Rumour Source Detection in Social Networks using Partial Observations

Roxana Alexandru and Pier Luigi Dragotti
Department of Electrical and Electronic Engineering,
Imperial College London, South Kensington, London SW7 2AZ, UK
email: roxana.alexandru12@imperial.ac.uk, p.dragotti@imperial.ac.uk

***Abstract*—The spread of information on graphs has been extensively studied in engineering, biology, and economics. Recently, however, several authors have started to address the more challenging inverse problem, of localizing the origin of an epidemic, given observed traces of infection. In this paper, we introduce a novel technique to estimate the location of a source of multiple epidemics on a general graph, assuming knowledge of the start times of rumours, and using observations from a small number of monitors.**

***Index Terms*—Rumour source detection, diffusion of information, SI epidemic model, social networks.**

I. Introduction

In the past few years, the inverse problem of detecting the source of an epidemic has started to receive considerable attention. Some real-world applications range from finding the origin of rumours in social networks, to finding faults in power networks, or the source of computer viruses. A lot of research has concentrated on finding origins in tree-like networks, assuming the susceptible-infected (SI) spreading model [1]–[4]. Some other methods are designed for generic network topologies, such as the techniques in [5]–[10]. Typical methods designed for complete observations of a network are the rumour center and eigenvector center based techniques [11]–[15]. For example, the approach introduced in [12] defines the rumour centrality as the number of distinct infection paths starting at the source, for a tree-like network. This work was extended to identify multiple sources in [2] and to source detection in a general graph in [8]. Methods with snapshot include the Jordan center [16]–[19], dynamic message passing [20], and effective distance based methods [21]. Techniques based on sensor observations in the network were developed in [7] and [22]–[24]. In [7] the authors propose a Monte Carlo method for single source estimation in generic graphs, achieving notable results. The probability of the source to be within the first 10 ranked nodes in a random geometric graph of 100 nodes is around 0.85 when observing 30% of the nodes.

Most of these current methods are very computationally expensive. Moreover, most tree-based approaches cannot easily be extended to generic networks, and those methods which are designed for general graphs are typically sensitive to the network topology. Furthermore, only some methods consider realistic temporal diffusion dynamics [7], [11], [22], [25], [26].

In this paper, we present a novel technique to efficiently solve the diffusion source inference problem in a general network of known topology, assuming knowledge of the rumour start time, and using multiple snapshots from a sparse set of monitors, in a fixed time window. We find the theoretic probability of infection at a node, as a function of its distance to the source of the rumour. Then, by fitting a monitor's measurements to the analytical model of infection, we are able to estimate the shortest distance between this monitor and the information source. Here, we leverage the assumption that the source emits multiple rumours, and this makes the fitting more reliable. Triangulation is then used to find potential sources, by considering the estimated locations of all the monitor nodes relative to the rumour origin. We finally introduce a method to find the most likely information source.

This paper is organized as follows. In Section II we define the rumour source detection problem. In Section III we formalize the mathematical models of information propagation within a network. Then, in Section IV we show how the probabilistic models of infection can be used to achieve inference of a single rumour source. In Section V, we discuss the performance of the detection algorithm in experiments on synthetic and real data. Lastly, we conclude in Section VI.

II. Problem Formulation

In this section we formally define the problem of estimating the rumour source location.

A. Network Topology

A social network will be modelled by a graph in which nodes are individuals and edges denote the relationships between them. The (i, j) entry in the graph's adjancency matrix will be 1 if nodes i and j are connected, and 0 otherwise.

B. Epidemic Model

We consider a discrete-time version of the susceptible-infected model, which means that at any time step a node is either infected or susceptible. We mathematically model this process by assigning a node a value of 1 when infected, and 0 otherwise. We assume that the rumour source is initially chosen uniformly at random at time $t_0 = 0$ and that we observe the diffusion for a time length T. Then, at each discrete time $t \in \{0, 1, ...T\}$, any infected node will remain infected for the subsequent time $t + 1$, and a susceptible node becomes infected if it receives the information from at least one of its infected neighbours. We assume all infections are independent and the likelihoods of transmission in one discrete time step are constant within the graph.

C. Source Localization

Suppose a source emits multiple rumours and that we have knowledge of their propagation start times. Without loss of

generality, we assume that the start time for all rumours is $t_0 = 0$. Moreover, we can observe the states of a set S_M of M monitors for the duration of the observation window, at discrete times $t \in \{0, 1, ...T\}$. At each time t we know the number of rumours $R_i(t)$ that have reached a sensor i, out of the total R rumours initiated by the source . Then, the probability of infection of a monitor i at time t is given by:

$$\tilde{F}_i(t) = \frac{R_i(t)}{R}. \quad (1)$$

We aim to localize the source of rumours, by leveraging knowledge of the monitors' observed infection probabilities, $\tilde{F}_i(t)$, for $t \in \{0, 1, ...T\}$ and $i \in S_M$.

III. Mathematical Models of Information Diffusion

In this section we formalize the mathematical models of information diffusion in a network. First, we give an approximate formulation for the probability of infection, for a given network topology. Then, we derive the probability of infection at a node, as a function of its shortest distance to the source. These mathematical models of infection will be used for an efficient source detection algorithm, in Section IV.

A. Infection Likelihood

We aim to find the probability of infection at node i, at time t. Let A be the event of at least one of node i's infected neighbours passing the rumour to i in one discrete time step, between $t-1$ and t, with probability $P(A)$. Moreover, let B denote the event of node i being in a susceptible state at time $t-1$, and $P(B)$ the corresponding event likelihood. Then, we define the probability of first infection at node i as:

$$f_i(t) = P(A \cap B) = P(A|B) \times P(B), \quad (2)$$

where we apply Bayes' rule to get the last identity.

Being in a susceptible state at time $t-1$ implies not getting the infection at any point before $t-1$. Since the events of a node not getting the initial infection at different times are mutually disjoint, the probability of being susceptible at $t-1$ is:

$$P(B) = \prod_{\tau=1}^{t-1}(1 - f_i(\tau)). \quad (3)$$

Given the constant pairwise transmission rate μ, the probability that a node j transmits the infection to its neighbour i between $t-1$ and t is:

$$P_{j\to i}(t) = \mu \times F(x_j(t-1) = 1). \quad (4)$$

where:

$x_j(t)$ = state of node j at time t,
$F(x_j(t) = 1)$ = probability of infection of node j at time t.

Therefore, a node j does not infect a neighbour i between $t-1$ and t, with probability:

$$P_{j\nrightarrow i}(t) = 1 - \mu \times F(x_j(t-1) = 1). \quad (5)$$

Since we assume that the information propagates independently across different edges, the probability that no neighbour transmits the rumour to node i between time instances $t-1$ and t is the product of the individual probabilities:

$$P(\bar{A}) = \prod_{j\in N_i} P_{j\nrightarrow i}(t) = \prod_{j\in N_i} (1-\mu\times F(x_j(t-1) = 1)), \quad (6)$$

where N_i is the set of neighbours of node i.

As a result, i gets infected at t with probability:

$$P(A) = 1-P(\bar{A}) = 1- \prod_{j\in N_i} (1-\mu\times F(x_j(t-1) = 1)). \quad (7)$$

Then, the conditional probability that at least one neighbour transmits the rumour to node i, given that this node was previously in a susceptible state, is given by:

$$P(A|B) = 1 - \prod_{j\in N_i} (1 - \mu F(x_j(t-1) = 1|x_i(t-1) = 0)). \quad (8)$$

The infection process at a node j is determined by complex dynamics in the network, and is not notably influenced by the state of a single neighbour i. Hence, we approximate the conditional probability as follows:

$$F(x_j(t-1) = 1)|x_i(t-1) = 0) \approx F(x_j(t-1) = 1)), \quad (9)$$

which implies that:

$$P(A|B) \approx 1 - \prod_{j\in N_i} (1 - \mu F(x_j(t-1) = 1)). \quad (10)$$

As a result of Eq. (2), Eq. (3), and Eq. (10), the probability of first infection at node i can be approximated as:

$$\begin{aligned} f_i(t) \approx &[1 - \prod_{j\in N_i} (1 - \mu F(x_j(t-1) = 1))] \\ &\times \prod_{\tau=1}^{t-1}(1 - f(x_i(\tau) = 1)). \end{aligned} \quad (11)$$

Finally, a node i is infected at time t if it initially received the rumour at any step before. Since the events of a node getting the initial infection at different times are mutually disjoint, the probability of infection is given by the sum of the likelihoods of first infection at different discrete times:

$$F_i(t) = F(x_i(t) = 1) = \sum_{\tau=1}^{t} f_i(\tau). \quad (12)$$

Fig. 1 plots the actual and theoretic cumulative infection distributions in a small-world network of 200 nodes, with average node degree 6, and re-wiring probability $\beta = 0.5$, generated using the Watts-Strogatz model [27]. The actual distribution is computed using Eq. (1), where measurements are generated through a spreading of 1000 rumours from a randomly selected source, with transmission rate $\mu = 0.5$. The theoretic distribution is computed with Eq. (11) and Eq. (12), and using the fact that if s is the source of the rumours, then $f_s(t) = 1$ if $t = 0$, and $f_s(t) = 0$ otherwise.

B. Distance-Dependent Infection Likelihood

In this section we derive a mathematical formulation for the probability of a node i, located at shortest distance d from the source, to get the infection at discrete time t.

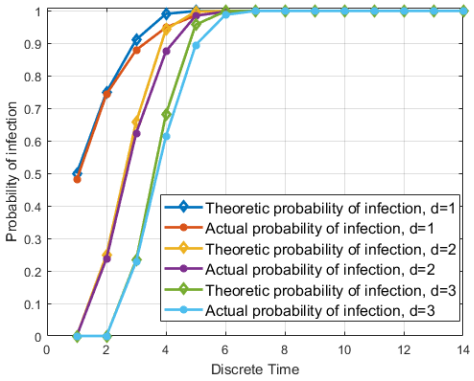

Fig. 1: Approximate theoretic probabilities of infection and observed infection likelihoods of three nodes in a small-world graph, with shortest distances to the origin, $d = 1, 2$, and 3.

Supposing $h<d$, let us define A as the event of transmitting the infection from nodes at distance $d-h$ from node i, to a *sufficient* number of nodes located $d-h-1$ hops away from node i. Spreading the rumour to a *sufficient* number of nodes at each time step t ensures that at the next time step, the rumour can propagate to nodes even closer to node i, i.e. at shortest distance $d-h-2$ to this node.

Then, in order for node i to get the infection for the first time at t, event A must occur d times up to time t, whilst the complementary event $\bar{A}$ must occur during the remaining $t-d$ discrete time steps. Moreover, there are multiple ways in which the succession of events A and $\bar{A}$ can happen within the time interval up to t. As we are interested to find the probability of *first* infection at time t, we restrict the event from time t to $t-1$ to be of type A. Then, the number of combinations in which node i can get the infection for the first time at t is the number of successions of events A and $\bar{A}$ up to time $t-1$:

$$C(t,d) = \binom{t-1}{d-1} = \frac{(t-1)!}{(d-1)!(t-d-1)!}. \quad (13)$$

Furthermore, let us denote the probability of occurrence of event A by $P(A)$. Then the probability of a succession of d events of type A and $t-d$ events of type $\bar{A}$ is:

$$p(t,d) = P(A)^d \times P(\bar{A})^{t-d}. \quad (14)$$

Moreover, different successions of events A and $\bar{A}$ up to $t-1$ are mutually disjoint, since events A and $\bar{A}$ cannot occur simultaneously during the same discrete time step. Hence, the probability of any node i at shortest distance d from the source, to get the infection at time t is the sum of the likelihoods of the different successions of events A and $\bar{A}$:

$$f_d(t) = p(t,d) \times C(t,d) = P(A)^d P(\bar{A})^{t-d} \binom{t-1}{d-1}. \quad (15)$$

The epidemic model assumed ensures that an infected node cannot later recover from this state. Moreover, if the node's shortest distance to the rumour source is d, then it cannot become infected sooner than discrete time $\tau = d$. Therefore, a node i has the infection at time t if it got infected at any time instance $\tau \in \{d, d+1, ...t\}$. Since the events of getting the initial infection at different times are mutually disjoint, the probability of any node i at distance d to have the infection at time t is given by the sum of the individual likelihoods of infection at different times:

$$F_d(t) = \sum_{\tau=d}^{t} f_d(\tau) = \sum_{\tau=d}^{t} P(A)^d P(\bar{A})^{\tau-d} \binom{\tau-1}{d-1}. \quad (16)$$

We define the probability $P(A)$ as follows. From the epidemic model defined in Section II, the pairwise transmission likelihood μ is constant within the graph. The probability of event A is proportional to the transmission rate μ, as the bigger μ is, the larger the likelihood of transmitting the infection from infected nodes $d-h$ hops away from node i to nodes closer to node i.

Moreover, $P(A)$ should capture the topological properties of a network. If the graph is more densely connected, a node $d-h$ hops away from node i will spread to more neighbours located $d-h-1$ hops away from i, for the same transmission rate μ, which increases the likelihood of event A.

We can approximately model this effect by multiplying the transmission rate by a distance-dependent factor α_d, which reflects the network characteristics. Therefore, we define $P(A) = \alpha_d \times \mu$ and Eq. (16) becomes:

$$F_d(t) = \sum_{\tau=d}^{t} (\alpha_d \times \mu)^d (1 - \alpha_d \times \mu)^{\tau-d} \binom{\tau-1}{d-1}. \quad (17)$$

Finally, the network-dependent parameters α_d are obtained as follows. A spreading of rumours is artificially generated from a random source in the graph according to the epidemic model introduced in Section II, resulting in the observations $\tilde{F}_i(t)$. Then, for each shortest distance d to the source s, the optimal parameter α_d minimizes the cumulative mean-squared error between the observed and the theoretic likelihoods of all nodes located at distance d from the origin:

$$\alpha_d^{opt} = \underset{\alpha_d \in (0, \frac{1}{\mu})}{\arg\min} [\sum_{i \in N_d} \sum_{t=0}^{T} \left\| F_d(t) - \tilde{F}_i(t) \right\|^2], \quad (18)$$

where N_d is the set of nodes at shortest distance d from the source, and the upper bound $\frac{1}{\mu}$ ensures stability of Eq. (16).

Fig. 2 shows a comparison between the theoretical probabilities of infection $F_d(t)$, and the observed infection likelihoods $\tilde{F}_i(t)$ for different distances d. These are obtained by spreading 1000 rumours in a small-world network of 200 nodes, with rewiring probability $\beta = 0.5$ and average node degree 4.

IV. Single Diffusion Source Detection

A. Estimation of Monitor Location

The distance between a monitor i and the origin s is estimated by fitting the measurements $\tilde{F}_i(t)$ to the theoretical model of infection $F_d(t)$, introduced in Section III-B. The optimal distance between i and s is determined by the minimum mean-squared error between the analytical distribution $F_d(t)$ and the monitor measurement $\tilde{F}_i(t)$, computed as:

$$d_{i,s}^{opt} = \underset{d}{\arg\min} [\sum_{t=0}^{T} \left\| F_d(t) - \tilde{F}_i(t) \right\|^2]. \quad (19)$$

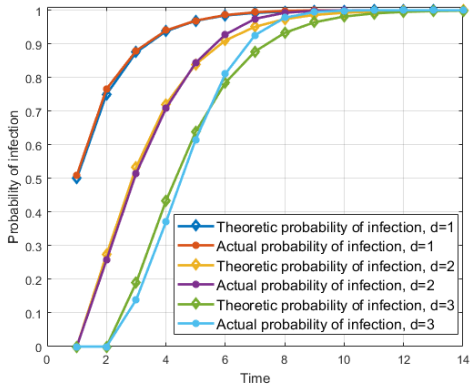

Fig. 2: Distance-dependent theoretic probabilities of infection and average observed infection likelihoods for different shortest distances to the rumour origin, $d = 1, 2$, and 3.

B. Estimation of a Set of Candidate Sources

The method used is triangulation. Using the estimated shortest distance of any monitor node to the rumour origin, we keep as potential rumour origins, the nodes within a 1-hop range of this distance. For example, if the estimated shortest distance to a monitor i is d, then we consider all nodes at $d-1$, d, or $d+1$ from i, as potential sources. Finally, we discard any candidate source if a monitor located at real shortest distance d from this potential origin has strictly positive infection probability $\tilde{F}_i(t) > 0$ at a time $t < d$.

C. Single Source Estimation

Given the set of potential sources constructed with triangulation, we aim to find the most likely rumour origin. The infection probability distributions of a monitor i may be different for two different rumour sources s_1 and s_2, even if the shortest distances from i to s_1 and s_2 are the same.

This dissimilarity between observations corresponding to different potential sources could be used to find the most likely rumour origin. The distance-dependent formula in Eq. (17) fails to capture the dissimilarity of observations resulting from different rumour origins. Nevertheless, the theoretic infection probability $F_i(t)$ defined in Eq. (12) is able to capture this behaviour, as its computation depends on the location of the rumour source. Therefore, we define the cost for a given potential source s as:

$$\tilde{C}(s) = \sum_{i \in S_M} \sum_{t=0}^{T} \left\| F_i(t) - \tilde{F}_i(t) \right\|^2, \qquad (20)$$

where:

$F_i(t) =$ theoretic infection probability of monitor i,
$\tilde{F}_i(t) =$ observed infection probability of monitor i.

Finally, the potential source s with the smallest cost $\tilde{C}(s)$ is the most likely rumour origin.

V. Experimental Results

We evaluate the performance of the source detection algorithm on: (i) syntethic small-world networks which mimic the structure of social networks and (ii) real network topologies extracted from the SNAP dataset [28]. Fig. 3 shows that the algorithm discovers the real rumour source with 100% accuracy in a small-world network when observing at least 5% of the nodes. Fig. 3 shows 94% accuracy in a real Facebook network, when observing at least 15% of the network. In both cases, the results are averaged over 100 different simulations, with different source and set of monitors in each case. Moreover, the number of rumours initiated by the source is realistically small, $R = 10$.

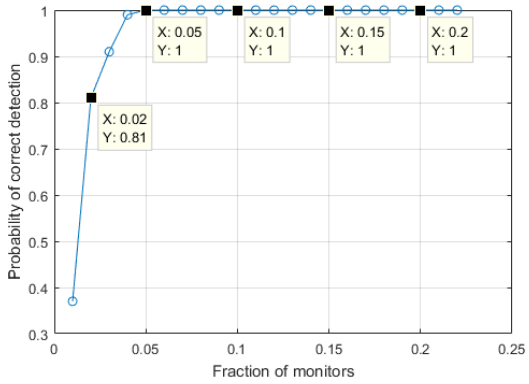

Fig. 3: Probability of correct detection of a single rumour source, in a small-world network of 1000 nodes.

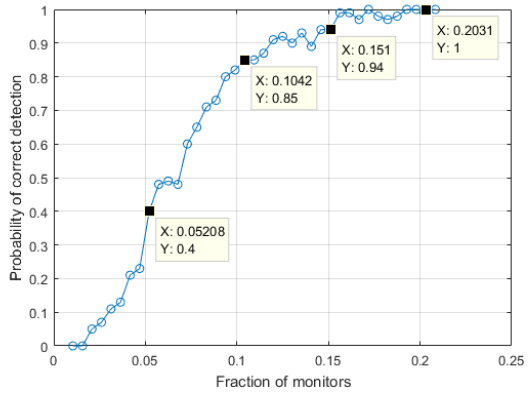

Fig. 4: Probability of correct detection of a single rumour source, in a Facebook subgraph of 192 nodes.

VI. Conclusions

In this paper we introduced a novel technique to infer a unique rumour source in a social network, given observations of a subset of nodes at discrete times during an observation window. The method relies on mathematical models which accurately capture the diffusion process. We have shown how we can use these theoretical models of infection to estimate the shortest distances between the monitor nodes and the source, and how triangulation can then be used to find a set of candidate sources. Moreover, we have introduced a technique to identify the unique rumour origin, from a set of potential sources. Experimental results on synthetic and real data show that high detection accuracy is achieved when a small fraction of the network is observed. Finally, the complexity of the algorithm is dominated by the computation of shortest distances in the network, which can be efficiently computed using an appropriate algorithm [29].

REFERENCES

[1] D. Shah and T. Zaman. Rumor Centrality: A Universal Source Detector. *SIGMETRICS Performance Evaluation Review*, 40(1):199–210, June 2012.

[2] W. Luo, W. P. Tay, and M. Leng. Identifying Infection Sources and Regions in Large Networks. *IEEE Transactions on Signal Processing*, 61(11):2850–2865, June 2013.

[3] N. Karamchandani and M. Franceschetti. Rumor source detection under probabilistic sampling. pages 2184–2188, Istanbul, Turkey, 2013. IEEE International Symposium on Information Theory (ISIT).

[4] D. T. Nguyen, N. P. Nguyen, and M. T. Thai. Sources of misinformation in Online Social Networks: Who to suspect? pages 1–6, Orlando, FL, USA, 2012. Proc. IEEE Military Communications Conference (MILCOM).

[5] W. Tang, F. Ji, and W. P. Tay. Multiple sources identification in networks with partial timestamps. In *2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pages 638–642, Nov 2017.

[6] S. Zejnilovi, J. Gomes, and B. Sinopoli. Sequential source localization on graphs: A case study of cholera outbreak. In *2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pages 1010–1014, Nov 2017.

[7] A. Agaskar and Y. M. Lu. A fast Monte Carlo algorithm for source localization on graphs. San Diego, CA, USA, 2013. SPIE Optical Engineering and Applications.

[8] J. Vrekeen B. A. Prakash and C. Faloutsos. Spotting Culprits in Epidemics: How many and Which ones? pages 11–20, Brussels, Belgium, 2012. Proc. IEEE 12th International Conference on Data Mining (ICDM).

[9] W. Luo and W. P. Tay. Identifying multiple infection sources in a network. In *2012 Conference Record of the Forty Sixth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, pages 1483–1489, Nov 2012.

[10] V. Fioriti and M. Chinnici. Predicting the sources of an outbreak with a spectral technique. *Applied Mathematical Sciences*, 9(135):6775–6782, 2014.

[11] J. Jiang, S. Wen, S. Yu, Y. Xiang, and W. Zhou. Identifying Propagation Sources in Networks: State-of-the-Art and Comparative Studies. *IEEE Communications Surveys and Tutorials*, 19(1):465–481, 2017.

[12] D. Shah and T. Zaman. Detecting Sources of Computer Viruses in Networks: Theory and Experiment. pages 203–214, New York, NY, USA, December 2010. Proc. ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems.

[13] D. Shah and T. Zaman. Rumors in a Network: Who's the Culprit? *IEEE Transactions on Information Theory*, 57(8):5163–5181, August 2011.

[14] 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*, SIGMETRICS '14, pages 1–13, New York, NY, USA, 2014. ACM.

[15] W. Dong, W. Zhang, and C. W. Tan. Rooting out the rumor culprit from suspects. *2013 IEEE International Symposium on Information Theory*, pages 2671–2675, 2013.

[16] K. Zhu and L. Ying. Information source detection in the sir model: A sample-path-based approach. *IEEE/ACM Transactions on Networking*, 24(1):408–421, Feb 2016.

[17] W. Luo and W. P. Tay. Finding an infection source under the sis model. In *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, pages 2930–2934, May 2013.

[18] W. Luo, W. P. Tay, and M. Leng. How to identify an infection source with limited observations. *IEEE Journal of Selected Topics in Signal Processing*, 8(4):586–597, Aug 2014.

[19] K. Zhu and L. Ying. A robust information source estimator with sparse observations. In *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, pages 2211–2219, April 2014.

[20] A. Y. Lokhov, M. Mézard, H. Ohta, and L. Zdeborová. Inferring the origin of an epidemic with a dynamic message-passing algorithm. 90(1):012801, Jul 2014.

[21] D. Brockmann and D. Helbing. The hidden geometry of complex, network-driven contagion phenomena. *Science*, 342:1337–1342, 2013.

[22] P. C. Pinto, P. Thiran, and M. Vetterli. Locating the Source of Diffusion in Large-Scale Networks. *Physical Review Letters*, 109(6), August 2013.

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

[24] F. Altarelli, A. Braunstein, L. DallAsta, A. Lage-Castellanos, and R. Zecchina. Bayesian Inference of Epidemics on Networks via Belief Propagation. *Physical Review Letters*, 112(11), 2014.

[25] M. Gomez Rodriguez, J. Leskovec, and A. Krause. Inferring networks of diffusion and influence. In *Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, KDD '10, pages 1019–1028, New York, NY, USA, 2010. ACM.

[26] S. Wen, W. Zhou, J. Zhang, Y. Xiang, W. Zhou, and W. Jia. Modeling propagation dynamics of social network worms. *IEEE Transactions on Parallel and Distributed Systems*, 24(8):1633–1643, Aug 2013.

[27] D. J. Watts and S. H. Strogatz. Collective dynamics of small-world networks. *Nature*, 393:440–442, 1998.

[28] J. Leskovec and A. Krevl. SNAP Datasets: Stanford large network dataset collection. http://snap.stanford.edu/data, June 2014.

[29] K. Magzhan, K. Magzhan, and H. M. Jani. A Review And Evaluations Of Shortest Path Algorithms. *International Journal of Scientific and Technology Research*, 2(6), June 2013.