2016 IEEE 24th International Conference on Network Protocols (ICNP)
Workshop on Machine Learning in Computer Networks (NetworkML 2016)

# Estimating the Rumor Source with Anti-Rumor in Social Networks

Jaeyoung Choi, Sangwoo Moon, Jinwoo Shin and Yung Yi
Department of Electrical Engineering
KAIST, Republic of Korea
Emails: {jychoi14,mununum,jinwoos,yiyung}@kaist.ac.kr

***Abstract*—Recently, the problem of detecting the rumor source in a social network has been much studied, where it has been shown that the detection probability cannot be beyond 31% even for regular trees. In this paper, we study the impact of an anti-rumor on the rumor source detection. We first show a negative result: the anti-rumor's diffusion does not increase the detection probability under Maximum-Likelihood-Estimator (MLE) when the number of infected nodes are sufficiently large by *passive diffusion* that the anti-rumor starts to be spread by a special node, called the *protector,* after is reached by the rumor. We next consider the case when the distance between the rumor source and the protector follows a certain type of distribution, but its parameter is hidden. Then, we propose the following learning algorithm: a) learn the distance distribution parameters under MLE, and b) detect the rumor source under Maximum-A-Posterior-Estimator (MAPE) based on the learnt parameters. We provide an analytic characterization of the rumor source detection probability for regular trees under the proposed algorithm, where MAPE outperforms MLE by up to 50% for 3-regular trees and by up to 63% when the degree of the regular tree becomes large. We demonstrate our theoretical findings through numerical results, and further present the simulation results for general topologies (e.g., Facebook and US power grid networks) even without knowledge of the distance distribution, showing that under a simple protector placement algorithm, MAPE produces the detection probability much larger than that by MLE.**

## I. Introduction

Information spread is universal in many types of online/offline and social/physical networks. Examples include the propagation of infectious diseases, the technology diffusion, the computer virus/spam infection in the Internet, and tweeting and retweeting of popular topics. Finding the source in those information spreads is one of the indispensable and useful tasks, arising in many different contexts, e.g., detecting a malicious agent, a patient zero, or an influential person, because pre-action can be taken by some authorities to limit the possible damages due to spreading of such diffused objects that are harmful, if spread in an uncontrolled manner. Since the seminal work by Shah and Zaman [1], extensive research efforts have been made [2]–[4], where the main focus has been on how to design an estimator and provide theoretical (positive and negative) limits on the detection performance. However, for example, it is shown [1] that in the regular tree topologies, the detection probability cannot be above 31% under Maximum-Likelihood-Estimator (MLE), and even worse, in other realistic topologies such as power grid graphs, scale-free graphs and Internet autonomous system (AS) graphs, the detection probability is less than 5% under a MLE-based heuristic.

In this paper, our interest lies in how much detection performance can be improved by installing hidden agents, called *protectors* that spread "anti-rumor." The role of these protectors is to spread the information against the rumor, vaccinate humans against infectious disease, or install security updates against computer virus. Intuitively, the existence of protectors and their infection with anti-rumor seem beneficial in detecting the rumor source, because they both block the rumor spread and the snapshot of both protected and infected nodes, compared to that of only infected nodes, discloses more information to the detector. However, understanding which nodes should be estimated to be the rumor source and quantifying the detection performance in presence of protectors is far from trivial. In this paper, we assume that initially there exists a single rumor source and an anti-rumor source (also called protector source throughout this paper), where the the anti-rumor source responds passively in the sense that it is initially dormant and becomes active and starts to infect other nodes (with anti-rumor) only when the rumor reaches itself. Our main contributions are summarized in what follows:

1) First, we show that under MLE, the protector's anti-rumor spread does not improve the detection probability in regular trees under the passive diffusion. However, we show that this is not the case if some statistical feature on the distance between the rumor and protector sources is given. In particular, we assume that the distance distribution is of a specific type, where their parameters are *unknown.* In practice, the parameters can be learnt using certain prior records on the rumor source or the diffusion snapshot. If such prior records do not exist, one can use a learning algorithm such as MLE to estimate the parameters (see Section III for more details). We study three example distance distributions, Zipf, Geometric or Poisson, where the probability that the protector source is located decays with distance in all distributions, but their decaying patterns differ.
2) Second, for a given quality in estimating the distribution parameters, we quantify how much the detection probability increases in regular trees under Maximum-A-Posterior-Estimator (MAPE) due to the usage of the protector's anti-rumor spreads. In particular, we show that the difference of

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.B0717-16-0034,Versatile Network System Architecture for Multi-dimensional Diversity).

978-1-5090-3281-5/16/$31.00 ©2016 IEEE

the detection probabilities between MLE and MAPE is up to 50% for the 3-regular tree and up to 63% for the regular tree with infinite degree. This implies that if the protector source is appropriately placed around the rumor source, the detection probability significantly increases.

3) Finally, we design a MAPE-based heuristic for general topologies such as *Erdös-Rényi* (ER) graph, small world graph, scale-free graph, as well as a Facebook ego network and a US power grid network, where we observe that the prior information based on the protector source significantly helps to detect the rumor source.

Thus, we conclude that utilizing the anti-rumor is a simple way of detecting the rumor source better, where in literature several different approaches have been considered for a similar purpose, *e.g.,* multiple observations [2], suspect set [3] and Jordan center-based [4] methods. We believe that ours shed new lights on this area, being of broad interest in the future.

## II. Model and Preliminaries

### A. Information Spreading Model

We consider an undirected graph $G = (V, E)$, where $V$ is a countably infinite set of nodes and $E$ is the set of edges of the form $(i, j)$ for $i, j \in V$. Each node represents an individual in human social networks or a computer host in the Internet, and each edge corresponds to a social relationship between two individuals or a physical connection between two Internet hosts. As in other works, *e.g.,* [1], we assume a countably infinite set of nodes for avoiding the boundary effects.

There exist two spreading sources: a *rumor source* and a *protector source*, which we denote by $v^*, p^* \in V$, respectively. The rumor source is the staring node which spreads a rumor, and the protector source corresponds to a node which spreads an "anti-rumor", *e.g.,* an anti-virus for virus spreading and a true fact for feigned rumor spreading. We consider the case when the protector source is *passive* in the sense that it is initially dormant, but becomes active and starts to infect its neighboring node only when the rumor reaches it (see Fig. 1). As a model of spreading rumor and anti-rumor, we consider a variant of SI (Susceptible-Infected) model that each node is one of the following three states: *susceptible*, *infected*, or *protected*, where all nodes are initialized to be susceptible except the initially-infected rumor source $v^*$ and the initially-protected protector source $p^*$. Once a node $i$ has rumor or anti-rumor, it is able to spread it to another susceptible node $j$ if and only if there is an edge between them, *i.e.,* $(i, j) \in E$. We assume that once a node becomes either *infected* or *protected*, it does not change its state, as in the classical SI model. For each edge $(i, j) \in E$, let a random variable $\tau_{ij}$ be the time it takes for susceptible node $j$ to receive the information (irrespective of being rumor or anti-rumor) from non-susceptible node $i$. We assume $\tau_{ij}$ is exponentially distributed with rate $\lambda > 0$ independently with everything else. Without loss of generality, we assume that $\lambda = 1$.

### B. Source Estimators: MLE and MAPE

**MLE and MAPE.** Let $I_N$ and $P_M$ be the sets of infected and protected nodes, respectively, when one intends to detect the rumor source. Here, the subscripts $N$ and $M$ are used to express the number of infected and protected nodes. To

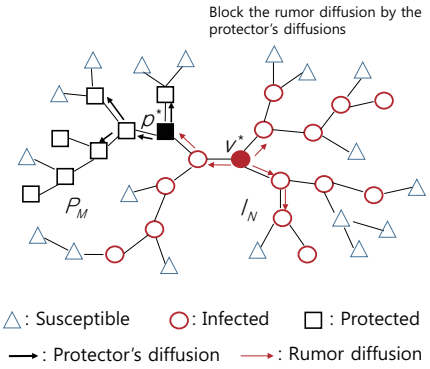



Fig. 1. Illustrative example of information spreading model for 3-regular tree. Here, $v^*$ is a rumor source and $p^*$ is a protector source (anti-rumor source), respectively.

estimate the rumor source $v^*$, we consider the following two popular estimators, MLE and MAPE:

$$\begin{aligned} v_{\texttt{ml}} &= \arg\max_{v \in I_N} \mathbb{P}(I_N, P_M | v, p^*), \\ v_{\texttt{map}} &= \arg\max_{v \in I_N} \mathbb{P}(v | I_N, P_M, p^*), \end{aligned} \tag{1}$$

where we assume that these have the knowledge of the protector $p^*$. Note that the relation between MLE and MAPE can be explained by:

$$\begin{aligned} v_{\texttt{map}} &= \arg\max_{v \in I_N} \mathbb{P}(v | I_N, P_M, p^*) \\ &\overset{(a)}{=} \arg\max_{v \in I_N} \frac{\mathbb{P}(I_N, P_M | v, p^*)\mathbb{P}(v, p^*)}{\mathbb{P}(I_N, P_N, p^*)} \\ &= \arg\max_{v \in I_N} \mathbb{P}(I_N, P_M | v, p^*) \cdot \mathbb{P}(v, p^*), \end{aligned}$$

where $(a)$ is from the Bayes' rule and $\mathbb{P}(I_N, P_M | v, p^*)$ is the probability that the realizations $I_N$ and $P_M$ occur, given a rumor source $v$ and the protector source $p^*$. Therefore, MLE is equivalent to MAPE if $\mathbb{P}(v, p^*)$ is uniform over $v \in V$.

To further characterize two estimators, let $\sigma = (\omega_1 = v^*, \omega_2, ..., \omega_{M+N})$ be an infection sequence resulting in $I_N, P_M$, where the rumor source $v^*$ generates the rumor first, and all other nodes in the sequence $\omega_2, ..., \omega_{M+N}$ are arranged in ascending order of their propagation times. Then, we have

$$\mathbb{P}(I_N, P_M | v, p^*) = \sum_{\sigma \in \Omega(v, p^*, I_N, P_M)} \mathbb{P}(\sigma | v, p^*), \tag{2}$$

where $\Omega(v, p^*, I_N, P_M)$ be the set of all possible propagation sequences given $I_N, P_M$. Then, under a regular tree $G$, one can follow the same approach as that in [1] and characterize MLE and MAPE based on the number of possible propagation sequences, *i.e.,*

$$v_{\texttt{ml}} = \arg\max_{v \in I_N} R(v, p^*, I_N, P_M), \tag{3}$$

$$v_{\texttt{map}} = \arg\max_{v \in I_N} R(v, p^*, I_N, P_M) \cdot \mathbb{P}(v, p^*), \tag{4}$$

where

$$\begin{aligned} R(v, p^*, I_N, P_M) &= |\Omega(v, p^*, I_N, P_M)| \\ &= (M+N)! \prod_{u \in I_N \cup P_M} |T_u^v|^{-1}. \end{aligned} \tag{5}$$

In the above, we let $|T_u^v|$ be the number of nodes in the subtree $T_u^v$ rooted at node $u$ when $v$ is the rumor source. One can

compute $R(\cdot)$ for every infected node $v \in I_N$ in $O(M+N)$ time using a similar message passing algorithm to that in [1].

**Distance distribution.** For computing MAPE in (4), one has to know the probability $\mathbb{P}(v, p^*)$. To this end, we assume that the distance between $v$ and $p^*$ is a random variable following a specific distribution. In this paper, we consider three distributions: '$L$-truncated' Zipf, Geometric or Poisson, where $L$ is a non-negative integer constant, *i.e.,* for $1 \le l \le L$,

$$\mathbb{P}\left(d(v,p^*)=l\right) \propto \begin{cases} 1/l^{\theta} & \text{for Zipf } (\theta \ge 0), \\ \theta(1-\theta)^{l-1} & \text{for Geometric } (0<\theta\le 1), \\ \theta^l e^{-\theta}/l! & \text{for Poisson } (\theta \ge 0), \end{cases} \tag{6}$$

and $\mathbb{P}(d(v,p^*)=l)=0$ for $l>L$. The main reason why we study these three distributions is because higher probabilities are assigned to nearer rumor sources from the protector source under them and these distributions will give how the distance information effect to detect the rumor source. We consider the sufficiently large $L$ but finite. Nevertheless, our analytical results can be easily extended to other distributions. We also remark that it is reported the distance of two nodes follows Zipf distribution in some social networks [5], [6]. Throughout this paper, we commonly use $\theta$ to mean the parameter of any of three distance distributions, where the true parameter $\theta=\theta^*$ might be unknown a priori and one has to run MAPE with an estimated parameter $\theta=\hat{\theta}$.

**Detection probability.** We let $C_{M+N}$ be the event of detecting the (rumor) source using a given estimator, where we are interested in the asymptotic case, *i.e.,* $\lim_{M+N\to\infty}\mathbb{P}(C_{M+N})$.[1] We denote by $\pi_d^{\mathtt{ml}}$ and $\pi_d^{\mathtt{map}}$ the detection probabilities of MLE and MAPE for $d$-regular tree, respectively. In addition, we use just $\pi_d$ to refer to that of MLE without protectors (*i.e.,* $M=0$) for a comparative purpose, where the following formula is known for $\pi_d$.

*Lemma 1 ( [7]):* Under $d$-regular tree $G$,

$$\pi_d = \begin{cases} 0 & \text{if } d=2 \\ 1-d\left(1-I_{1/2}\left(\frac{1}{d-2},\frac{d-1}{d-2}\right)\right) & \text{if } d\ge 3. \end{cases}$$

where $I_x(\alpha,\beta)$ is the incomplete Beta function[2] with parameters $\alpha$ and $\beta$.

Using the above lemma, one can easily check that the detection probability for MLE without protectors is at most $0.307$.

## III. Detection Probability with Protectors

### A. MLE-based Detection

We first provide the performance of MLE for detecting the rumor source in presence of anti-rumors under regular trees.

*Theorem 1:* Under $d$-regular tree $G$,

$$\pi_d^{\mathtt{ml}} \;=\; \pi_d \qquad \text{for all } d\ge 2.$$

We present the proof in our technical report [8]. This result implies that the existence of anti-rumors does *not* improve the detection performance when there are sufficiently large infected and protected nodes. This seems somewhat counter-intuitive, because the diffusion of anti-rumors may provide a side information so as to enable better detection. This negative result can be explained for the following reasons. Depending on the distance between the protector source and the rumor source, two cases can be considered. First, when $I_N$ is much larger than $P_M$, the MLE is highly likely to be equal to the original rumor center (without anti-rumors), resulting in the same detection probability. Second, however, when $P_M$ is larger than $I_N$, the MLE is highly likely to be located in $P_M$, which leads MLE to estimate a border node between $I_N$ and $P_M$ (because a rumor source should be in $I_N$), but the number of such border nodes is negligible (in fact, there exists a single border node in tree topologies), when $N, M \to \infty$.

### B. MAPE with Parameter Learning

In this subsection, we provide the performance of MAPE in presence of anti-rumors under regular trees. It turns out that obtaining the exact formula of MAPE's detection probability, as in Lemma 1 in absence of protectors, is technically challenging. However, in this section, we will provide a lower bound of the detection probability with protectors, as stated in Theorem 2, even when the unknown parameter of the distance distribution is not exactly equal to the true parameter.

*Theorem 2:* Let $\pi_d^{\mathtt{map}}(\hat{\theta})$ be the detection probability of MAPE for the learnt parameter $\hat{\theta}$ and the true parameter $\theta^*$. Then for $d$-regular trees it follows that

$$\pi_d^{\mathtt{map}}(\hat{\theta}) - \pi_d \;\ge\; \left(p(\theta^*)-1/2\right)^{\frac{2d-3}{3(d-2)}} \tag{7}$$

$$- 6|1-p(\hat{\theta})/p(\theta^*)||\theta^*-\hat{\theta}|, \tag{8}$$

where

$$p(\theta) = \begin{cases} \frac{2^\theta}{2^\theta+1} & \text{for} \quad \text{Zipf}(\theta), \quad \theta \ge 0, \\ \frac{1}{2-\theta} & \text{for} \quad \text{Geometric}(\theta), \quad 0<\theta\le 1, \\ \frac{2+\theta}{2+2\theta} & \text{for} \quad \text{Poisson}(\theta), \quad \theta \ge 0. \end{cases} \tag{9}$$

Due to space limitation, we provide the proof sketch in Section III-D (see our technical report in [8] for the full proof). A few interpretations of Theorem 2 are in order.

(a) Theorem 2 states that depending on how well we learn the true parameter $\theta^*$, the detection probability $\pi_d^{\mathtt{map}}$ is determined. In other words, if $\hat{\theta}$ is far from $\theta^*$, $\pi_d^{\mathtt{map}}$ may be lower than $\pi_d$.

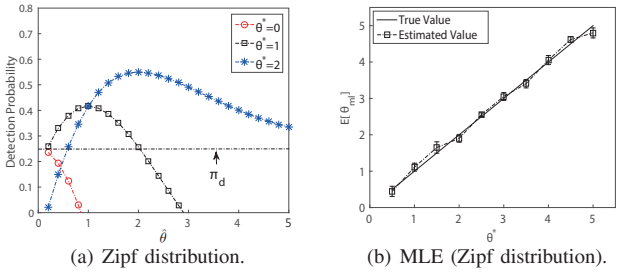
(b) In fact, we see that the protectors help in detecting the rumor source, *i.e.,* $\pi_d^{\mathtt{map}}(\hat{\theta}) - \pi_d \ge 0$, when the following condition holds:

$$|\theta^*-\hat{\theta}| \le \frac{\left(p(\theta^*)-1/2\right)^{\frac{2d-3}{3(d-2)}}}{6|1-p(\hat{\theta})/p(\theta^*)|}. \tag{10}$$

For an example, consider a Zipf distribution with $\theta^*=1$ for 3-regular tree (*i.e.,* $d=3$). Then, (10) holds if $|\theta^*-\hat{\theta}| \le 0.8$, and the condition for other cases are similarly mild, where as we will present in Section III-C, $\hat{\theta}$ can be learnt with a high-accuracy and low-cost parameter learning algorithm.

[1] Note that since the distance between the rumor and the protector sources are bounded by $L<\infty$, $M+N\to\infty$ implies that $M\to\infty$ and $N\to\infty$.

[2] The incomplete Beta function $I_x(\alpha,\beta)$ is the probability that a Beta random variable with parameters $\alpha$ and $\beta$ is less than $x\in[0,1]$, whose form is $I_x(\alpha,\beta)=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}\int_0^x t^{\alpha-1}(1-t)^{\beta-1}dt$ where $\Gamma(\cdot)$ is the standard Gamma function [7].




(a) Zipf distribution. (b) MLE (Zipf distribution).

Fig. 2. Theoretical result of Theorem 2 for Zipf distribution (a) and learning the parameter (b) of this distribution by MLE in Algorithm 1 for $d = 3$ and $L = 50$, respectively. (In (a), $\pi_d = 0.25$ for $d = 3$.)

(c) To roughly quantify our analytical result, if the distribution parameter estimation is almost perfect, *i.e.,* $\theta^* \approx \hat{\theta}$, then $\pi_d^{\texttt{map}}(\hat{\theta}) - \pi_d \gtrsim (p(\theta^*) - 1/2)^{\frac{2d-3}{3(d-2)}}$ . The value of $p(\theta^*)$ ranges in all three distributions as: $1/2 \leq p(\theta^*) \leq 1$. Thus, the detection performance *gap* from MLE without protectors is up to 50% for $d = 3$ and up to 63% for $d \to \infty$. This gap will reduce slightly, depending on the quality of true parameter $\theta^*$.

We plot the numerical result of Theorem 2 for Zipf distribution in Fig 2(a) (see [8] for other distributions). We consider three true parameters $\theta^* = 0, 1, 2$ and change the learning parameter from $\hat{\theta} = 0$ to $\hat{\theta} = 5$. We see that if $\theta^* = 0$ (Uniform distribution) then there is no gain of detection probability for any learnt parameter $\hat{\theta}$ due to lack of any distance information of the two sources. However, if $\theta^* > 0$ then there exists non-negligible enhancement of the detection probability.

### C. Learning $\theta^*$

In practice, there is no knowledge of the true parameter $\theta^*$ a priori. In this case, one can estimate it using prior records of rumor sources, or apply the following MLE simply based on the current 'snapshot':

$$\begin{aligned}\theta_{\texttt{ml}} &= \arg\max_{\theta} \mathbb{P}(I_N, P_M, p^*|\theta)\\ &= \arg\max_{\theta} \sum_{l=1}^{L} \mathbb{P}(I_N, P_M, p^*|d(v,p^*)=l)\mathbb{P}(d(v,p^*)=l|\theta)\\ &\overset{(a)}{=} \arg\max_{\theta} \sum_{l=1}^{L} \left(\sum_{k=1}^{|V_l|} \mathbb{P}(I_N, P_M, p^*|v_{l,k})\right) \mathbb{P}(d(v,p^*)=l|\theta)\\ &\overset{(b)}{=} \arg\max_{\theta} \sum_{l=1}^{L} R(V_l)\mathbb{P}(d(v,p^*)=l|\theta), \qquad (11)\end{aligned}$$

where $v_{l,k}$ is the $k$-th infected nodes at distance $l$ to the protector source $p^*$ and $V_l$ is the set of these nodes for $0 \leq k \leq |V_l|$. The equality $(a)$ is from the fact that $d(v, p^*) = l$ which implies that $v \in V_l$ and $(b)$ is from the fact that for each $v_{l,k} \in V_l$, $\mathbb{P}(I_N, P_M, p^*|v_{l,k}) \propto R(v_{l,k}, p^*, I_N, P_M)$ as in (3) where $R(V_l) = \sum_{k=1}^{|V_l|} R(v_{l,k}, p^*, I_N, P_M)$. Since $R(V_l)$ can be obtained from the snapshot and $\mathbb{P}(d(v, p^*) = l|\theta)$ is determined when the distribution is given, MLE is obtained by solving the optimization problem (11). To do this, let $f(\theta) := \sum_{l=1}^{L} R(V_l)\mathbb{P}(d(v, p^*) = l|\theta)$ then we see that this function does not guarantee the concavity in terms of $\theta$ (thus not a convex program), but from the monotonicity and differentiability of $\mathbb{P}(d(v, p^*) = l|\theta)$, it is easy to check that the function $f(\theta)$ is a differentiable unimodular function[3]. Thus, we can apply a popular algorithm for maximizing a unimodular function [9] to solve (11) as in Algorithm 1 where $\varepsilon > 0$ is the termination constraint. One can easily check that the algorithm is terminated in polynomial time of $M + N$ and $1/\varepsilon$.

**Algorithm 1** Maximum Likelihood Estimation (MLE) of $\theta^*$ for Regular Trees

**Input:** $(I_N, P_M, d, L, \theta_{min}, \theta_{max}, \varepsilon, \mathbb{P}(v, p^*))$
**for** $v \in I_N$ **do**
  Compute $R(v, p^*, I_N, P_M)$ by a message passing algorithm [1] and obtain $d(v, p^*)$ by a shortest path algorithm;
  $R(V_l) \leftarrow 0$; $(1 \leq l \leq L)$
  **if** $d(v, p^*) = l$ **then**
    $R(V_l) \leftarrow R(V_l) + R(v, p^*, I_N, P_M)$;
  **end if**
**end for**
Set $f(\theta) = \sum_{l=1}^{L} R(V_l)\mathbb{P}(d(v, p^*) = l|\theta)$;
$\theta^{new} \leftarrow \frac{\theta_{min}+\theta_{max}}{2}$; (initialize)
**while** $|\nabla f(\theta^{new})| \geq \varepsilon$ **do**
  Use Brent method [9] to find the root of $\nabla f(\theta^{new})$;
**end while**
**return** $\theta_{\texttt{ml}} = \theta^{new}$

Fig. 2(b) shows numerical results on the performance of learning $\theta^*$ for various values of $\theta^*$ in three distributions. For the graphs, we consider the total number of diffused nodes $M+N = 500$ under the 3-regular tree ($d = 3$) and we generate 100 random diffusion snapshots. We plot the average value of the estimated parameters with 95% confidence interval. Our numerical results reveal that MLE-based parameter estimation is highly accurate.

### D. Proof Sketch of Theorem 2

In this subsection, we will provide the proof sketch of Theorem 2 whose complete version is in [8]. To see this, we first consider the detection probability $\pi_d^{\texttt{map}}(\hat{\theta})$ of MAPE for $d$-regular tree as

$$\begin{aligned}\pi_d^{\texttt{map}}(\hat{\theta}) &= \sum_{v \in \mathcal{V}_L} \mathbb{P}(v_{\texttt{map}} = v)\mathbb{P}(v = v^*)\\ &= \sum_{l=1}^{L} \left(\sum_{v \in V_l} \mathbb{P}(v_{\texttt{map}} = v)\right) \mathbb{P}(d(v,p^*)=l|\theta^*)\\ &= \sum_{l=1}^{L} \varphi_l^{\texttt{map}}(\hat{\theta}, d)\mathbb{P}(d(v,p^*)=l|\theta^*),\end{aligned}$$

where $\mathcal{V}_L := \cup_{l=1}^{L} V_l$ and $\varphi_l^{\texttt{map}}(\hat{\theta}, d) := \sum_{v \in V_l} \mathbb{P}(v_{\texttt{map}} = v)$ is the detection probability of the MAPE when the distance of two sources is $l \geq 1$. We first present a lemma that states the lower bound of $\varphi_l^{\texttt{map}}(\hat{\theta}, d)$ for any distribution with the learning parameter $\hat{\theta}$ and degree $d$ for a given distance distribution.

[3] $f(\theta)$ is differentiable unimodular $\partial f(\theta)/\partial\theta > 0$ for one side of some $\theta$ and $\partial f(\theta)/\partial\theta < 0$ for the other side.

*Lemma 2:* For the rumor source $v \in I_N$ with $d(v,p^*) = l$ $(1 \le l \le L)$, let $\mathbb{P}_l := \mathbb{P}(d(v,p^*) = l|\hat{\theta})$ then we have

$$\varphi_l^{\mathtt{map}}(\hat{\theta}, d) \ge 1 - (d-1)\left(1 - I_{p_l}\left(\frac{1}{d-2}, \frac{d-1}{d-2}\right)\right) - \left(1 - I_{q_l}\left(\frac{1}{d-2}, \frac{d-1}{d-2}\right)\right), \tag{12}$$

where $p_l = \frac{\mathbb{P}_l}{\mathbb{P}_{l+1}+\mathbb{P}_l}$ and $q_l = \frac{\mathbb{P}_l}{\mathbb{P}_{l-1}+\mathbb{P}_l}$ for any distribution.

This result is similar to that of Lemma 1. We present the detailed proof of the lemma in [8]. Using Lemma 2, we obtain the following result.

*Lemma 3:* For $d$-regular tree $(d \ge 2)$,

$$\pi_d^{\mathtt{map}}(\theta^*) - \pi_d \ge (p(\theta^*) - 1/2)^{\frac{2d-3}{3(d-2)}}, \tag{13}$$

where $p(\cdot)$ is defined in (9) for each distribution, respectively.

To obtain this result, we subtract the incomplete beta function in Lemma 1 from that in Lemma 2 however, it is not easy due to quite complex form of the function. To handle this, we provide a new technique to find a tight lower bound of these difference as a simple polynomial form (See the details in [8]). Next, we consider the following result for the upper bound of the detection probability difference between the true and the learnt parameters.

*Lemma 4:* For $d$-regular trees $(d \ge 2)$,

$$\pi_d^{\mathtt{map}}(\theta^*) - \pi_d^{\mathtt{map}}(\widehat{\theta}) \le 6|1 - p(\hat{\theta})/p(\theta^*)||\theta^* - \hat{\theta}|. \tag{14}$$

This result is also obtained by using a similar technique to that in Lemma 3 and in addition to this, we use some contraction mapping properties to derive the difference of detection probability as a function of $|\theta^* - \hat{\theta}|$. We also give the full proof in [8]. Then, by combining (13), (14), we obtain the Theorem 2 and this completes the proof.

## IV. General Graphs and Simulation Results

We have so far assumed that the underlying graph is a regular tree, which is simply for analytical tractability as done in other related works [1]–[3], [7]. In this section, inspired by our analytical findings in earlier sections, we study the detection performance of a MAPE-based heuristic algorithm in more practical and general graphs.

**MAP-BFS estimator with $\theta^*$ learning.** We first describe a heuristic estimator motivated by MAPE, which is necessary due to the computational intractability [4] of the problem MAPE in (1). Motivated by the heuristic in [1], we propose a heuristic algorithm based on Breadth-First Search (BFS), as described in what follows: Let $\sigma_v$ be the infection sequence of the BFS ordering of the nodes in the given graph, then we estimate the source $v_{\mathtt{map}}^{\mathtt{b}}$ that solves the following:

$$v_{\mathtt{map}}^{\mathtt{b}} = \arg\max_{v \in G_N} \mathbb{P}(\sigma_v|v,p^*)\Big[R(v,p^*,T_b(v)) \times \mathbb{P}(d(v,p^*))\Big],$$

where $T_b(v)$ is a BFS tree rooted at $v$ and the rumor spreads along it and $d(v,p^*)$ is the shortest distance between $v$ and $p^*$. Note that $\mathbb{P}(d(v,p^*))$ uses an MLE-estimated parameter as in Section III-C based on $T_b(v)$, where computing the rumor centrality $R(\cdot)$ (in (11)) with $T_b(v)$ is the key component. This $T_b(v)$-based parameter learning is also a heuristic since obtaining the exact $\theta_{\mathtt{ml}}$ for a general graph is hard to solve. Except for the complexity in learning the distribution parameter, we can estimate a rumor source in $O(N(M+N))$ time.

[4]We can easily prove that this is ♯P-complete similarly to the proof of MLE without protectors in [1].

**Algorithm 2** Distance Centrality-Based Algorithm (DSBA)

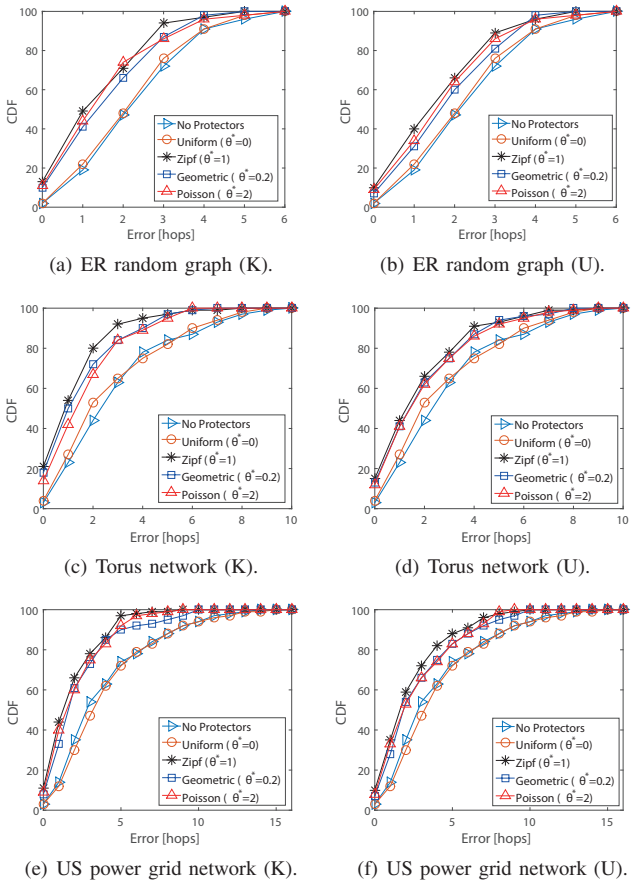
**Input:** $(G, n, L)$
Select a subgraph $G_L \subseteq G$ with diameter $L$ randomly and generate a rumor source $v_i^* \in G_L$ uniformly at random up to $1 \le i \le n$;
**for** $v \in G_L$ **do**
  Compute the distance $d(v, v_i^*)$ by a shortest path algorithm for all $i$ and calculate the distance centrality of $v$ by $C(v) = 1/\sum_{i=1}^{n} d(v, v_i^*)$;
**end for**
$P \leftarrow \phi$;
$v = \arg\max_{v \in G_L} C(v)$;
$P \leftarrow P \cup \{v\}$;
**if** $|P| > 1$ **then**
  Choose $v \in P$ uniformly at random;
**end if**
$p^* \leftarrow v$;
**return** $p^*$

**Algorithm 3** Degree Centrality-Based Algorithm (DGBA)

**Input:** $(G, L)$
Select a subgraph $G_L \subseteq G$ with diameter $L$ randomly ;
Set $D(v)$ by the degree of node $v$ in $G_L$;
$P \leftarrow \phi$;
$v = \arg\max_{v \in G_L} D(v)$;
$P \leftarrow P \cup \{v\}$;
**if** $|P| > 1$ **then**
  Choose $v \in P$ uniformly at random;
**end if**
$p^* \leftarrow v$;
**return** $p^*$

**Graphs.** We consider (i) three *synthetic random* graphs: *Erdös-Rényi* (ER) random graphs, small-world (SW), scale-free (SF) graphs, and Torus grid (TG) and (ii) two *real-world* graphs; a Facebook (FB) ego network and a US power (US) grid network. First, in synthetic random graphs, we set the average degree as 4 when there are 2000 nodes in the networks. For the Torus grid network, we consider a 60×60 grid torus network (thus 3600 nodes). Second, the Facebook ego network [10] is a undirected graph consisting of 4039 nodes and 88234 edges where each edge corresponds to a social relationship (called FriendList) and the diameter is 8 hops. The US power grid network [11] consists of 4941 nodes and 6594 edges and the diameter is 46 hops.

**Protector Source Selection Algorithms.** In practice, the distance distribution may not be known as a priori so that we need to estimate or to assume some proper distributions to obtain the detection behaviors by MAP-BFS estimator. In this simulation, we consider the following two scenarios: (i)




(a) ER random graph (K). (b) ER random graph (U).

(c) Torus network (K). (d) Torus network (U).

(e) US power grid network (K). (f) US power grid network (U).

Fig. 3. Simulation results of MAP-BFS detection performances where the Cumulative Distribution Function (CDF) of the distance between true source and estimator (Error) with 100 iterations under the general topologies when $M + N = 600$. (K: known, U:Unknown)

Known distribution (K) and (ii) Unknown distribution (U), respectively. For the first case, since the distribution is given as a priori, we only need to estimate the hidden true parameter of the distribution by some heuristic learning algorithm as we mentioned earlier. However, in the second case, due to the lack of the knowledge of distribution, we use some statistical information about the history of location for previous rumor sources. Based on this, we provide two protector source selection algorithms as follows. First, we consider an algorithm based on distance centrality (DSBA) of locations for them if the diameter of the network is huge. Second, we consider an algorithm based on the degree centrality (DGBA) of the networks, otherwise. In both algorithms, we use the notion $G_L$ to denote a subgraph of $G$ which the diameter is $L > 0$.

**Setup.** We use the true parameters: $\theta^* = 1$ for Zipf, $\theta^* = 0.2$ for Geometric and $\theta^* = 2$ for Poisson distributions and compare the results to the case without protectors in the network and no priori information about the source (*i.e.,* MLE). We use MATLAB for the simulations and generate 200 random graph samples for synthetic random graphs and a torus graph, where we diffuse rumors and anit-rumors until we have $M + N = 600$. By considering the total network size, we set the value $L$ as 50 % to the diameter of networks and we performed 100 iterations for all graphs.

**Simulation Results.** In the simulation, we obtain two different

TABLE I. DETECTION PROBABILITIES WITH UNKNOWN DISTRIBUTION FOR GENERAL GRAPHS ($L = 50\%$ OF NETWORK DIAMETER, (K):KNOWN DISTRIBUTION)

| **Distribution** | ER | SW | SF | Torus | FB | US |
|---|---|---|---|---|---|---|
| No Protector | 0.02 | 0.03 | 0.02 | 0.03 | 0.01 | 0.03 |
| Uniform | 0.02 | 0.03 | 0.04 | 0.04 | 0.02 | 0.03 |
| Zipf | **0.10** | **0.08** | **0.10** | **0.15** | **0.06** | **0.10** |
| (K) | **(0.13)** | **(0.10)** | **(0.11)** | **(0.21)** | **(0.07)** | **(0.11)** |
| Geometric | **0.07** | **0.07** | **0.07** | **0.13** | **0.04** | **0.07** |
| (K) | **(0.10)** | **(0.08)** | **(0.09)** | **(0.18)** | **(0.06)** | **(0.08)** |
| Poisson | **0.09** | **0.09** | **0.08** | **0.12** | **0.05** | **0.08** |
| (K) | **(0.11)** | **(0.11)** | **(0.10)** | **(0.14)** | **(0.09)** | **(0.09)** |

results as in Fig. 3 such as the known distribution (K) and unknown distribution (U), respectively. The x-axis of the figure indicates the distance between true source and estimator (Error) and the y-axis indicates Cumulative Distribution Function (CDF) of the errors. Clearly, zero error means the exact detection probability. We use DGBA for ER, SW, SF and FB graphs, and use DSBA for Torus and US networks. The results show that if the distance distribution is known as a priori, the detection performances of MAP-BFS heuristic are better than that of the case of no protector and no priori information (*i.e.,* Uniform distribution). It is hard to be beyond 5% for the case of no protector and no priori information but, if the distance information is given, we see that the detection probabilities can be beyond 10 % for the synthetic as well as real world topology even for our parameter setting with the estimated parameter. In the case of unknown distribution, the detection performances decrease compared to those of known distribution case. However, there are non-negligible enhancements from the result of no protector (See Table I).

## V. CONCLUSION

In this paper, we consider the rumor source detection problem in presence of passive protector that spreads the anti-rumor, where we provide the analytical results that MLE does not increase the detection capability as increasing the number of infected nodes, but MAPE with learning of the distribution parameters of the distance between the protector source and the rumor source significantly contributes to improving the detection power. As a future works, we will consider the active protector's diffusion that the anti-rumor starts spreading simultaneously to the rumor source.

## REFERENCES

[1] D. Shah and T. Zaman, "Detecting Sources of Computer Viruses in Networks: Theory and Experiment," in *Proc. ACM SIGMETRICS*, 2010.

[2] Z. Wang, W. Dong, W. Zhang, and C. W. Tan, "Rumor source detection with multiple observations: fundamental limits and algorithms," in *Proc. ACM SIGMETRICS*, 2014.

[3] W. Dong, W. Zhang, and C. W. Tan, "Rooting Out the Rumor Culprit from Suspects," in *Proc. ISIT*. IEEE, 2013.

[4] K. Zhu and L. Ying, "Information Source Detection in the SIR Model: A Sample Path Based Approach," in *Proc. ITA*. IEEE, 2013.

[5] A. Clauset, C. R. Shalizi, and M. E. J. Newman, "Power-law distributions in empirical data," in *arXiv:0706.1062v2*, 2009.

[6] D. Braha, B. Stacey, and Y. Bar-Yam, "Corporate competition: A self-organized network," *Elsevier Social Networks*, vol. 33, no. 3, pp. 219–230, July 2011.

[7] D. Shah and T. Zaman, "Rumor Centrality: A Universal Source Estimator," in *Proc. ACM SIGMETRICS*, 2012.

[8] J. Choi [Technical] On the Impact of Anti-Rumors on Rumor Source Detection https://www.dropbox.com/s/aprb0iltkw8gslw/main.pdf?dl=0.

[9] J. Solomon, *Numerical Algorithms: Methods for Computer Vision, Machine Learning, and Graphics*. CRC Press, 2015.

[10] J. McAuley and J. Leskovec, "Learning to discover social circles in ego networks," in *Proc. NIPS*, 2012.

[11] D. J. Watts and S. H. Strogatz, "Collective dynamics of small-world networks," *Nature*, vol. 393, no. 6684, pp. 440–442, June 1998.