013; Fan, et al., 2014). There are different types of models derived to study the rumor propagation in online and offline social networks. Rumor propagation model was first derived from the inspiration of human epidemic propagation in the population (Daley & Kendall, 1964) (Maki & Thompson, 1973). Those classical models are called the DK model (Daley & Kendall, 1964) and the MK model (Maki & Thompson, 1973). Both of these models serve as the base for the rumor propagation methods in social networks. In the DK model, the whole population was split into three states. Susceptible-Infectious-Recovered (SIR). In this model, the rumors spread on one-to-one communication among individuals. The MK model added another hypothesis to this model stating when two susceptible individuals communicate, one of them will inevitably turn to the recovered state and stop spreading the rumor. Following to these classical models, there were various rumor propagation models developed in stochastic theory (Dauhoo, Juggurnath, & Adam, 2016), applied mathematical theory (Li, Ma, Tian, & Zhu, 2015; Giorno & Spina, 2016), and applied physics theory (Han, Zhuang, He, Shi, & Ao, 2014; Ma, Li, & Tian, 2016; Huo, Wang, Song, Ma, & He, 2017). All these models considered the different spreading natures of participants and derived rumor propagation model. But none of these models studied the rumor control through the anti-rumor propagation to compete or defend against the rumors.

Recently there were some rumor propagation models (Zhao, Cui, Qiu, Wang, & Wang, 2013; Wang, Zhao, & Huang, 2014) derived to study the anti-rumor propagation in social networks, considering both rumor and anti-rumor exist in the network at the same time (Afassinou, 2014; Huo & Ma, 2017). Komi has introduced a propagation model called SEIR (Afassinou, 2014) based on education against the rumor. This model argued educating the individuals in the network can block rumor propagation and reduces the spread. Another model called SIHR (Zhao L., et al., 2012) extended the classical SIR model. In this model, a new state called 'the hibernators' was introduced to represent those who forget or remember the rumor. Authors argued such users play an important role in deciding the longevity of rumors in the network. Some of the other models extending the SIR epidemic model were ILSCR (Chen, 2019), SIRaRu (Wang, Zhao, & Huang, 2014), and so on. Also, few models considered anti-rumor propagation as vaccination to the rumor propagation (Huo & Ma, 2017; Santhoshkumar & Babu, 2019). These models relied on the amount of time the anti-rumor spread to reduce the rumor propagation.

Though these models were able to control the rumor in the network, the basic nature of anti-rumor propagation is to spread true information as a countermeasure to compete or defend against the rumor propagation. These models discussed anti-rumor propagation as a distinct information propagation during the rumor propagation. None of these anti-rumor measures discussed the anti-rumor propagation as a defensive or competitive propagation. There were few competitive propagation models (He, Song, Chen, & Jiang, 2012; Liu, et al., 2016) derived using the Independent cascade approach. But SIR epidemic model is widely used and accepted epidemic model for rumor propagation in recent days (Zhao, Cui, Qiu, Wang, & Wang, 2013). Also, those competing models did not give greater results in rumor control, leaving room for improvement (Li, Zhang, & Huang, 2018). To solve these issues, in the proposed work, a defensive rumor propagation model called the PP model based on the SIR epidemic model is proposed. This model considers anti-rumor propagation as a defensive protector approach.

Rumor control is the main goal of anti-rumor propagation approaches. There were different types of rumor control approaches proposed in research community like blocking rumor spread through node blocking (Hu, Pan, Hou, & He, 2018) and link blocking (Kimura, Saito, & Motoda, 2009), 'anti-rumor' propagation (Li, Zhu, Li, Kim, & Huang, 2013; Afassinou, 2014; Tong, et al., 2017). The rumor blocking mechanism proposed in (Hu, Pan, Hou, & He, 2018) was to block the influential nodes from propagating any information. This approach ensured the information does not pass through the node. This kind of blocking reduces the rumor propagation in the network. Another blocking mechanism was proposed in (Kimura, Saito, & Motoda, 2009). In this method, instead of blocking the influencer nodes in the network, it blocked the links in the network. In rumor blocking methodologies, rumor propagation is controlled by minimizing the influence of rumors in the network. This sort of rumor control takes time due to the minimization of influence only by blocking the node or link is difficult.

Most of the recent anti-rumor propagation approaches considered various factors such as cost (Fan, et al., 2013; Kotnis, 2014), community structure (Fan, et al., 2013), education (Kotnis, 2014), number of influencers (Li, Zhu, Li, Kim, & Huang, 2013; Fan, et al., 2014), emergency condition (Huo & Song, 2016), and so on. Rumor control using a greedy algorithm was proposed in (Li, Zhu, Li, Kim, & Huang, 2013). In this method, the anti-rumor initial spreaders were identified from infected and normal users. In (Fan, et al., 2013), an anti-rumor approach at the community level was proposed considering the cost as an important factor. Another anti-rumor approach (Fan, et al., 2014) considered the budget as well as time constraints in spreading true information. Kotnis, (2014) proposed to provide training to higher degree individuals who can propagate true information efficiently. Similarly, online training to employees also can alleviate organizational security breaches

(Jenkins, Durcikova, & Burns, 2013; San Nicolas-Rocca & Olfman, 2013). This activity increases the secured information propagation at organization level (Aurigemma, 2013). Tripathy and others considered the time taken by participants to believe the rumor as an important factor to strategize the anti-rumor propagation (Tripathy, Bagchi, & Mehta, 2010). During an emergency condition, Huo & Song (2016) analyzed the interplay between rumor and true information. The authors concluded that official authority should be wise to control the rumors quicker in the network. Recently, a new rumor containing approach using anti-rumor called Rumor Containing (RC) model (Pan, Yang, Yang, Wu, & Tang, 2018) was proposed. This model considered budget and time constraints in the approach. The model also evaluates the forgetting rate of the participants. Anti-rumor approaches, discussed so far, are considering different factors in controlling the rumors in social networks. Most of these approaches do not consider or pays the least attention to the importance of influential initiators in spreading anti-rumors in the network. But initial spreaders can control rumors in the network when they are influential in their community. Also, these approaches provide lesser importance to the strength of rumors in the network. When rumors are more, the strategy of anti-rumor should be aggressive.

The common problems of existing approaches discussed so far are 1. The defensive nature of anti-rumor is not studied in most of the approaches. Some approaches considered defensive nature but those were not derived from the widely studied SIR epidemic model. 2. The influential importance of initial spreaders of anti-rumors is not properly handled in most of the anti-rumor propagation methods. 3. None of the anti-rumor spreaders consider opinion dynamics in finding initial spreaders, 4. Very few anti-rumor methods consider the strength of rumor to spread anti-rumors. The proposed approach addresses all these issues and introduces a new rumor control method called Rumor Control via Defensive Protection.

3. DEFENSIVE PROTECTION OF SOCIAL INSECTS

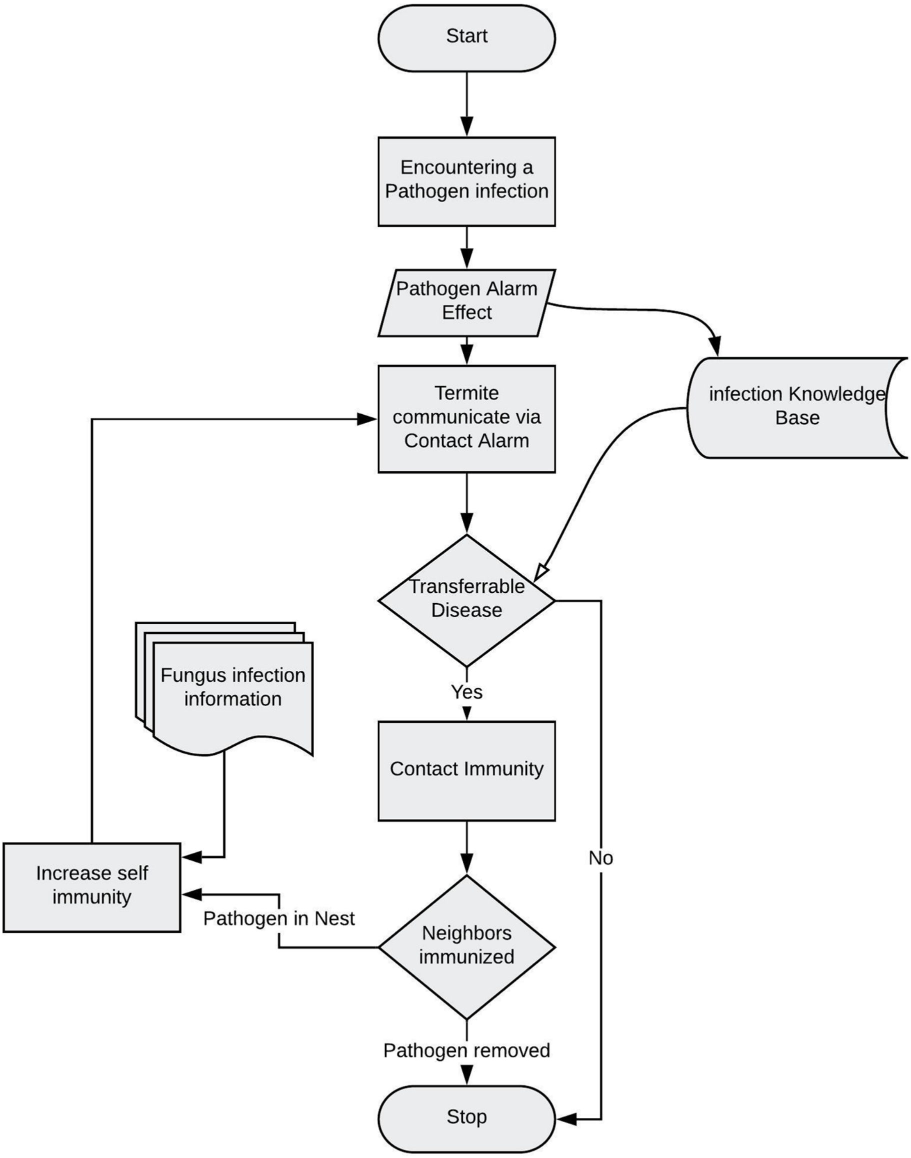
Social insects like dampwood termites, ants are leading a dependent living in colonies. They lead this dependent living on every aspect of their life, from food foraging to immunization against external threats like parasites and pathogens. To achieve the immunization against the parasites and pathogens, they co-operatively communicate in various different ways. This behavior helps other participants in defending or protecting themselves against the infection. The nature of defensive protection starts only after the infection of disease in the colony. The insect identifies the infection and tries to communicate with others. This communication makes the neighboring broods across the colony act against infection. This act not only reduces the infection to a local level but also protects the colony at the earliest.

Figure 1 shows the immunization approach of dampwood termite against the fungus. This figure explains the combined immunization of *pathogen alarm* (Rosengaus, Jordan, Lefebvre, & Traniello, 1999) and *contact immunity* (Traniello, Rosengaus, & Savoie, 2002). Dampwood termites have many approaches to control the immunization against the pathogenic fungus (Rosengaus & Traniello, 2001; Myles, 2002; Traniello, Rosengaus, & Savoie, 2002). Pathogen alarm and contact immunity are two majorly used communication behavior of dampwood termites to control the propagation of pathogens within and across the broods (Cremer, Armitage, & Schmid-Hempel, 2007).

Pathogen alarm is an alarm response created by '*Zootermopsis angusticollis*', a dampwood termite, on the detection of spores of the fungus '*Metarhizium anisopliae*' (Rosengaus, Jordan, Lefebvre, & Traniello, 1999). On direct contact with spores, termites show a vibratory display to nearby nestmates. This act conveys the presence of pathogens in the nest. The unexposed termites understand this vibrating alert and protect themselves by distancing from the vibrating termites. This 'fungus alarm behavior' is a co-operative approach of termites to act against the pathogen.

Another approach dampwood termites use to defend against the pathogen is called *contact immunity* (Traniello, Rosengaus, & Savoie, 2002). When the termite immunizes itself from the pathogen infection, the other termites in the nest also get the immunization as a contagious effect.

Figure 1. Defensive protection immunization of social insects



These termites significantly improve their immunization to resist the infection against pathogens when they placed in contact with the already immunized termites. This kind of improving immunization through contact is called ‘contact immunity’.

Defensive Protection of Dampwood Termite

The flow of immunization approaches followed by dampwood termites is elaborated in figure 1 as a combined defense against fungus pathogen (Rosengaus, Jordan, Lefebvre, & Traniello, 1999; Traniello, Rosengaus, & Savoie, 2002). Upon affected by the pathogen infection, the termite shows a vibrating display as an alarm response to neighbors. This act is recognized by nestmates and immunize themselves. If the pathogen infection needs to be controlled by contact immunity, the termites initiate the contact immunity approach. In contact immunity, termites acquire the immunization against pathogens through direct contact with immunized termites. Such immunization is transferred across the broods until the pathogen removed from the nest. This immunization flow is utilized in the proposed work to act against the rumor.

4. PROPAGATION MODEL AND INFLUENCE UPDATE

First, this section studies the rumor and true information propagation by introducing a new propagation model called Protective Propagation (PP) model. This model is based on the classic epidemic model called the SIR epidemic model (Daley & Kendall, 1964). Under this PP model, the proposed defensive rumor control approach is studied. Next, this section also formally defines the problem of rumor control.

4.1 Protective Propagation Model

The PP model studies the behavior of rumor spreaders and the respective defenders who spread 'anti-rumor' information. This model is derived from the widely adopted epidemic mode, SIR. Let G be an undirected graph denoting the OSNs in this work. Eqn. (1) represents the network G .

In Eqn. (1), τ represents the influence of nodes as spreaders among their neighbors in the spreading process. It is considered as the interaction influence of spreader on their neighbors.

Based on the nature of information propagation, each node in PP model split into four states: Uncertain (U), Rumor Spreader (S), Defensive Protector (DP), and Prosocial (P). Uncertain (U): The individuals who are neutral to any kind of information and prone to be affected by rumor or 'anti-rumor'. Rumor Spreader (S): The individuals who spread the rumor will be in this state. Defensive Protector (DP): The individuals who try to propagate the 'anti-rumor' information as a defensive act against the rumor to protect the network are called as defensive protectors. Prosocial (P): The set of users who recovered from the rumor and will not be affected by those rumors any more are grouped in this state. At any time t , The number of participants in the network G will be

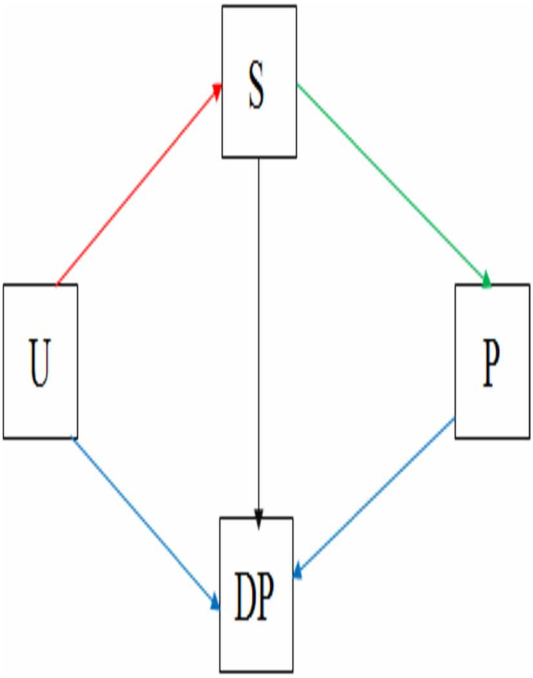
$$S(t)+U(t)+DP(t)+P(t)=|V|$$

The state diagram of this PP model is shown in figure 2. Let a random variable $X_i(t)$ represents the state of node i at time t . At time 0 , it is assumed that all nodes in the network are at the state $X_i(t)=U$. Here, $U(0)=|V|$. At time t , If the user i believes the rumor and started to spread the rumor, then the state of the user will be $X_i(t)=S$. This state is transitioned from state U . If user S recovers from rumor infection, then the state of the user is $X_i(t)=P$. If user i believes true information, then the state of the user will be $X_i(t)=DP$. The users from state U , S and P can become Protector.

4.2 Interaction Influence Update

In every communication among the participants, the spreader tries to convince the receiver. On succeeding the process, the receiver receives the message; otherwise, the receiver ignores the message. The spreader can succeed in this process only if the spreader can influence the receiver in this interaction (Raj & Babu, 2015). i.e., The spreader should be trustworthy among the neighbors (Li, Rong, & Thatcher, 2012; Srinivasan & Babu, 2019). This paper calls the influence value of spreaders as interaction influence. Opinion dynamics (Li, Scaglione, Swami, & Zhao, 2012; Cho, 2018) is

Figure 2. Protective propagation model



utilized in this work to calculate the interaction influence of the individuals in the PP model. This paper extends the HK opinion model proposed in (Li, Scaglione, Swami, & Zhao, 2012) for a non-linear update of participants' interaction influence. In this update model, a confidence belief threshold ϑ is set for interaction influence update. If the influence of spreader is greater than the threshold, then the receiver accepts the information; otherwise, it is ignored.

Let the interaction influence of node $i \in V$ at time t be represented as $I_i(t) = [I_1, I_2, I_3, \ldots, I_u]$. In $I_i(t)$, u is the possible number of outcomes from any interaction with neighbors. The neighborhood function of node i is defined as,

$$Neigh_i(t) = \{ j \in V \| I_i - I_j | \rangle \vartheta \ \forall \ neigbors \ of \ i \}$$

The opinion update of node i using neighborhood function is defined as,

$$I_i(t+1) = k * \frac{1}{|Neigh_i(t)|} \sum_{v \in Neigh_i(t)} I_v(t)$$

In Eqn. (4), k represents the degree of node i. The interaction influence of an individual is measured as follows.

$$IIF_i\left(t\right)=\frac{1}{I_i\left(t\right)}$$

The interaction influence updated in this model is used to identify the flocking and gushing influencers in the network. Such influencers enable the co-operative defense against the rumor. The PP model is used to propagate true information against the rumor as a defensive protection measure.

4.3 Problem Definition

Rumor control – Defending Protection: Given the social network G having rumor R and the respective 'anti-rumor' P, this problem of 'rumor control via defending protection' is aiming to propagate P against R in such a way that P breaks the propagation of R through co-operative behavior of participants.

5. PROPOSED APPROACH FOR RUMOR CONTROL

The proposed work controls the spread of the rumor by spreading 'anti-rumor' to break the rumor in OSNs. True information propagates among participants as a defensive approach for rumor propagation. This behavior of one-to-one connection between neighbors is the same as the co-operative defense of social insects. In this rumor containment approach, the most influential spreaders who can act against the rumor is identified at first. Then, true information is spread as a defensive act against the rumor. The overall framework of this defense act to control rumors is explained in figure 3.

The amount of rumor available in the network is important to identify the required intensity of 'anti-rumor' propagation in the network. Recent researches on rumor control are not widely studied the strength of rumor in the 'anti-rumor' propagation. In this rumor control approach, the rumor strength is defined as below.

$$rs\left(t\right)=\frac{Number\ of\ rumor\ affected\ nodes}{Number\ of\ total\ nodes}$$

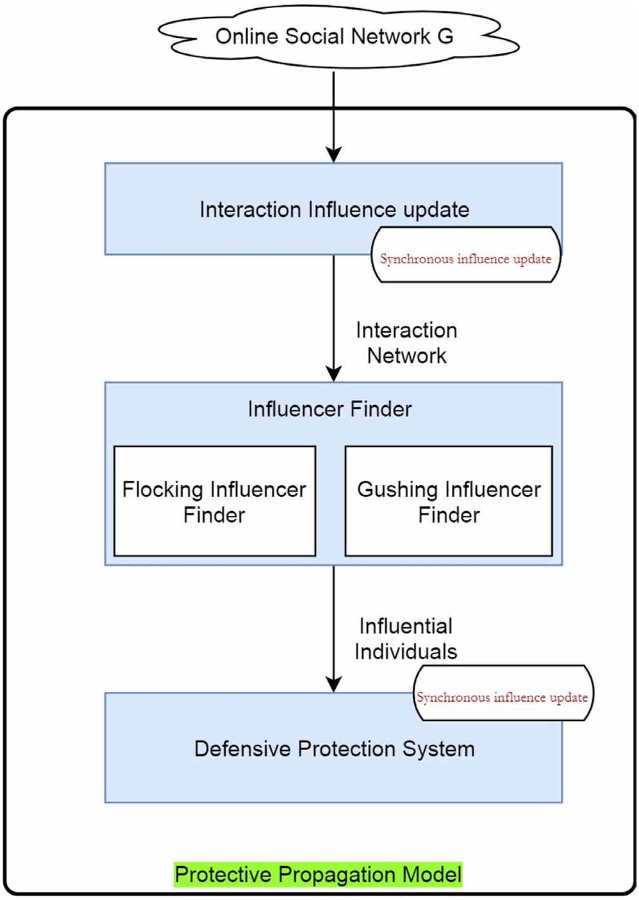
Rumor strength $rs\left(t\right)$ is used to find the most influential spreaders. The most influence finder method proposed in this work is two-fold. i.e., It identifies the most influencers from flocking influencers and gushing influencing individuals.

In complex networks like OSNs, the community structure plays a major role in information propagation (Raj & Babu, 2016). The participants within the community communicate frequently than with individuals on inter-community (Zhao Z., Wang, Zhang, & Zhu, 2015). Also, bridge communicators have more influence in spreading faster across the communities (Zhang & Li, 2017). So, the influencers in the proposed work are identified from within the community as well as the bridging influencers across the communities.

5.1 Influencer Finder

This paper aims to control the spreading of rumors by propagating 'anti-rumor' using the most influential spreaders as initial spreaders in OSNs. This work is inspired by the defensive method of social insects to protect the nests. The participants in the social networking system communicate through direct connection by one-to-one contact. The sender communicates the information to the receiver. If the receiver gets convinced, the receiver turns to be a spreader and propagate to their neighbors. This chain behavior of influencing one person on another and so on is called as

Figure 3. Overall Framework of RC-DP in OSNs


Online Social Network G
Interaction Influence update
Synchronous influence update
Interaction Network
Influencer Finder
Flocking Influencer Finder
Gushing Influencer Finder
Influential Individuals
Synchronous influence update
Defensive Protection System
Protective Propagation Model

social influence. This social influence is useful in identifying the sociability of individuals and communication strength among their neighbors in online social networks (Xiao & Wang, 2016; Cheikh-Ammar & Barki, 2016).

5.1.1 Flocking Influencers

In social networks, the subsequent spreaders completely imitate the actions of predecessors in information propagation without imposing their own judgment. This process of unanimous propagation is called as flocking propagation. In information diffusion, the spreader who can influence others and enable the flocking information diffusion is called as flocking influencer.

In a scale-free network like OSNs, the participants can influence other participants within the community easier (Zhang & Li, 2017). So, the influential spreaders identified from the community level have the ability to quickly convince the neighbors of the same community (Zhang, Zhu, Wang, & Zhao, 2013). This approach is used to identify the flocking influencers in the proposed work. In dampwood termite immunization, the termite affected by pathogen shows alarm behavior which helps in controlling the rumor. Inspiring from this, the proposed approach selects anti-rumor spreaders from the rumor spreading participants as well along with other participants. So, the individuals from states such as Uncertain, Rumor Spreader and Prosocial can become the true information spreader at any point in time.

```
Algorithm 1 - Flocking Influencers Finder
INPUT: $G=(V,E,\tau)$, a $n$ set of communities $C=\{C_1,C_2,C_3,\ldots,C_n\}$, rumor depth $rs(t)$
OUTPUT: Flocking Influencer set $FL$.
$FL \leftarrow \theta, U' \leftarrow V-FL,$
foreach $Ci$ in $C$ do:
        $IC_{Ci} = \frac{Round\left(rs(t)*\left(\left|P_{Ci}(t)+U_{Ci}(t)+S_{Ci}(t)\right|\right)\right)}{C*\left|P_{Ci}(t)+U_{Ci}(t)+S_{Ci}(t)+FL_{Ci}(t)\right|}$
    for $range(IC_{Ci}))$:
            $v = \arg max_{i\in Ci/FL}\{(IIF_i)|i\in[S(t),P(t),U(t)]\};$
            $FL = FL \cup v;$
    endfor
endforeach
return set $FL$
```

The higher influencers from states S, P and U are identified and considered to be flocking spreaders in the network. The number of participants from flocking influencers is directly proportional to the strength of the rumor. The number of flocking influencers per community is identified as,

$$IC_{Ci} = \frac{Round\left(rs(t)*\left|P_{Ci}(t)+U_{Ci}(t)+S_{Ci}(t)\right|\right)}{C*\left|P_{Ci}(t)+U_{Ci}(t)+S_{Ci}(t)+FL_{Ci}(t)\right|}$$

The total number of flocking influencers in the network for true information propagation is calculated as,

5.1.2 Gushing Influencers

Gushing information propagation is an information flowing process where individuals try to imitate the predecessors in almost all the time. These influenced individuals may or may not impose their judgment. Gushing influencers are individuals who initiate gushing information propagation. The set of influencers who enable the flow of information across the communities are called as gushing influencers. The individuals who act as a bridge between the communities with higher interaction influence are considered for true information propagation.

```
Algorithm 2 - Gushing Influencer Finder
INPUT: $G=(V,E,\tau)$, a $n$ set of communities $C=\{C_1,C_2,C_3,\ldots,C_n\}$,
OUTPUT: Gushing influencer set $GI$ for time $t$
$GI \leftarrow \theta, U' \leftarrow V-GI,$
foreach $Ci$ in $C$ do
    foreach node $i$ in $Ci$:
            if $\exists eof(i,j)\ |i\in Ci\ \&j\nexists Ci$:
            $Br_{Ci} = Br_{Ci} \cup i;$
        endif
    endforeach
      $w = \arg\max_{k\in Br_{Ci}}\{(IIF_k)|k\in[S(t),P(t),U(t)]\};$
```

```
        $GI = GI \cup w$;
endforeach
return set $GI$
```

GI is the set of bridging individuals who can disseminate the anti-rumor information across the communities to enable the gushing propagation. This enables every community to receive information through bridges. Hence, the total influential initiators combining flocking and gushing influencers are,

$$\eta = FL \cup GI$$

$$\left|\eta\right| = \sum_{Ci \in C} IC_{Ci} + n$$

The total initiators for this defensive protection are η. The flocking initiators of each community are directly proportional to the strength of rumors. The number of gushing influencers is equal to the number of communities in the network.

5.2 Rumor Control – A Defensive Protection Approach

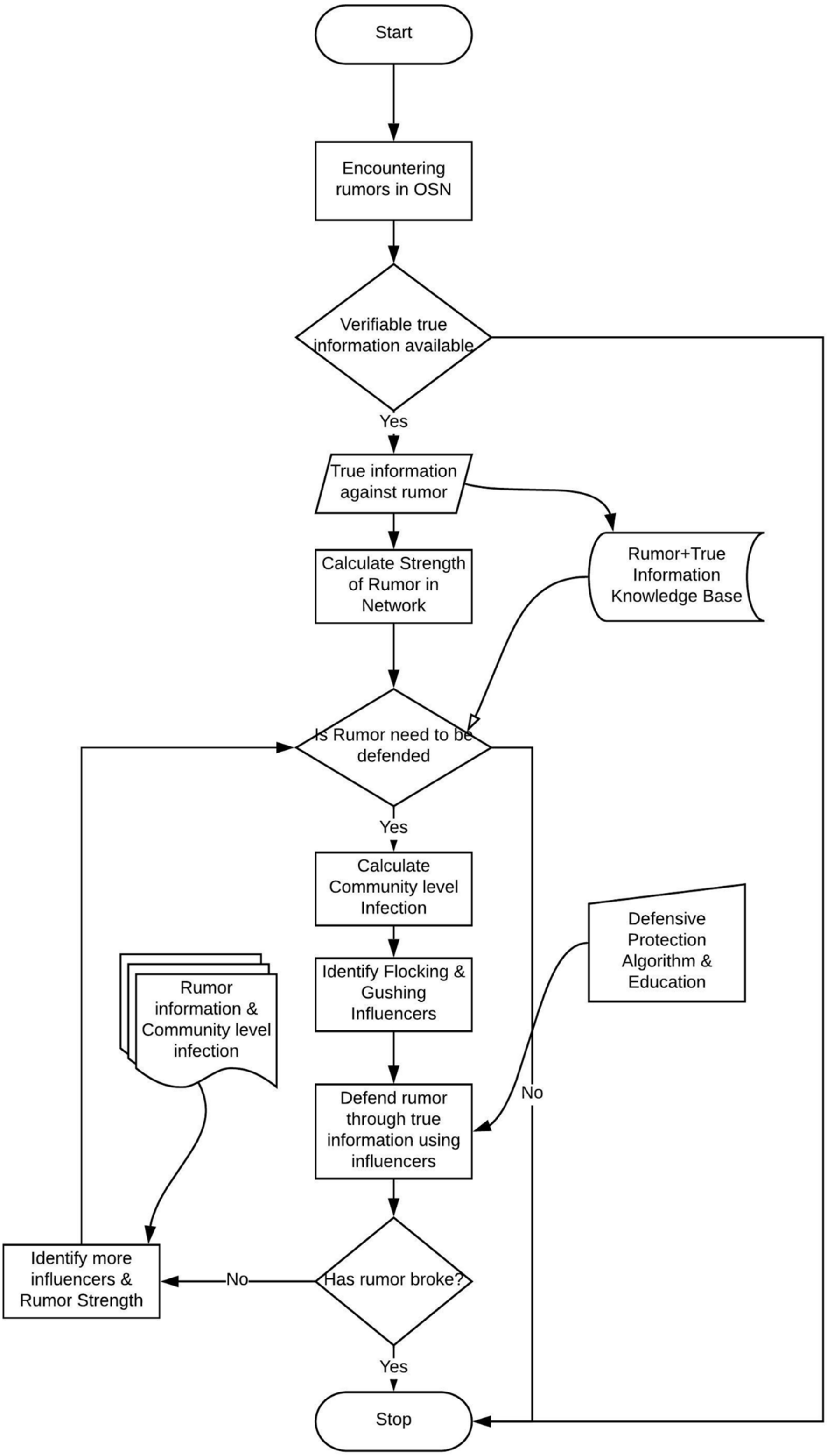
This subsection explains the propagation of true information against the rumor. Upon identification of rumor existence, the number of influencers identified who can enable the flocking and gushing information propagation. Those influencers are educated about the falseness of rumor and initiate the ‘anti-rumor’ propagation. The immunization approach of dampwood termite is to show alarm behavior through affected termites. This act is identified by other participants and co-operatively spread across the nest faster. In the proposed work, the initiators are also co-operative spreaders. Once the rumor identified, the affected individuals and other participants who can enable true information propagation are initiating the ‘anti-rumor’ propagation. The ‘anti-rumor’ spread until the rumor breaks in the system or the end condition meets. This rumor breaking condition is identified from the rumor strength in the network. Algorithm 3 shows the defensive protection mechanism of the proposed approach.

```
Algorithm 3 - Defensive protection
Input: $G=\left(V,E,B\right)$, a $n$ set of communities
$C=\left\{C_1,C_2,C_3,\dots,C_n\right\} G_c=\left\{\gamma,\delta_c\right\} | \gamma=\left\{1,2,3,\dots n\right\} nodes \,\&\, \delta_c \; set \; of \; edges$
Input: $\eta, where \; \eta \in V \,\&\, \left|\eta\right| \le \left|V\right|\}$
Input:

Output: Updated

foreach node $i$ in $\eta$:
    if $i \in U\left(t\right)$ then:
    $I\left(t\right)=I\left(t\right)-i$
    $DP\left(t\right)=DP\left(t\right)\cup i$
elseif $i \in P\left(t\right)$ then:
            $P\left(t\right)=P\left(t\right)-i$
    $DP\left(t\right)=DP\left(t\right)\cup i$
```

Figure 4. Defensive Protection immunization of OSNs


Start
Encountering rumors in OSN
Verifiable true information available
Yes
No
True information against rumor
Rumor+True Information Knowledge Base
Calculate Strength of Rumor in Network
Is Rumor need to be defended
Yes
No
Calculate Community level Infection
Identify Flocking & Gushing Influencers
Defensive Protection Algorithm & Education
Rumor information & Community level infection
Defend rumor through true information using influencers
Has rumor broke?
No
Identify more influencers & Rumor Strength
Yes
Stop

```
elseif $i \in S(t)$ then:
    $S(t) = S(t) - i$
        $DP(t) = DP(t) \cup i$
  endif
endforeach
```

Rumor control in this work is explained in figure 4. From figures 1 and 4, it is known that the proposed work is spreading ‘anti-rumor’ similar to the pathogen defense nature of dampwood termite. The main similarities between the defense of dampwood termite against pathogen and rumor containment in the proposed work are as follows: 1. Both approaches are defensive protection. i.e., once after identifying the infection, the immunization starts. 2. The immunization approach in both is through the co-operative activity. The individuals who can enable flocking and gushing propagation are helping in co-operative propagation in OSNs. 3. The contact immunity propagates the immunization within and across the broods/communities in both approaches.

6. EXPERIMENTAL EVALUATIONS

The experimental evaluation considers six social networking datasets to demonstrate the effectiveness of the proposed rumor containment approach in controlling the rumor propagation in the OSNs. It also compares the rumor control ability of different anti-rumor methods against the proposed approach to ensure efficiency. The comparison methods are recent and well-known in controlling the rumor propagation.

6.1 Datasets and Competing Methods

In this experiment, six social networking datasets, sizes ranging from small to large, are used. Two datasets are randomly generated, and the remaining four datasets are available publicly (Krevl, 2014). Topological statistics of the datasets are available in table 1.

The proposed rumor control approach is compared with state-of-the-art anti-rumor propagation approaches. The approaches are chosen from recent and well-known anti-rumor propagation methods. The competing methods are D-C model (D-C) (Liu, et al., 2016), SIHR model (Zhao L., et al., 2012), and a recent rumor-containing approach RC model (Pan, Yang, Yang, Wu, & Tang, 2018). All these models discuss the significance of truth spreading against the rumor.

Table 1. Topological features of datasets

Dataset Name	Network Features					
	n	e	<k>	H	β_{th}	β
Karate Club	34	78	4.5882	1.6895	0.129	0.242
RandNW_1	1000	5178	13	2.11	0.08	0.24
RandNW_2	2000	14324	20	2.33	0.11	0.14
ego-Facebook	4,039	88,234	34	3.22	0.12	0.24
ego-Twitter	81306	1768149	42	3.45	0.134	0.15
ca-Condmat	21363	196972	22	2.99	0.02	0.035

Here <k> is average degree, H = <k2>/<k>2 – Degree Heterogenicity index, β_{th} = <k>/<k2> - epidemic threshold

- **D-C Model:** This is **the** Diffusion-Containment model based on Linear Threshold (LT) model to contain one of the competing influences and enhance the propagation of another influence. In this model, the state of a participant is carried by a probability value called activation probability. Here, the higher probability neighbor only can influence the participant. D-C model is implemented in the experiments by extending the LT model.
- **SIHR Model:** The Susceptible-Infected-Hibernator-Removed (SIHR) model is an extension of the SIR model which considers forgetting and remembering mechanisms of participants. Authors argue forgetting/remembering users play an important role in the longevity of rumors in the network. i.e., In this model, the rumor may reinitiate its propagation in a later point of time or breaks its propagation due to forgetting participants.
- **RC Model:** RC model defines suppressing the rumor by spreading true as a constrained optimization problem. This model considers budget and time constraints for rumor control. The model also evaluates the forgetting rate of the participants. The epidemic propagation model of this approach is uncertain-rumor-truth-uncertain (URTU). In experiments, the URTU model is implemented for comparisons.

The implementation of the competing and proposed approach is implemented in Python language. The experimental setup for the evaluations is explained in the next section.

6.2 Experimental Setup and Results

The experimental evaluation in this work is performed on a server with 16 GB ram, 4.0 GHz octa-core processor. This system is running on 64-bit JAVA VM 1.8. To load the existing datasets and to generate random networks, NetworkX (Developers, 2010), a python package, is used. The spreading rate of rumor spreader and defense protector is set to 1 where the spreader and protector can spread the information only once to the same neighbor. The simulations are averaged for at least fifty runs for proposed and competing methods.

The first evaluation in this experiment is to explore the amount of rumors left in the network after every iteration. The proposed work evaluates the percentage of rumors left for a different number of initiators. The results are plotted in a three-dimension chart as shown in figures below for all six datasets.

Figures 5(a)-5(f) show the rumor percentage left in the network for all six datasets. The iterations are the timesteps of the rumor control process. The timesteps plotted are 10,20,30,40 and 50. The number of initiators for every dataset is based on the algorithms 1 and 2 that is described in Eqn. (10).

The rumor percentage of Karate Club and RandNW_1 has decreased from 12% to 2% from the iteration 10 to 50. These results are obtained for the higher initiator level. Similarly, the rumor percentage of RandNW_2 is reduced from 8.6% to 5%. One must note that these three are the small-sized social networks with lesser clustering coefficient and the number of communities is lesser. The larger social networking datasets considered in the experiments are ego-Facebook, ego-Twitter, and ca-Condmat. Rumor percentage reduced in these datasets for higher-level initiators are ego-Facebook – from 21% to 3%, ego-Twitter – from 33% to 9%, ca-Condmat – from 31.38% to 7.32%. These large networks have a higher clustering coefficient value with a relatively higher number of communities than small networks.

Next, the comparison of rumor control with other competing methods is presented. The results shown in the figures are for 50th timestep and varying initial influencer sizes. The competing methods in comparison are RC, SIHR, and D-C and those are elaborated in subsection 6.1.

Figures 6(a)-6(f) show the rumor control of competing methods for all the datasets. All datasets show superior results for the proposed RC-DP method. i.e., RC-DP outperforms other competing methods in all datasets. For smaller datasets such as Karate Club, RandNW_1 and RandNW_2, the methods SIHR and D-C are performing almost similar but this performance is lesser than competing methods RC and proposed RC-DP. In these networks, RC-DP performs little higher than the recent

Figure 5. Karate Club Rumor Percentage, Rand, NW_1 Rumor Percentage RandNW_2 Rumor Percentage, Ego-Facebook Rumor Percentage, Figure 5e. Ego-Twitter Rumor Percentage,. ca-Condmat Rumor Percentage

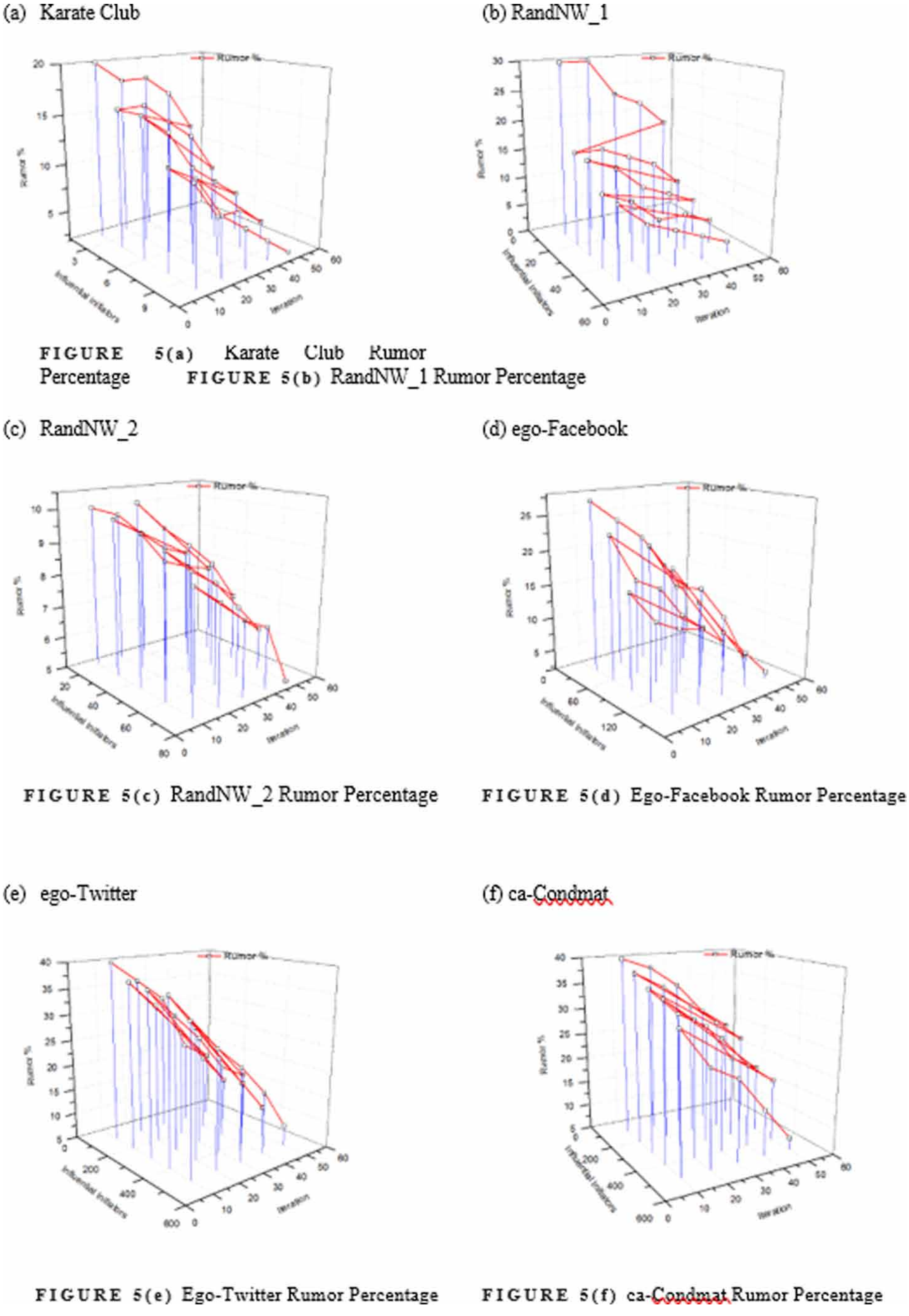


FIGURE 5(a) Karate Club Rumor Percentage

FIGURE 5(b) RandNW_1 Rumor Percentage

FIGURE 5(c) RandNW_2 Rumor Percentage

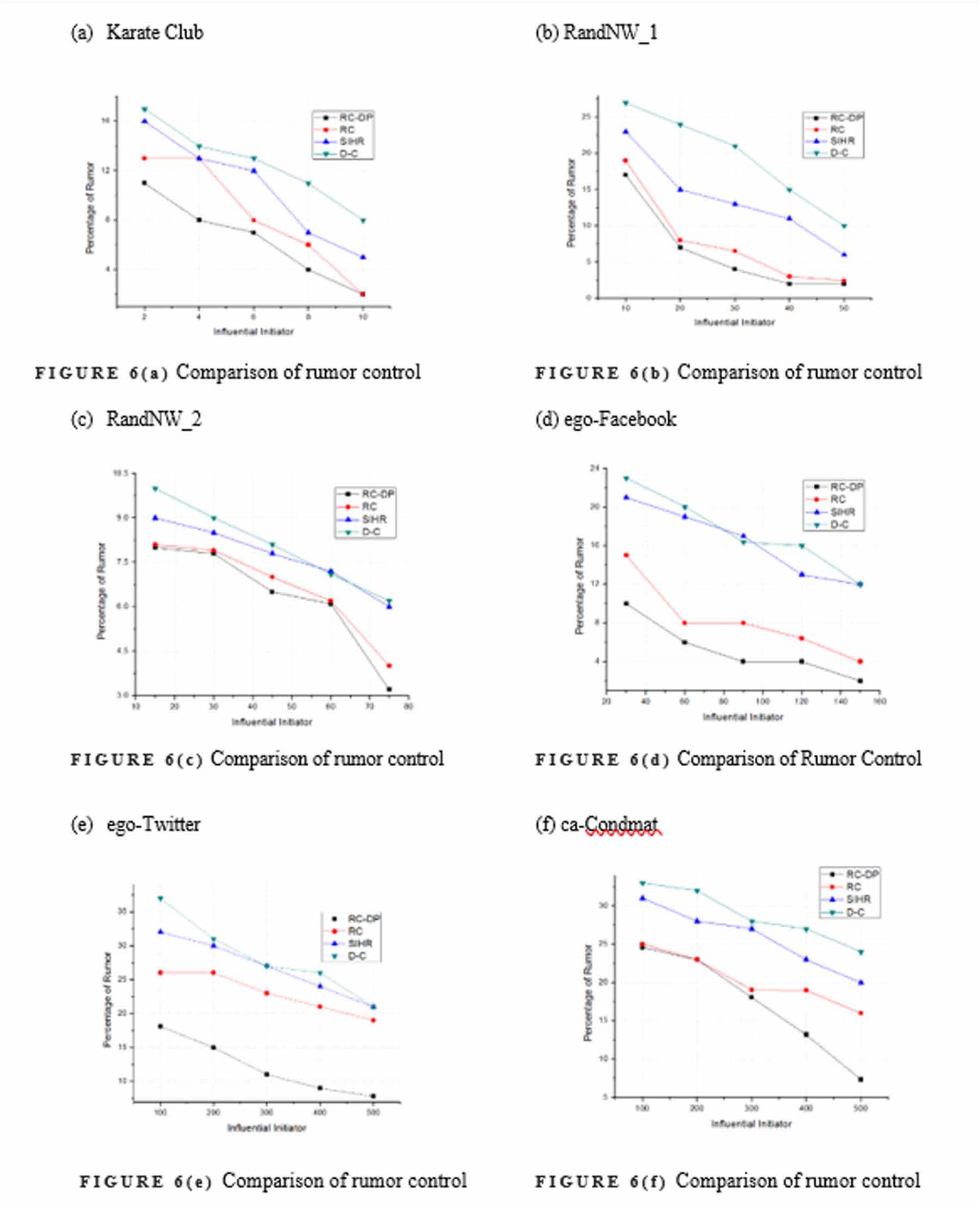
FIGURE 5(d) Ego-Facebook Rumor Percentage

FIGURE 5(e) Ego-Twitter Rumor Percentage

FIGURE 5(f) ca-Condmat Rumor Percentage

rumor containing method RC. RC-DP outperform other competing methods for all the larger datasets. For one of the larger datasets ca-Condmat, the proposed work provides results almost the same as RC for small initiator sizes. But when initiator size increases, the proposed work perform better. It is visible that the number of initiators is not higher in aligning to the strength of rumor which provides

Figure 6. Comparison of rumor control



(a) Karate Club

(b) RandNW_1

FIGURE 6(a) Comparison of rumor control

FIGURE 6(b) Comparison of rumor control

(c) RandNW_2

(d) ego-Facebook

FIGURE 6(c) Comparison of rumor control

FIGURE 6(d) Comparison of Rumor Control

(e) ego-Twitter

(f) ca-Condmat

FIGURE 6(e) Comparison of rumor control

FIGURE 6(f) Comparison of rumor control

comparatively lesser results. This implies that the proposed work performs better for scale-free, larger datasets.

Overall RC-DP is performing better than other existing methods in controlling the rumors faster in the network. This proves the proposed work is efficient in rumor containment as defensive protection.

7. DISCUSSION

In this paper, a novel anti-rumor propagation approach is presented as a defensive act against the rumor propagation in OSNs. The intensity of anti-rumor propagation is directly proportional to the strength of rumors available when the anti-rumor spread begins. The key advantages of proposed work over other anti-rumor propagation approaches are as follows.

1. The epidemic model proposed in this work imitates the real-world information propagation. The PP model defines the defensive protection of anti-rumors against the rumor. The advantage of using this approach is to efficiently control the rumor as a defensive act. The PP model can be easily deployed in any real-world social networking applications where the rumor propagation is possible.
2. The initial spreaders identified in this approach are flocking and gushing influencers. The initial spreaders play a major role in letting true information reaching a greater number of participants faster in the network. Flocking and gushing influencers provide the advantage of spreading the information quicker. The experiment with a different number of initiators is conducted and results are shown in figures 5(a)-5(f). The results show that the chosen initial spreaders control rumors faster.
3. Opinion dynamics is used to identify efficient initial spreaders. Opinion dynamics has applications in group decision making, trust-aware applications. From the best of our knowledge, opinion dynamics is not used in any of the previous rumor control approaches. The proposed work efficiently uses this to identify influential spreaders. The experimental results shown in figures 6(a)-6(f) prove that the initial spreaders found using opinion dynamics control the rumors efficiently.
4. A novel anti-rumor propagation approach using PP model is controlling the rumors faster in larger, scale-free social networks. The results shown in 6(d), 6(e) and 6(f) depict the rumor control comparison of the proposed approach. The rumors are controlled from more than 30% to lesser than 5%. It is evident that the proposed work is a better approach for enhanced rumor control in scale-free networks.

The efficiency of the anti-rumor approach in controlling the rumor can be measured using the amount of rumors removed from the network after applying the ‘anti-rumor’ approach. To measure the ability of rumor control of an anti-rumor approach, we have introduced a metric called Rumor Control Rate (RCR). This can be defined as follows,

$$RCR = 100 - \left| \frac{rs(t)}{rs(0)} \right| * 100 \Bigg| \eta \in V \;\&\; |\eta| \, is \ constant$$

In this equation, $rs(t)$ is the strength of rumors at time t after applying the anti-rumor propagation approach in the network using η set of influential initiators and $rs(0)$ is the strength of rumors before applying the anti-rumor approach. Rumor control rates using the lowest and the highest number of initiators are considered for this comparison. In this experiment, the number of influencers for the lowest number of influencers and the highest number of influencers is obtained from the experiments applied in subsection 6.2 for every dataset. The results are obtained from 50th timestep.

The results are shown in figures 7(a) and 7(b) for the lowest number of influencers and the highest number of influencers respectively. From these figures, the proposed RC-DP method is performing

Figure 7. Rumor Control Rate for the lowest number of influential initiators

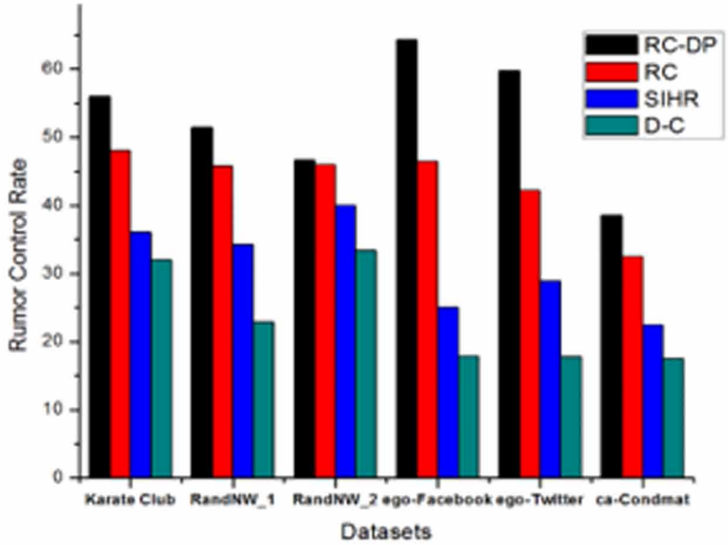
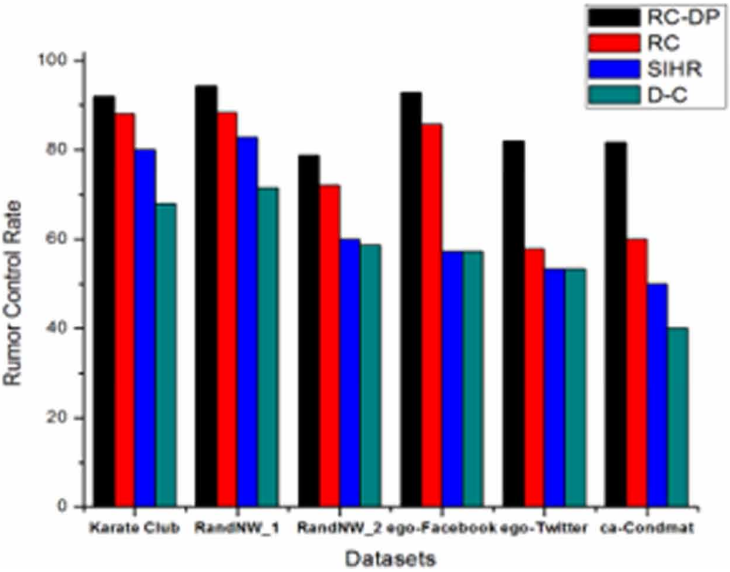


FIGURE 7(a) Rumor Control Rate for the lowest number of influential initiators



better than other competing methods by having higher rumor control rate for every dataset in the lowest and highest number of influencers. It is also visible that RC-DP is controlling the rumors around 21% higher than other competing methods. From figures 7(a) and 7(b), the proposed method is performing better for larger and scale-free networks such as ego-Facebook, ego-Twitter, and ca-

Condmat. The amount of rumor controlled using RC-DP method with higher influential spreaders is more than 84% for all the datasets. RC-DP controlled rumors up-to 94% for ego-Facebook network and this is the only method that controlled more than 90% of rumors when compared with other methods.

The proposed approach utilizes the strength of the rumor and interaction influence of participants in controlling the rumor. The previous works have not used both together in rumor control. The advantage of using these two measures together is to efficiently identify the number of initial spreaders in proportional to the percentage of rumors in the network. These spreaders can influence the neighbors quicker to enable defensive act against rumor.

8. CONCLUSION

Rumor propagation in OSNs is a major threat to the network and society. Controlling the rumor propagation is of greater value in avoiding the threat. This paper proposes a defensive rumor control approach called Rumor Control via Defensive Protection. It is a co-operative rumor control approach that spreads anti-rumors as defending protection against the rumor propagation. In this work, a novel information propagation model called the PP model is derived to imitate real-world propagation of rumors and anti-rumors in OSNs. Then, two sets of initiators namely the flocking and gushing influencers who can disseminate anti-rumors faster are identified. Using these initial spreaders, anti-rumors spread in PP model. The experimental evaluations using six social networking datasets demonstrate that the proposed work is controlling the rumors efficiently. For the scale-free networks, the proposed work controlled the rumors from 33% to 9% (ego-Twitter) and from 31.38% to 7.32% (ca-Condmat). This proves that the proposed work is efficient in controlling the rumor. Hence, anti-rumor propagation as defensive protection is providing better results and considered to be an effective approach.

The anti-rumor propagation approach is having a few optimization factors such as the strength of rumor and spreading ability of initiators. In future, other optimization factors such as the coreness of spreaders can be considered to optimize this propagation. The defensive protection approach relies on the maximization of influence using the strength of rumor and opinion dynamics. In future, an improved opinion dynamics system can be employed for finding the flocking and gushing influencers.

REFERENCES

Afassinou, K. (2014). Analysis of the impact of education rate on the rumor spreading mechanism. *Physica A*, *414*, 43–52. doi:10.1016/j.physa.2014.07.041

Afassinou, K. (2014). Analysis of the impact of education rate on the rumor spreading mechanism. *Physica A*, *414*, 43–52. doi:10.1016/j.physa.2014.07.041

Ahn, G.-J., Shehab, M., & Squicciarini, A. (2011). Security and privacy in social networks. *IEEE Internet Computing*, *15*(3), 10–12. doi:10.1109/MIC.2011.66

Aurigemma, S. (2013). A Composite Framework for Behavioral Compliance with Information Security Policies. *Journal of Organizational and End User Computing*, *25*(3), 32–51. doi:10.4018/joeuc.2013070103

Bakshy, E., Rosenn, I., Marlow, C., & Adamic, L. (2012). The role of social networks in information diffusion. *Proceedings of the 21st international conference on World Wide Web*, 519-528. doi:10.1145/2187836.2187907

Cheikh-Ammar, M., & Barki, H. (2016). The influence of social presence, social exchange and feedback features on SNS continuous use: The Facebook context. *Journal of Organizational and End User Computing*, *28*(2), 33–52. doi:10.4018/JOEUC.2016040103

Chen, G. (2019). ILSCR rumor spreading model to discuss the control of rumor spreading in emergency. *Physica A*, *522*, 88–97. doi:10.1016/j.physa.2018.11.068

Cho, J.-H. (2018). Dynamics of Uncertain and Conflicting Opinions in Social Networks. *IEEE Transactions on Computational Social Systems*, *5*(2), 518–531. doi:10.1109/TCSS.2018.2826532

Cremer, S., Armitage, S. A., & Schmid-Hempel, P. (2007). Social immunity. *Current Biology*, *17*(16), R693–R702. doi:10.1016/j.cub.2007.06.008 PMID:17714663

Daley, D. J., & Kendall, D. G. (1964). Epidemics and rumours. *Nature*, *204*(4963), 1118. doi:10.1038/2041118a0 PMID:14243408

Dauhoo, M. Z., Juggurnath, D., & Adam, N.-R. B. (2016). The stochastic evolution of rumors within a population. *Mathematical Social Sciences*, *82*, 85–96. doi:10.1016/j.mathsocsci.2016.05.002

DiFonzo, N., & Bordia, P. (2007). *Rumor psychology: Social and organizational approaches* (Vol. 1). American Psychological Association Washington. doi:10.1037/11503-000

Doerr, B., Fouz, M., & Friedrich, T. (2011). Social networks spread rumors in sublogarithmic time. *Proceedings of the forty-third annual ACM symposium on Theory of computing*, 21-30. doi:10.1145/1993636.1993640

Domm, P. (2013). *False rumor of explosion at White House causes stocks to briefly plunge; AP confirms its Twitter feed was hacked.* CNBC.COM.

Fan, L., Lu, Z., Wu, W., Thuraisingham, B., Ma, H., & Bi, Y. (2013). Least cost rumor blocking in social networks. *Distributed Computing Systems (ICDCS), 2013 IEEE 33rd International Conference on*, 540-549.

Fan, L., Wu, W., Zhai, X., Xing, K., Lee, W., & Du, D.-Z. (2014). Maximizing rumor containment in social networks with constrained time. *Social Network Analysis and Mining*, *4*(1), 214. doi:10.1007/s13278-014-0214-4

Foster, P. (2013, Apr). *'Bogus' AP tweet about explosion at the White House wipes billions off US markets*. Retrieved from Telegraph: https://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html

Giorno, V., & Spina, S. (2016). Rumor spreading models with random denials. *Physica A*, *461*, 569–576. doi:10.1016/j.physa.2016.06.070

Guille, A., Hacid, H., Favre, C., & Zighed, D. A. (2013). Information diffusion in online social networks: A survey. *SIGMOD Record*, *42*(2), 17–28. doi:10.1145/2503792.2503797

Han, S., Zhuang, F., He, Q., Shi, Z., & Ao, X. (2014). Energy model for rumor propagation on social networks. *Physica A*, *394*, 99–109. doi:10.1016/j.physa.2013.10.003

He, X., Song, G., Chen, W., & Jiang, Q. (2012). Influence blocking maximization in social networks under the competitive linear threshold model. *Proceedings of the 2012 SIAM International Conference on Data Mining*, 463-474. doi:10.1137/1.9781611972825.40

Hu, Y., Pan, Q., Hou, W., & He, M. (2018). Rumor spreading model considering the proportion of wisemen in the crowd. *Physica A*, *505*, 1084–1094. doi:10.1016/j.physa.2018.04.056

Huber, M., Weippl, E., Kitzler, G., & Goluch, S. (2011). Friend-in-the-middle attacks: Exploiting social networking sites for spam. *IEEE Internet Computing*, *15*(3), 28–34. doi:10.1109/MIC.2011.24

Huo, L., & Ma, C. (2017). Dynamical analysis of rumor spreading model with impulse vaccination and time delay. *Physica A*, *471*, 653–665. doi:10.1016/j.physa.2016.12.024

Huo, L., & Song, N. (2016). Dynamical interplay between the dissemination of scientific knowledge and rumor spreading in emergency. *Physica A*, *461*, 73–84. doi:10.1016/j.physa.2016.05.028

Huo, L., Wang, L., Song, N., Ma, C., & He, B. (2017). Rumor spreading model considering the activity of spreaders in the homogeneous network. *Physica A*, *468*, 855–865. doi:10.1016/j.physa.2016.11.039

Jenkins, J. L., Durcikova, A., & Burns, M. B. (2013). Simplicity is bliss: Controlling extraneous cognitive load in online security training to promote secure behavior. *Journal of Organizational and End User Computing*, *25*(3), 52–66. doi:10.4018/joeuc.2013070104

Ji, K., Liu, J., & Xiang, G. (2014). Anti-rumor dynamics and emergence of the timing threshold on complex network. *Physica A*, *411*, 87–94. doi:10.1016/j.physa.2014.06.013

Kimura, M., Saito, K., & Motoda, H. (2009). Blocking links to minimize contamination spread in a social network. *ACM Transactions on Knowledge Discovery from Data*, *3*(2), 9. doi:10.1145/1514888.1514892

Kotnis, B. a. (2014). *Cost effective rumor containment in social networks.* arXiv preprint arXiv:1403.6315

Krevl, J. L. (2014, June). *{SNAP Datasets}: {Stanford} Large Network Dataset Collection*. Retrieved from http://snap.stanford.edu/data

Leskovec, J., Backstrom, L., & Kleinberg, J. (2009). Meme-tracking and the dynamics of the news cycle. *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, 497-506. doi:10.1145/1557019.1557077

Li, D., Ma, J., Tian, Z., & Zhu, H. (2015). An evolutionary game for the diffusion of rumor in complex networks. *Physica A*, *433*, 51–58. doi:10.1016/j.physa.2015.03.080

Li, K., Zhang, L., & Huang, H. (2018). Social influence analysis: Models, methods, and evaluation. *Engineering*, *4*(1), 40–46. doi:10.1016/j.eng.2018.02.004

Li, L., Scaglione, A., Swami, A., & Zhao, Q. (2012). Phase transition in opinion diffusion in social networks. *Acoustics, speech and signal processing (ICASSP), 2012 IEEE international conference on*, 3073-3076.

Li, L., Scaglione, A., Swami, A., & Zhao, Q. (2012). Phase transition in opinion diffusion in social networks. *2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 3073-3076. doi:10.1109/ICASSP.2012.6288564

Li, S., Zhu, Y., Li, D., Kim, D., & Huang, H. (2013). Rumor restriction in online social networks. *2013 IEEE 32nd International Performance Computing and Communications Conference (IPCCC)*, 1-10.

Li, X., Rong, G., & Thatcher, J. B. (2012). Does Technology Trust Substitute Interpersonal Trust?: Examining Technology Trust's Influence on Individual Decision-Making. *Journal of Organizational and End User Computing*, *24*(2), 18–38. doi:10.4018/joeuc.2012040102

Liu, W., Yue, K., Wu, H., Li, J., Liu, D., & Tang, D. (2016). Containment of competitive influence spread in social networks. *Knowledge-Based Systems*, *109*, 266–275. doi:10.1016/j.knosys.2016.07.008

Ma, J., Li, D., & Tian, Z. (2016). Rumor spreading in online social networks by considering the bipolar social reinforcement. *Physica A*, *447*, 108–115. doi:10.1016/j.physa.2015.12.005

Maki, D. P., & Thompson, M. (1973). *Mathematical models and applications: with emphasis on the social life, and management sciences*. Academic Press.

Myles, T. G. (2002). Alarm, aggregation, and defense by Reticulitermes flavipes in response to a naturally occurring isolate of Metarhizium anisopliae. *Sociobiology*, *40*(2), 243–256.

Naug, D., & Camazine, S. (2002). The role of colony organization on pathogen transmission in social insects. *Journal of Theoretical Biology*, *215*(4), 427–439. doi:10.1006/jtbi.2001.2524 PMID:12069487

Ngamassi, L., Ramakrishnan, T., & Rahman, S. (2016). Use of social media for disaster management: A prescriptive framework. *Journal of Organizational and End User Computing*, *28*(3), 122–140. doi:10.4018/JOEUC.2016070108

Pan, C., Yang, L.-X., Yang, X., Wu, Y., & Tang, Y. Y. (2018). An effective rumor-containing strategy. *Physica A*, *500*, 80–91. doi:10.1016/j.physa.2018.02.025

Pham, L. M., Tran, L. T.-T., Thipwong, P., & Huang, W. T. (2019). Dynamic Capability and Organizational Performance: Is Social Networking Site a Missing Link? *Journal of Organizational and End User Computing*, *31*(2), 1–21. doi:10.4018/JOEUC.2019040101

Raj, E. D., & Babu, L. D. (2015). A firefly swarm approach for establishing new connections in social networks based on big data analytics. *International Journal of Communication Networks and Distributed Systems*, *15*(2-3), 130–148. doi:10.1504/IJCNDS.2015.070968

Raj, E. D., & Babu, L. D. (2016). A fuzzy adaptive resonance theory inspired overlapping community detection method for online social networks. *Knowledge-Based Systems*, *113*, 75–87. doi:10.1016/j.knosys.2016.09.015

Rosengaus, R. B., & Traniello, J. F. (2001). Disease susceptibility and the adaptive nature of colony demography in the dampwood termite Zootermopsis angusticollis. *Behavioral Ecology and Sociobiology*, *50*(6), 546–556. doi:10.1007/s002650100394

Rosengaus, R., Jordan, C., Lefebvre, M., & Traniello, J. (1999). Pathogen alarm behavior in a termite: A new form of communication in social insects. *Naturwissenschaften*, *86*(11), 544–548. doi:10.1007/s001140050672 PMID:10551951

San Nicolas-Rocca, T., & Olfman, L. (2013). End user security training for identification and access management. *Journal of Organizational and End User Computing*, *25*(4), 75–103. doi:10.4018/joeuc.2013100104

Santhoshkumar, S., & Babu, L. D. (2019). An Effective Rumor Control Approach for Online Social Networks. *Information Systems Design and Intelligent Applications*, 63-73.

Srinivasan, S., & Babu, L. D. (2019). Interest aware influential information disseminators in social networks. *SN Applied Sciences*, *1*(11), 1456. doi:10.1007/s42452-019-1436-x

Srinivasan, S. (2019). A Parallel Neural Network Approach for Faster Rumor Identification in Online Social Networks. *International Journal on Semantic Web and Information Systems*, *15*(4), 69–89. doi:10.4018/IJSWIS.2019100105

Subramaniyaswamy, V., Logesh, R., Abejith, M., Umasankar, S., & Umamakeswari, A. (2017). Sentiment analysis of tweets for estimating criticality and security of events. *Journal of Organizational and End User Computing*, *29*(4), 51–71. doi:10.4018/JOEUC.2017100103

Tong, G., Wu, W., Guo, L., Li, D., Liu, C., Liu, B., & Du, D.-Z. (2017). An efficient randomized algorithm for rumor blocking in online social networks. *IEEE Transactions on Network Science and Engineering*.

Traniello, J. F., Rosengaus, R. B., & Savoie, K. (2002). The development of immunity in a social insect: Evidence for the group facilitation of disease resistance. *Proceedings of the National Academy of Sciences of the United States of America*, *99*(10), 6838–6842. doi:10.1073/pnas.102176599 PMID:12011442

Tripathy, R. M., Bagchi, A., & Mehta, S. (2010). A study of rumor control strategies on social networks. *Proceedings of the 19th ACM international conference on Information and knowledge management*, 1817-1820. doi:10.1145/1871437.1871737

Wang, J., Zhao, L., & Huang, R. (2014). SIRaRu rumor spreading model in complex networks. *Physica A*, *398*, 43–55. doi:10.1016/j.physa.2013.12.004

Wen, S., Haghighi, M. S., Chen, C., Xiang, Y., Zhou, W., & Jia, W. (2015). A sword with two edges: Propagation studies on both positive and negative information in online social networks. *IEEE Transactions on Computers*, *64*(3), 640–653. doi:10.1109/TC.2013.2295802

Xiao, X., & Wang, T. (2016). The implications of social influence theory on continuance intention for social networking among Chinese university students. *Journal of Organizational and End User Computing*, *28*(4), 55–72. doi:10.4018/JOEUC.2016100104

Zhang, R., & Li, D. (2017). Rumor propagation on networks with community structure. *Physica A*, *483*, 375–385. doi:10.1016/j.physa.2017.05.006

Zhang, X., Zhu, J., Wang, Q., & Zhao, H. (2013). Identifying influential nodes in complex networks with community structure. *Knowledge-Based Systems*, *42*, 74–84. doi:10.1016/j.knosys.2013.01.017

Zhao, L., Cui, H., Qiu, X., Wang, X., & Wang, J. (2013). SIR rumor spreading model in the new media age. *Physica A*, *392*(4), 995–1003. doi:10.1016/j.physa.2012.09.030

Zhao, L., Wang, J., Chen, Y., Wang, Q., Cheng, J., & Cui, H. (2012). SIHR rumor spreading model in social networks. *Physica A*, *391*(7), 2444–2453. doi:10.1016/j.physa.2011.12.008

Zhao, Z., Wang, X., Zhang, W., & Zhu, Z. (2015). A community-based approach to identifying influential spreaders. *Entropy (Basel, Switzerland)*, *17*(4), 2228–2252. doi:10.3390/e17042228

Santhoshkumar S. received MS degree in Software Engineering from VIT University, Vellore, India. Currently he is a research scholar in School of Information Technology and Engineering at VIT University, Vellore. His primary research interests include Cloud Computing, Big Graph analytics and Social Network analysis

Dhinesh Babu L. D. received BE in Electrical and Electronics Engineering and M.E in Computer Science and Engineering from the University of Madras and PhD from VIT University. He is currently a faculty in the School of Information Technology and Engineering at VIT University, Vellore, India. He has served as Division Leader of Software Engineering Division. His research interests include Social Computing, Recommender Systems, Big Data Analytics, Cloud Computing, and Internet of Things.