This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2016.2522436, IEEE Transactions on Dependable and Secure Computing

Rumor Source Identification in Social Networks with Time-varying Topology

Jiaojiao Jiang, Sheng Wen, Shui Yu, Yang Xiang and Wanlei Zhou

Abstract—Identifying rumor sources in social networks plays a critical role in limiting the damage caused by them through the timely quarantine of the sources. However, the temporal variation in the topology of social networks and the ongoing dynamic processes challenge our traditional source identification techniques that are considered in static networks. In this paper, we borrow an idea from criminology and propose a novel method to overcome the challenges. First, we reduce the time-varying networks to a series of static networks by introducing a time-integrating window. Second, instead of inspecting every individual in traditional techniques, we adopt a reverse dissemination strategy to specify a set of suspects of the real rumor source. This process addresses the scalability issue of source identification problems, and therefore dramatically promotes the efficiency of rumor source identification. Third, to determine the real source from the suspects, we employ a novel microscopic rumor spreading model to calculate the maximum likelihood (ML) for each suspect. The one who can provide the largest ML estimate is considered as the real source. The evaluations are carried out on real social networks with time-varying topology. The experiment results show that our method can reduce $60\% - 90\%$ of the source seeking area in various time-varying social networks. The results further indicate that our method can accurately identify the real source, or an individual who is very close to the real source. To the best of our knowledge, the proposed method is the first that can be used to identify rumor sources in time-varying social networks.

Index Terms—Time-varying social networks, rumor spreading, source identification, scalability.

1 Introduction

Rumors spreading in social networks have long been a critical threat to our society. A recent incident of rumors "Obama was injured in two explosions of White House" led to 10 billion USD losses in a few hours. This demonstrates that a single rumor can cause great damage to business and life [1]. Nowadays, with the development of mobile devices and wireless techniques, the temporal nature of social networks (time-varying social networks) has a deep influence on dynamical information spreading processes occurring on top of them [2]. The ubiquity and easy access of social networks not only promote the efficiency of information sharing but also dramatically accelerate the speed of rumor spreading [3]. Rumors combine the characteristics of the "word-of-mouth" spreading scheme with the dynamic connections between individuals in time-varying social networks [4].

For either forensic or defensive purposes, it has always been a significant work to identify the source of rumors in time-varying social networks [5]. However, the existing techniques generally require firm connections between individuals (*i.e.*, static networks) so that administrators can trace back along the determined connections to reach the spreading sources. For example, many methods rely on identifying spanning trees in networks [6]–[8], then the roots of the spanning trees are regarded as the rumor sources. The firm connections between users are the premise of constructing spanning trees in these methods. Some other methods detect rumor sources by measuring node centralities [9], [10]. The individual who has the maximum centrality value is considered as the rumor source. All of these centrality measures are based on static networks. Time-varying social networks, where users and interactions evolve over time, have led to great challenges to the traditional rumor source identification techniques.

In this paper, we propose a novel source identification method to overcome the challenges. First, to represent a time-varying social network, we reduce it to a sequence of static networks, each aggregating all edges and nodes present in a time-integrating window. This is the case, for instance, of rumors spreading in Bluetooth networks, for which the fine-grained temporal resolution is not available, whose spreading can be studied through different integrating windows Δt (*e.g.*, Δt could be minutes, hours, days or even months). In each integrating window, if users did not activate the Bluetooth on their devices (*i.e.*, *offline*), they would not receive or spread the rumors. If they moved out the bluetooth coverage of their communities (*i.e.*, *physical mobility*), they would not receive or spread the rumors. Second, similar to the detective routine in criminology, a small set of suspects will be identified by adopting a reverse dissemination process to narrow down the scale of the source

• *J. Jiang, S. Wen, S. Yu, Y. Xiang, W. Zhou are with the School of Information Technology, Deakin University, VIC 3125, Australia. Email: {jjiaoj, wesheng, syu, yang, wanlei}@deakin.edu.au.*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2016.2522436, IEEE Transactions on Dependable and Secure Computing

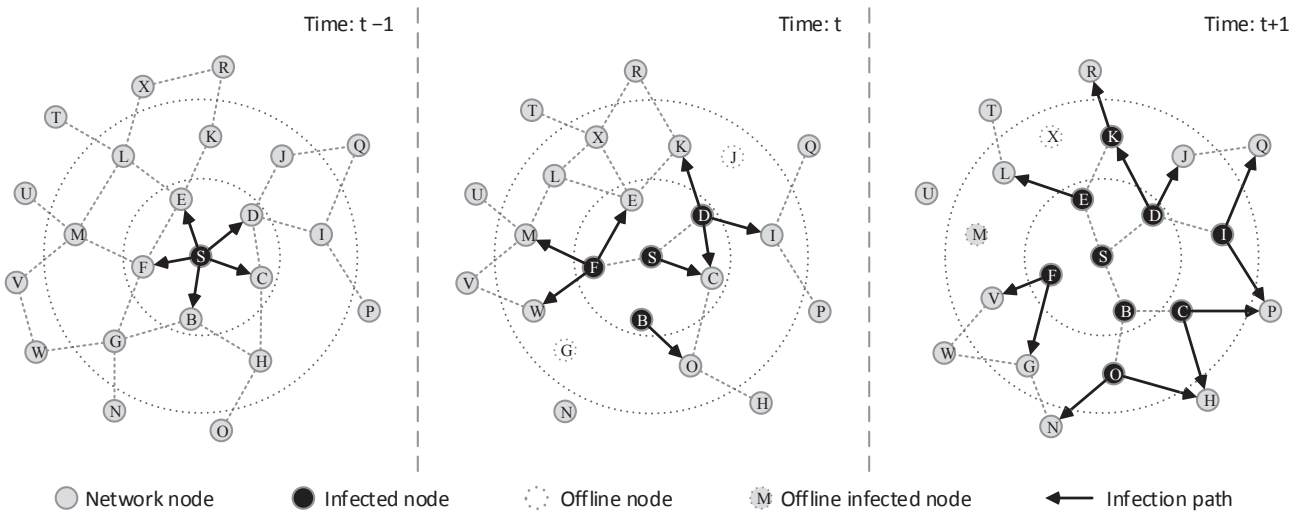


Fig. 1. Example of a rumor spreading in a time-varying social network. The random spread is located on the black node, and can travel on the links depicted as line arrows in the time windows. Dashed lines represent links that are present in the system in each time window.

seeking area. The reverse dissemination process distributes copies of rumors reversely from the users whose states have been determined based on various observations upon the networks. The ones who can simultaneously receive all copies of rumors from the infected users are supposed to be the suspects of the real sources. This reverse dissemination process is inspired from the Jordan Center method [9], which is used to detect rumor sources in static neworks. The method adopted here is different from the Jordan Center method, because our method is based on time-varying social networks rather than static networks. We find that the reverse dissemination method addresses the scalability in rumor source identification, and therefore, dramatically promotes the efficiency of rumor source identification. In contrast, the traditional methods inspect every user in networks, which costs a lot of time in estimating the real sources [10]–[12]. Third, to determine the real source from the suspects, we employ a microscopic rumor spreading model to analytically estimate the probabilities of each user being in different states in each time window. Since this model allows for the time-varying connections among users, it can feature the dynamics of each user. More specifically, assuming any suspect as the rumor source, we can obtain the probabilities of the observed users to be in their observed states. Then, for any suspect, we can calculate the maximum likelihood (ML) of obtaining the observation. The one who can provide the maximum ML will be considered as the real rumor source.

To the best of our knowledge, the proposed two-stage method is the first one that can be used to identify rumor sources in time-varying social networks. The major contribution of this paper is two-fold:

- We adopt a reverse dissemination method to narrow the scale of the source seeking area, and therefore significantly promotes the efficiency of source identification.
- We introduce a novel ML-based method that can overcome the connection-always-changing challenge through a novel rumor spreading model in time-varying social networks.
- Experiment results show significant advantages of our method in the identification of rumor sources, the estimation of spreading time, and the prediction of infection scale of rumors.

The rest of this paper is organized as follows. We introduce the preliminary knowledge of source identification in Section 2. Section 3 presents the details of the reverse dissemination method. We elaborate upon the ML-based method in Section 4 followed by Section 5 which shows a series of evaluations on our methods. Section 7 presents the state-of-the-art in this area, and finally, Section 8 concludes this paper.

2 Source Identification Primer

In this section, we introduce the primer for rumor source identification in social networks with time-varying topology, including the features of time-varying social networks, the state transition of users when they hear a rumor, and the categorization of partial observations in time-varying social networks.

2.1 Time-varying Social Networks

The essence of social networks lies in its time-varying nature. For example, the neighborhood of individuals moving over a geographic space evolves over time (*i.e.*, ***physical mobility***), and the interaction between the individuals appears and disappears in online social networks (*i.e.*, ***online/offline***) [2]. Time-varying

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2016.2522436, IEEE Transactions on Dependable and Secure Computing

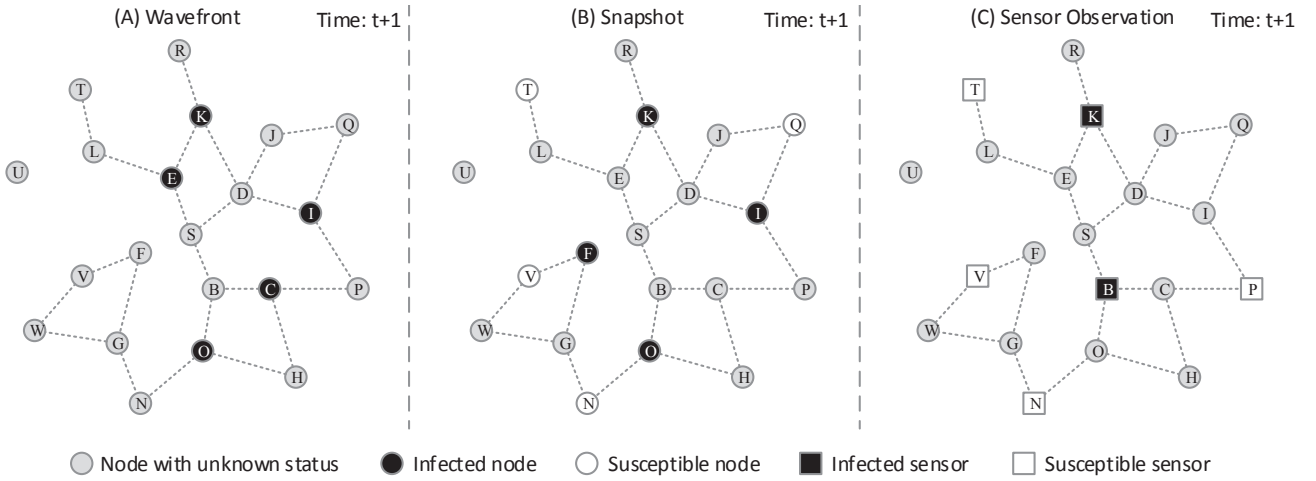


Fig. 3. Three types of observations in regards to the rumor spreading in Fig. 1. (A) Wavefront; (B) Snapshot; (C) Sensor.

social networks are defined by an ordered stream of interactions between individuals. In other words, as time progresses, the interaction structure keeps changing. Examples can be found in both face-to-face interaction networks [13], and online social networks [3]. The temporal nature of such networks has a deep influence on information spreading on top of them. Indeed, the spreading of rumors is affected by duration, sequence, and concurrency of contacts among people.

In this work, we reduce time-varying networks to a series of static networks by introducing a time-integrating window. Each integrating window aggregates all edges and nodes present in the corresponding time duration. In Fig. 1, we show an example to illustrate the time-integrating windows. In the time window $t-1$ (or, at time $t-1$), a rumor started to spread from node S who had interaction with 5 neighbors in this time window. In the next time window t, nodes B, D and F were successfully infected. In this time window, we notice that node O moved next to B (*i.e.*, *physical mobility*), and node G had no interaction with its neighbors (*i.e.*, *offline*). Other examples of physical mobility or online/offline status of nodes can be found in the time window $t+1$.

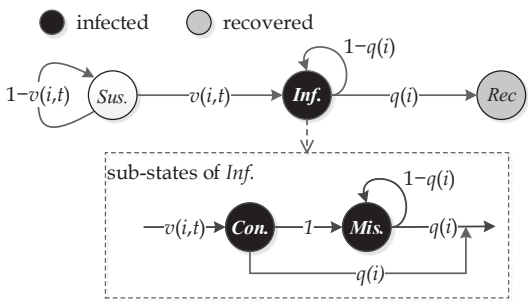


Fig. 2. State transition of a node in rumor spreading model.

2.2 Security States of Individuals

For the convenience of description, we borrow the notions from epidemiology to describe the spreading of rumors in time-varying social networks [14]. We say a user is infected when he/she accepts the rumors, and an infected user is recovered if he/she abandons the rumors. In this paper, we adopt the classic susceptible-infected-recovered (SIR) scheme to present the infection dynamics of each user. Fig. 2 shows the state transition graph of an arbitrary user in this model. Every user is initially susceptible (*Sus.*). They can be infected (*Inf.*) by their neighbors with probability $v(i,t)$, and then recover (*Rec.*) with probability $q(i)$. Rumors will be spread out from infected users to their social neighbors until they get recovered. There are also many other models of rumor propagation, including the SI, SIS, SIRS models [15]–[17]. In present work, we adopt the SIR model because it can reflect the state transition of users when they hear a rumor, from being susceptible to being recovered. Generally, people will not believe the rumor again after they know the truth. Therefore, recovered users will not transit their states any more. For other propagation models, readers can refer to Section 6 for further discussion.

To more precisely describe node states in different types of observations, we introduce two sub-states of nodes being infected: 'contagious' (*Con.*) and 'misled' (*Mis.*), see Fig. 2. An infected node first becomes contagious and then transit to being misled. The *Con.* state describes the state of nodes newly infected. More specifically, a node is *Con.* at time t means this node is susceptible at time $t-1$ but becomes infected at time t. An misled node will stay being infected until it recovers. For instance, sensors can record the time at which they get infected, and the infection time is crucial in detecting rumor sources because it reflects the infection trend and speed of a rumor. Hence, the introduction of contagious and misled states is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2016.2522436, IEEE Transactions on Dependable and Secure Computing

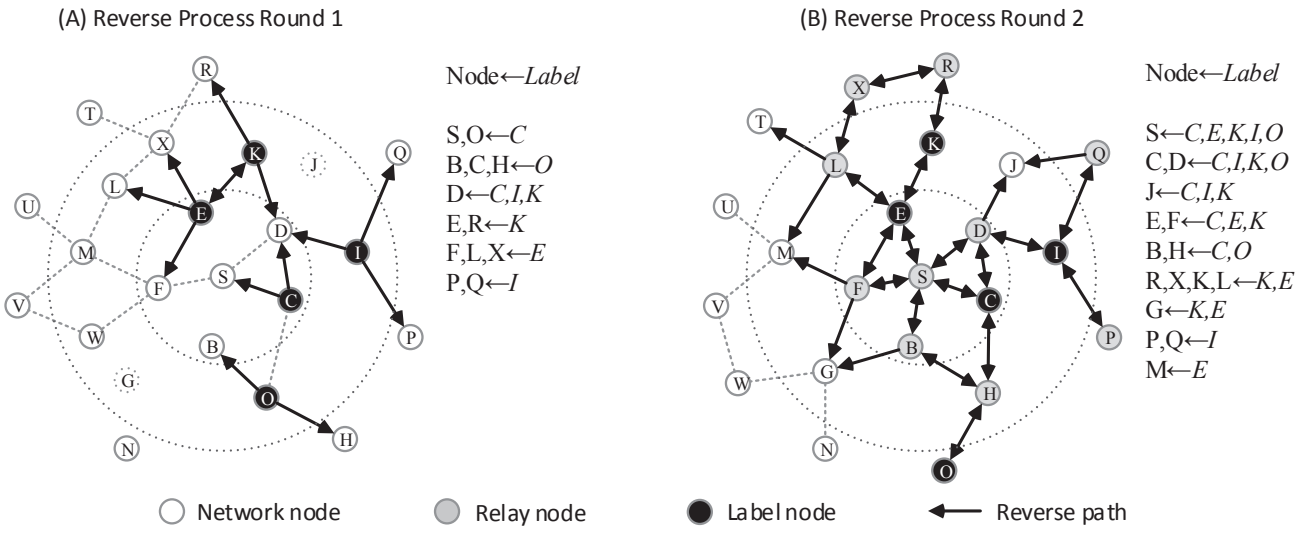


Fig. 4. Illustration of the reverse dissemination process in regards to the wavefront observation in Fig. 3 (A). (A) The observed nodes broadcast labeled copies of rumors to their neighbors in time window t; (B) The neighbors who received labeled copies will relay them to their own neighbors in time window $t-1$.

intrinsic to the rumor spreading framework.

2.3 Observations for Source Identification

Prior knowledge for source identification is provided by various types of partial observations upon time-varying social networks. According to previous work on static networks, we collect three categories of partial observations: wavefronts, snapshots, and sensor observations. We denote the set of observed nodes as $O = \{o_1, o_2, ..., o_n\}$. Following the rumor spreading in Fig. 1, we will explain each type of the partial observations as follows:

Wavefront [11]: Given a rumor spreading incident, a wavefront provides partial knowledge of the time-varying social network status. Only the users who are in the wavefront of the spreading can be observed (*i.e.*, all the contagious nodes in the latest time window are observed), leaving the states of the other users unknown. Fig. 3(A) shows an example of the wavefront in the rumor spreading in Fig. 1. We see that nodes C, E, I, K and O are in the wavefront as they transit to being contagious at time $t+1$.

Snapshot [7]: Given a rumor spreading incident, a snapshot also provides partial knowledge of the time-varying social network status. In this case, only a group of users can be observed in the latest time window when the snapshot is taken. The states of the observed users can be susceptible, infected or recovered. We use O_S, O_I and O_R to denote the observed users who are susceptible, infected or recovered, respectively. This type of observations is the most common one in our daily life. Fig. 3(B) shows an example of the snapshot in the rumor spreading in Fig. 1 . We see that $O_S = \{N, Q, T, V\}$, $O_I = \{F, I, K, O\}$ and $O_R = \emptyset$.

Sensor Observation [10]: Sensors are a group of preselected users in time-varying social networks. The sensors can record the rumor spreading dynamics over them, including the security states and the time window when they get infected (more specifically, become contagious). We introduce O_S and O_I to denote the set of susceptible and infected sensors, respectively. For each $o_i \in O_I$, the infection time is denoted by t_i. This type of observation is usually obtained from sensor networks. Fig. 3(C) shows an example of the sensor observations in the rumor spreading in Fig. 1. In this case, $O_S = \{N, P, T, V\}$, $O_I = \{K, B\}$, and the infection time of node K is $t+1$, and node B is infected at time t.

We can see that these three types of partial observations provide three different categories of partial knowledge of the time-varying social network status. Different types of observations are suitable for different circumstances in real-world applications. Readers could refer to [9]–[11] for further discussion on different types of partial observations. The partial knowledge together with the physical mobility and online/offline status of users make the tracing back of rumor sources much more difficult.

3 Narrowing Down the Suspects

Current methods of source identification need to screen every node in the underlying network. This is a bottlenecks of identifying rumor sources: scalability. It is necessary to narrow down the set of suspects, especially in large-scale networks. In this section, we adopt a reverse dissemination strategy to identify a small set of suspects. The details of the method are presented in Section 3.1, and its efficiency will be evaluated in Section 3.2.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2016.2522436, IEEE Transactions on Dependable and Secure Computing

3.1 Reverse dissemination Method

In this subsection, we first present the rationale of the reverse dissemination method. Then, we show how to apply the reverse dissemination method into different types of observations.

3.1.1 Rationale

The rationale of the reverse dissemination method is to send copies of rumors along the reversed dynamic connections from observed nodes to exhaust all possible spreading paths leading to the observation. The node from which all the paths, covering all the observed nodes' states, originated is more likely to be a suspect. The reverse dissemination method is inspired from the Jordan method [9]. The reverse dissemination method is different from the Jordan method, because our method is based on time-varying social networks (involving the physical mobility and online/offline status of users) rather than static networks. In Fig. 4, we show a simple example to illustrate the reverse dissemination process. This example follows the rumor spreading in Fig. 1 and the wavefront observation in Fig. 3(A). All wavefront nodes $O_I = \{E, C, I, K, O\}$ observed in time window $t+1$ are labeled as black in Fig. 4 (A). The whole process is composed of two rounds of reverse dissemination. In round 1 (Fig. 4 (A)), all observed nodes broadcast labeled copies reversely to their neighbors in time window t. For example, nodes S and O received copies of node C ($S, O \leftarrow C$), and node D received copies of three observed nodes C, I and K ($D \leftarrow C, I, K$). In round 2 (Fig. 4 (B)), the neighbors who have received labeled copies will relay them to other neighbors in time window $t-1$. In each round, the labels will be recorded in each relay node. We can see from Fig. 4(B) that node S has received all copies from all the observed nodes ($S \leftarrow C, E, K, I, O$). Then, node S is chosen to be a suspect.

We notice that the starting time for each observed node starting their reverse dissemination processes varies in different types of observations. For a wavefront, since all the observed nodes are supposed to be contagious in the latest time window, all the observed nodes need to simultaneously start their reverse dissemination processes. For a snapshot, the observed nodes stay in their states in the latest time window. Therefore, the reverse dissemination processes will also simultaneously starts from all the observed nodes. However, for a sensor observation, because the infected sensors record their infection time, the starting time of reverse dissemination for each sensor will be determined by t_i. More specifically, the latest infected sensors first start their reverse dissemination processes, and then the sensors infected in the previous time window, until the very first infected sensors.

Algorithm 1: Reverse dissemination

Input: A set of observed nodes $O = \{o_1, o_2, ..., o_n\}$, a set of infection times of the observed nodes $\{t_1, t_2, ..., t_n\}$, a threshold α, and a threshold t_{max}.
Initialize: A set of suspects $U = \emptyset$, and $t_1 = ... = t_n = T$ if O is a snapshot/wavefront, otherwise $T = \max\{t_1, t_2, ..., t_n\}$.
for *(t starts from 1 to a given maximum value t_{max})* **do**
  for *(o_i: i starts from 1 to n)* **do**
    if *(o_i has not started to disseminate the rumor)* **then**
      Start to propagate the rumor from user o_i separately and independently at time $t + T - t_i$.
    end
  end
  for *(u: any node in the whole network)* **do**
    if *(user u received n separate rumors from O)* **then**
      Compute the maximum likelihood $L(u, t)$ for user u;
      Add user u into the set U.
    end
  end
  if *($|U| \geq \alpha N$)* **then**
    Keep the first αN suspects with large maximum likelihoods in U, and delete all the other suspects.
    Stop.
  end
end
Output: A set of suspects U.

3.1.2 Wavefront

Given a reverse dissemination process starting from an observed node o_i, we use $P_C(u, t|o_i)$ to denote the probability of an arbitrary node u to be contagious after time t, where t denotes the time span of the whole reverse dissemination process. Let all observed nodes o_i start their reverse dissemination processes in the latest time window. To match the wavefront, it is expected a suspect u can simultaneously receive rumor copies from all $o_i \in O$ (*i.e.*, the rumor copies sent from all observed nodes can make node u become contagious simultaneously). Mathematically, we identify those nodes who can provide the maximum likelihood, $L(u, t)$, of being a suspect receiving copies from all the observed nodes, as in

$$L(u, t) = \sum_{o_i \in O} \ln(P_C(u, t|o_i)). \quad (1)$$

For the convenience of computation, we adopt logarithmic function $\ln(\cdot)$ in Eq. (1) to derive the maximum likelihood. We use U to denote the set of suspects. The ones who provide larger values of $L(u, t)$ are recognized as a member of set U.

3.1.3 Snapshot

To match the snapshot observation (which includes susceptible, infected or recovered nodes), it is expected that a suspect u needs to satisfy the following three principles at time t. First, copies of rumors disseminated from observed *susceptible* nodes $o_i \in O_S$ cannot reach node u at time t (*i.e.*, u is still susceptible). Second, copies of rumors disseminated from observed *infected* nodes $o_j \in O_I$ can reach node u at time t (*i.e.*, u becomes infected). Third, copies of rumors disseminated from observed *recovered* nodes

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2016.2522436, IEEE Transactions on Dependable and Secure Computing

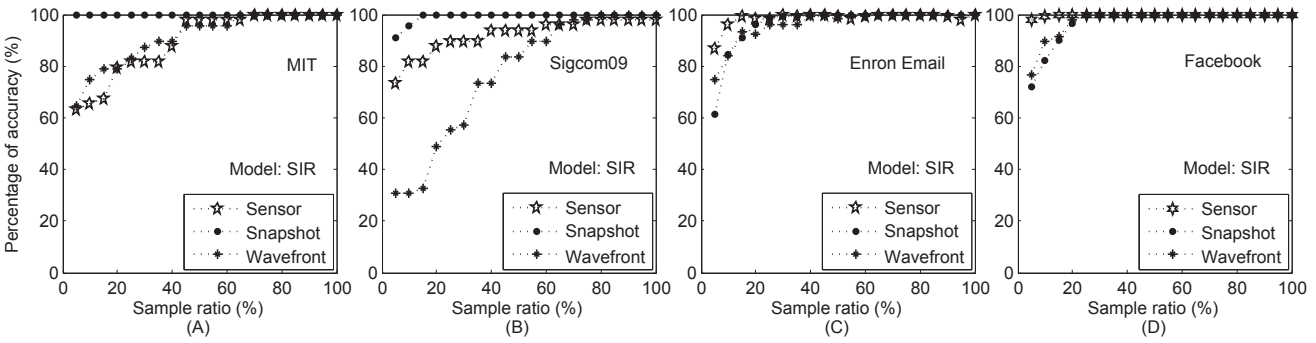


Fig. 5. Accuracy of the reverse dissemination method in networks. (A) MIT; (B) Sigcom09; (C) Enron Email; (D) Facebook.

$o_k \in O_R$ can arrive at node u before time t (*i.e.*, u becomes recovered). Again, we employ maximum likelihood to capture this kind of nodes, as in

$$L(u,t) = \sum_{o_i \in O_S} \ln(P_S(u,t|o_i)) + \sum_{o_j \in O_I} \ln(P_I(u,t|o_j)) + \sum_{o_k \in O_R} \ln(P_R(u,t|o_k)), \tag{2}$$

where $P_S(u,t|o_i)$, $P_I(u,t|o_i)$ and $P_R(u,t|o_i)$ denote the probabilities of u to be susceptible, infected or recovered after time t, respectively, given that the reverse dissemination started from o_i.

3.1.4 Sensor

For sensor observations, according to our previous discussion, we let infected sensor $o_i \in O_I$ start to reversely disseminate copies of the rumor at time $\hat{t}_i = T - t_i$, where $T = \max\{t_i | o_i \in O_I\}$. We also let the susceptible sensors $o_j \in O_S$ start to reversely disseminate copies of rumors at time t=0. To match a sensor observation, it is expected a suspect u needs to satisfy the following two principles at time t. First, copies of rumors disseminated from *susceptible* sensors $o_i \in O_S$ cannot reach node u at time t (*i.e.*, node u is still susceptible). Second, copies of rumors disseminated from all *infected* sensors $o_j \in O_I$ can be received by node u at time t (*i.e.*, node u becomes contagious). Mathematically, we determine the suspects by computing their maximum likelihood, as in

$$L(u,t) = \sum_{o_i \in O_I} \ln(P_C(u, t+\hat{t}_i|o_i)) + \sum_{o_j \in O_S} \ln(P_S(u,t|o_j)). \tag{3}$$

The values of $P_S(u,t|o_i)$, $P_C(u,t|o_i)$, $P_I(u,t|o_i)$ and $P_R(u,t|o_i)$ will be calculated by the model introduced in Section 4.2. We summarize the reverse dissemination method in Algorithm 1.

3.2 Performance Evaluation

We evaluate the performance of the reverse dissemination method in real time-varying social networks. Similar to Lokhov et. al's work [18], we consider the infection probabilities and recovery probabilities to be uniformly distributed in (0,1), and the average infection and recovery probabilities are set to be 0.6 and 0.3. We also use α to denote the ratio of suspects over all nodes, $\alpha = |U|/N$, where N is the number of all nodes in a time-varying social network. The value of α ranges from 5% to 100%. We randomly choose the real source in 100 runs of each experiment. The number of 100 comes from the wrok in [14].

We consider four real time-varying social networks in Table 1: The MIT reality [19] dataset captures communication from 97 subjects at MIT over the course of the 2004-2005 academic year. The Sigcom09 [20] dataset contains the traces of Bluetooth device proximity of 76 persons during SIGCOMM 2009 conference in Barcelona, Spain. The Enron Email [21] dataset contains record of email conversations from 143 users in 2001. The Facebook [22] dataset contains communications from 45,813 users during December 29th, 2008 and January 3rd, 2009. All of these datasets reflect the physical mobility and online/offline features of time-varying social networks. According to the study in [2], an appropriate temporal resolution Δt is important to correctly characterize the dynamical processes on time-varying networks. Therefore, we need to be cautious when we choose the time interval of size Δt. Furthermore, many social networks have been shown small-world, *i.e.*, the average distance l between any two nodes is small, generally $l \leq 6$. Previous extensive works show that rumors can spread quickly in social networks, generally after 6-10 time ticks of propagation (see [5]). Hence, we divided the social networks into 6-10 time windows. Therefore, for the datasets used in this paper, we uniformly divide each into 6-10 discrete time windows [2]. For other division of temporal resolution, readers could refer to [2] for further discussion.

Fig. 5 shows the experiment results in the four real datasets. We find the proposed method works quite well in reducing the number of suspects. Especially for snapshots, the searching scale can be narrowed to 5% of all users for the MIT dataset, 15% for the Sigcom09 dataset, and 20% for the Enron Email and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2016.2522436, IEEE Transactions on Dependable and Secure Computing

Facebook datasets. The number of suspects can be reduced to 45% of all users in the MIT reality dataset under snapshot and wavefront observations. For the Enron Email and Facebook datasets, the number of suspects can be reduced to 20% of all users. The worst case occurred in the Sigcom09 dataset with wavefronts, but our method still achieved a reduction of 35% in the total number of users.

The experiment results on real time-varying social networks show that the proposed method is efficient in narrowing down the suspects. Real-world social networks usually have a large number of users. Our proposed method addresses the scalability in source identification, and therefore is of great significance.

4 Determining the Real Source

Another bottleneck of identifying rumor sources is to design a good measure to specify the real source. Most of the existing methods are based on node centralities, which ignore the propagation probabilities between nodes. Some other methods consider the BFS trees instead of the original networks. These violate the rumor spreading processes. In this section, we adopt an innovative method to identify the real source from the suspects. A novel rumor spreading model will also be introduced to model rumor spreading in time-varying social networks.

4.1 ML-based Method

4.1.1 Rationale

The key idea of the ML-based method is to expose the suspect from set U that provides the largest maximum likelihood to match the observation. It is expected that the real source will produce a rumor propagation which not only temporally but also spatially matches the observation more than other suspects. Given an observation $O = \{o_1, o_2, ..., o_n\}$ in a time-varying network, we let the spread of rumors start from an arbitrary suspect $u \in U$ from the time window that is t_u before the latest time window. For an arbitrary observed node o_i, we use $P_S(o_i, t_u|u)$ to denote the probability of o_i being susceptible at time t_u, given that the spread of rumors starts from suspect u. Similarly, we have $P_C(o_i, t_u|u)$, $P_I(o_i, t_u|u)$ and $P_R(o_i, t_u|u)$ representing the probabilities of o_i being contagious, infected and recovered at time t_u, respectively. We use $\tilde{L}(t_u, u)$ to denote the maximum likelihood of obtaining the observation when the rumor started from suspect u. Among all the suspects in U, we can estimate the real source by choosing the maximum value of the ML, as in

$$(u^*, t^*) = \arg\max_{u \in U} \tilde{L}(t_u, u). \quad (4)$$

The result of Eq. (4) suggests that suspect u^* can provide a rumor propagation not only temporally but also spatially matches the observation better than other suspects. We also have an estimation of infection scale $I(t^*, u^*)$ as a byproduct, as in

$$I(t^*, u^*) = \sum_{i=1}^{N} P_I(i, t^*|u^*). \quad (5)$$

Later, we can justify the effectiveness of the ML-based method by examining the accuracy of t^* and $I(t^*, u^*)$.

Algorithm 2: Targeting the suspect

Input: A set of suspects U, a set of observed nodes O, and a threshold t_{max}.
Initialize: $L_{max} = 0$, $u^* = \emptyset$, $t^* = 0$.
for *($\tilde{u}$: any node in set U)* **do**
  for *(t starts from 1 to a given maximum value t_{max})* **do**
    Disseminate the rumor from suspect $\tilde{u}$.
    if *(We can obtain the observation O)* **then**
      Compute the maximum likelihood value $\tilde{L}(t, \tilde{u})$.
      if *($\tilde{L}(t, \tilde{u}) > L_{max}$)* **then**
        $L_{max} = \tilde{L}(t, \tilde{u})$;
        $u^* = \tilde{u}$;
        $t^* = t$.
      end
      if *($\tilde{L}(t, \tilde{u}) < \tilde{L}(t-1, \tilde{u})$)* **then**
        Stop.
      end
    end
  end
end
Output: The rumor source u^* and propagation time t^*.

4.1.2 Wavefront

In a wavefront, all observed nodes are contagious in the time window when the wavefront is captured. Supposing suspect u is the rumor source, the maximum likelihood $\tilde{L}(t_u, u)$ of obtaining the wavefront O is the product of the probabilities of any observed node $o_i \in O$ being contagious after time t_u. We also adopt a logarithmic function to present the computation of the maximum likelihood. Then, we have $\tilde{L}(t_u, u)$ for a wavefront, as in

$$\tilde{L}(t_u, u) = \sum_{o_i \in O} \ln(P_C(o_i, t_u|u)). \quad (6)$$

4.1.3 Snapshot

In a snapshot, the observed nodes can be susceptible, infected or recovered in the time window when the snapshot is taken. Supposing suspect u is the rumor source, the maximum likelihood of obtaining the snapshot is the product of the probabilities of any observed node $o_i \in O$ being in its observed state.

TABLE 1
Comparison of Data Collected in the Experiments.

Dataset	MIT	Sigcom09	Email	Facebook
Device	Phone	Phone	Laptop	Laptop
Network type	Bluetooth	Bluetooth	WiFi	WiFi
Duration (days)	246	5	14	6
# of devices	97	76	143	45,813
# of contacts	54,667	69,189	1,246	264,004

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2016.2522436, IEEE Transactions on Dependable and Secure Computing

Then, we have the logarithmic form of the calculation for $\tilde{L}(t_u, u)$ in a snapshot, as in

$$\tilde{L}(t_u, u) = \sum_{o_i \in O_S} \ln(P_S(o_i, t_u|u)) + \sum_{o_j \in O_I} \ln(P_I(o_j, t_u|u)) + \sum_{o_k \in O_R} \ln(P_R(o_k, t_u|u)). \quad (7)$$

4.1.4 Sensor

In a sensor observation, each infected sensor $o_i \in O_I$ records its infection time t_i. Although the absolute time t_i cannot directly suggest the spreading time of the rumor, we can derive the relative infection time of each sensor. Supposing suspect u is the rumor source, for an arbitrary infected sensor o_i, its relative infection time is $\tilde{t}_i = t_i - \tilde{t} + t_u$ where $\tilde{t} = \min\{t_i | o_i \in O_I\}$, and t_u is obtained from Algorithm 1. For suspect $u \in U$, the maximum likelihood $\tilde{L}(t_u, u)$ of obtaining the observation is the product of the probability of any sensor o_i to be in its observed state at time $\tilde{t}_i$. Then, we have the logarithmic form of the calculation for $\tilde{L}(t_u, u)$ in a sensor observation, as in

$$\tilde{L}(t_u, u) = \sum_{o_i \in O_I} \ln(P_C(u, \tilde{t}_i|o_i)) + \sum_{o_j \in O_S} \ln(P_S(u, t_u|o_j)). \quad (8)$$

Note that, $P_S(u, t|o_i)$, $P_C(u, t|o_i)$, $P_I(u, t|o_i)$, and $P_R(\tilde{u}, t|o_i)$ can be calculated in the rumor spreading model in Section 4.2. We summarize the method of determining rumor sources in Algorithm 2.

4.2 Propagation Model

In this subsection, we introduce an analytical model to present the spreading dynamics of rumors in time-varying social networks. The state transition of each node follows the SIR scheme introduced in Section 2.2. For rumor spreading processes among users, we use this model to calculate the probabilities of each user in various states.

In the modeling, every user is initially susceptible. We use $\eta_{ji}(t)$ to denote the spreading probability from user j to user i in time window t. Then, we can calculate the probability of a susceptible user being infected by his/her infected neighbors as in

$$v(i, t) = 1 - \prod_{j \in N_i} [1 - \eta_{ji}(t) \cdot P_I(j, t-1)], \quad (9)$$

where, N_i denotes the set of neighbors of user i. Then, we can compute the probability of an arbitrary user to be susceptible at time t as in

$$P_S(i, t) = [1 - v(i, t)] \cdot P_S(i, t-1). \quad (10)$$

Once a user gets infected, he/she becomes contagious. We then have the probability that an arbitrary user is contagious at time t as in

$$P_C(i, t) = v(i, t) \cdot P_S(i, t-1). \quad (11)$$

Since an infected user can be either contagious or misled, we can obtain the value of $P_I(i, t)$ as in

$$P_I(i, t) = P_C(i, t) + (1 - q_i(t)) \cdot P_I(i, t-1). \quad (12)$$

Then, the value of the $P_R(i, t)$ can be derived from

$$P_R(i, t) = P_R(i, t-1) + q_i(t) \cdot P_I(i, t-1). \quad (13)$$

This model analytically derives the probabilities of each user in various states in an arbitrary time t. This in addition constitutes the maximum likelihood $L(u, t)$ of an arbitrary user u being a suspect in time window t in Section 3.1. This also supports the calculation of the maximum likelihood $\tilde{L}(t, u)$ to match the observation in time window t, given that the rumor source is the suspicious user u in Section 4.1.

5 Evaluation

In this section, we evaluate the efficiency of our source identification method. The experiment settings are the same as those presented in Section 3.2. Specifically, we let the sampling ratio α range from 10% to 30%, as the reverse dissemination method has already achieved a good performance with α dropping in this range.

5.1 Accuracy of Rumor Source Identification

We evaluate the accuracy of our method in this subsection. We use δ to denote the error distance between a real source and an estimated source. Ideally, we have $\delta = 0$ if our method accurately captures the real source. In practice, we expect that our method can accurately capture the real source or a user very close to the real source (i.e., δ is very small). As the user close to the real source usually has similar characteristics with the real source, quarantining or clarifying rumors at this user is also very significant to diminish the rumors [6].

Our method shows good performances in the four real time-varying social networks. Fig. 6 shows the frequency of the error distances (δ) in the MIT reality dataset under different categories of observations. When the sampling ratio $\alpha \geq 20\%$, our method can identify the real sources with an accuracy of 78% for the sensor observations, more than 60% for the snapshots, and around 36% for the wavefronts. For the wavefronts, although our method cannot identify real sources with very high accuracy, the estimated sources are very close to the real sources, and are generally 0-2 hops away. Fig. 7 shows the frequency of the error distances δ in the Sigcom09 dataset. When the sampling ratio $\alpha \geq 20\%$, the proposed method can identify the real sources with an accuracy of more than 70% for the snapshots. For the other two categories of observations, although our method cannot identify real sources with very high accuracy, the estimated sources are very close to the real sources, with an average of 1-2 hops away in the sensor observations, and 1-3 hops away for the wavefronts. Fig. 8

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2016.2522436, IEEE Transactions on Dependable and Secure Computing

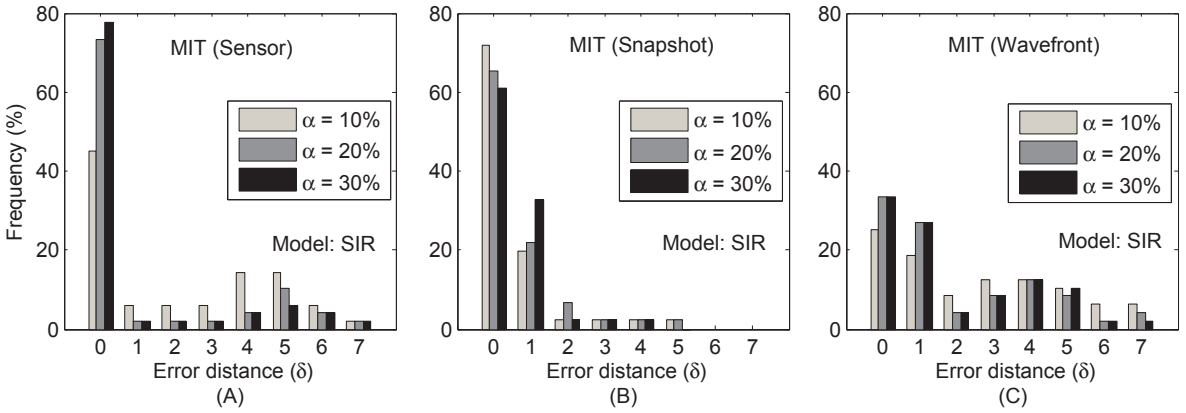


Fig. 6. The distribution of error distance (δ) in the MIT Reality dataset. (A) Sensor; (B) Snapshot; (C) Wavefront.

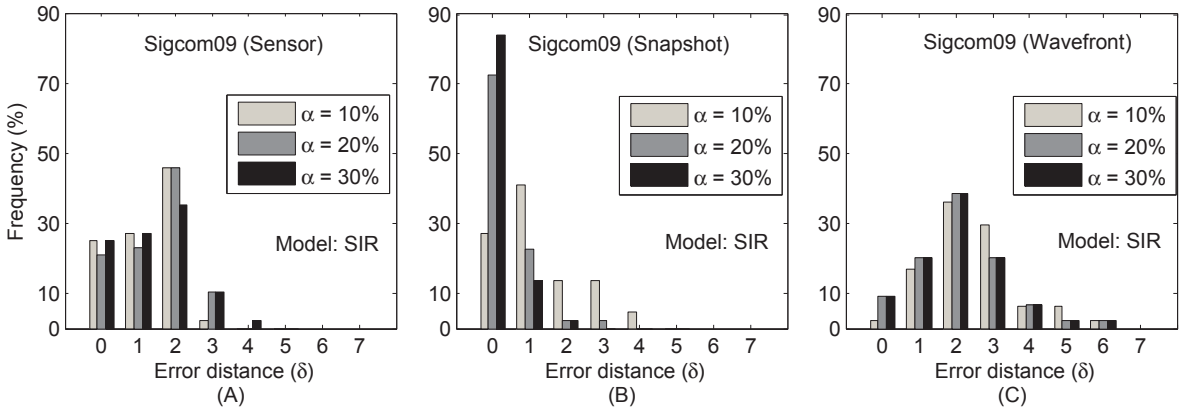


Fig. 7. The distribution of error distance (δ) in the Sigcom09 dataset. (A) Sensor; (B) Snapshot; (C) Wavefront.

shows the performance of our method in the Enron Email dataset. When the sampling ratio $\alpha \geq 20\%$, our method can identify the real sources with an accuracy of 80% for the snapshots, and more than 45% for the wavefronts. The estimated sources are very close to the real sources, with an average 1-3 hops away in the sensor observations. Fig. 9 shows the performance of our method in the Facebook dataset. Similarly, when the sampling ratio $\alpha \geq 20\%$, the proposed method can identify the real sources with an accuracy of around 40% for the snapshots. The estimated sources are very close to the real sources, with an average of 1-3 hops away from the real sources under the sensor and wavefront observations.

Compared with previous work, our proposed method is superior because our method can work in time-varying social networks rather than static networks. Our method can achieve around 80% of all experiment runs that accurately identify the real source or an individual very close to the real source. However, the previous work of [8] and [23] has theoretically proven their accuracy was at most 25% or 50% in tree-like networks, and their average error distance is 3-4 hops away.

5.2 Effectiveness Justification

We justify the effectiveness of our ML-based method from three aspects: the correlation between the ML of the real sources and that of the estimated sources, the accuracy of estimating rumor spreading time, and the accuracy of estimating rumor infection scale.

5.2.1 Correlation between real sources and estimated sources

We investigate the correlation between the real sources and the estimated sources by examining the correlation between their maximum likelihood values. For different types of observation, the maximum likelihood of an estimated source can be obtained from Eq. (6), Eq. (7) or Eq. (8), *i.e.*, $\tilde{L}(t^*, u^*)$. The maximum likelihood of a real source is obtained by replacing u^* and t^* as the real source and the real rumor spreading time, respectively. If the estimated source is in fact the real source, their maximum likelihood values should present high correlation.

The correlation results of the maximum likelihood values when $\alpha = 20\%$ in the four time-varying social networks are shown from Fig. 10 to Fig. 13. We see that the maximum likelihood values of the real sources and that of the estimated sources are highly correlated with each other. Their maximum likelihood

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2016.2522436, IEEE Transactions on Dependable and Secure Computing

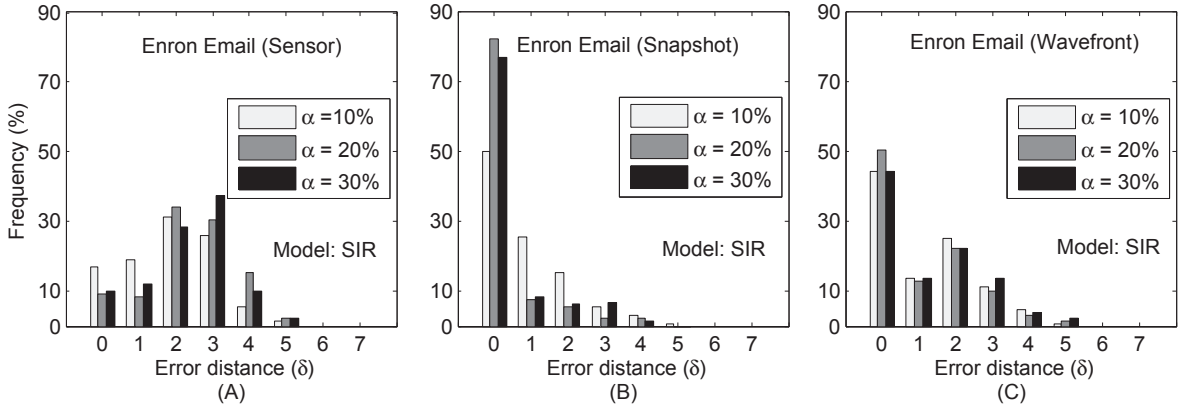


Fig. 8. The distribution of error distance (δ) in the Enron Email dataset. (A) Sensor; (B) Snapshot; (C) Wavefront.

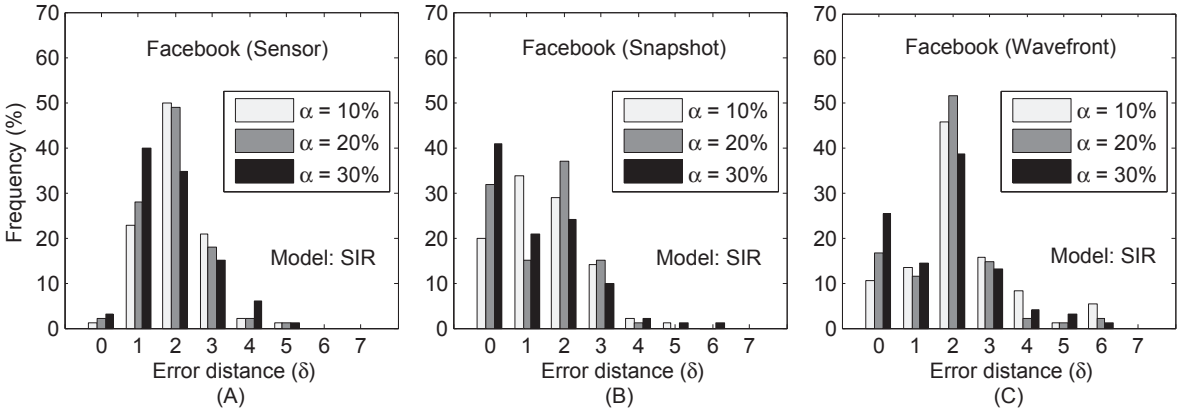


Fig. 9. The distribution of error distance (δ) in the Facebook dataset. (A) Sensor; (B) Snapshot; (C) Wavefront.

values approximately form linear relationships to each other. Fig. 10 shows the results in the MIT reality dataset. We can see that the maximum likelihood values of the real sources and that of the estimated sources are highly correlated in both sensor and snapshot observations. The worst results occurred in wavefront observations, however the majority of the correlation results still tend to be clustered in a line. These exactly reflect the accuracy of identifying rumor sources in Fig. 6. The results in the Sigcom09 dataset are shown in Fig. 11. We see that the maximum likelihood values are highly correlated in both snapshot and wavefront observations. The worst results occurred in sensor observations, however the majority of the correlation results still tend to be clustered in a line. These exactly reflect the accuracy of identifying rumor sources in Fig. 7. The results in the Enron Email dataset are shown in Fig. 12. We see that the maximum likelihood values are highly correlated in both snapshot and wavefront observations, and slightly correlated in sensor observations. These exactly reflect the accuracy of identifying rumor sources in Fig. 8. The results in the Facebook data are presented in Fig. 13. Similar results can be found in the Facebook dataset in Fig. 13, which precisely reflects the accuracy of identifying rumor sources in Fig. 9.

The strong correlation between the ML values of the real sources and that of the estimated sources in time-varying social networks reflects the effectiveness of our ML-based method.

5.2.2 *Estimation of spreading time*

As a byproduct, our ML-based method can also estimate the spreading time (in Eq. (4)) of rumors. In order to justify the effectiveness of our proposed method, we further investigate the effectiveness of this byproduct. We expect the estimate can accurately expose the real spreading time of rumors. We let the real spreading time vary from 2 to 6 in four real time-varying social networks. The experiment results are shown in Table 2.

As shown in Table 2, we analyze the means and the standard deviations of the estimated spreading time. We see that the means of the estimated spreading time are very close to the real spreading time, and most results of the standard deviations are smaller than 1. Especially when the spreading time $T = 2$, our ML-based method in sensor observations and wavefront observations can accurately estimate the spreading time in the MIT reality, Sigcom09 and Enron Email datasets. The results are also quite accurate in the Facebook dataset. From Table 2, we can see that

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2016.2522436, IEEE Transactions on Dependable and Secure Computing

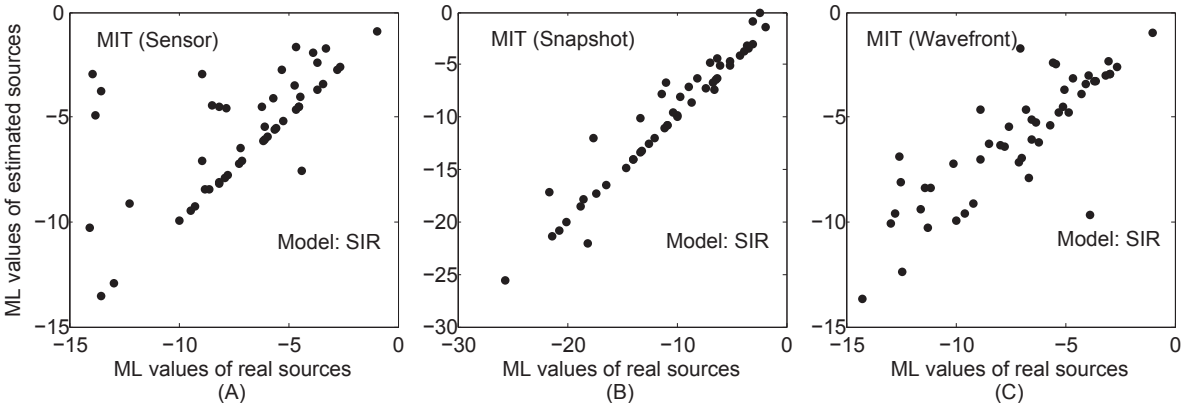


Fig. 10. The correlation between the maximum likelihood of the real sources and that of the estimated sources in the MIT reality dataset. (A) Sensor observation; (B) Snapshot observation; (C) Wavefront observation.

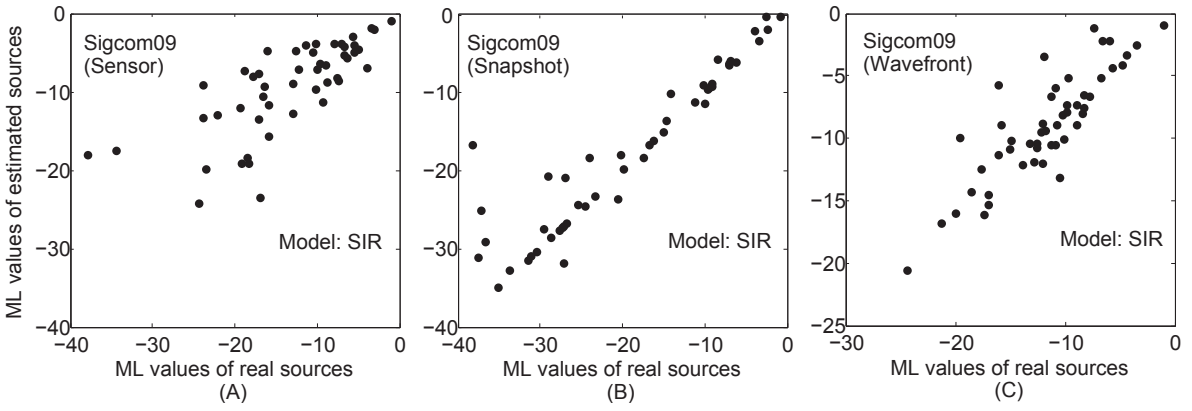


Fig. 11. The correlation between the maximum likelihood of the real sources and that of the estimated sources in the Sigcom09 dataset. (A) Sensor observation; (B) Snapshot observation; (C) Wavefront observation.

our method can estimate the spreading time with extremely high accuracy in wavefront observations, and relatively high accuracy in snapshot observations.

Both the means and standard deviations indicate that our method can estimate the real spreading time with high accuracy. The accurate estimate of the spreading time indicates that our method is effective in source identification from a different aspect.

5.2.3 Estimation of infection scale

We further justify the effectiveness of our ML-based method by investigating its accuracy in estimating the infection scale of rumors provided by the second byproduct in Eq. (5). We expect that the ML-based method can accurately estimate the infection scale of each propagation incident. Particularly, we let the rumor spreading initiate from the node with largest degree in each full time-varying social network and spread for 6 time windows in experiments.

In Fig. 14, we show the real infection scales at each time tick, and also the estimated infection scales in different types of observations. We can see that the proposed method can provide a fairly accurate estimate of on the infection scales of rumors in the MIT reality dataset, the Sigcom09 dataset and the Facebook dataset in different types of observations. As shown in Fig. 14(C), the worst result occurred in the Enron Email dataset after time tick 4. According to our investigation, this was caused by a great deal of infected nodes that tend to be in the recovered stage in the SIR scheme, which leads to a fairly large uncertainty in the estimate.

To summarize, all of the above evaluations reflect the effectiveness of our method from different aspects: the high correlation between the ML values of the real sources and that of the estimated sources, the high accuracy in estimating spreading time of rumors, and the high accuracy of the infection scale.

6 Further Discussion

In this paper, we adopt a microscopic SIR model to simulate the rumor dynamics over each user (see Fig. 2 for the state transition graph of an arbitrary user). There are also many other models of rumor propagation, such as the models in [15]–[17]. These models can be basically divided into two categories: the macroscopic models and the microscopic models. The macroscopic models, which are based on differential equations, only provide the overall infection trend of rumor propagation, such as the total number of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2016.2522436, IEEE Transactions on Dependable and Secure Computing

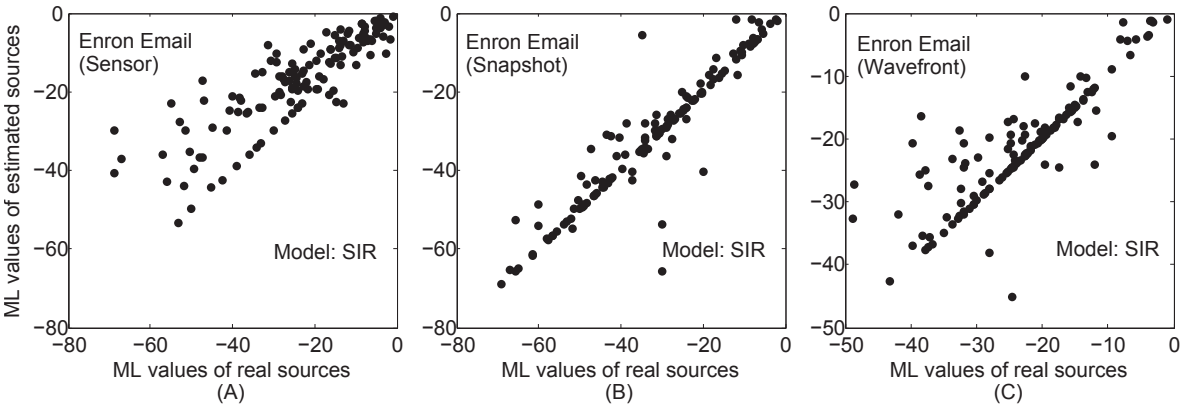


Fig. 12. The correlation between the maximum likelihood of the real sources and that of the estimated sources in the Enron Email dataset. (A) Sensor observation; (B) Snapshot observation; (C) Wavefront observation.

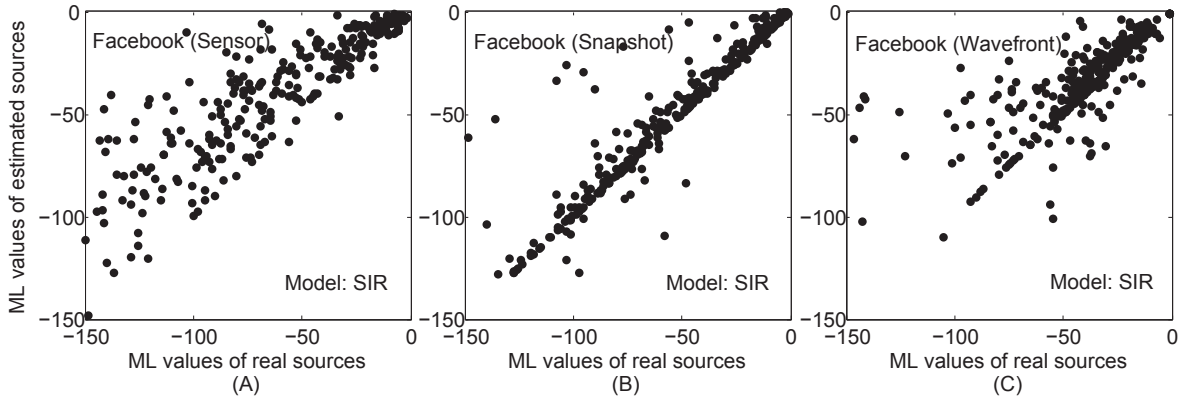


Fig. 13. The correlation between the maximum likelihood of the real sources and that of the estimated sources in the Facebook dataset. (A) Sensor observation; (B) Snapshot observation; (C) Wavefront observation.

infected nodes [14]. The microscopic models, which are based on difference equations, not only provide the overall infection status of rumor propagation, but they also can estimate the probability of an arbitrary node being in an arbitrary state [10]. In the field of identifying propagation sources, researchers generally choose microscopic models, because it requires to estimate which specific node is the first one getting infected. As far as we know, so far there is no work that is based on the macroscopic models to identify rumor sources in social networks. Future work may also investigate combining microscopic and macroscopic models, or even adopting the mesoscopic models [24], [25], to estimate both the rumour sources and the trend of the propagation. There are also many other microscopic models other than the SIR model adopted in this paper, such as the SI, SIS, and SIRS models [9], [10]. As we discussed in Section 2.2, people generally will not believe the rumor again after they know the truth, i.e., after they get recovered, they will not transit to other states. Thus, the SIR model can reflect the state transition of people when they hear a rumor. We also evaluate the performance of the proposed method on the SI model. Since the performance of our method on the SI model is similar to that on the SIR model, we only present the results on the SIR model in this paper.

Furthermore, there is another challenging and practical problem. In this paper, we considered rumor spreading in a single network. In the real world, rumors can spread across various social networking sites. For example, a rumor started to spread from Facebook. Later, people who saw the rumor on Facebook and post it on Twitter or some other public networking sites. Finally, the rumor spreads quickly among different social networking sites. Identifying rumour sources across different networking sites involves information propagation through various media, i.e., information diffusion among interconnected networks. These interconnected networks can be connected through users who have accounts in two or more networking sites, i.e., the overlaps among different networks. Therefore, we need to know the overlaps among interconnected network. This part of work is out of the scope of this paper. Future work may investigate identifying the sources of rumors spreading across various network platforms.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2016.2522436, IEEE Transactions on Dependable and Secure Computing

TABLE 2
Accuracy of estimating rumor spreading time.

Environment settings		Estimated spreading time			
Observation	Spreading time (T)	MIT	Sigcom09	Email	Facebook
Sensor	2	2±0	2±0	2±0	1.787±0.411
	4	4.145±0.545	3.936±0.384	4.152±0.503	3.690±0.486
	6	6.229±0.856	5.978±0.488	6.121±0.479	5.720±0.604
Snapshot	2	1.877±0.525	2.200±1.212	2.212±0.781	2.170±0.761
	4	3.918±0.862	3.920±0.723	3.893±0.733	4.050±0.716
	6	6.183±1.523	6.125±1.330	5.658±1.114	5.650±1.266
Wavefront	2	2±0	2±0	2±0	1.977±0.261
	4	4.117±0.686	4±0	3.984±0.590	4.072±0.652
	6	6±0	5.680±1.096	5.907±0.640	5.868±0.864

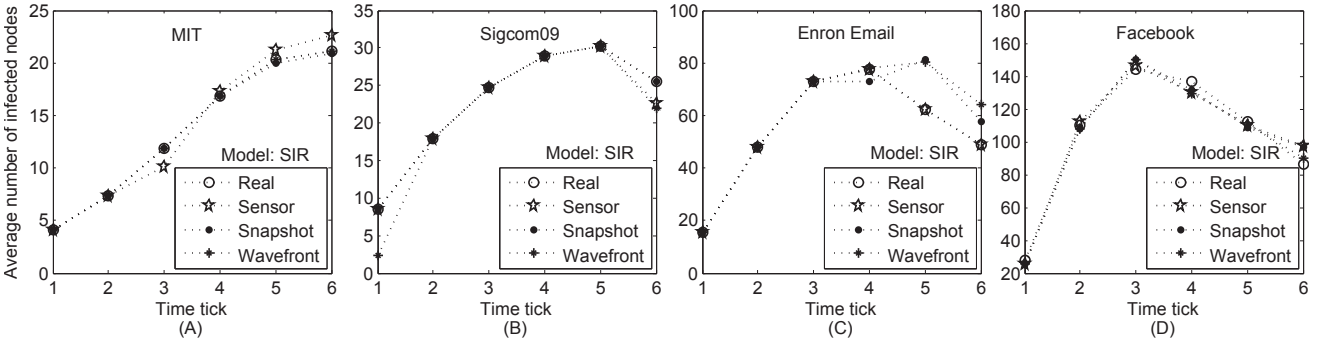


Fig. 14. The accuracy of estimating infection scale in real networks. (A) MIT; (B) Sigcom09; (C) Enron Email; (D) Facebook.

7 Related Work

In this section, we give a brief overview on the related work in this field. The majority of existing work focuses on source identification in tree networks.

The pioneer work of rumor source identification is based on complete observations on tree-like networks with the SI spreading model. Shah et al. [6] proposed the rumor center method to detect rumor sources in tree-like networks. They claimed that the user with maximum closeness centrality is the rumor source. Later, the rumor center method was extended by many other researchers, which can identify rumor sources with different propagation models and observations [17], [26]. Luo et al. [7] extended the rumor center method by considering multiple sources instead of a single source. Following the assumptions of the rumor center method, Dong et al. [27] further proposed a local rumor center method, which designates a set of nodes as suspicious sources. Therefore, it reduces the scale of the searching area. Wang et al. [8] extended the rumor center method to the circumstance of multiple observations. All of these methods use the breadth-first-search (BFS) technique to construct tree topologies upon networks. According to previous studies, only a few runs in the experiments can accurately capture the real sources [28].

Researchers also proposed many techniques on source identification in tree-like networks with partial observations. Zhu et al. [9] proposed the Jordan center method to identify rumor sources. They claimed that, started from the Jordan center, a rumor can construct the optimal sample path to the observed nodes. We can find similar work to the Jordan center method in [29]. Chen et al. [30] extended the Jordan center method to identify multiple sources in networks under the SIR model. Zang et al. [31] introduced a score based method extending the rumor center method to identifying the rumor source based on snapshots. Further, Pinto et al. [10] proposed a method based on sensor observations. They adopted the central limit theorem on the temporal differences on the infection times of sensors. Louni et al. [32] improved this method by taking community recognition techniques into account, which could reduce 3% sensors less than the method in [10]. In addition, some researchers identify rumor sources through detecting influential spreaders in a network [33]. Comin et al. [34] identified rumor sources by measuring various centralities of users in a network. They claimed that ones who captured the larger centrality values are more likely to be the rumor source.

Recently, researchers also proposed many methods for source identification in generic networks with partial observations. For sensor observations, Agaskar et al. [35] adopted the Monte Carlo algorithm and extended the method in [10] from trees to generic networks. For snapshot observations, Altarelli et al. [36] proposed using the Bayesian belief modeling to detect rumor source in generic networks. Further, Prakash et al. [37] proposed to identify rumors in generic network by minimizing the description length of the snapshot observation. In addition, Lokhov et

al. [38] adopted a dynamic message-passing (DMP) method to identify the rumor source in snapshots. For wavefront observations, Brockmann et al. [11] proposed a concept, effective distance, which can convert the propagation probability between nodes to the effective distance between them. They detect rumor sources as the node that has the same effective distance to all the nodes in the wavefront.

8 Conclusion and Future Work

In this paper, we explore the problem of rumor source identification in time-varying social networks that can be reduced to a series of static networks by introducing a time-integrating window. In order to address the challenges posted by time-varying social networks, we adopted two innovative methods. First, we utilized a novel reverse dissemination method which can sharply narrow down the scale of suspicious sources. This addresses the scalability issue in this research area and therefore dramatically promotes the efficiency of rumor source identification. Then, we introduced an analytical model for rumor spreading in time-varying social networks. Based on this model, we calculated the maximum likelihood of each suspect to determine the real source from the suspects. We conduct a series of experiments to evaluate the efficiency of our method. The experiment results indicate that our methods are efficient in identifying rumor sources in different types of real time-varying social networks.

There is some future work can be done in identifying rumor sources in time-varying social networks. In this paper, we collect and analyze three types of observations in networks. However, further types of observations can be considered in future work, such as multiple observations explored in static networks. Further, the discrete time-integrating windows in expressing time-varying social networks may lead to new ideas in identifying rumor sources in continuous time windows. In addition, we considered rumor spreading in a single network in this paper. Future work may investigate identifying the sources of rumors spreading across various network platforms.

References

[1] F. Peter. (2013, April 23) 'bogus' ap tweet about explosion at the white house wipes billions off us markets. The Telegraph, Finance/Market. Washington.

[2] B. Ribeiro, N. Perra, and A. Baronchelli, "Quantifying the effect of temporal resolution on time-varying networks," *Scientific reports*, vol. 3, 2013.

[3] M. P. Viana, D. R. Amancio, and L. d. F. Costa, "On time-varying collaboration networks," *Journal of Informetrics*, vol. 7, no. 2, pp. 371–378, 2013.

[4] M. Karsai, N. Perra, and A. Vespignani, "Time varying networks and the weakness of strong ties," *Scientific reports*, vol. 4, 2014.

[5] B. Doerr, M. Fouz, and T. Friedrich, "Why rumors spread so quickly in social networks," *Commun. ACM*, vol. 55, no. 6, pp. 70–75, Jun. 2012.

[6] D. Shah and T. Zaman, "Detecting sources of computer viruses in networks: Theory and experiment," in *Proceedings of the ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems*, ser. SIGMETRICS '10. ACM, 2010, pp. 203–214.

[7] W. Luo, W. P. Tay, and M. Leng, "Identifying infection sources and regions in large networks," *Signal Processing, IEEE Transactions on*, vol. 61, no. 11, pp. 2850–2865, 2013.

[8] Z. Wang, W. Dong, W. Zhang, and C. W. Tan, "Rumor source detection with multiple observations: Fundamental limits and algorithms," in *The 2014 ACM International Conference on Measurement and Modeling of Computer Systems*, ser. SIGMETRICS '14. ACM, 2014, pp. 1–13.

[9] K. Zhu and L. Ying, "Information source detection in the sir model: A sample path based approach," in *Information Theory and Applications Workshop (ITA)*, 2013, pp. 1–9.

[10] P. C. Pinto, P. Thiran, and M. Vetterli, "Locating the source of diffusion in large-scale networks," *Phys. Rev. Lett.*, vol. 109, Aug 2012.

[11] D. Brockmann and D. Helbing, "The hidden geometry of complex, network-driven contagion phenomena," *Science*, vol. 342, no. 6164, pp. 1337–1342, 2013.

[12] B. A. Prakash, J. Vreeken, and C. Faloutsos, "Spotting culprits in epidemics: How many and which ones?" in *Proceedings of the 2012 IEEE 12th International Conference on Data Mining*, ser. ICDM '12. Washington, DC, USA: IEEE Computer Society, 2012, pp. 11–20.

[13] C. Cattuto, W. Van den Broeck, A. Barrat, V. Colizza, J.-F. Pinton, and A. Vespignani, "Dynamics of person-to-person interactions from distributed rfid sensor networks," *PloS one*, vol. 5, no. 7, p. e11596, 2010.

[14] C. C. Zou, D. Towsley, and W. Gong, "Modeling and simulation study of the propagation and defense of internet e-mail worms," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 2, pp. 105–118, 2007.

[15] D. H. Zanette, "Dynamics of rumor propagation on small-world networks," *Physical review E*, vol. 65, no. 4, p. 041908, 2002.

[16] Y. Moreno, M. Nekovee, and A. F. Pacheco, "Dynamics of rumor spreading in complex networks," *Physical Review E*, vol. 69, no. 6, p. 066130, 2004.

[17] W. Luo, W. P. Tay, and M. Leng, "Rumor spreading and source identification: A hide and seek game," *arXiv preprint arXiv:1504.04796*, 2015.

[18] Y. Li, P. Hui, D. Jin, L. Su, and L. Zeng, "Optimal distributed malware defense in mobile networks with heterogeneous devices," *Mobile Computing, IEEE Transactions on*, 2013, accepted.

[19] N. Eagle and A. Pentland, "Reality mining: sensing complex social systems," *Personal and ubiquitous computing*, vol. 10, no. 4, pp. 255–268, 2006.

[20] A.-K. Pietilainen, "CRAWDAD data set thlab/sigcomm2009 (v. 2012-07-15)," Downloaded from http://crawdad.org/thlab/sigcomm2009/, Jul. 2012.

[21] J. Shetty and J. Adibi, "The enron email dataset database schema and brief statistical report," *Information Sciences Institute Technical Report, University of Southern California*, vol. 4, 2004.

[22] B. Viswanath, A. Mislove, M. Cha, and K. P. Gummadi, "On the evolution of user interaction in facebook," in *Proceedings of the 2nd ACM workshop on Online social networks*, ser. WOSN '09, 2009, pp. 37–42.

[23] D. Shah and T. Zaman, "Rumors in a network: Who's the culprit?" *IEEE Transactions on Information Theory*, vol. 57, pp. 5163 – 5181, 2011.

[24] Y. Ma, X. Jiang, M. Li, X. Shen, Q. Guo, Y. Lei, and Z. Zheng, "Identify the diversity of mesoscopic structures in networks: A mixed random walk approach," *EPL (Europhysics Letters)*, vol. 104, no. 1, p. 18006, 2013.

[25] S. Meloni, A. Arenas, S. Gómez, J. Borge-Holthoefer, and Y. Moreno, "Modeling epidemic spreading in complex networks: concurrency and traffic," in *Handbook of Optimization in Complex Networks*. Springer, 2012, pp. 435–462.

[26] Z. Dezső and A.-L. Barabási, "Halting viruses in scale-free networks," *Phys. Rev. E*, vol. 65, p. 055103, May 2002.

[27] W. Dong, W. Zhang, and C. W. Tan, "Rooting out the rumor culprit from suspects," in *Information Theory Proceedings (ISIT),*

2013 IEEE International Symposium on. IEEE, 2013, pp. 2671–2675.

[28] J. Jiang, S. Wen, S. Yu, Y. Xiang, and W. Zhou, "K-center: An approach on the multi-source identification of information diffusion," *Information Forensics and Security, IEEE Transactions on*, 17 August 2015.

[29] W. Luo and W. P. Tay, "Finding an infection source under the sis model," in *Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on*, 2013, pp. 2930 – 2934.

[30] Z. Chen, K. Zhu, and L. Ying, "Detecting multiple information sources in networks under the sir model," in *Information Sciences and Systems (CISS), 2014 48th Annual Conference on*. IEEE, 2014, pp. 1–4.

[31] W. Zang, P. Zhang, C. Zhou, and L. Guo, "Discovering multiple diffusion source nodes in social networks," *Procedia Computer Science*, vol. 29, pp. 443–452, 2014.

[32] A. Louni and K. Subbalakshmi, "A two-stage algorithm to estimate the source of information diffusion in social media networks," in *Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on*. IEEE, 2014, pp. 329–333.

[33] P. Basaras, D. Katsaros, and L. Tassiulas, "Detecting influential spreaders in complex, dynamic networks," *Computer*, no. 4, pp. 24–29, 2013.

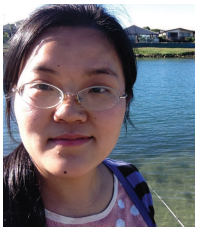
[34] C. H. Comin and L. da Fontoura Costa, "Identifying the starting point of a spreading process in complex networks," *Phys. Rev. E*, vol. 84, p. 056105, Nov 2011.

[35] A. Agaskar and Y. M. Lu, "A fast monte carlo algorithm for source localization on graphs," in *SPIE Optical Engineering and Applications*. International Society for Optics and Photonics, 2013.

[36] F. Altarelli, A. Braunstein, L. DallAsta, A. Lage-Castellanos, and R. Zecchina, "Bayesian inference of epidemics on networks via belief propagation," *Physical review letters*, vol. 112, no. 11, p. 118701, 2014.

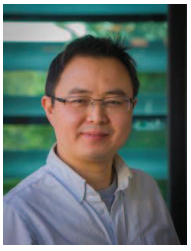
[37] B. A. Prakash, J. Vreeken, and C. Faloutsos, "Efficiently spotting the starting points of an epidemic in a large graph," *Knowledge and Information Systems*, vol. 38, no. 1, pp. 35–59, 2014.

[38] A. Y. Lokhov, M. Mézard, H. Ohta, and L. Zdeborová, "Inferring the origin of an epidemy with dynamic message-passing algorithm," *arXiv preprint arXiv:1303.5315*, 2013.

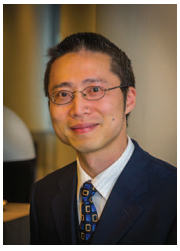


Jiaojiao Jiang received Master degree in College of Applied Sciences at Beijing University of Technology in 2011. She is currently working toward the Ph.D. degree at School of Information Technology, Deakin University, Melbourne, Australia. She served as a reviewer of the International Telecommunication Networks and Applications Conference 2015, and IEEE/CIC ICCC SNBD: Social Networks and Big Data 2015. Her research interests include cyber security, complex networks, big data, and signal processing.

Sheng Wen received the graduate degree in computer science and technology from Lanzhou Jiaotong University, Gansu, China, in 2003. He received the PhD (Computer Science) from Deakin University, Australia. His research interests include modeling of virus spread, defence strategies of the Internet threats, and locating the authors of computer viruses.



Shui Yu received his B.Eng (Electronic Engineering) and M.Eng (Computer Science) degree from University of Electronic Science and Technology of China, P. R. China in 1993 and 1999, respectively. He also obtained an Associate Degree in Mathematics from the same university in 1993. He received his PhD (Computer Science) from Deakin University in 2004. He is currently a Senior Lecturer of School of Information Technology, Deakin University, Melbourne, Australia. Before joining Deakin University, he was a Lecturer of Computer College in University of Electronic Science and Technology of China. He is also a Guest Professor of South West University of China. He is a Member of AAAS and a Senior Member of IEEE.



Yang Xiang received the PhD degree in computer science from Deakin University, Australia. Currently, he is with the School of Information Technology, Deakin University. In particular, he is currently leading in a research group developing active defense systems against large-scale distributed network attacks. He is the chief investigator of several projects in network and system security, funded by the Australian Research Council (ARC). His research interests include network and system security, distributed systems, and networking. He has published more than 100 research papers in many international journals and conferences, such as IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Information Security and Forensics, and IEEE Journal on Selected Areas in Communications. He has served as the program/general chair for many international conferences such as ICA3PP 12/11, IEEE/IFIP EUC 11, IEEE TrustCom 11, IEEE HPCC 10/09, IEEE ICPADS 08, NSS 11/10/09/08/07. He has been the PC member for more than 50 international conferences in distributed systems, networking, and security.

Wanlei Zhou received the B.Eng and M.Eng degrees from Harbin Institute of Technology, Harbin, China in 1982 and 1984, respectively; the PhD degree from The Australian National University, Canberra, in 1991; and the DSc degree from Deakin University, Victoria, Australia, in 2002. He is currently the Chair Professor of Information Technology, Faculty of Science and Technology, Deakin University, Melbourne, Australia. His research interests include network security, distributed and parallel systems, bioinformatics, mobile computing, and elearning. Before joining Deakin University, Professor Zhou worked in a number of organisations including University of Electronic Science and Technology of China in Chengdu, China, Apollo/HP in Massachusetts, USA, National University of Singapore in Singapore, and Monash University in Melbourne, Australia. His research interests include network security, distributed and parallel systems, bioinformatics, mobile computing, and elearning. He is a senior member of the IEEE. He has published more than 200 papers in refereed international journals and refereed international conferences proceedings. Professor Zhou was the General Chair / Program Committee Chair / Co-Chair of a number of international conferences, including ICA3PP, ICWL, PRDC, NSS, ICPAD, ICEUC, HPCC, etc., and has been invited to deliver keynote address in a number of international conferences, including TrustCom, ICWL, CIT, ISPA, etc.