Chapter 4
Restrain Malicious Attack Propagation

Restraining the propagation of malicious attacks in complex networks has long been an important but difficult problem to be addressed. In this chapter, we particularly use rumor propagation as an example to analyze the methods of restraining malicious attack propagation. There are mainly two types of methods: (1) blocking rumors at the most influential users or community bridges, and (2) spreading truths to clarify the rumors. We first compare all the measures of locating influential users. The results suggest that the degree and betweenness measures outperform all the others in real-world networks. Secondly, we analyze the method of the truth clarification method, and find that this method has a long-term performance while the degree measure performs well only in the early stage. Thirdly, in order to leverage these two methods, we further explore the strategy of different methods working together and their equivalence. Given a fixed budget in the real world, our analysis provides a potential solution to find out a better strategy by integrating both kinds of methods together.

4.1 Introduction

The popularity of online social networks (OSNs) such as Facebook [171], Google Plus [74] and Twitter [102] has greatly increased in recent years. OSNs have become important platforms for the dissemination of news, ideas, opinions, etc. Unfortunately, OSN is a double-edged sword. The openness of OSN platforms also enables rumors, gossips and other forms of disinformation to spread all around the Internet. In the real world, rumor has caused great damages to our society. For example, the rumor "Two explosions in White House and Obama is injured" happened in April 23, 2013 led to 10 billion USD losses before the rumor was clarified [143].

J. Jiang et al., *Malicious Attack Propagation and Source Identification*, Advances in Information Security 73,
https://doi.org/10.1007/978-3-030-02179-5_4

Currently, there are mainly two kinds of strategies used for restraining rumors in OSNs, including blocking rumors at important users [41, 49, 83, 96, 122, 129, 190, 193, 206] and clarifying rumors by spreading truths [25, 69, 71, 107, 165, 173]. We can further categorize the first strategy into two groups according to their measures in identifying the most important users: the most influential users [34, 70, 80, 96, 110, 159, 185] and the community bridges [31, 33, 106, 137–139, 174].

Every kind of strategy has pros and cons. Each method claims the better performance among all the others according to their own considerations and environments. However, there must be one standing out of the rest. Because there does not exist a universal standard to evaluate all them together, the question of which method is the best has long been important but difficult to be answered. Accordingly, previous work mainly focused on the 'vertical' comparison (methods inside their own category), such as the work [96, 110], but not on the 'horizontal' comparison (methods from different categories). All these methods are proposed to restrain the spread of rumors in OSNs.

To numerically evaluate different methods, we introduce a mathematical model to present the spread of rumors and truths. This is a discrete model so as to easily locate the most important nodes in the modeling. We can thus implement different strategies on this mathematical platform in order to evaluate their impacts to the spread of rumors and truths. Through a series of empirical and theoretical analysis using real OSNs, we are able to disclose the answer to the unsolved question.

In the real world, blocking rumors at important users may incur criticism since it has risk of violating human rights. On the other hand, the probability of people believing the truths varies according to many social factors. Therefore, it is very important to find out the optimal strategy of restraining rumors, which possibly should integrate both strategies together. The discussion on which method is the best will be a small, but an important, step towards the solution of this part of work. Thus, we are further motivated to explore the numerical relation and equivalence between different methods. Wen et al. [184] systematically analyzed different strategies for restraining rumors.

4.2 Methods of Restraining Rumors

Scientists have proposed many methods in order to restrain the propagation of rumors, such as controlling influential users, controlling bridges of social communities and clarifying the rumors by spreading the truths. The taxonomy of these methods is shown in Fig. 4.1.

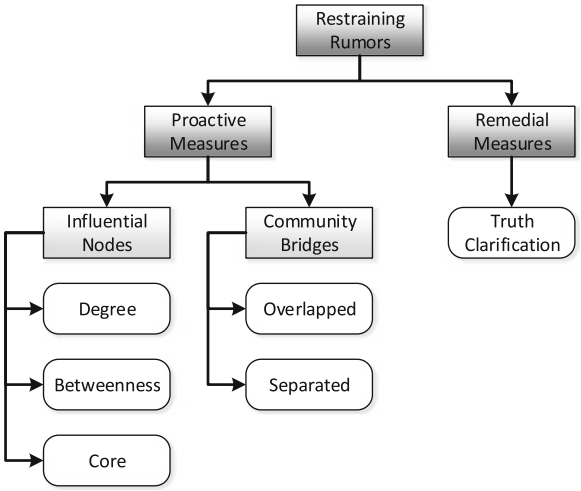

Fig. 4.1 The taxonomy of the methods used to restrain the spread of malicious attacks

4.2.1 Controlling Influential Users

The most common but popular method is to monitor a group of influential users and block their outward communication when rumors are detected on them. According to the way they choose the influential users, we category current methods into three types: degree, betweenness and core.

Degree The most direct and intuitive methods are to control the popular OSN users. In social graphs, these users correspond to the nodes with large degrees in OSNs. The theoretical bases of these methods are the scale-free and power-law properties of the Internet matters that a few highly-connected nodes play a vital role in maintaining the network's connectivity [136, 147]. We illustrate this method in Fig. 4.2a. We can see that when adequate popular users are controlled in OSNs, the spread of rumors will be limited in a small branch of the whole topology.

Betweenness Researchers have found that some nodes which do not have large degrees in topologies also play a vital role in the dissemination of social information. As shown in Fig. 4.2b, the degree of node E is smaller than node A, B, C and D. However, node E is noticeably more important to the spread of rumors as it is the connector of two large groups of users. To locate this kind of nodes in OSNs, scientists introduced the measure of betweenness which stands for the number of shortest paths passing through a given node [67]. We can also find some other variants of betweenness, such as the RW betweenness [132]. The work [34, 70, 80, 110, 185] argued that controlling the nodes with higher betweenness values is more efficient than controlling those with higher degrees.

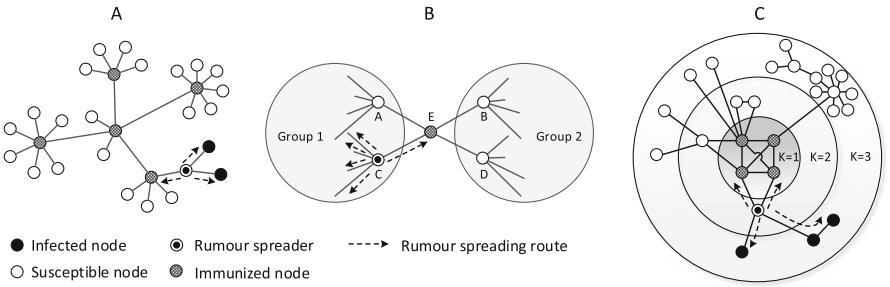

Fig. 4.2 Restraining the rumors by controlling the influential nodes. (**a**): the influential nodes are those of large degree; (**b**): the influential nodes are those of large betweenness; (**c**): the influential nodes are those in the innermost core

Core In this case, the network topologies are decomposed using the k-shell analysis. Some researchers have found that the most efficient rumor spreaders are those located within the core of the OSNs as identified by the decomposition analysis [96, 159]. We illustrate this viewpoint in Fig. 4.2c. We can see that the nodes in the innermost component of the network may possibly have smaller degrees, but they contribute to the kernel of the network and build the connectivity between the outside components. Thus, the nodes in the core are more crucial for restraining the rumors in OSNs.

4.2.2 Controlling Community Bridges

Most real OSNs typically contain parts in which the nodes are more highly connected to each other than to the rest of the network. The sets of such nodes are usually called communities in OSNs. The existing methods used to identify communities mainly have two types: finding overlapped communities [138, 139] and finding separated communities [31, 33, 33, 106, 137, 174, 174].

Overlapped Every OSN user in the real world has numerous roles. For example, a user is a student so that he or she belongs to a schoolmate community. This user may also belong to the communities of a family and various hobby groups. Therefore, most of the actual OSNs are made of highly overlapping cohesive groups of users [138, 140]. The nodes which locate at more than one community are the bridges between communities. The bridges forward the information from one community to another. If we control the bridges and block the spread of rumors on them, the scale of the rumors propagation will be limited to the local community. We illustrate this kind of methods [138, 139] in Fig. 4.3a.

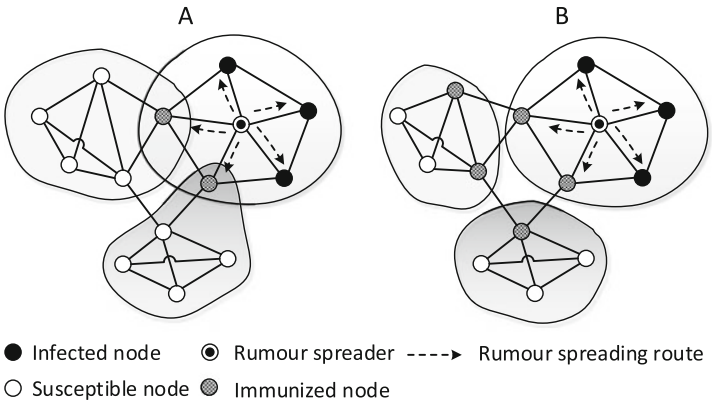

Fig. 4.3 Restraining the rumors by controlling the bridges between communities. (**a**): communities are overlapped; (**b**): communities are separated

Separated Some researchers [31, 33, 33, 106, 137, 174, 174] extract social relationship graphs by partitioning the topologies of OSNs into numerous separated communities. The premise of these methods is that users are more likely to receive and forward information from their social friends. Thus, these separated communities are representative of the most likely propagation paths of the rumors and the truths. Compared with the overlapped communities, the bridges are the nodes which have outward connections to the nodes of other communities. As shown in Fig. 4.3b, when the bridges between separated communities are controlled, the spread of rumors will also be limited to a small scale.

4.2.3 Clarification Through Spreading Truths

Except banning the outward communication on those influential users or the community bridges, people can adopt the strategy of spreading truths [25, 69, 71, 107, 165, 173] to the public in order to eliminate the critical rumors. As shown in Fig. 4.4, the scale of the rumors' propagation will be restrained after the truths start to spread. In the real world, this strategy respects the freedom of speech, but its efficiency is highly related to the credibility of the truth origins. If the origins of the truths have high prestige among the masses, people will definitely accept the truths when both the rumors and the truths are received. Otherwise, people make decisions using the "minority is subordinate to majority" rule. We will model and elaborate the processes of people making choices in the following section.

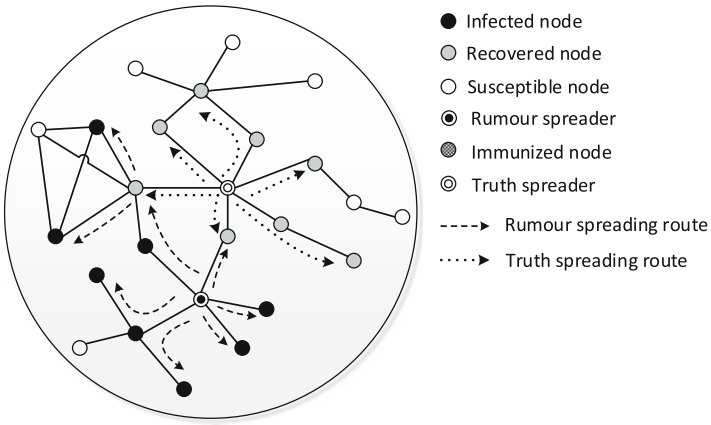

Fig. 4.4 Restraining the rumors by spreading truth in OSNs

4.3 Propagation Modeling Primer

We build up in this section the mathematical model in order to analyze the spread of rumors and investigate the methods of restraining their propagation.

4.3.1 Modeling Nodes, Topology and Social Factors

In the real world, people may believe rumors, truths or have not heard of any information from OSN. Let random variable $X_i(t)$ represent the state of user i at discrete time t. We borrow the concepts from epidemics and derive the values of $X_i(t)$ as follows

$$X_i(t) = \begin{cases} Sus., \ susceptible \\ Def., \ defended \\ Rec., \ recovered \begin{cases} Act., \ \ active \\ Imm., \ immunized \end{cases} \\ Inf., \ \ Infected \begin{cases} Con., \ contagious \\ Imm., \ misled \end{cases} \end{cases} \tag{4.1}$$

Firstly, every user is presumed to be susceptible ($X_i(t) = Sus.$) at the beginning. If a user is proactively controlled and will block the rumors, the node of this user is at the Def. state. An arbitrary user i believes the rumor if $X_i(t) = Inf.$ or the truth if $X_i(t) = Rec$. Secondly, seldom users will forward the same messages of the rumor or the truth multiple times to 'persuade' their social friends into accepting what they have believed. Thus, we assume OSN users distribute the rumor or the

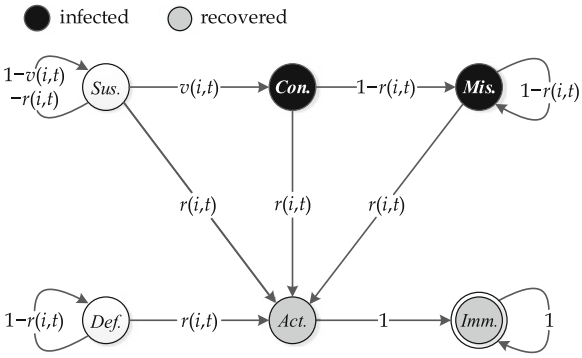

Fig. 4.5 The state transition graph of a node in the topology

truth only once at the time when they get infected ($X_i(t) = Con.$) or recovered ($X_i(t) = Act.$). After that, they will stop to spread the rumor ($X_i(t) = Mis.$) or the truth ($X_i(t) = Imm.$). Thirdly, the origins of the true news in the real world usually have high prestige among the masses. Thus, an infected user can be recovered and will not be infected again. The user will stay being immunized after he or she trusts the truth. We provide the state transition graph for an arbitrary user in Fig. 4.5. We can see that most users will finally believe the truth as the Imm. state is an absorbing state.

The nodes and the topology are the basic elements for the propagation of OSN rumors and truths. Given an OSN, we derive the topology of it. A node in the topology denotes a user in the OSN. Here, we propose employing $m \times m$ square matrix with elements $\langle \eta_{ij}^R, \eta_{ij}^T \rangle$ ($\eta_{ij}^R, \eta_{ij}^T \in [0, 1]$) to describe the topology of an OSN with m nodes, as in

$$\begin{bmatrix} \langle \eta_{11}^R, \eta_{11}^T \rangle & \cdots & \langle \eta_{1m}^R, \eta_{1m}^T \rangle \\ \vdots & \langle \eta_{ij}^R, \eta_{ij}^T \rangle & \vdots \\ \langle \eta_{m1}^R, \eta_{m1}^T \rangle & \cdots & \langle \eta_{mm}^R, \eta_{mm}^T \rangle \end{bmatrix}$$

where, η_{ij}^R and η_{ij}^T denote the probability of rumors and truths spreading from user i to user j respectively. If user i has contact with user j, we have $\eta_{ij}^R \neq 0$, $\eta_{ij}^T \neq 0$. Otherwise, $\eta_{ij}^R = 0$, $\eta_{ij}^T = 0$.

4.3.2 Modeling Propagation Dynamics

We introduce a widely approved discrete model [9, 29, 109, 185, 186, 195] to present the propagation of rumors and truths in OSNs. The discrete model can locate each influential node and evaluate its impact to the spread. Given a topology of an OSN with m nodes, we can estimate the number of susceptible and recovered users at time t, $S(t)$ and $R(t)$, as in

$$\begin{cases} S(t) = \sum_{i=1}^{m} P(X_i(t) = Sus.) \\ R(t) = \sum_{i=1}^{m} P(X_i(t) = Rec.) \end{cases} \tag{4.2}$$

where, $P(\cdot)$ denotes the probability of a variable. Similarly, the number of defended nodes at time t, $D(t)$, is derived by computing $\sum_{i=1}^{m} P(X_i(t) = Def.)$. Then, we can obtain the number of infected nodes at time t, $I(t)$, as in

$$I(t) = m - S(t) - R(t) - D(t). \tag{4.3}$$

As shown in Fig. 4.5, a susceptible user may accept the rumor and the node enters the $Inf.$ state. An infected node may also be recovered if this user accepts the truth. We use $v(i,t)$ and $r(i,t)$ to denote the probability of user i being infected or recovered. Then, the values of $P(X_i(t) = Sus.)$, $P(X_i(t) = Rec.)$ and $P(X_i(t) = Def.)$ can be iterated using the discrete difference equations as in

$$P(X_i(t) = Sus.) = [1 - v(i,t) - r(i,t)] \cdot P(X_i(t-1) = Sus.) \tag{4.4}$$

$$P(X_i(t) = Rec.) = r(i,t) \cdot [1 - P(X_i(t-1) = Rec.)] + P(X_i(t-1) = Rec.) \tag{4.5}$$

$$P(X_i(t) = Def.) = [1 - r(i,t)] \cdot P(X_i(t-1) = Def.) \tag{4.6}$$

We introduce $Neg(i,t)$ and $Pos(i,t)$ to be the probability of user i not believing the rumor or the truth. Since the rumor and the truth come from social neighbors, the values of $Neg(i,t)$ and $Pos(i,t)$ can be derived by assuming all social neighbors cannot convince user i of the rumor or the truth. Then, according to the principle of multiplication, we have

$$\begin{cases} Neg(i,t) = \Pi_{j \in N_i} \left[1 - \eta_{ji}^{R} \cdot P(X_j(t-1) = Con.) \right] \\ Pos(i,t) = \Pi_{j \in N_i} \left[1 - \eta_{ji}^{T} \cdot P(X_j(t-1) = Act.) \right] \end{cases} \tag{4.7}$$

where N_i denotes the set of user i's neighbors. We assume the states of nodes in the topology are independent. Then, according to the state transitions in Fig. 4.5, the values of $P(X_i(t) = Con.)$ and $P(X_i(t) = Act.)$ can be derived as in

$$P(X_i(t) = Con.) = P(X_i(t-1) = Sus.) \cdot v(i,t) \tag{4.8}$$

$$P(X_i(t) = Act.) = [1 - P(X_i(t-1) = Rec.)] \cdot r(i,t) \tag{4.9}$$

From the above equations, we adopt discrete time to model the propagation dynamics. Note that the length of each time tick relies on the real environment. It can be 1 min, 1 h or 1 day.

4.3.3 Modeling People Making Choices

According to the ways people believe rumors and truths, we drive different values of $v(i,t)$ and $r(i,t)$. In part, we summarize two major cases on the basis of our analysis in the real world.

Absolute Belief In this case, we optimistically assume OSN users absolutely believe the truths except they only receive rumors. Then, we can derive the values of $v(i,t)$ and $r(i,t)$ as in

$$\begin{cases} v(i,t) = [1 - Neg(i,t)] \cdot Pos(i,t) \\ r(i,t) = 1\ Pos(i,t) \end{cases} \tag{4.10}$$

In the real world, this case happens generally when the origins of true news have high prestige among the masses. For example, when the rumor "two explosions in White House and Barack Obama is injured" fast spread in twitter [143], White House, as an origin which has absolute credibility among most people, swiftly stopped the rumor by clarifying and spreading the truth "Obama is fine and no explosion happened".

Minority is Subordinate to Majority In this case, people do not absolutely trust the origins of the truths. They believe either the rumor or the truth according to the ratio of believers among their OSN friends. We can estimate the number of received rumor and truth copies ($C_R(i,t)$ and $C_T(i,t)$) for each user i as in

$$\begin{cases} C_R(i,t) = \sum_{j \in N_i} \left[\eta_{ij} \cdot P(X_j(t-1) = Con.)\right] \\ C_T(i,t) = \sum_{j \in N_i} \left[\eta_{ij} \cdot P(X_j(t-1) = Act.)\right] \end{cases} \tag{4.11}$$

Then, we derive the values of $v(i,t)$ and $r(i,t)$ as in

$$\begin{cases} v(i,t) = \frac{[1-Neg(i,t)\cdot Pos(i,t)]\cdot C_R(i,t)}{C_R(i,t)+C_T(i,t)} \\ r(i,t) = \frac{[1-Neg(i,t)\cdot Pos(i,t)]\cdot C_T(i,t)}{C_R(i,t)+C_T(i,t)} \end{cases} \tag{4.12}$$

where, the value of $Neg(i,t) \cdot Pos(i,t)$ is the probability of people refuting both kinds of information. In the real world, "minority is subordinate to majority" (M-S-M) is a more general case. When more friends choose to accept one kind of information, the probability of the user believe this kind of information is larger than the probability of choosing the opposite one.

4.3.4 The Accuracy of the Modelling

Before we carry out analysis using the mathematical model, we set up simulations to validate its correctness. The experiment topologies are two real OSNs: Facebook

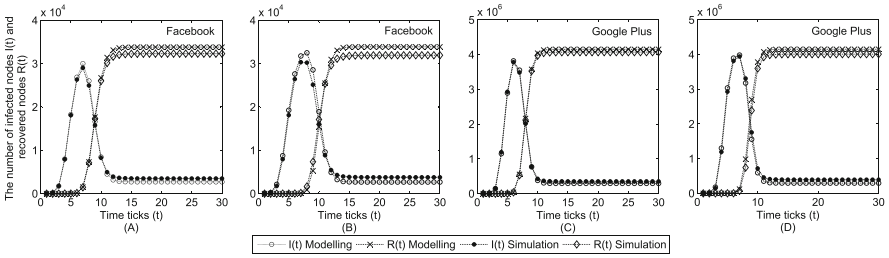

Fig. 4.6 The accuracy evaluation of the modelling compared with simulations

[171], Google Plus [74]. The simulations are implemented on the basis of existing simulation work [192]. We mainly focus on the critical rumors ($\eta_{ij}^R > 0.5$). Thus, we set the propagation probabilities as $\eta_{ij}^R = \eta_{ij}^T = 0.75$. The spread of rumors starts at $t = 0$. Since the truths start to propagate after many users have believed the rumors, we set the truth injection time, t_{infect}, as $t_{infect} = 3$. The implementation is in C++ and Matlab2012b.

We show the validation results in Fig. 4.6. We can see that the modelling results are quite accurate compared with the simulations. In Eq. (4.7), we assume the states of nodes in the topology are independent. The independent assumption has been widely used in this field, such as the works [29, 109, 185]. However, this assumption may causes errors in the modeling. Readers could find extensive analysis in the works [186, 195]. In fact, the errors will be compromised when the modelling results of conflicting information mutually subtract each other. Here, we simply adopt this assumption as we mainly focus on the comparison of different defense methods.

4.4 Block Rumors at Important Users

In this section, we analyze the proactive measures in order to find out the most efficient one for blocking rumors. The degree measure can be directly derived from the OSN topology. The betweenness measure is worked out using the standard algorithm [132]. We also implement the k-shell decomposition algorithm [26] to identify the core of OSNs. To locate community bridges, we use CFinder [28] to identify the overlapped communities and NetMiner [130] for the separated ones. We focus on the Facebook network [171] in this section.

4.4.1 Empirical Studies

We first work out all proactive measures and show the sorted results of influential nodes in Fig. 4.7. For the degree measure (Fig. 4.7a), we can see that the node

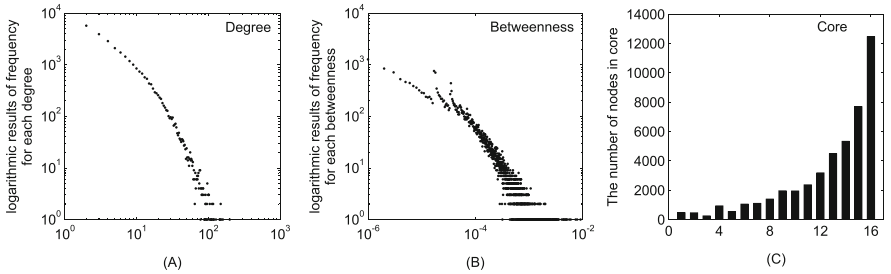

Fig. 4.7 The sorted results of the influential nodes in the Facebook topology

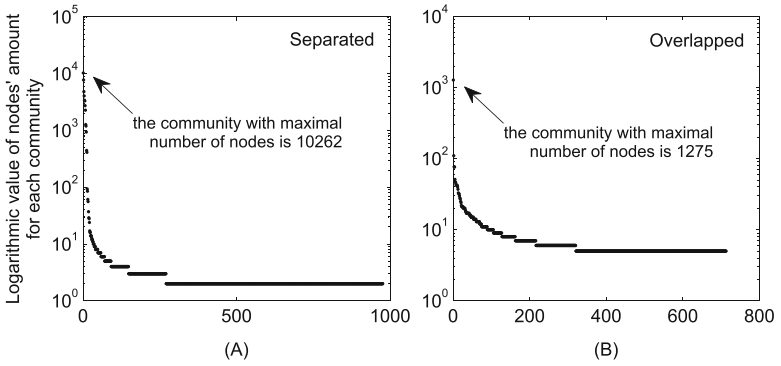

Fig. 4.8 The sorted results of community bridges

degrees follow the power-laws [147]. This means the nodes with large degrees are rare in the topology but have significant contribution to the OSN connectivity. Similar results can also be observed in the measure of betweenness (Fig. 4.7b). For the core measure (Fig. 4.7c), we can see that the innermost part finally leaves to be a quite small group of nodes in the network.

The results of network communities are shown in Fig. 4.8. For the separated communities (Fig. 4.8a), we find several large communities dominate the majority of nodes in the network. In Fig. 4.8b, we set $k = 5$ (refer to CFinder [28]) and obtain similar results for the overlapped communities.

From the empirical perspective, we examine which proactive measure can be more efficient. We use λ to denote the defense ratio of nodes in OSNs, and λ ranges from 1% to 30%. We mainly focus on critical rumors in this chapter ($E(\eta_{ij}^R) > 0.5$). To be typical, we set $E(\eta_{ij}^R) = E(\eta_{ij}^T) = 0.6$ or 0.9. In the real world, since critical rumors often originate from the most popular users, we let the rumors in the modelling spread from the node with large degree. The results of the rumor spreading scale are shown in Fig. 4.9.

Observation 1 If we set the defense ratio (λ) close to 30%, the degree and betweenness measures will almost stop the spread of rumors. This result is in

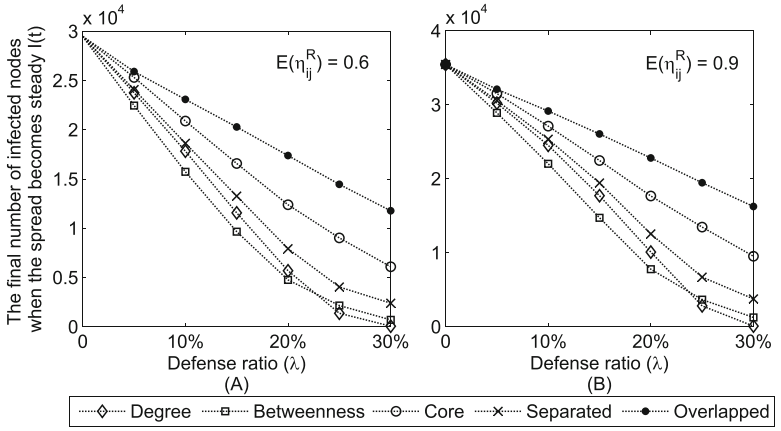

Fig. 4.9 The final steady amount of infected nodes when we apply proactive measures with different defense ratios

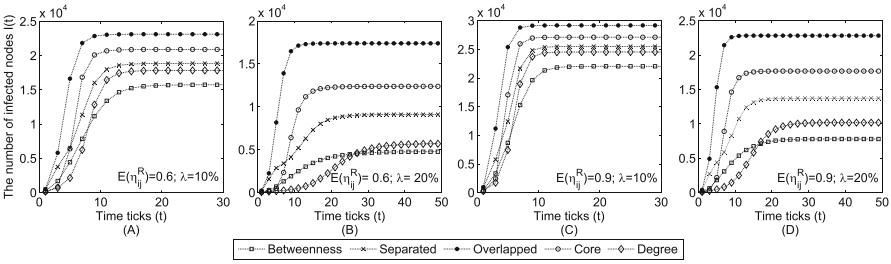

Fig. 4.10 The propagation dynamics of rumors when we carry out defense according to different proactive measures

accordance with the percolation ratio used to stop viruses in Email network [207]. However, the real OSNs generally have large-scales. Blocking rumors at 30% users in OSNs is too many to be realized in the real world.

Observation 2 The betweenness and degree measures outperform all the other measures, and the betweenness measure performs much better than the degree measure if $\lambda \leq 20\%$. This result is in accordance with the work [110, 185]. Figure 4.9 has presented the final amount of infected users given a rumor spreading in network. We further investigate the propagation dynamics of those measures (typically setting $\lambda = 10\%$ or 20%). The results are shown in Fig. 4.10.

Observation 3 The degree measure performs better than the betweenness measure in the early stage. The degree and betweenness measures outperform all the others all over the spreading procedure. However, different from the observation 2, the degree measure has a short-term better efficiency than the betweenness measure. This degree measure is also suggested by the work [5].

4.4.2 Theoretical Studies

In this subsection, we carry out mathematical analysis in order to theoretically justify the empirical results. To numerically evaluate different measures, we first introduce a new concept, the contagious ability.

Definition 4.1 (Contagious Ability) Given an OSN and an incident of rumor spreading in this network, the contagious ability of an arbitrary node i, A_i, is defined as the number of the following nodes which can be directly or indirectly infected by node i after this node being infected.

An arbitrary user i may possibly get infected at any time in the rumor propagation dynamics. We use A_i^t to denote the contagious ability of node i if the user of this node gets infected at time t. On the basis of our mathematical model, we can then estimate the overall contagious ability of an arbitrary node i as in

$$E(A_i) = \sum_{t=0}^{\infty} \left[P(X_i(t) = Con.) \cdot E(A_i^t) \right] \tag{4.13}$$

OSN users receive and send rumors from and to their neighboring users. We use A_{ij}^t to denote the potential contagious ability caused by the rumor spread from node i to node j at time j. We also introduce P_{ij}^t to denote the potential contagious probability of node j contributed by node i at time t. The mean value of A_i^t can then be recursively worked out as in

$$E(A_i^t) = \sum_{j \in N_i} \left[E(A_{ij}^{t+1}) + P_{ij}^{t+1} \right] \tag{4.14}$$

We can further compute $E(A_i^{t+1})$ and P_{ij}^{t+1} as in

$$\begin{cases} E(A_{ij}^{t+1}) = \delta_{ij}^t \cdot E(A_j^{t+1}) \\ P_{ij}^{t+1} \quad\quad = \delta_{ij}^t \cdot P(X_j(t+1) = Con.) \end{cases} \tag{4.15}$$

where δ_{ij}^t denotes the ratio of node i's contribution to the infection of node j at time t among all the father nodes of node j, and we have

$$\delta_{ij}^t = \frac{P(X_i(t) = Con.) \cdot \eta_{ij}^R}{\sum_{k \in N_j} \left[P(X_k(t) = Con.) \cdot \eta_{kj}^R \right]} \tag{4.16}$$

As shown in Fig. 4.5, the $Imm.$ state is an absorbing state. Given an OSN with finite number of users, we can predict that the spread of rumors finally becomes steady and the values of A_i^t and $P(X_i(t) = Con.)$ converge to zero if $0lleqt \leq \infty$. As a

result, the contagious ability of each node in OSNs can be recursively and reversely worked out by setting a large final time of the spread.

We further calculate the contagious time in order to numerically evaluate the temporal efficiency of those measures against the spread of rumors.

Definition 4.2 Given an OSN and an incident of rumor spreading in this network, the contagious time of an arbitrary node i, T_i, is defined as the mean time of node i getting infected in the whole propagation.

Conceptually, the contagious time of node i, T_i, can be easily computed as in

$$T_i = \sum_{t=0}^{\infty} \frac{P(X_i(t) = Con.) \cdot t}{\sum_{t=0}^{\infty} P(X_i(t) = Con.) \cdot} \tag{4.17}$$

Among the three observations, we mainly focus on the observations 2 and 3 since the observation 1 is practically infeasible in real OSNs. Moreover, previous work [207] has proved that the connection ratio and the link remaining ratio almost reach zero if we remove the top 30% of the most connected nodes from the OSN topologies. Under this situation, the rumors definitely cannot spread out.

Justification 1 (Observation 2) The contagious ability, A_i, denotes the potential number of the following nodes infected by node i. Thus, a node with stronger contagious ability is conceptually more worthwhile for blocking rumors in OSNs. We sort the nodes according to the contagious abilities and choose the result as a benchmark. With different values of λ, we work out the intersection between the benchmark and the sorted nodes of various proactive measures. The results are shown in Fig. 4.11. We can see that the betweenness and degree measures capture more nodes with higher contagious abilities. This may be the reason why the betweenness measure performs best and the second best belongs to the degree measure.

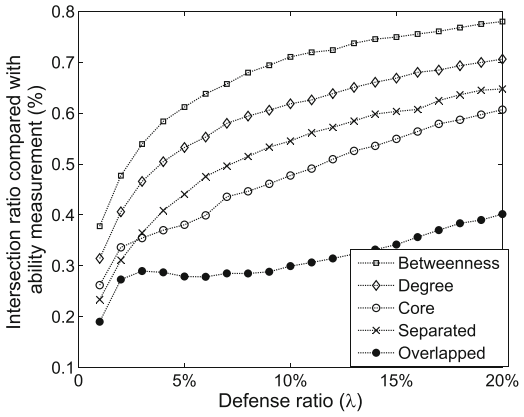

Fig. 4.11 The intersection ratio between the sorted nodes of contagious ability and various proactive measures

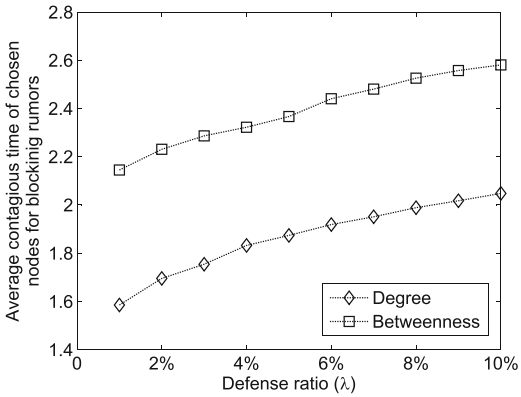

Fig. 4.12 The average contagious time of the degree and betweenness measures when $\lambda < 10\%$

Justification 2 (Observation 3) Let a rumor spread in the network, we then calculate the contagious time of each node in order to justify the superior short-term performance of the degree measure. We can use $\frac{1}{|\omega|}\sum_{i\in\omega} T_i$ to estimate the average contagious time among the nodes in ω. Given a defense ratio λ, ω is the set of nodes chosen for blocking rumors. The results are shown in Fig. 4.12. We can see that the average contagious time of nodes chosen by the degree measure is much less than the nodes chosen by the betweenness measure. This means the nodes with large degrees will be infected earlier. Thus, if we use the nodes chosen by the degree measure to block rumors, the spread in the short-term will be restrained faster compared with the nodes chosen by the betweenness measure.

4.5 Clarify Rumors Using Truths

In this section, we will analyze the remedial measure using the mathematical model. There are mainly two factors, t_{inject} and $E(\eta_{ij}^T)$. They can greatly affect the inject efficiency of restraining rumors by spreading truths.

4.5.1 Impact of the Truth Injection Time

To exclusively investigate the impact of t_{inject}, we typically set $E(\eta_{ij}^R) = E(\eta_{ij}^T) = 0.75$. Based on the spreading dynamics shown in Fig. 4.10, we assign t_{inject} as

- truth starts with rumor,
- truth starts in the early stage of rumor spread,
- truth starts in the late stage of rumor spread.

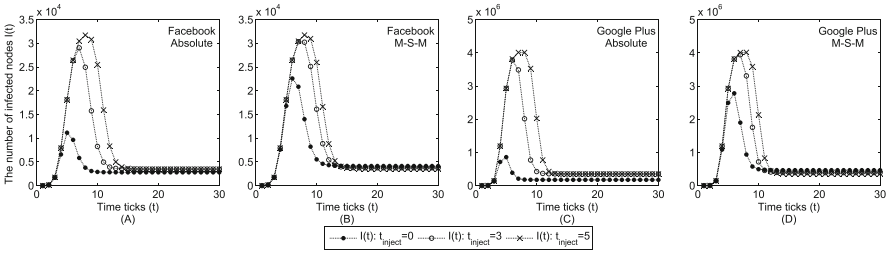

Fig. 4.13 The number of infected users by varying truth injecting time. Setting: $E(\eta_{ij}^R) = 0.75$

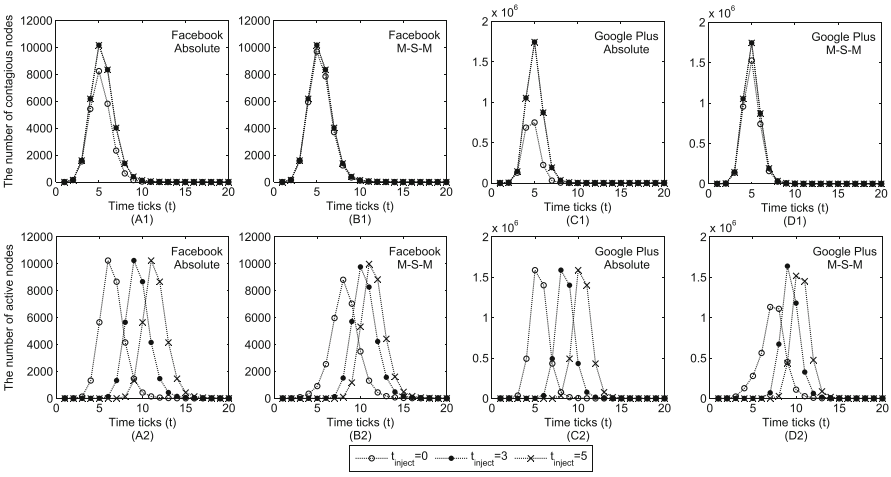

Fig. 4.14 The number of the contagious and the active nodes at any time t in the propagation. Setting: $E(\eta_{ij}^R) = 0.75$

The experiments are executed on both the Facebook and Google Plus networks, and with both the cases of the people making absolute choices and and making M-S-M choices. The results are shown in Fig. 4.13.

Observation 4 *The truth clarification method performs better if the spread of truths starts earlier, but if not, this method has a weak performance in the early stage since the rumors are distributed incredibly fast.* We can see that the propagation scale will decrease dramatically after we inject the truth into the network. Both the spread of rumors and truths will finally become steady. The results in Fig. 4.13 indicate that the remedial measure of spreading truth mainly perform a long-term effectiveness in restraining rumors.

We further investigate the number of the contagious nodes ($\sum_i^m P(X_i(t) = Con.)$) and the active nodes ($\sum_i^m P(X_i(t) = Act.)$) at any time t during the spread. The results are shown in Fig. 4.14. We can see from Figs. 4.14(A1) and 4.14(C1) that t_{inject} has some effect on restraining the number of contagious nodes when people

making *absolute* choices. However in Figs. 4.14(B1) and 4.14(D1), we find t_{inject} has no obvious effect when people making M-S-M choices. Moreover, we can see from Fig. 4.14(A2–D2) that the number of active nodes will take effect according to the value of t_{inject}. The results of Fig. 4.14, both from the number of contagious nodes and active nodes in the propagation dynamics, have well explained the impact of t_{inject} observed in Fig. 4.13.

4.5.2 Impact of the Truth Propagation Probability

To exclusively examine the impact of the truth propagation probability $E(\eta_{ij}^T)$, we typically set $t_{inject} = 3$ and $E(\eta_{ij}^R) = 0.6$. The value of $E(\eta_{ij}^T)$ will be set as

- 0.3: people are not willing to believe the truth,
- 0.6: people fairly believe the truth,
- 0.9: people most likely believe the truth.

Both the Facebook and Google Plus networks will be used in the experiments. Similarly, the cases of people making absolute choices or M-S-M choices will also be considered. The results are shown in Fig. 4.15.

Observation 5 The efficiency of restraining rumors using the remedial measure largely decreases when people are not willing to spread the truths. In accordance with the reality, we find $E(\eta_{ij}^T)$ has extraordinary impact on restraining rumors by spreading truths in OSNs. We additionally examine the number of active nodes $\sum_i^m P(X_i(t) = Act.)$ at any time t during the spread dynamics. As shown in Fig. 4.16, a smaller value of $E(\eta_{ij}^T)$ will lead to a smaller number of active nodes. This exactly corresponds to the limited efficiency of the remedial measure shown in Fig. 4.15.

Given a critical rumor spreading in the network $E(\eta_{ij}^R) > 0.5$, we can summarize two real cases according to the values $E(\eta_{ij}^R)$ as follows:

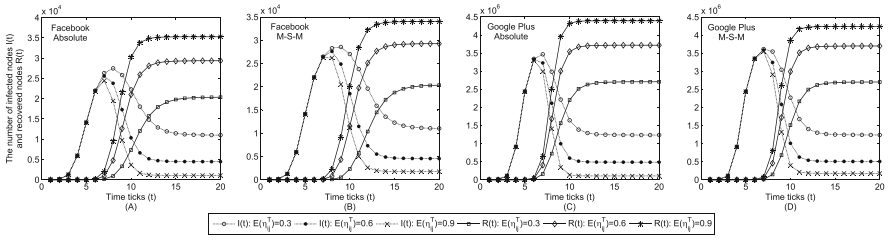

Fig. 4.15 The number of infected nodes and recovered nodes with different values $E(\eta_{ij}^T)$. Setting: $t_{inject} = 3$, $E(\eta_{ij}^R) = 0.75$

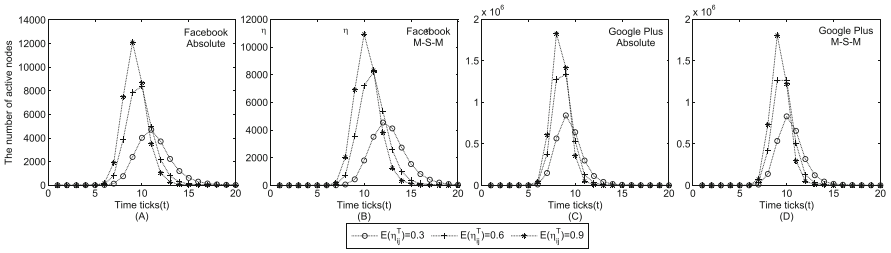

Fig. 4.16 The number of active nodes with different values $E(\eta_{ij}^T)$. Setting: $t_{inject} = 3$, $E(\eta_{ij}^R) = 0.6$

$E(\eta_{ij}^R) > 0.5$ In the real world, through the propaganda or other measurements, people may be willing to believe and spread truths. According to previous analysis, the truth holder can receive an acceptable or even better results by spreading truths to restrain rumors when $E(\eta_{ij}^R) > 0.5$.

$E(\eta_{ij}^R) < 0.5$ According to the results of Fig. 4.15, the remedial measure may not be able to counter the spread of rumors at this case. Actually, this is a common phenomenon always happened in the real world.

4.6 A Hybrid Measure of Restraining Rumors

In this section, we investigate the pros and cons when different measures work together. We also explore the equivalence of these measures.

To numerically evaluate the effectiveness of these measures, we use the maximal number of infected users (I_{max}) and the final number of infected users (I_{final}) to present the damage caused by rumors. In the real world, when either I_{max} or I_{final} becomes larger, more damages will be caused to the society.

4.6.1 Measures Working Together

Firstly, we examine the values of I_{max} and I_{final} on the basis of the mathematical model. We typically set $t_{inject} = 3$ and $E(\eta_{ij}^T)$ ranges from 0.1 to 0.9. The results are shown in Fig. 4.17. We can see that the values of I_{max} always stay large while the values of I_{final} gradually decrease with the increasing $E(\eta_{ij}^T)$. This indicates the remedial measure cannot alleviate the damage denoted by I_{max}. On the contrary, the proactive measures are able to reduce I_{max}.

Secondly, the spread of rumors and truths actually presents a common issue in the psychology field when $E(\eta_{ij}^T) < 0.5 < E(\eta_{ij}^R)$. That is the "rumor has wings while truth always stays indoors" since people naturally have 'negativity bias' on the

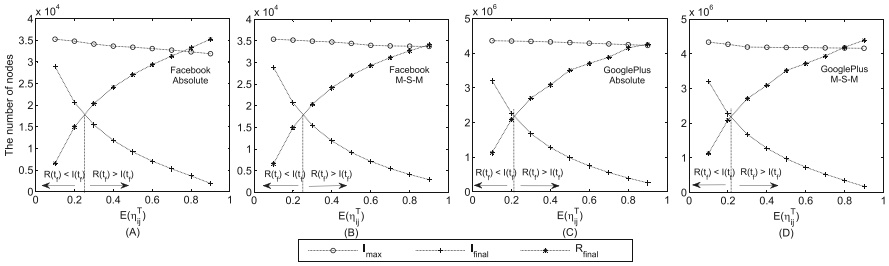

Fig. 4.17 The maximum number of infected users (I_{max}), the final number of infected users (I_{final}) and the final number of recovered users (R_{final}). Settings: $t_{inject} = 3$, $E(\eta_{ij}^R) = 0.75$, $E(\eta_{ij}^R) \in [0.1, 0.9]$

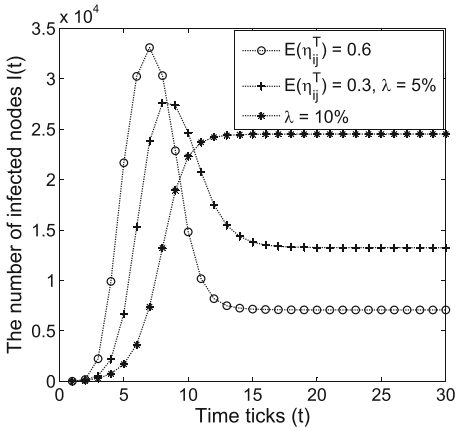

Fig. 4.18 A case study of measures working together. Settings: $t_{inject} = 3$, $E(\eta_{ij}^R) = 0.75$

received information [120]. According to the observation 5, the remedial measure cannot largely reduce the value of I_{final} when $E(\eta_{ij}^T) < 0.5 < E(\eta_{ij}^R)$. We notice in the observation 4 that the remedial measure only has a long-term performance, while in the observation 3 that the degree measure has a short-term best performance.

To address the specific case "rumor has wings while truth always stays indoors", we propose to put the eggs in different baskets. Both the degree measure and the truth clarification method will be used for restraining rumors in OSNs. As an example, we set $E(\eta_{ij}^R) = 0.9$ and $t_{inject} = 3$ to do case study. Besides, $E(\eta_{ij}^T)$ and λ will be assigned as: (1) $\lambda = 10\%$, $E(\eta_{ij}^T) = 0$: proactive measures, (2) $\lambda = 0$, $E(\eta_{ij}^T) = 0.6$: remedial measures, (3) $\lambda = 5\%$, $E(\eta_{ij}^T) = 0.3$: two methods together. The results are shown in Fig. 4.18. We find that if we set $\lambda = 5\%$, $E(\eta_{ij}^T) = 0.3$, both I_{max} and I_{final} will decrease compared with another two extreme settings which can only reduce either I_{max} or I_{final}.

4.6.2 Equivalence of Measures

In the real world, the surveillance on influential users needs much financial support. The propaganda used to prompt the spread of truths also costs much money. Given a limited budget, we explore the equivalence between the proactive and remedial measures in order to leverage these two different strategies.

Firstly, we investigate I_{final} when we apply different defense ratios (λ) and values of $E(\eta_{ij}^T)$ on the propagation of rumors and truths. On the basis of our mathematical model, this part of analysis will disclose the congruent relationship between the values of λ and $E(\eta_{ij}^T)$ in networks. Typically, we set $t_{inject} = 3$, $E(\eta_{ij}^T) = 0.75$ and use the Facebook and Google Plus topologies. The results are shown in Fig. 4.19. Given a pair of λ and $E(\eta_{ij}^T)$, we can find several equivalent solutions with different values of λ and $E(\eta_{ij}^T)$. These different solutions have the same performance as the original pair of λ and $E(\eta_{ij}^T)$. This means we can leverage the proactive and remedial measures according to the fixed budget.

Secondly, we further examine the numeric equivalence in the Facebook and Google Plus networks. We will also consider people making absolute and M-S-M choices. Following the settings of Fig. 4.19, we provide the results in Fig. 4.20. We find the numeric equivalence exists in most cases. On the basis of the results in Fig. 4.20, we are able to identify the exact schema to replace the original pair of λ and $E(\eta_{ij}^T)$. This part of analysis and the results are of great significance from the practical view of point in the real world.

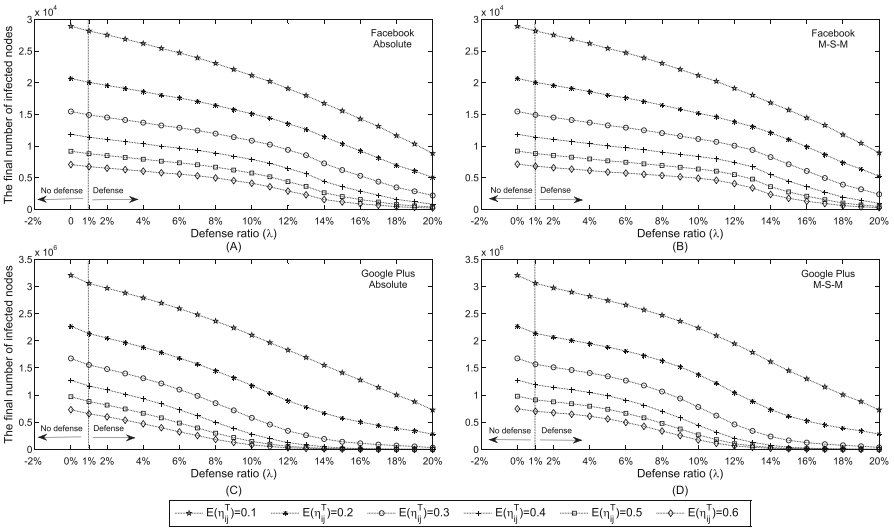

Fig. 4.19 The final number of infected nodes (I_{final}) when we set a series of different defense ratios (λ) and truth spreading probability $E(\eta_{ij}^T)$. Setting: $t_{inject} = 3$, $E(\eta_{ij}^R) = 0.75$

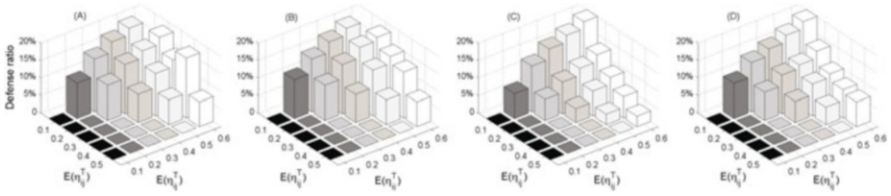

Fig. 4.20 The numeric equivalence between the degree measure and the remedial measure when we set a series of different defense ratios (λ) and truth spreading probabilities $E(\eta_{ij}^{T})$. Setting: $t_{inject} = 3$, $E(\eta_{ij}^{R}) = 0.75$

4.7 Summary

In this section, we first discuss the robustness of the contagious ability. Then, we discuss the fairness to the community bridges when we evaluate the efficiency of restraining rumors. We finally summarize the work in this chapter.

4.7.1 The Robustness of the Contagious Ability

In this section, we firstly discuss the robustness of the contagious ability. According the definition of contagious ability, its usage relies on the rumor spreading origins. However, it can be directly used for numeric evaluation of other measures when the spread of rumors originates from highly connected nodes. To confirm the robustness of this usage, we examine the average degree of contagious nodes, D_t, at each time tick t, as in

$$D_t = \sum_{i=0}^{m} \frac{P(X_i(t) = Con.)}{\sum_{i=0}^{m} P(X_i(t) = Con.)} \cdot d_i. \tag{4.18}$$

wherein d_i is the degree of node i. In the experiments, we randomly choose the rumor origins and average the values of D_t at each time tick t according to 100 runs. The results are shown in Fig. 4.21. It is clear that D_t stays high at the beginning and then sharply decreases till the end of the spread. This means the nodes with higher degrees are more easily to be infected in the early stage. Actually, this feature may be caused by the power-law and the scale-free properties of OSNs [56]. As a result, the contagious ability based on randomly chosen origins will not largely deviate from the ones based on the identical highly-connected origins. This explains the robustness of the usage of the contagious ability.

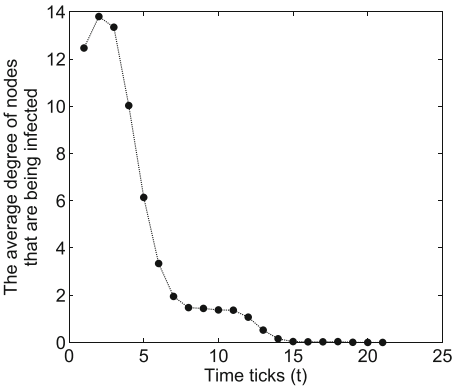

Fig. 4.21 The average degree of nodes that are being infected at each time tick

4.7.2 The Fairness to the Community Bridges

In the real world, people form various communities according to their interests, occupations and social relationships. They are more likely to contact the ones within the same communities. Thus, it would be more precise to consider this premise in our analysis. However, the algorithms (CFinder [28] and NetMiner [130]) have not considered the communication bias between community members. This may cause some unfairness to the community bridges when we evaluate the rumor restraining efficiency.

In fact, the spread of information in community environment is a more complex process. We plan to corporate the communication bias in communities from the records of the real OSNs. This may help us more accurately evaluate the efficiency of different measures. Due to the page limit, we will move this part to our future work.

In summary, we carry out a series of analysis on the methods of restraining rumors. On the basis of our mathematical model, the analysis results suggest that the degree and betweenness measure outperform all the other proactive measures. In addition, we observe that the degree measure has better short-term performance in the early stage. We also investigate the efficiency of spreading truth in order to restrain the rumors. We find the truth clarification method mainly has a long-term performance. In order to address the critical case "rumor has wings while truth always stays indoors", we further explore the strategies of different measures working together and the equivalence leveraging both of them. From both the academic and practical perspective, our work is of great significance to the work in this field.