Chapter 2
Modeling of Epidemic Information Dissemination for MSNs

In this chapter, the modeling of epidemic information dissemination in MSNs is discussed. We introduce two new elements, i.e., pre-immunity and immunity. Then, we study the features of information dissemination for users. Based on the process of the epidemic information dissemination, a novel dissemination mechanism is proposed with four dissemination rules. An analytical model is also developed through ordinary differential equations to mimic epidemic information dissemination.

2.1 Information Dissemination in MSNs

The MSNs [1–4] enable users to exchange and share information via opportunistic peer-to-peer links with short range wireless communication techniques, such as Wi-Fi and Bluetooth [5–8]. With the opportunistic links in MSNs, users adopt store-carry-and-forward mode to disseminate information [9, 10]. When a user moves to the communication coverage area of others, the information can be successfully forwarded; when the user is out of the communication range of others, this user stores and carries the information and waits for the next connection with others.

As users receive information by employing opportunistic contacts (as shown in Fig. 2.1), the user's mobility has a significant impact on information dissemination [11, 12]. However, since the opportunistic peer-to-peer links cannot be easily observed, the procedures of information dissemination are unpredictable. Therefore, a model to analyze the epidemic information dynamics of MSNs is necessary to efficiently capture the realistic features of information dissemination in MSNs.

Although many research studies [13–15] have investigated the analytical model for wireless networks, most of them assume that the transmission path between two nodes is stable so that they cannot be directly applied to MSNs. Moreover, the social ties among users have impacts on information dissemination in MSNs. For example, a

Z. Su et al., *Modeling and Optimization for Mobile Social Networks*,
DOI 10.1007/978-3-319-47922-4_2

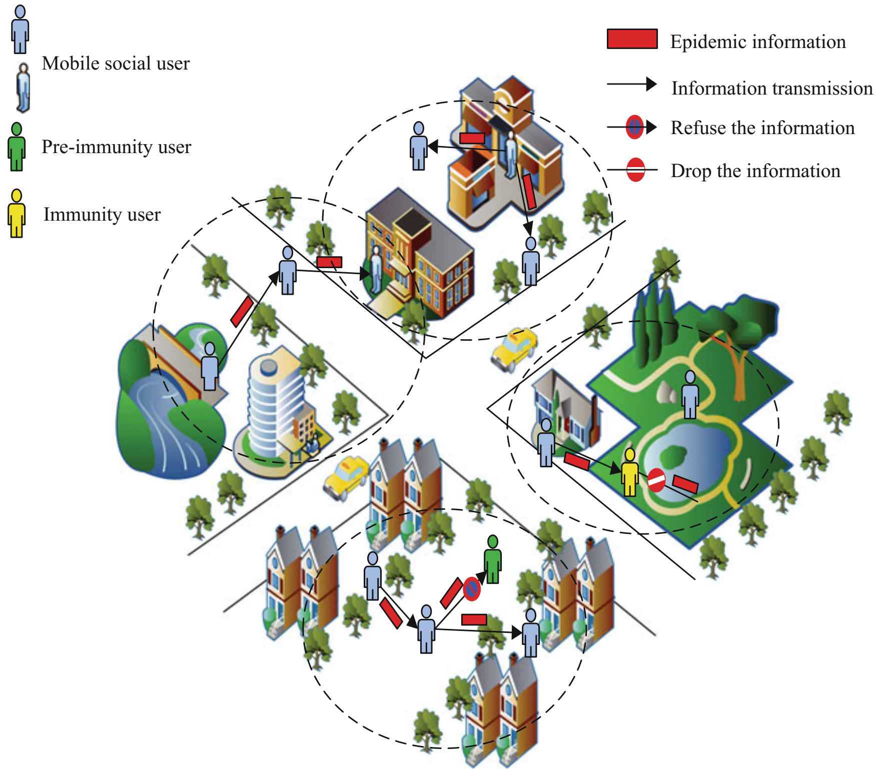

Fig. 2.1 Epidemic information dissemination among users

user may be willing to help forward information from his friends or the users with high social ties instead of a stranger. It is preferred to select social friends to store-carry-and-forward the information other than the users with high mobility. Therefore, how to balance the social tie and mobility becomes a challenging issue for information dissemination in MSNs. In addition, the user's interests may also vary during the information dissemination in MSNs. For example, in a local commercial street, a user has interests in food or Italian restaurant during the lunch time, while he may be interested in clothes and shoes after lunch. As the user changes his interests or social preferences, he would be willing to forward the current interested information rather than the one with old interests. Therefore, it is very important to develop an analytical model to investigate information dissemination in MSNs with the consideration of social impacts.

2.2 Related Work

2.2.1 Epidemic Information Dissemination Model

In the conventional epidemic information dissemination model, users have susceptible, infected and recovered status. Their states can be denoted by S, I and R, respectively. Here, S denotes the susceptible individuals. I denotes the infected individuals who have already obtained the information. R means the ones who are recovered and will not spread information.

The SI model [16] consists of S and I users. The infected users, who spread the information to the susceptible one with a given probability, are the source of the epidemic information spreading. Because S users get infectiousness after being infected, only I users exist at the end of information spreading. The SIS model [17] also has S and I users. In this model, I users can be recovered and then become S users, who may be infected when they contact I users.

Compared with the above models, the SIR [17] model can have R users. If S users are recovered, they will obtain the immunity and change to be R users who do not spread information. In the SIR model, the fraction of infected users grows gradually firstly. Then, the density of I users keeps decreased until 0 due to the low number of S users as time passes. The main difference between SIR model and other models is that there is no infected user in SIR model after information spreading.

All of the above three models focus on capturing the relations among users. They assume that any of the infected user has the possibility to infect other users. However, in real life an S user only infects his friends with the information. Therefore, in MSNs, the user who is to forward the information can only infect his neighbors when they are still not infected.

SCIR model [18] improves the SIR model by further considering the status that a user receives information and has no plan to forward it immediately. This status can also be changed to be infected or refractory. In the SCIR model, the nodes mean the user and the edges denote the relation between them. Zhang et al. [19] shows an information spreading model based on epidemics dynamics, which is an improved SIR model. Based on the topology of nodes and the effect on information spreading, the probability that a susceptible user becomes infectious after getting the information is studied, and the probability that an infected user becomes a recovered user after contacting recovered users is also analyzed. In addition, infected nodes can stop forwarding information with a certain speed.

With the development of mobile networks, more and more information is delivered over the users. Information spreading dynamically varies under the mobile environment, where the mobility of users [20], available bandwidth and communication frequency may affect the performance of spreading. Therefore, new studies related to the information spreading model in MSNs should be given.

2.2.2 General Information Dissemination Model

In traditional social networks, Zou et al. [14] present an Internet e-mail worm simulation model and find that the topology of network has the impact on the spread of e-mail worms in social networks. Wang et al. [15] study a rumor dissemination mode in complex social networks, which is similar to epidemic dissemination among humans. Nekovee et al. [21] introduce a rumor dissemination model in complex social networks and discuss the threshold behavior and dynamics of the model in different networks such as random graphs, scale-free networks, etc. Zhang et al. [19] propose an information dissemination model in online social networks, which considered the degrees of nodes and epidemiology. Zhang et al. [22] present an improved susceptible infectious (SI) model to mimic information spreading in online social networks, by taking the relationship of topology into consideration.

There are also several existing works about information dissemination in mobile networks. Dang and Wu [23] present a cluster-based routing protocol for delay-tolerant mobile networks, where mobile nodes with similar mobility pattern are gathered into a cluster to share limited resources. Taipov et al. [24] propose an efficient data sharing scheme called discover-predict-deliver in delay tolerant smartphone networks, which utilizes a mobility learning algorithm and a hidden Markov model to provide mobility information of individuals. Sammou et al. [25] exploit history contact and frequency of visiting different zones of networks to improve routing protocol. Ma and Jamalipour [26] propose a cooperative cache-based content dissemination framework (CCCDF) to provide caching and cooperative requesting strategies.

Recently, there have been an increasing number of studies on MSNs [27, 28]. Most of these studies focus on content distribution. Nazir et al. [5] present a content delivery scheme to perform relay selection by considering both the mobility patterns and encounter time of users. Using this scheme, content delivery can be optimized with lower end-to-end delay in time critical applications. Bulut and Szymanski [29] present a friendship-based routing scheme to make the forwarding decision with a novel metric which can help each node to define its friendship. By introducing a novel concept called destination cloud, Wang et al. [30] propose a scheme to provide multicasting services with feedback control mechanism in MSNs. Costa et al. [31] present a routing framework called SocialCast for publish-subscribe MSNs, which exploits predictions based on social interaction metrics to identify the best information carrier.

Several existing works investigate modeling information dissemination in MSNs. Sun and Wu [32] present a social aware epidemic forwarding model in MSNs, which studied the end-to-end delivery delay and considered both the limited and unlimited message validity in models. Wu et al. [33] model epidemic-like information dissemination in MSNs with selfish nodes, where the number of hops is limited. AduGyamfi et al. [34] model passive worms spreading in MSNs and carry out the analysis to find an effective antidote to fight against passive worms. Wu et al. [35] present a basic model and an extended model to evaluate the performance of information, where information can be shared between any pair of nodes whether they are friends or not.

Although the existing literature has studied several interesting aspects of MSNs, in most of the aforementioned and other related works, the model reflecting the dynamical social features of mobile nodes in the information has not been thoroughly studied. In this chapter, we develop an analytical model to analyze epidemic information in MSNs, which considers the dynamical characteristics of social features of mobile nodes.

2.3 System Model

In this section, we present the system model consisting of three parts: MSN-based social graph, opportunistic links and information dissemination mechanism.

2.3.1 MSN-Based Social Graph

We consider N mobile nodes (or users) take smartphones to bi-directionally communicate with others and self-organize an MSN, where there are some physical constraints [36] including battery and channel fading. Hence, it is impractical for each node to spread all information to all nodes. The mobile nodes in MSNs select a part of nodes as their friends and have social ties with them to spread information. An undirected social graph $G(V, E)$ is used to represent social ties among the mobile nodes, where V denotes the set of nodes, and E denotes the set of edges among nodes. Nodes in $G(V, E)$ can be the users or devices in MSNs. An edge exists between two nodes if they have a social tie, e.g., relatives, friends, and etc. For simplicity, two nodes which have social ties are considered to be friends in this chapter. The number of the nodes in MSNs is $|V| = N$.

To study the impact of social ties, we need to know the distribution of the friendship. Let $P(k)$ denote the probability that a node has degree k, where the degree of a node in the network refers to the number of its friends. The degree distribution $P(k)$ can be calculated by the fraction of nodes in the network with degree k. Thus, if there are N_k nodes having the degree k, we have $P(k) = N_k/N$.

Existing studies have shown that a great number of social networks have scale-free structures [37]. In other words, $P(k)$ conforms to a power-law distribution [32]:

$$P(k) \sim k^{(-\gamma)}, \gamma \in (2, 3), \tag{2.1}$$

where γ is called skewness of the degree distribution, and can be adjusted according to the scale of the network. Furthermore, the expectation of the degree distribution can be denoted by $\langle k \rangle = \sum_m^{N-1} kP(k)$, where m is the smallest degree of nodes in the network.

2.3.2 Opportunistic Links

Nodes in the MSN communicate with each other in a store-carry-and-forward mode with the short range communication techniques. Only when two nodes come within the transmission range, there is an opportunistic link between them to exchange information. Therefore, the mobility patterns of nodes have a significantly influence on the information dissemination in MSNs. Recently, some complicated models have been employed to predict the mobility patterns of nodes, such as Edge-Markov model [38]. However, due to the complexity, it is still difficult to use the above algorithms in practice. Thus, some simple mobility models are still required, such as [39, 40], although the performance cannot be completely guaranteed. Most of these models indicate that the inter-contact time between two nodes conforms to an exponential distribution [41]. Karagianis et al. [42] also shows that an exponential decay of inter-contact time between mobile devices is reasonable. Therefore, we assume that the inter-contact time between two nodes follows an exponential distribution with parameter λ in this chapter. The probability that two nodes encounter with each other within $[t, t + \Delta t]$ becomes

$$P(T \leq \Delta t) = \int_0^{\Delta t} \lambda e^{-\lambda t} dt = 1 - e^{-\lambda \Delta t}. \tag{2.2}$$

2.3.3 Information Transmission Mechanism

To introduce the information transmission mechanism clearly, nodes in the network can have three states: ignorant, spreading and recovered. A node is ignorant if it is interested in the information but has not yet received it. Nodes that have possessed a copy of information and are willing to disseminate the information to others can be seen as spreading nodes. If a node is not interested in the information and not willing to disseminate it either, this node can be looked upon as a recovered node.

Combined with three states of mobile nodes mentioned above, the detailed information dissemination process is introduced. Usually, users may be willing to help their friends rather than anyone upon contact, which is a practical concern in the real world but ignored in most of previous studies. In MSNs, we consider that there is only one node having the information initially, which is the spreading node. All of other nodes are interested in the information at first, and willing to receive the information. However, most of the nodes cannot always maintain the same interest. Some ignorant nodes may lose the interest later, and refuse to receive it. In other words, an ignorant node can directly become a recovered node, which is called pre-immunity. An information delivery occurs from one node to another node only when they are friends and encounter with each other. In the real world, a spreading node cannot successfully deliver the information to its friends all the time due to the constraints of QoS during data transmission. A spreading node successfully forwards the information to one of its ignorant friends with a certain probability. In addition, a spreading node may stop dissemination when it encounters a recovered friend-node, which is called immunity. Moreover, spreading nodes may stop dissemination without any contacts due to their disinclination to deliver the information.

According to the information dissemination process, we summarize the following four rules.

1. When a spreading node meets an ignorant friend-node, the ignorant node receives the information from the spreading node and becomes a spreading node with probability β, which is called spreading parameter.
2. An ignorant node may lose interests and directly become a recovered node. We assume that this change is based on an exponential distribution with parameter μ, where this assumption is also used in [35].
3. When a spreading node meets a recovered friend-node, the spreader becomes a recovered node with probability δ, which is called immune parameter.
4. Due to the decrease of interest in information, the spreading node may cease delivering information and become a recovered node spontaneously without meeting other nodes. The spreading node becomes recovered node based on an exponential distribution with the parameter ν.

Parameters μ and ν are the self-immune parameter of ignorant nodes and spreading nodes, respectively. According to these four dissemination rules, the state transition diagram of a node can be shown by Fig. 2.2.

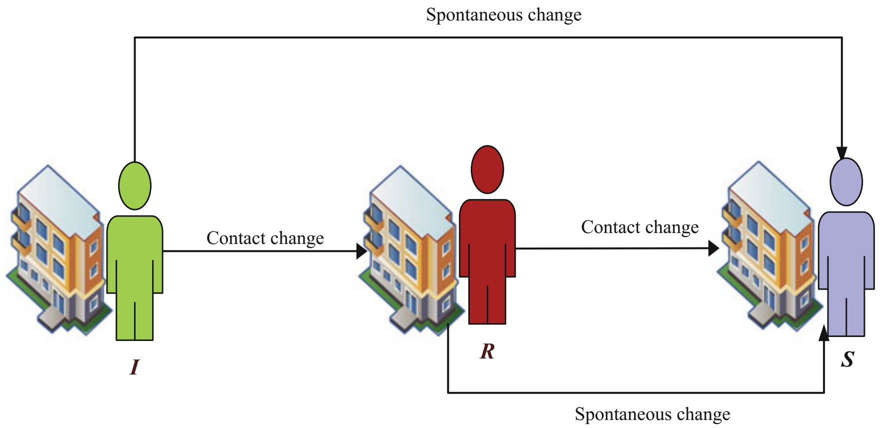

Fig. 2.2 State transition diagram of a node. Symbols I, S, and R represent the ignorant, spreading and recovered state, respectively

2.4 Proposed Analytical Scheme for Information Dissemination

In this section, we develop the analytical model through ordinary differential equations (ODEs) to mimic epidemic information dissemination in an MSN with N nodes, which can move around all the time in a region. The information can be delivered from one node to another only when they encounter and are socially connected with each other. The objective of this chapter is to study the success rate of the information transmission in MSNs, which is the total number of nodes receiving the information over time.

Let $I(k,t)$, $S(k,t)$, and $R(k,t)$ denote the number of ignorant nodes, spreading nodes, and recovered nodes with degree k at time t, respectively. The number of nodes with degree k at time t is represented by $N(k,t)$. In addition, $i(k,t)$, $s(k,t)$ and $r(k,t)$ are defined as the fraction of $I(k,t)$, $S(k,t)$ and $R(k,t)$ in $N(k,t)$, respectively. So we have

$$\begin{cases} i(k,t) = I(k,t)/N(k,t) \\ s(k,t) = S(k,t)/N(k,t) \\ r(k,t) = R(k,t)/N(k,t) \end{cases}, \tag{2.3}$$

where $i(k,t) + s(k,t) + r(k,t) = 1$.

According to the dissemination mechanism, given by the time interval $[t, t+\Delta t]$, we can obtain

$$i(k, t+\Delta t) - i(k,t) = -i(k,t)P(C_k). \tag{2.4}$$

where $i(k, t+\Delta t)$ is the number of ignorant nodes with degree k at time $t + \Delta t$. Parameter C_k denotes the event that an ignorant node with degree k changes its state, and $P(C_k)$ means the probability that this event happens.

In our model, C_k consists of two aspects according to rule 1 and 2. On one hand, an ignorant node may change to be a spreading node (rule 1), which is denoted by A. On the other hand, an ignorant node can spontaneously become a recovered node (rule 2), which is denote by B.

Regarding to event A, it is assumed that an ignorant node with degree k has g friends in the dissemination state. It is independent whether the friend of an ignorant node is a spreading node or not. So the number of spreaders g is a variable that follows a binomial distribution, i.e. $g \sim b(k, w(k,t))$, where $w(k,t)$ represents the probability that the friend of an ignorant node with degree k is a spreading node at time t.

To derive $w(k,t)$, two steps are considered as follows. First, the probability that an ignorant node with degree k has a link with a node with degree k' should be calculated. Second, we obtain the probability that this node is a spreader connected by the ignorant node with degree k. According to [21],

$$w(k,t) = \sum_{k'} P(k'|k) P(s_{k'}|i_k), \tag{2.5}$$

where $P(k'|k)$ denotes the probability that a node with degree k' is the neighbor of a node with degree k. Here, $P(s_{k'}|i_k)$ is defined as the probability that a node with degree k' is a spreading node, under the condition that it connects to an ignorant with degree k. For simplicity, $w(k,t)$ can be approximately written as [14]:

$$w(k,t) \approx \sum_{k'} P(k'|k) s(k',t), \tag{2.6}$$

where $s(k',t)$ denotes the fraction of degree-k' spreading nodes in degree-k' nodes at time t.

Let C_1 denote the event that an ignorant node encounters one of its friends who are in the dissemination state within $[t, t+\triangle t]$. According to (2.2), the probability that this event happens is

$$P(C_1) = 1 - \int_0^{\Delta t} \lambda e^{-\lambda x} dx = 1 - e^{-\lambda \Delta t}. \tag{2.7}$$

The event that an ignorant node receives the information from its dissemination neighbor under the condition that these two nodes have encountered each other is denoted by S_1. The probability of this event is given by

$$P(S_1|C_1) = \beta. \tag{2.8}$$

Combining (2.7) and (2.8), we can obtain the probability that an ignorant node does not receive the information (referred to event NM_1) in the time interval $[t, t+\Delta t]$ as

$$P(NM_1) = 1 - (1 - e^{-\lambda \Delta t})\beta. \tag{2.9}$$

Therefore, the probability $P(A)$ that an ignorant node with degree k becomes a spreader within $[t, t+\Delta t]$ is given by

$$\begin{aligned} P(A) &= 1 - P(\overline{A}) \\ &= 1 - \sum_{g=0}^{k} \binom{k}{g} w(k,t)^g \left(1 - w(k,t)\right)^{k-g} \left(P(NM_1)\right)^g \\ &= 1 - \sum_{g=0}^{k} \binom{k}{g} \left(w(k,t) P(NM_1)\right)^g \left(1 - w(k,t)\right)^{k-g} \\ &= 1 - \left(1 - w(k,t) + w(k,t) P(NM_1)\right)^k \\ &= 1 - \left(1 - w(k,t) + w(k,t)\left(1 - (1 - e^{-\lambda \Delta t})\beta\right)\right)^k. \end{aligned} \tag{2.10}$$

Next, we discuss event B that an ignorant node changes its state to the recovered state spontaneously within $[t, t + \Delta t]$. Let $P(\overline{B})$ denote the probability that an ignorant node remains ignorant. According to information dissemination rule (2), we have

$$P(\overline{B}) = 1 - \int_0^{\Delta t} \mu e^{-\mu t} dt = e^{-\mu \Delta t}. \tag{2.11}$$

Therefore, by combining (2.10) with (2.11), we have

$$\begin{aligned} P(C_k) &= 1 - P(\overline{A})P(\overline{B}) \\ &= 1 - (1 - w(k,t) + w(k,t)P(NM_1))^k \, e^{-\mu \Delta t} \\ &= 1 - \left(1 - w(k,t) + w(k,t)\left(1 - (1 - e^{-\lambda \Delta t})\beta\right)\right)^k e^{-\mu \Delta t}. \end{aligned} \tag{2.12}$$

where the term of $P(\overline{A})P(\overline{B})$ denotes the probability that the ignorant node does not change its state within $[t, t + \Delta t]$. Thus, the probability that the ignorant node changes its state to be spreading or recovered node is $1 - P(\overline{A})P(\overline{B})$.

Based on (2.4), the derivative of $i(k,t)$ becomes

$$\begin{aligned} \frac{\partial i(k,t)}{\partial t} &= \lim_{\Delta t \to 0} \frac{i(k, t + \Delta t) - i(k,t)}{\Delta t} \\ &= -i(k,t) \lim_{\Delta t \to 0} \frac{P(C_k)}{\Delta t}. \end{aligned} \tag{2.13}$$

According to (2.12), in the limit $\Delta t \to 0$, we obtain

$$\lim_{\Delta t \to 0} P(C_k) = \lim_{\Delta t \to 0} 1 - (1 - \theta)^k e^{-\mu \Delta t} = 0, \tag{2.14}$$

where $\theta = w(k,t) - w(k,t)(1 - (1 - e^{-\lambda \Delta t})\beta)$ and $\lim\limits_{\Delta t \to 0} \theta = 0$.

Therefore, the right side of (2.13) conforms to L'Hospital's rule [43]. Thus we can have

$$\begin{aligned} \lim_{\Delta t \to 0} \frac{P(C_k)}{\Delta t} &= \lim_{\Delta t \to 0} \frac{1 - (1 - \theta)^k e^{-\mu \Delta t}}{\Delta t} \\ &= \lim_{\Delta t \to 0} \lambda \beta k w(k,t)(1 - \theta)^{k-1} e^{-\lambda \Delta t} e^{-\mu \Delta t} + \mu e^{-\mu \Delta t}(1 - \theta)^k \\ &= \lambda \beta k w(k,t) + \mu. \end{aligned} \tag{2.15}$$

Combining (2.6), (2.13), and (2.15), we have

$$\begin{aligned} \frac{\partial i(k,t)}{\partial t} &= -\lambda \beta k i(k,t) w(k,t) - \mu i(k,t) \\ &= -\lambda \beta k i(k,t) \sum_{k'} P(k'|k) s(k',t) - \mu i(k,t), \end{aligned} \tag{2.16}$$

For the spreading nodes, we have

$$s(k, t + \Delta t) - s(k, t) = i(k, t)P(A) - s(k, t)P(D_k). \tag{2.17}$$

where D_k denotes the event that a spreading node with degree k becomes a recovered node within $[t, t+\Delta t]$. The probability that this event happens is $P(D_k)$. The variation of the number of spreading nodes is caused by two reasons. One is that the ignorant nodes meet the dissemination friend-nodes and may become the spreading nodes. The other is that the spreading nodes meet the recovered friend-nodes and become the recovered nodes or their states may be spontaneously changed to be recovered. There is an increase in $s(k, t)$ due to the former aspect, while the latter decreases $s(k, t)$.

Similar to C_k, event D_k comprises two aspects according to the information dissemination rule (2) and rule (3). At first, a spreading node may change its status to be recovered (rule 3), which is denoted by event E. In addition, a spreading node can spontaneously become a recovered node (rule 4) denoted by event F.

About event E, we assume that a spreading node with degree k has l friends in the recovered state. Similarly, l is a binomial random variable $l \sim b(k, q(k, t))$, where $q(k, t)$ is the probability that a friend of the spreading node with degree k is a recovered node at time t. Then, we can obtain

$$q(k, t) \approx \sum_{k'} P(k'|k)r(k', t). \tag{2.18}$$

The event that a spreading node meets a friend in the recovered state within $[t, t + \Delta t]$ is denoted by C_2 with a probability as

$$P(C_2) = \int_0^{\Delta t} \lambda e^{-\lambda x} dx = 1 - e^{-\lambda \Delta t}. \tag{2.19}$$

Let $P(S_2|C_2)$ denote the probability that the spreading node becomes a recovered one, under the situation that this node has encountered a recovered friend-node in $[t, t + \Delta t]$. Thus, we have

$$P(S_2|C_2) = 1 - \delta. \tag{2.20}$$

According to (2.19) and (2.20), the probability $P(NM_2)$ that a spreader does not convert to a recovered node in $[t, t + \Delta t]$ becomes

$$P(NM_2) = 1 - (1 - e^{-\lambda \Delta t})\delta. \tag{2.21}$$

The probability $P(E)$ that a spreading node with degree k becomes a recovered node within $[t, t + \Delta t]$ is

$$\begin{aligned} P(E) &= 1 - P(\overline{E}) \\ &= 1 - \sum_{l=0}^{k} \binom{k}{l} q(k,t)^l \left(1 - q(k,t)\right)^{k-l} \left(P(NM_2)\right)^l \\ &= 1 - \left(1 - q(k,t) + q(k,t)P(NM_2)\right)^k \\ &= 1 - \left(1 - q(k,t) + q(k,t)\left(1 - (1 - e^{-\lambda \Delta t})\delta\right)\right)^k . \end{aligned} \tag{2.22}$$

Then, we discuss event F that a spreading node becomes a node in the recovered state spontaneously in $[t, t + \Delta t]$. According to dissemination rule (4), by neglecting event E, the probability $P(F)$ that the spreading node stays in the dissemination state in $[t, t + \Delta t]$ is

$$P(\overline{F}) = 1 - \int_0^{\Delta t} \nu e^{-\nu t} dt = e^{-\nu \Delta t}. \tag{2.23}$$

Combining (2.22) and (2.23), we have

$$\begin{aligned} P(D_k) &= 1 - P(\overline{E})P(\overline{F}) \\ &= 1 - \left(1 - w(k,t) + w(k,t)P(NM_2)\right)^k e^{-\nu \Delta t} \\ &= 1 - \left(1 - w(k,t) + w(k,t)\left(1 - (1 - e^{-\lambda \Delta t})\delta\right)\right)^k e^{-\nu \Delta t}. \end{aligned} \tag{2.24}$$

Based on (2.11), (2.17), and (2.24), by setting $\Delta t \to 0$, we have

$$\begin{aligned} \frac{\partial s(k,t)}{\partial t} &= i(k,t) \lim_{\Delta t \to 0} \frac{P(A)}{\Delta t} - s(k,t) \lim_{\Delta t \to 0} \frac{P(D_k)}{\Delta t} \\ &= \lambda \beta k i(k,t) \sum_{k'} P(k'|k) s(k',t) - \lambda \delta k s(k,t) \sum_{k'} P(k'|k) r(k',t) - \nu s(k,t). \end{aligned} \tag{2.25}$$

For the recovered nodes, we have

$$r(k, t + \Delta t) - r(k,t) = i(k,t)P(B) + s(k,t)P(D_k). \tag{2.26}$$

By combining (2.11) and (2.24), it can be updated as

$$\frac{\partial r(k,t)}{\partial t} = \lambda \delta k s(k,t) \sum_{k'} P(k'|k) r(k',t) + \nu s(k,t) + \mu i(k,t). \tag{2.27}$$

To simplify the problem, by ignoring the correlation of degrees among nodes, the probability that an edge points to a spreading node is independent of the degree of the node from which the edge is emanating. From [44], we have

$$P(k'|k) = \frac{k'P(k')}{< k >}. \tag{2.28}$$

The ODEs of the densities of ignorant, dissemination and recovered nodes become

$$\frac{\partial i(k,t)}{\partial t} = -\lambda\beta k i(k,t)\sum_{k'}\frac{k'P(k')}{< k >}s(k',t) - \mu i(k,t), \tag{2.29}$$

$$\frac{\partial s(k,t)}{\partial t} = \lambda\beta k i(k,t)\sum_{k'}\frac{k'P(k')}{< k >}s(k',t) - \lambda\delta k s(k,t)\sum_{k'}\frac{k'P(k')}{< k >}r(k',t) - \nu s(k,t), \tag{2.30}$$

$$\frac{\partial r(k,t)}{\partial t} = \lambda\delta k s(k,t)\sum_{k'}\frac{k'P(k')}{< k >}r(k',t) + \nu s(k,t) + \mu i(k,t). \tag{2.31}$$

As $\frac{\partial i(k,t)}{\partial t} + \frac{\partial s(k,t)}{\partial t} + \frac{\partial r(k,t)}{\partial t} = 0$, the quantities satisfy the normalization condition where $i(k,t) + s(k,t) + r(k,t) = 1$.

We can obtain the number of nodes in the ignorant state at time t, which is denoted by $I(t)$.

$$I(t) = \sum_{k=m}^{N-1} P(k)i(k,t)N. \tag{2.32}$$

Define $S(t)$ and $R(t)$ as the number of nodes in the dissemination state and recovered state, respectively. We have

$$S(t) = \sum_{k=m}^{N-1} P(k)s(k,t)N. \tag{2.33}$$

$$R(t) = \sum_{k=m}^{N-1} P(k)r(k,t)N. \tag{2.34}$$

According to the above analysis, we can obtain following observations: (1) From (2.29), it can be known that the differential of $i(k,t)$ is negative. So the number of ignorant nodes keeps decreasing gradually. (2) In the earlier stage of the dissemination, there are a few spreading nodes and recovered nodes in the network. Thus, the right side of (2.30) is positive at this moment. However, with the increasing number of spreading nodes and recovered nodes, the differential of $s(k,t)$ becomes negative. Therefore, the number of spreading nodes firstly increases and then gradually decreases. (3) Since the right side of (2.31) is positive, the number of recovered nodes keeps increasing from 0.

Here, in our analytical model developed through the ordinary differential equations, the information is transmitted among nodes based on the distributed MSNs.

By introducing the aforementioned four rules, the process of epidemic information dissemination can be concisely presented, where the computational complexity can be also reduced.

2.5 Performance Evaluation

2.5.1 Simulation Setup

In this section, we conduct trace-driven simulation to validate the proposed analytic model, time evolutions of nodes, and performance of information dissemination. The trace data are from the logs of MSN system developed by Xi'an Jiaotong University, based on the XMPP Protocol. The MSN system is used for the students in the university. And the data for our simulation was taken during the period from Aug. 26, 2013 to Sept. 2, 2013. Based on the communication between two friends, a social graph can be generated by the above trace. We use the largest connected sub-graph of this social graph to conduct our experiments. The basic parameters of this graph are $N = 802$, $E = 1222$, where the average degree is 3.05. The largest degree and smallest degree in the social graph are 72 and 1, respectively, which indicates a large degree fluctuation. Since the existing empirical studies show that the average inter-contact time between two users is around 5 h [40], we determine that the parameter of the exponential distribution of inter-contact is $\lambda = 0.002$ with the unit time of the system as 0.01 h.

2.5.2 Model Validation

To validate the analytical model of epidemic information dissemination, we develop a simulation platform of the epidemic information dissemination in Matlab. Moreover, to compare with other conventional models, the number of infected nodes $F(t)$ is used as the metric, which is the number of nodes receiving information at time t. $F(t)$ can be calculated as follows in our model.

$$F(t) = S(t) + R(t) = \sum_{k=m}^{N-1} +P(k)(s(k) + r(k))N, \; for \mu = 0. \tag{2.35}$$

At the beginning of the simulation, there is only one spreading node picked randomly, while all other nodes are ignorant. To obtain $F(t)$, we set $\mu = 0$, which denotes that all recovered nodes and spreading nodes have received information at time t. The time of information dissemination process T varies from 0 to 5000. For other parameters, we set $\beta = 0.7$, $\delta = 0.3$ [19], and $\nu = 0.0001$ [35]. We compare our model with the conventional models including epidemic forwarding model [32], information dissemination model in online social network [22], and the basic model

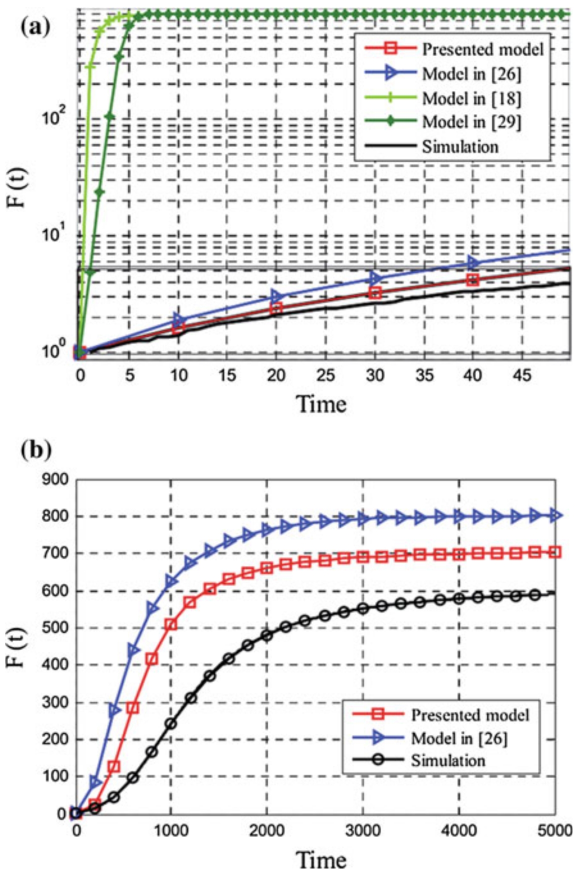

Fig. 2.3 Comparison of models and simulation. **a** Comparison in 45 time slots. **b** Comparison 5000 time slots

in [35]. Through 100 times of simulations, the results in Fig. 2.3 show that the difference between our presented model and the simulation result is the smallest. In addition, it is observed that the other three models have deviations, compared with our model. The reason is that the model in [32] ignores spreading parameter and makes information certainly to be delivered between two friend-nodes when they meet. Therefore, it is faster than our model to deliver information. The model in [22], where the friend-nodes are connected all the time, causes information to be forwarded to the entire network during an extremely short period. The basic model in [35] considers that a node can forward information to any node when they meet. In other words, there is no social relation in the model. Nevertheless, our model, taking into account the social nature and users' behaviors, is consistent with the simulation results. Accordingly, our model can be used to evaluate the effects of relevant parameters on information dissemination.

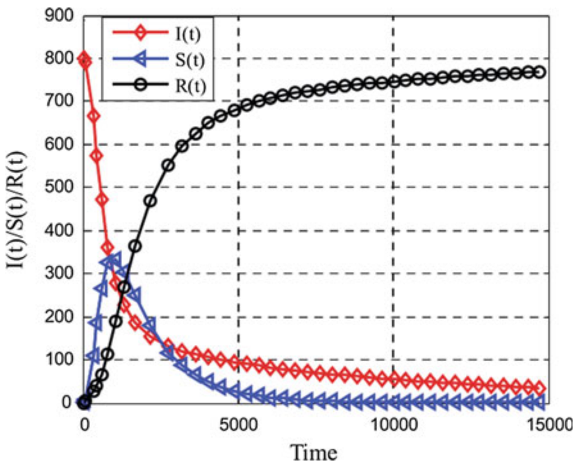

Fig. 2.4 Time evolutions of the number of ignorant nodes, spreading nodes and recovered nodes

2.5.3 Time Evolutions of Nodes

In this subsection, we discuss the time evolution of information dissemination process based on our model. First, we investigate the time evolutions of the number of ignorant, dissemination, and recovered nodes. We only change $\mu = 0.0001$ and $T = 15{,}000$. As shown in Fig. 2.4, the number of spreading nodes $S(t)$ sharply increases at first, and then reaches a peak value. Finally, the number of spreading nodes keeps decreasing until reaching 0. The number of ignorant nodes $I(t)$ sharply falls within an extremely short time. The number of recovered nodes $R(t)$ grows from 0 at a fast rate in a short period. Obviously, these numerical results are consistent with our analysis in Sect. 2.4.

We study the pre-immunity using the presented model. In Fig. 2.4, the value of $S(t)$ becomes around 0 when dissemination time $t = 10{,}000$, which indicates that there is no spreading node in the network. In other words, the information dissemination process is stopped at this moment. At the same time, there are still a few ignorant nodes in the network, which would lose the interest and become recovered nodes gradually. Obviously, the process of transition is considerably slow since the self-immune parameter μ is very small. For example, in Fig. 2.4, the value of $I(t)$ is reduced about 0.2 % in each unit of time when the value of $S(t)$ is almost 0. In order to further exhibit pre-immunity, we set $\mu = 0$ to study time evolutions of the number of three types of nodes without pre-immunity in Fig. 2.5. We can observe that three curves become stable when there is no spreading node in the network. The reason is that ignorant nodes maintain interests all the time if $\mu = 0$, and thus ignorant nodes cannot directly become recovered nodes.

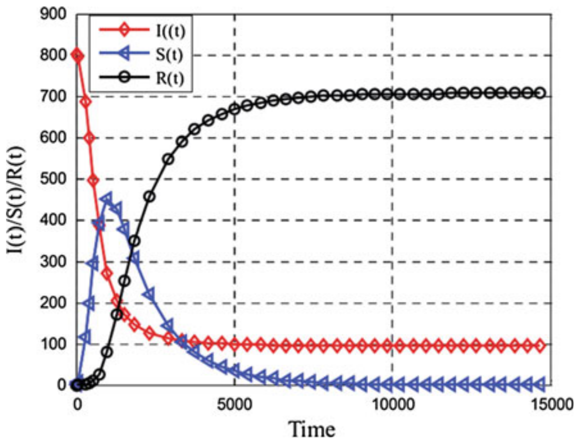

Fig. 2.5 Time evolutions of the number of ignorant nodes, spreading nodes, and recovered nodes, where $\mu = 0$

2.5.4 Performance of Information Dissemination

In this subsection, we evaluate the performance of information dissemination with relevant factors of the proposed model.

2.5.4.1 Effects of Spreading Parameter and Immune Parameter

We evaluate the effects of spreading parameter and immune parameter on the information dissemination. Here, $R(t)$ is used as the performance metric. In order to study the impact of spreading parameter and immune parameter, we ignore the self-immune parameter such that all recovered nodes can have the information under this situation. Here, the spreading parameter β increases from 0 to 1, and four values of δ are randomly chosen for comparison, which are 0.1, 0.3, 0.7, and 1. Other settings are the same as those in Fig. 2.5. Figure 2.6 shows the final number of the recovered nodes R versus different values of β and δ. From Fig. 2.6, it is observed that the information can be still transmitted if β is very small. For example, when $\beta = 0.1$ and $\delta = 0.3$, the number of the recovered node R is close to 200. Another phenomenon is that the final R increases with the increase of the value of β, while the increasing speed decreases gradually. Moreover, the larger immune parameter has smaller value of the final R. A large spreading parameter β can promote information dissemination, while immune parameter δ has a negative effect on information dissemination. Moreover, when δ is smaller, the network is more robust to β. For example, when $\delta = 0.1$, the value of final R remains stable when $\beta > 0.6$.

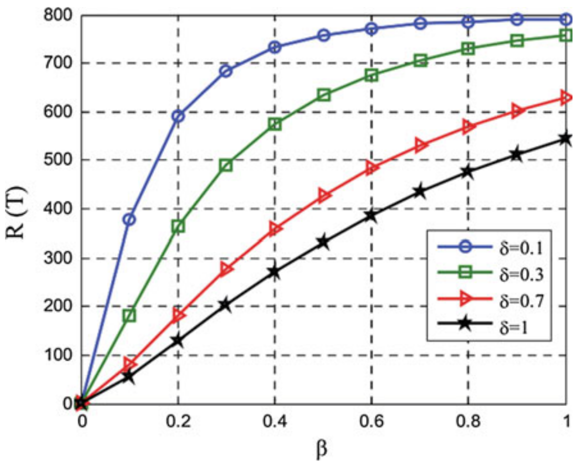

Fig. 2.6 The final number of recovered nodes R with different spreading parameter β and different immune parameter δ

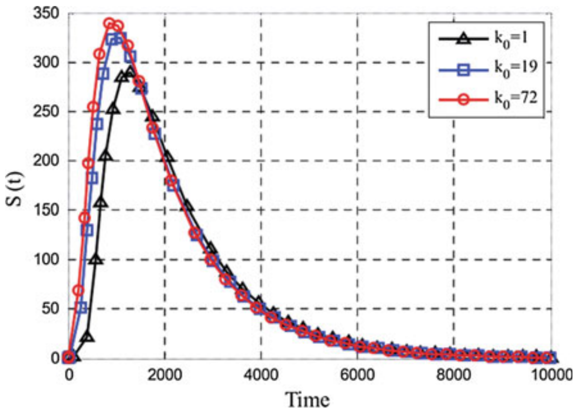

Fig. 2.7 Time evolutions of the number of spreading nodes $S(t)$ with different initial spreading nodes

2.5.4.2 Effects of Node Degree

We study the effect of the initially spreading node with different degrees. We assume that the degree of the initially spreading node is k_0. Three categories of degrees are selected for comparison to study the impact, which are $k_0 = 1$, $k_0 = 19$ and $k_0 = 72$. The result is shown by Fig. 2.7 which describes the time evolutions of the number of spreading nodes $S(t)$ with different initial spreading nodes. It is observed that the initial spreader's degree has a significant effect on information dissemination. When the degree is larger, the information dissemination speed is faster and the peak value of $S(t)$ is also larger. Actually, in MSNs, the nodes with large degree can accelerate the information dissemination, because they can recommend the information to a large number of their friends.

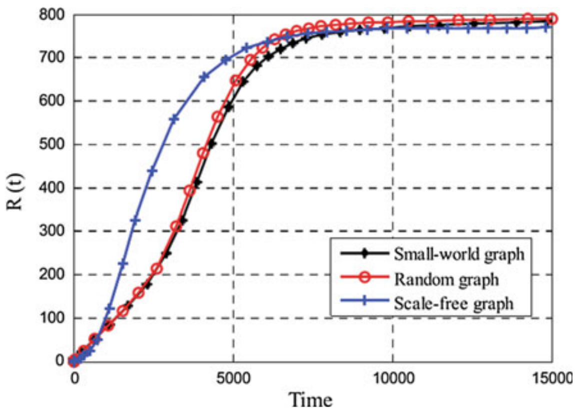

Fig. 2.8 Comparison of information dissemination based on small world graph, random graph and scale-free graph

2.5.4.3 Effects of MSN-Based Social Graph

We evaluate the performance of our model based on different types of MSN-based social graphs, which are scale-free graph model [45], random graph model [46], and small-world model [47]. All of the three networks have the same number of nodes and average degree, where $\langle k \rangle = 2$ and $|V| = 802$. From Fig. 2.8, we can see that the dissemination speed is slower in the small-world graph than that in a random graph. The reason is that the clustering coefficient in the small-world graph is larger than that in the random graph [46]. As the clustering coefficient shows how close the neighbor nodes are, there are many edges interconnected among nodes when the clustering coefficient is large. Therefore, the information is transmitted more quickly and widely in a network. Figure 2.8 also shows that information dissemination in a scale-free graph is the fastest. One reason is that the scale-free graph follows the power-law distribution. If a node with high degree becomes a spreader, a large number of nodes receive information from this spreading node at the early stage of dissemination process. Then, most nodes are spreading nodes and become recovered nodes quickly. Similarly, the recovered node with a higher degree can make spreading nodes to become recovered nodes more quickly. The other reason is that the characteristic path length of the scale-free graph is the smallest compared with others [48]. Here, the characteristic path length represents the average length of the shortest path between two nodes, randomly selected from the graphs [46]. Therefore, in scale-free graph, the information can be quickly delivered to the given node. More details can be seen in [49].

2.6 Summary

In this chapter, we have developed an analytical model to analyze the epidemic information dissemination in MSNs. The model considers the change of mobile nodes' interests by introducing two novel elements called pre-immunity and immunity.

With these elements, we have proposed information dissemination mechanism with four rules for epidemic information dissemination process. According to these four rules, the analytical model has been developed through ordinary differential equations. By conducting extensive trace-driven simulations, we have demonstrated that our analytical model is more accurate than existing ones.

References

1. N. Kayastha, D. Niyato, P. Wang, E. Hossain, Applications, architectures, and protocol design issues for mobile social networks: a survey. Proc. IEEE **99**(12), 2130–2158 (2011)
2. Y. Wang, P. Ren, F. Gao, Z. Su, A hybrid underlay/overlay transmission mode for cognitive radio networks with statistical quality-of-service provisioning. IEEE Trans. Wirel. Commun. **13**(3), 1482–1498 (2014)
3. K. Zhang, X. Liang, X. Shen, R. Lu, Exploiting multimedia services in mobile social networks from security and privacy perspectives. IEEE Commun. Mag. **52**(3), 58–65 (2014)
4. X. Liang, K. Zhang, X. Shen, X. Lin, Security and privacy in mobile social networks: challenges and solutions. IEEE Wirel. Commun. **21**(1), 33–41 (2014)
5. F. Nazir, J. Ma, A. Seneviratne, Time critical content delivery using predictable patterns in mobile social networks, in *Proceedings of the CSE*, vol. 4 (Vancouver, 2009), pp. 1066–1073
6. Y. Zhang, L. Song, W. Saad, Z. Dawy, Z. Han, Exploring social ties for enhanced device-to-device communications in wireless networks, in *Proceedings of the IEEE GLOBECOM* (Atlanta, 2013), pp. 4597–4602
7. Y. Zhang, E. Pan, L. Song, W. Saad, Z. Dawy, Z. Han, Social network aware device-to-device communication in wireless networks. IEEE Trans. Wirel. Commun. **14**(1), 177–190 (2015)
8. Z. Wang, Y. Chen, C. Li, Corman: a novel cooperative opportunistic routing scheme in mobile ad hoc networks. IEEE J. Sel. Areas Commun. **30**(2), 289–296 (2012)
9. Y. Wang, M.C. Chuah, Y. Chen, Incentive based data sharing in delay tolerant mobile networks. IEEE Trans. Wirel. Commun. **13**(1), 370–381 (2014)
10. F. Kevin, A delay-tolerant network architecture for challenged internets, in *Proceedings of the CATAPCC* (New York, 2003), pp. 27–34
11. A. Khosravi, J. Pan, Exploring personal interest in intermittently connected wireless mobile social networks, in *Proceedings of the IEEE CCNC* (Las Vegas, 2011), pp. 503–508
12. H. Zhu, S. Du, M. Li, Z. Gao, Fairness-aware and privacy-preserving friend matching protocol in mobile social networks. IEEE Trans. Emerg. Top. Comput. **1**(1), 192–200 (2013)
13. L. Buttyan, J.-P. Hubaux, *Security and cooperation in wireless networks: thwarting malicious and selfish behavior in the age of ubiquitous computing* (Cambridge University Press, Cambridge, 2007)
14. C. Zou, D. Towsley, W. Gong, Modeling and simulation study of the propagation and defense of internet e-mail worms. IEEE Trans. Dependable Secur. Comput. **4**(2), 105–118 (2007)
15. Y. Wang, X. Yang, Y. Han, X. Wang, Rumor spreading model with trust mechanism in complex social networks. Commun. Theor. Phys. **59**(4), 510–516 (2013)
16. S. Boccaletti, V. Latora, Y. Moreno, Complex networks: structure and dynamics. Phys. Rep. **424**(4), 175–308 (2006)
17. H. Wang, J. Han, L. Deng, K. Cheng, Dynamics of rumor spreading in mobile social networks. Acta Phys. Sin. **62**(11), 1–12 (2013)
18. F. Xiong, Y. Liu, Z. Zhang, Z. Jiang, Y. Zhang, An information diffusion model based on retweeting mechanism for online social media. Phys. Lett. **376**(30), 2103–2108 (2012)
19. Y. Zhang, Y. Liu, H. Zhang, H. Cheng, F. Xiong, The research of information dissemination model on online social network. Acta Phys. Sin. **60**(5), 1–7 (2011)

20. K. Zhang, X. Liang, R. Lu, X. Shen, H. Zhao, Vslp: Voronoi-socialspot-aided packet forwarding protocol with receiver location privacy in msns, in *Proceedings of the IEEE GLOBECOM* (CA, 2012), pp. 348–353
21. M. Nekovee, Y. Moreno, G. Bianconi, M. Marsili, Theory of rumour spreading in complex social networks. Phys. A **374**(1), 457–470 (2007)
22. W. Zhang, Y. Ye, H. Tan, Q. Dai, T. Li, Information diffusion model based on social network, in *Proceedings of the ICMCSA* (Wuhan, 2013), pp. 145–150
23. H. Dang, H. Wu, Clustering and cluster-based routing protocol for delay-tolerant mobile networks. IEEE Trans. Wirel. Commun. **9**(6), 1874–1881 (2010)
24. E. Talipov, Y. Chon, H. Cha, Content sharing over smartphone-based delay-tolerant networks. IEEE Trans. Mob. Comput. **12**(3), 581–595 (2013)
25. E. Sammou, Efficient probabilistic routing in delay tolerant networks, in *Proceedings of the ICMCS* (Tangier, 2012), pp. 584–589
26. Y. Ma, A. Jamalipour, A cooperative cache-based content delivery framework for intermittently connected mobile ad hoc networks. IEEE Trans. Wirel. Commun. **9**(1), 366–373 (2010)
27. K. Zhang, X. Liang, M. Barua, R. Lu, X. Shen, Phda: a priority based health data aggregation with privacy preservation for cloud assisted wbans. Inf. Sci. **284**, 1–12 (2014)
28. K. Zhang, X. Liang, R. Lu, X. Shen, Exploiting private profile matching for efficient packet forwarding in mobile social networks. Oppor. Mob. Soc. Netw. 283–312 (2014)
29. E. Bulut, B. Szymanski, Exploiting friendship relations for efficient routing in mobile social networks. IEEE Trans. Parallel Distrib. Syst. **23**(12), 2254–2265 (2012)
30. Y. Wang, J. Wu, W. Yang, Cloud-based multicasting with feedback in mobile social networks. IEEE Trans. Wirel. Commun. **12**(12), 6043–6053 (2013)
31. P. Costa, C. Mascolo, M. Musolesi, G. Picco, Socially-aware routing for publish-subscribe in delay-tolerant mobile ad hoc networks. IEEE J. Sel. Areas Commun. **26**(5), 748–760 (2008)
32. H. Sun, C. Wu, Epidemic forwarding in mobile social networks, in *Proceedings of the IEEE ICC* (Ottawa, 2012), pp. 1421–1425
33. Y. Wu, S. Deng, H. Huang, Hop limited epidemic-like information spreading in mobile social networks with selfish nodes. J. Phys. A: Math. Theor. **46**(26), 1–14 (2013)
34. D. Adu-Gyamfi, Y. Wang, F. Zhang, M. Domenic, I. Memon, Y. Gustav, Modeling the spreading behavior of passive worms in mobile social networks, in *Proceeding of the ICIII*, vol. 1 (Xi'an, 2013), pp. 380–383
35. Y. Wu, S. Deng, H. Huang, Information propagation through opportunistic communication in mobile social networks. Mob. Netw. Appl. **17**(6), 773–781 (2012)
36. K. Zhang, X. Liang, R. Lu, X. Shen, Pif: a personalized fine-grained spam filtering scheme with privacy preservation in mobile social networks. IEEE Trans. Comput. Soc. Syst. **2**(3), 41–52 (2015)
37. A. Clauset, C. Shalizi, M. Newman, Power-law distributions in empirical data. SIAM Rev. **51**(4), 661–703 (2009)
38. A. Clementi, C. Macci, A. Monti, F. Pasquale, R. Silvestri, Flooding time in edge-markovian dynamic graphs, in *Proceedings of the ACM PDC* (Toronto, 2008), pp. 213–222
39. M. Karaliopoulos, Assessing the vulnerability of dtn data relaying schemes to node selfishness. IEEE Commun. Lett. **13**(12), 923–925 (2009)
40. Y. Li, G. Su, D. Wu, D. Jin, L. Su, L. Zeng, The impact of node selfishness on multicasting in delay tolerant networks. IEEE Trans. Veh. Technol. **60**(5), 2224–2238 (2011)
41. H. Zhu, L. Fu, G. Xue, Y. Zhu, M. Li, L. Ni, Recognizing exponential inter-contact time in vanets, in *Proceedings of the IEEE INFOCOM* (San Diego, 2010), pp. 1–5
42. T. Karagiannis, J.L. Boudec, M. Vojnovic, Power law and exponential decay of intercontact times between mobile devices. IEEE Trans. Mob. Comput. **9**(10), 1377–1390 (2010)
43. R. Boas, Counterexamples to l'hopital's rule. Am. Math. Mon. **93**(9), 644–645 (1986)
44. A. Vázquez, M. Weigt, Computational complexity arising from degree correlations in networks. Phys. Rev. E **67**(2), 1–4 (2003)
45. R. Albert, A.-L. Barabási, Statistical mechanics of complex networks. Rev. Mod. Phys. **74**(1), 47–49 (2002)

46. M. Newman, S. Strogatz, D. Watts, Random graphs with arbitrary degree distributions and their applications. Phys. Rev. E **64**(2), 1–17 (2001)
47. D. Watts, S. Strogatz, Collective dynamics of small-worldnetworks. Nature **393**(6684), 440–442 (1998)
48. B. Tian, D. Towsley, On distinguishing between internet power law topology generators, in *Proceedings of the IEEE INFOCOM* (Orlando, 2002), pp. 638–647
49. Q. Xu, Z. Su, K. Zhang, P. Ren, X. Shen, Epidemic information dissemination in mobile social networks with opportunistic links. IEEE Trans. Emerg. Top. Comput. **3**(3), 399–409 (2015)

http://www.springer.com/978-3-319-47921-7

Modeling and Optimization for Mobile Social Networks
Su, Z.; Xu, Q.; Zhang, K.; Shen, X.S.
2016, XII, 119 p. 41 illus., Hardcover
ISBN: 978-3-319-47921-7