How Robust Is A D2D-Based Messaging Service?

Sigit Aryo Pambudi Wenye Wang
Department of Electrical and Computer Engineering
North Carolina State University, Raleigh, NC 27606
Email: {sapambud,wwang}@ncsu.edu

Cliff Wang
Army Research Office
Research Triangle Park, NC 27709
Email: cliff.wang@us.army.mil

***Abstract*—Motivated by the massive and increasing number of online messaging service users, the idea of utilizing short-range device-to-device (D2D) communication has been adapted to the access of instant messaging services on-the-go, introducing a *D2D-based messaging service* (`D2D-Msg`) paradigm that promises traffic offloading capability and higher data rate. *The quality of message dissemination in such a new paradigm, however, remains largely unknown* due to the open nature of the D2D environment. To address this, we define a node survival probability that captures the impact of random and targeted node failures due to the open wireless environment. Further, to quantify the message dissemination robustness, we define a *secondary infection rate* R^* that measures how fast message propagates initially, and leverage a framework based on probability generating function to analyze R^* under random and targeted failures. Numerical results show that the D2D-Msg is more robust against random failure, the targeted node failure favors communication graph with narrow degree distribution, and R^* is proportional to the ratio between the number of message-receiving users to all users.**

I. Introduction

Online messaging services have successfully facilitated the exchange of vast amount of multimedia information, with at least one out of four people worldwide in 2014 are messaging service users [1]. Among the 700 million active Facebook Messenger users between April 2014 and June 2015, more than 95 % are accessing the service while being mobile [2], thus likely saturating the cellular data and WiFi networks due to the massive data exchanged by the vast amount of users. To offload traffic from the congested infrastructure networks, opportunistic device-to-device (D2D) communications has emerged as a promising alternative to the access of online messaging service over centralized network, leading to a so-called *D2D-based messaging service* (`D2D-Msg`) paradigm. For the vast messaging service users, this new paradigm offers numerous benefits, such as longer battery life and higher data rate due to shorter transmission range [3], as well as lower mobile data subscription fee. These are practical benefits, as exemplified by the "nearby" mode in FireChat app that successfully facilitates message exchange between hundreds of thousands of protesters in Hongkong and Taiwan [4].

Motivated by the vast amount of potential mobile users that may depend their information sharing activities on `D2D-Msg`, there exists a fundamental need to understand the quality of information dissemination in such a new paradigm. Unfortunately, message dissemination in `D2D-Msg` is hindered by the open nature of the wireless communication medium, in which interference and jamming attack may prevent legitimate users from sending and receiving data properly [5]. Toward this, there has been a long history of researches that investigate the impact of node failure to wireless network's performance. For example, the impact of random failure towards the size of connected component in large-scale networks was studied [6], while the network can further be partitioned into small components when the fraction of failed nodes exceeds a certain threshold [7]. But, `D2D-Msg` is different: users may accept and re-share messages from nearby D2D users, as exemplified by FireChat's "public" message feature. Thus, message dissemination performance is governed by both the dynamic underlying communication architecture as well as users' decision towards incoming message. Moreover, in addition to *random* origins, node failure can also be caused by an adversary that launches jamming attacks targeting important nodes with many neighbors, inducing a so-called *targeted* failure. Although both of these failures clearly affect how messages are disseminated, the impacts toward the message dissemination over `D2D-Msg` have not been studied. Thus, we ask, "*What is the robustness of message dissemination under random and targeted failures in `D2D-Msg`?*" The answer to this question is essential toward understanding the performance of `D2D-Msg` that may determine the success of its application.

To answer the research question stated above, we start by examining the `D2D-Msg`'s structure. *First*, motivated by the message dissemination that is highly affected by the architecture of the underlying wireless communication network, we define a *communication graph* to model how users are interconnected through D2D communications. In contrast to static contact networks [8], we introduce a *neighbor exchange* model that swaps the endpoints of to communication edges after every random interval [9] to account for `D2D-Msg` users' movement. *Second,* we also notice that the message dissemination is governed by the users' willingness to accept and spread an incoming content to its neighbor. To model such a decision process, we view a message containing the multimedia content as an infectious disease and leverage the susceptible, infectious, recovered (`SIR`)-based epidemics [9] to capture users' tendency to accept and spread newer messages and discard old ones.

After examining the underlying communication network architecture and the decision process at each user, we take on the problem of analyzing the robustness of message dis-

semination in D2D−Msg. Note that D2D−Msg can be viewed as a medium for exchanging multimedia contents, so that it is highly desirable that the contents can reach as many users as possible. To quantify the coverage of the content-encapsulating message over time, we measure how fast it propagates through the D2D−Msg by employing a *secondary infection rate* R^*, which is defined as the average number of nodes that are infected by infectious nodes in the early stage of the message dissemination but are not patient zero [10]. This metric indicates a threshold, in which the messages can reach all the D2D−Msg users if $R^* \geq 1$, while the message dissemination stops early if $R^* < 1$. Motivated by realistic mobile networks [11] and naturally-occurring networks [12], [13] that exhibit binomial and power law degree distributions, we derive the generating function of the second-generation infections and then take its mean to calculate R^* for both binomial and power law graphs, under random and topology-induced failures.

The message dissemination performance of D2D−Msg is then validated using numerical simulations, which show that D2D−Msg is more robust against random failure, while targeted node failure is demonstrated to favor D2D−Msg with binomial communication graph that has narrow degree distribution. Further, R^* is shown to increase with respect to the node recovery rate β and is inversely proportional to both node infection rate α and neighbor exchange rate ρ. Finally, R^* is shown to be proportional to the ratio between the number of message-receiving nodes divided by the total number of nodes.

The rest of this paper is organized as follows. Section II introduces the D2D−Msg's network model and the problem of analyzing the robustness of D2D−Msg. The secondary infection rate of D2D−Msg is analyzed in Section III, while its performance is evaluated in Section IV. Finally, the paper is concluded in Section IV.

II. Network Model and Problem Formulation

In this section, we introduce the D2D−Msg's network model, and formulate the problem of analyzing the robustness of message dissemination using a secondary infection rate metric.

A. Network Model

Because the message dissemination in D2D−Msg is affected by both the dynamic underlying wireless network and the decision process at each user, we first examine the former. Let $\mathbb{V}$ be the set of $n = |\mathbb{V}|$ users in a D2D−Msg. In this paper, the terms 'user' and 'node' are used interchangeably. We assume that D2D communication using Bluetooth, WiFi Direct, or near-field communication (NFC) technology is employed to enable message exchange between nearby users, and the transmission range r is limited due to battery power constraint. Let $\mathbb{E}_c(t) = \{(u, v) : u, v \in \mathbb{V}, d_{(u,v)}(t) \leq r\}$ be the set of communication edges (or *contacts*) at time $t \in (0, \infty)$, e.g., node pair $(u, v) \in \mathbb{E}_c(t)$ are within the transmission distance of each other ($d_{(u,v)}(t) \leq r$) and can communicate directly at time t. Put together, $\mathbb{E}_c(t)$ and the collection of users $\mathbb{V}$ form a tuple $\mathbb{G}_c(t) := (\mathbb{V}, \mathbb{E}_c(t))$ that is referred as a *communication graph*, which describes the message exchange opportunity between users that can be exploited for disseminating multimedia contents as messages in a D2D−Msg. In this paper, we assume that $\mathbb{G}_c(t)$ is *connected* [14] for all $t \in (0, \infty)$.

Since the D2D−Msg users are mobile, any pair of users may come into and out of each others' contact during the network lifetime. Thus, contacts are transitory events and the endpoints of a user's contacts change in time. To capture such heterogeneity and dynamism, we employ a *neighbor exchange* (NE) model [15] as a simple extension of the static contact-based communication network model. Let $e_i = (u, v) \in \mathbb{E}_c(t)$ be a communication edge. In the NE model, an endpoint of e_i is exchanged with an endpoint of another randomly-selected edge $e_j = (u', v') \in \mathbb{E}_c(t)$, e.g., $(u, v) + (u', v') \rightarrow (u, v') + (u', v)$, after every random interval that is exponentially-distributed with rate $\rho/2$. Since e_i can also be selected by another edge $e_k \neq e_j$, then every edge is swapped with an effective rate of ρ, which is proportional to the inverse of average node contact time [16]. Note that in NE, the degree of each node is *fixed* although their neighbors changes over time, such that if the likelihood that an edge occurs between every pair of nodes exceeds certain threshold [14], $\mathbb{G}_c(t)$ is *almost surely* connected for all $t \in (0, \infty)$.

After defining the communication graph $\mathbb{G}_c(t)$ and how its dynamics are captured using the NE model, we examine how messages are disseminated through the D2D−Msg. Let m be a message containing a multimedia content and $\mathcal{N}_c(u, t) = \{v : d_{(u,v)}(t) \leq r\}$ be the set of all communication neighbors of u. Let user u carries m and decides to spread it to the communication neighbors, $\mathcal{N}_c(u, t)$. The immediate questions are, "Will a neighboring node $v \in \mathcal{N}_c(u, t)$ decide to accept the incoming message? Further, until when will node u carry and spread m?" To answer these questions, let us view message m as an *infectious* disease such that upon being infected, user v will try to spread the infection to its communication neighbors. Then, we can define three states for node v: (i) *susceptible* (S), in which v has not been infected by m; (ii) *infectious* (I), where v is infected and actively spreads m; and (iii) *recovered* (R), in which v is healed and becomes immune to m. Note that the R state is necessary in the message dissemination process over D2D−Msg, since in practice users will not accept previously-accepted contents. To model how users transition between the SIR states, we follow the SIR-type epidemics for infectious diseases [9] and assume that an infectious node transmits m along each of its edge at a constant *infection rate* of α, causing susceptible neighbors to enter the I state, while infected users enter the R state with a constant *recovery rate* of β. Combined with $\mathbb{G}_c(t)$ that describes the set of next nodes to be infected, message dissemination over the D2D−Msg can be viewed as an SIR-based disease dynamics over the time-varying communication graph.

An illustration of how disease dynamics over the communication graph governs message dissemination in D2D−Msg is depicted in Fig. 1. Let user v_4 be in the I state at time $t = 0$

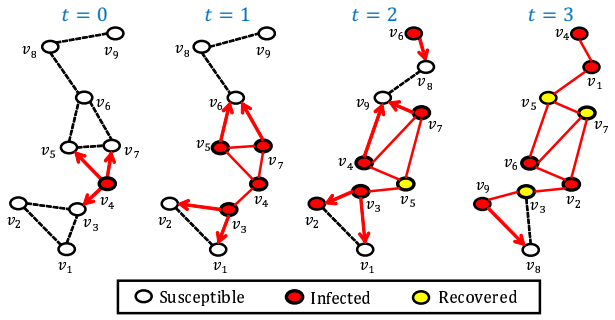


Fig. 1. Illustration of message dissemination over D2D−Msg.

and tries transmit m along its edges to users v_3, v_5, and v_7. As a result, these former three nodes becomes infected at $t = 1$ and also try to transmit m to their neighboring users. Since m is transmitted with rate α, users v_2 and v_6 becomes infected at time $t = 2$, but user v_1 remains at the same state. Additionally, due to the recovery rate β, v_5 decides to drop the message and enters R state. Note that the connectivity changes at this time due to the mobile users' movement, which is captured by the aforementioned NE model. At the next time, $t = 3$, v_1 and v_9 enters the I state, while v_3 and v_7 enters the R state. Eventually, depending on α, β, and the NE model, the message may or may not reach all the D2D−Msg users.

B. Problem Formulation

In a D2D−Msg, the open nature of the D2D wireless communication channels leads to numerous source of impairments. For example, an adversary may launch a randomized jamming attack [5] to prevent legitimate D2D−Msg users to exchange messages with their neighbor, or the D2D−Msg users simply cannot exchange messages because the noise floor is too high, resulting to *random* node failure. On the other hand, the adversary may concentrate the jamming attack to important nodes with large number of neighbors [5], resulting to node failure that is induced by the connectivity of the communication graph, referred as a *targeted* node failure. Both the random and targeted failures will disable D2D−Msg users' ability to spread m and hinder the message dissemination process. Intuitively, the extent of damage caused by these two failure types to the message dissemination will be different, such that we define the following model to capture such discrepancy. Let $k_u(t) = |\mathcal{N}_c(u,t)|$ be the communication degree of node $u \in \mathbb{V}$. For a D2D−Msg node with communication degree of k, let $\Phi_s(k)$ be a *failure survival probability*, i.e., the likelihood that the node does not fail and can still exchange messages over the D2D−Msg. Then, we have the following definition.

Definition 1: (Random and Targeted Failures) Random node failure is defined as the case where $\Phi_s(k) = \phi$ with $\phi \in [0,1]$ is a positive constant, while targeted node failure is the case where $\Phi_s(k) = c^k$ with $0 < c < 1$.

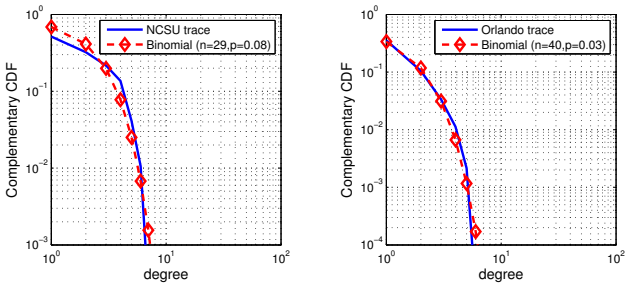
Since $\Phi_s(k)$ depends on k, then we define a *degree distribution* $p_k = Pr\{k_u(t) = k\}$ to capture the structure of $\mathbb{G}_c(t)$ [17] as well as the probability that an arbitrary node will fail.

After discussing how to model the random and targeted node failures, let us proceed by examining the message dissemination process over the D2D−Msg. As a medium of exchanging multimedia contents between its users, it is desirable that the messages as the content vessels can reach as many users as possible. This is in line with the users' desire that the content they shared becomes popular and wide spread among D2D−Msg users. For example, FireChat's public nearby mode had been used during the Hongkong protest to spread logistical information, such as the location of available water bottles, to maintain the survival of the protesters [4]. As the number of message recipient increases, more users can benefit from such information. On the other hand, message epidemics is also desirable from a commercial point-of-view, capturing advertisers' goal of delivering advertisement contents to all users through viral marketing [18]. Motivated by such usefulness, we want to study the robustness of message dissemination over D2D−Msg by quantifying the message coverage with respect to impairments due to random and targeted node failures.

To quantify the coverage of the message dissemination, we measure how fast a message propagates over the D2D−Msg. This is motivated by the fact that the SIR infection dynamics consists of both a *birth* and a *death* processes characterized by infection rate α and recovery rate β, respectively. If the birth rate of newly-infected users, e.g., those who accept and spread m, is faster than the death (recovery) rate, then message m may reach all the users. The birth-death in the D2D−Msg, however, operates on top of a dynamic communication network that is impaired by random and targeted failures, such that conventional analysis based on SIR-based epidemics [19] cannot be employed. To simplify the analysis of the birth-death process over the dynamic connectivity problem of the D2D−Msg, we concentrate on the early stage of the message infection and start with the following definition.

Definition 2: (Secondary Infection Rate [10]) Secondary infection rate R^* is defined as the number of message transmissions per unit time from an infected node $u \in \mathbb{V}$, which is chosen proportional to $k_u(t)$, by assuming that all of the neighboring nodes are susceptible except one that infected u.

Let *patient zero* be the nodes that initially spreads message m at $t = 0$, e.g., $\{v_4\}$ in Fig. 1. Then, the secondary infection rate R^* is proportional to the number of nodes that are contaminated by the nodes infected directly by the patient zero, and represents the effective message infection rate in the D2D−Msg. The higher R^*, the more likely that all nodes will become infected by m quickly. In terms of message dissemination coverage, R^* is known to indicate an *epidemic* threshold, in which m may reach all the D2D−Msg users if $R^* \geq 1$, while the infection dies out early and m only reaches a finite fraction of users if $R^* < 1$ [10]. In view of D2D−Msg as an information exchange medium, we want $R^* \geq 1$ such that messages can reach all users. However, the random and targeted failures in the D2D−Msg may prevent such condition to occur. Motivated by this, we ask "*What is the impact of random and targeted node failures to the secondary infection*



(a) NCSU ($MSE = 1.06\%$). (b) Orlando ($MSE = 0.44\%$).

Fig. 2. CCDF of node degree in `ncsu/mobilitymodels` data set [11].

rate, R^*, of a D2D-Msg?" The answer may serve as a key to determine the success of D2D-Msg's deployment.

III. Message Dissemination Robustness of Opportunistic Social Network

In this section, we start by describing a method of calculating R^* based on the generating function of the communication degree distribution. Then, based on realistic network traces [11] and naturally-occurring networks [12], [13], we analyze R^* for D2D-Msg with binomial and power law-distributed communication degree under random, targeted, and no failures.

A. Secondary Infection Rate Analysis

To take on our main objective of studying the impact of random and targeted node failures toward the secondary infection rate R^*, recall that there are three main mechanics behind the message dissemination process over D2D-Msg: (i) a time-varying D2D communication, which is parameterized using both NE rate ρ and degree distribution p_k; (ii) the SIR dynamics of message infection, which is captured by the infection rate α and recovery rate β; and (iii) node failures due to network impairments, which is parameterized by the node survival probability $\Phi_s(k)$. We employ these four parameters to calculate R^* as follows. Let *transmissibility* τ be the likelihood of an S node to be infected by an I node through a communication edge and let $g(x) = \sum_{k=0}^{n-1} p_k x^k$ be the communication degree distribution's generating function.

Theorem 1: The secondary infection rate of a D2D-Msg is

$$R^* = \tau \left(\frac{\rho}{\beta} + \frac{\beta + \rho}{\beta} \frac{\tilde{g}''(1)}{g'(1)} \right), \tag{1}$$

where $\tau = \frac{\alpha}{\alpha+\beta+\rho}$ and $\tilde{g}(x) = \sum_{k=0}^{n-1} \Phi_s(k) p_k x^k$.

Proof: Note that the passage of SIR-based infection over dynamic contact networks has been studied in [10]. Different to such existing study, each D2D-Msg node considered in this paper fails with survival probability $\Phi_s(k)$. Thus, to derive (1), we borrow the existing result in [10] and incorporate $\Phi_s(k)$ into the formulation of R^*. To do this, we employ the excess degree distribution $q_k = \frac{k p_k}{\mathbb{E}[K]}$, which is the degree distribution of a node with degree k selected with probability proportional to k but discounting one of its edges, and multiply it with $\Phi_s(k)$. Let *second generation infected* (SGI) be the nodes that are infected by the message from patient zero. Then, the average number of potential transmissions by the SGI [10, eq. (3.9)] is generated by $\tilde{H}_1(x) = \frac{\beta}{\beta-\rho(x-1)} + \sum_k \frac{\Phi_s(k) q_k x^{k-1} \beta}{\beta-\rho(x-1)(k-1)}$. The distribution of actual transmission by the SGI is approximately generated by $H_1(x) = \tilde{H}_1(1-\tau+\tau x)$ where $\tau = \frac{r}{r+\beta+\rho}$ [9, Eq. (3.4)], and the mean of the distribution is equal to R^*. Let us define $\tilde{g}(x) = \sum_{k=0}^{n} \Phi_s(k) p_k x^k$. Then, we can formulate

$$\begin{aligned} \tilde{H}_1'(1) &= \left[\frac{\beta\rho}{(\beta-\rho(x-1))^2} + \beta \sum_k \Big((k-1)\Phi_s(k) q_k x^{k-2} \right. \\ &\times \frac{\beta}{\beta-\rho(x-1)(k-1)} + \left. \frac{\Phi_s(k) q_k x^{k-1} (k-1)\beta\rho}{(\beta-\rho(x-1)(k-1))^2} \Big) \right]_{x=1}, \\ &= \frac{\rho}{\beta} + \frac{\beta+\rho}{\beta} \frac{\tilde{g}''(1)}{g'(1)}, \end{aligned} \tag{2}$$

with the secondary infection rate is calculated as $R^* = \frac{d}{dx} \tilde{H}_1(1-\tau+\tau x)|_{x=1} = \tau \tilde{H}_1'(1)$. ■

B. Secondary Infection Rate of Binomial Graph

From the derivation of the secondary infection rate in Thm. 1, we notice that (1) is a function of the degree distribution p_k. In order to perform an accurate secondary infection rate analysis we ask, "*what is the degree distribution of realistic communication graph?*" To answer this, we employ the `ncsu/mobilitymodels` traces [11], set the transmission range to $r = 50m$, and take the snapshot of $\mathbb{G}_c(t)$ at every $\Delta t = 1s$ time interval. The result for campus and theme park environments in Figs. 2(a) and 2(b), respectively, indicate that the communication degree distribution can well be modeled using a binomial distribution $p_k^{bin} = \binom{n-1}{k} p^k (1-p)^{n-k-1}$, which is verified by the low mean-squared error (MSE) values. Note that although not shown here due to space limit, similar observation holds for various other combinations of r and Δt.

After showing that the degree distribution of the communication graph based on realistic D2D wireless network follows a binomial distribution, we are ready to analyze the secondary infection rate of a D2D-Msg. Let us denote R_{nf}^*, R_{rf}^*, and R_{tf}^* as the secondary infection rates of D2D-Msg under no failure (NF), random failure (RF), and targeted failure (TF) models, respectively. Here, the NF model is included as a baseline for RF and TF. To maintain fairness, the average node survival probabilities of TF and RF models are set equal, e.g., $\phi = \sum_{k=0}^{n-1} p_k c^k = g(c)$. We have the following corollary.

Corollary 1: The secondary infection rates of D2D-Msg with binomial-distributed communication degree are given as

$$R_{nf}^* = \frac{\tau\rho}{\beta} + \frac{\beta+\rho}{\beta}\tau\lambda, \tag{3}$$

$$R_{rf}^* = \frac{\tau\rho}{\beta} + \frac{\beta+\rho}{\beta}\tau\lambda e^{\lambda(c-1)}, \tag{4}$$

$$R_{tf}^* = \frac{\tau\rho}{\beta} + \frac{\beta+\rho}{\beta}\tau\lambda c^2 e^{\lambda(c-1)}. \tag{5}$$

Proof: We assume that n is large, p is small, and approximate the degree into a Poisson distribution $p_k \approx \frac{\lambda^k e^{-\lambda}}{k!}$

with $\lambda = np$. For the case of no node failure, we have $\tilde{g}(x) = g(x) = e^{\lambda(x-1)}$, such that $g'(1) = \lambda$ and $\tilde{g}''(1) = \lambda^2$ can be used to obtain (3). For random failure, $\tilde{g}(x) = \phi e^{\lambda(x-1)}$ and the normalization $\phi = g(c)$ can be used to get (4). Similarly, (5) is obtained by employing $\tilde{g}(x) = \sum_k \frac{(cx)^k \lambda^k e^{-\lambda}}{k!} = e^{\lambda(cx-1)}$ for the targeted failure model. ■

Because $0 < c < 1$, we know that $R^*_{tf} < R^*_{rf} < R^*_{nf}$. Since R^* indicates how fast the message coverage increases, then the NF case exhibits the best message dissemination performance, followed by the RF case. The TF case in (5) shows the lowest secondary infection rate, such that the threshold $R^* = 1$ may not be achieved in some cases, resulting in the message to reach only a finite fraction of the D2D-Msg users.

Remark 1: Note that infection epidemic size has been shown to be proportional to R^* [9], such that the messages in TF and NF will respectively reach the least and most number of users. This indicates the results for D2D-Msg in (3)-(5) differs from the existing study [8] that shows both targeted and random immunizations, which are the counterparts of node failures in D2D-Msg, yield the *same* epidemic size for *static networks* with Poisson-distributed contact degree.

C. Secondary Infection Rate of Power Law Graph

In the previous subsection, we have derived the secondary infection rate for binomial-distributed communication graph. In real-life, however, many contact networks, such as user friendships in social networking services [12] and autonomous system (AS)-level connectivity [13], have been shown to exhibit a power law degree distribution. Note that the binomial distribution in Fig. 2 can be approximated into a Poisson distribution, which belongs to the family of exponentially-tailed distributions. Moreover, the exponential-tailed and power law distributions of inter-meeting time is shown to be tightly-related, separated only by whether the network area is bounded [20]. To this end, motivated by the wide prevalence of power law graphs and its close relationship with binomial distributions, we also examine the secondary infection rate for D2D-Msg with power law-distributed communication graph as follows. Let $p_k^{power} = k^{-s}/\sum_{k=0}^{n-1} k^{-s}$ be a power law-distributed communication degree with a power law exponent $s > 2$. Again, we normalize $\phi = g(c)$ to maintain fairness. Then, we have the following corollary.

Corollary 2: The secondary infection rates of D2D-Msg with power law-distributed communication degree are

$$R^*_{nf} = \frac{\tau\rho}{\beta} + \tau\frac{\beta+\rho}{\beta} \times \frac{\sum_k (k^{2-s} - k^{1-s})}{\sum_k k^{1-s}}, \quad (6)$$

$$R^*_{rf} = \frac{\tau\rho}{\beta} + \tau\frac{\beta+\rho}{\beta} \times \frac{\sum_k c^k k^{-s}}{\sum_k k^{-s}} \times \frac{\sum_k (k^{2-s} - k^{1-s})}{\sum_k k^{1-s}}, \quad (7)$$

$$R^*_{tf} = \frac{\tau\rho}{\beta} + \tau\frac{\beta+\rho}{\beta} \times \frac{\sum_k c^k (k^{2-s} - k^{1-s})}{c^2 \sum_k k^{1-s}}. \quad (8)$$

Proof: For no node failure, we have $\tilde{g}(x) = g(x) = \sum_k x^k k^{-s}/\sum_k k^{-s}$, such that $g'(1) = \sum_k k^{1-s}/\sum_k k^{-s}$ and $\tilde{g}''(1) = \sum_k (k^{2-s} - k^{1-s})/\sum_k k^{-s}$ can be used to obtain (6). For the case of random node failure, $\tilde{g}(x) = \phi g(x)$ such that $\tilde{g}''(1) = \phi \sum_k (k^{2-s} - k^{1-s})/\sum_k k^{-s}$ and the normalization $\phi = g(c)$ can be used to get (7). Similarly, (8) can be obtained by employing $\tilde{g}(x) = \sum_k c^k x^k k^{-s}/\sum_k k^{-s} = g(cx)$ and $\tilde{g}''(1) = c^2 g''(c)$ for the targeted failure model. ■

The corresponding secondary infection rates in (6)-(8) will be analyzed numerically in the next section.

IV. Numerical Simulations

Recall that our main objective is to analyze how robust message dissemination over D2D-Msg is with respect to random and targeted failures in the underlying communication layer. To do so, we consider binomial and power law communication graphs and then compare their secondary infection rate and epidemic size of message dissemination using numerical simulations. To ensure fair comparison, the mean degree of both communication graphs are set to be equal, *e.g.* $\lambda = \sum_{k=0}^{n-1} k^{1-s}/\sum_{k=0}^{n-1} k^{-s}$. We write our own source codes in python and C++ to get the results in Sections IV-A and IV-B, respectively. Unless specified otherwise, the simulation parameters are $(\alpha; \beta; c; s; \rho) = (0.2; 0.1; 0.8; 2.1; 0.05)$.

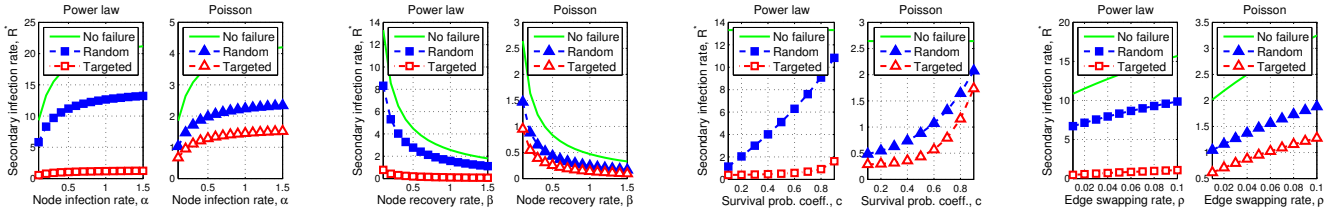
A. Secondary Infection Rate

To study the robustness of message dissemination over D2D-Msg, we first examine the secondary infection rate with respect to the SIR dynamics. According to (1), R^* is a linear function of the the transmission probability τ, which is increasing against infection rate α. Higher α means a node will spread m more often. Thus, R^* should increase with respect to α for both power law and binomial-distributed communication graphs, which is verified in Fig. 3(a). On the other hand, we can see that R^* decreases with respect to the node recovery rate β from Fig. 3(b). As β increases, the time interval in which a node can infect other node(s) is smaller, thus reducing the effective number of secondary-infected nodes.

Next, we examine the impact of survival probability coefficient c to R^* in Fig. 3(c), in which R^* is shown to increase with respect to c. Higher c means the total number of failed nodes is lower, such that more nodes can receive message m during the secondary infection. Note that R^*_{rf} and R^*_{tf} approaches R^*_{nf} as $c \uparrow 1$.

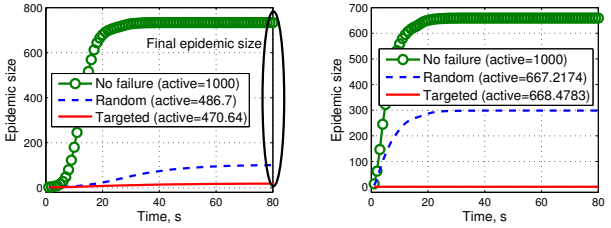
The impact of edge swapping rate ρ to R^*, on the other hand, is studied through Fig. 3(d). When the edge is swapped using the NE model more often, it will effectively be connected to more nodes during a fixed time interval, which implies that the number of opportunities to infect another susceptible node is also higher. Thus, R^* will increase with respect to ρ.

Finally, by comparing the results from different $\mathbb{G}_c(t)$ types in Fig. 3, we observe that the power law-distributed communication graph generally exhibit higher R^*_{nf} than that with binomial graph. This is because in the *heavy-tailed* power law communication graph, the population of nodes with high concurrent degree is higher than in binomial-distributed graph and the message can spread faster once it arrives at these nodes. The message dissemination heavily depends on these high-k



(a) Varying α. (b) Varying β. (c) Varying c. (d) Varying ρ.

Fig. 3. Secondary infection rate of D2D-Msg.



(a) Binomial-distributed $\mathbb{G}_c(t)$. (b) Power law-distributed $\mathbb{G}_c(t)$.

Fig. 4. Epidemic size of D2D-Msg.

nodes such that the power law communication graph will have an R^* that is lower than binomial graph under targeted failure. The opposite holds for random failure model.

B. Epidemic Size of Message Dissemination

Finally, to study the impact of RF, TF, and NF towards the number of users reached by m, we examine the epidemic size of message dissemination in Fig. 4. The figure shows that m can reach all the connected nodes under NF, albeit power law graph has higher R^*, such that the epidemic size grows faster. The final epidemic sizes of both graphs under no failure model are slightly different due to the *configuration model* [21] used to generate the graphs, in which the binomial p_k produces slightly less connected components. Note that $g(c)$ for both graphs are different such that the corresponding number of active nodes, $N\phi = Ng(c)$, are distinct. The less the number of active nodes, the more disconnected the network is. Hence, the ratio between the final epidemic size to the number of active users is proportional to both R^* and the number of active nodes, according to Fig. 3. For the binomial graph with targeted failure, the final size is very low since $R^*_{tf} = 1.156$, very close to 1, the epidemic threshold. For the power law graph with TF, the epidemic size is zero since $R^*_{tf} < 1$.

V. Conclusions

We studied a D2D-based messaging service (D2D-Msg) in which the dynamic underlying D2D network is captured using network exchange model and the users' decision to accept and re-share incoming messages is characterized by susceptible-infected-recovered (SIR) epidemics. To model the impact of random and targeted node failures, we propose a secondary infection metric R^* and analyze it for D2D-Msg with binomial and power law-distributed communication degree. Numerical results show that (i) D2D-Msg is more robust against random failure; (ii) targeted failure favors D2D-Msg with binomial communication graph that has narrow degree distribution; and (iii) R^* increases with the ratio between the number of message-receiving users to all users. In our future works, we will examine realistic power law-distributed communication graphs to investigate its analytical R^*, and derive its relationship to the epidemic size over time.

References

[1] "Active usage reach of the most popular mobile messaging apps worldwide as of Q3 2014," Downloaded from http://www.statista.com/statistics/324794/mobile-messenger-app-reach/, Oct. 2015.

[2] "Statistics and facts about mobile messenger app," Downloaded from http://www.statista.com/topics/1523/mobile-messenger-apps/, Oct. 2015.

[3] X. Lin, J. G. Andrews, and A. Ghosh, "Spectrum sharing for device-to-device communication in cellular networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 12, pp. 6727–6740, 2014.

[4] "FireChat in Hong Kong," Downloaded from http://www.cnn.com/2014/10/16/tech/mobile/tomorrow-transformed-firechat/, Oct. 2015.

[5] S. Bhattacharjee *et al.*, "Vulnerabilities in cognitive radio networks: A survey," *Comput. Commun.*, vol. 36, no. 13, pp. 1387–1398, 2013.

[6] M. Bradonjic *et al.*, "Performance of wireless sensor networks under random node failures," in *IEEE MILCOM 2011*, Nov 2011.

[7] J. Gao *et al.*, "Networks Formed From Interdependent Networks," *Nature Physics*, vol. 8, no. 1, pp. 40–48, Jan. 2012.

[8] R. Pastor-Satorras and A. Vespignani, "Immunization of complex networks," *APS*, vol. 65, no. 036104, pp. 036 104–1–036 104–8, 2002.

[9] E. Volz, "SIR dynamics in random networks with heterogeneous connectivity," *J. Math. Biol.*, vol. 56, no. 3, pp. 293–310, Mar 2008.

[10] E. Volz and L. A. Meyers, "Epidemic thresholds in dynamic contact networks," *J. Royal Soc. Interface*, vol. 6, no. 32, pp. 233–241, 2009.

[11] I. Rhee *et al.*, "CRAWDAD ncsu/mobilitymodels (v. 2009-07-23)," Downloaded from http://crawdad.org/ncsu/mobilitymodels/, Jul. 2009.

[12] Y.-Y. Ahn *et al.*, "Analysis of Topological Characteristics of Huge Online Social Networking Services," in *Proc. ACM WWW*, 2007, pp. 835–844.

[13] G. Siganos, M. Faloutsos, P. Faloutsos, and C. Faloutsos, "Power laws and the AS-level internet topology," *IEEE/ACM Trans. Netw.*, vol. 11, no. 4, pp. 514–524, Aug. 2003.

[14] P. Erdös and A. Rényi, "{On the evolution of random graphs}," *Publ. Math. Inst. Hung. Acad. Sci*, vol. 5, pp. 17–61, 1960.

[15] E. Volz and L. A. Meyers, "Susceptible-infected-recovered epidemics in dynamic contact networks," *Proc. R. Soc. B*, no. 274, pp. 2926–2933, Dec. 2007.

[16] P. Hui *et al.*, "Pocket switched networks and human mobility in conference environments," in *Proc. WDTN '05*, 2005, pp. 244–251.

[17] R. Van Der Hofstad, "Random graphs and complex networks," *Available on http://www.win.tue.nl/rhofstad/NotesRGCN.pdf*, 2009.

[18] J. Leskovec, L. A. Adamic, and B. A. Huberman, "The dynamics of viral marketing," *ACM Trans. Web*, vol. 1, no. 1, p. 5, 2007.

[19] M. Boguñá, C. Castellano, and R. Pastor-Satorras, "Nature of the epidemic threshold for the susceptible-infected-susceptible dynamics in networks," *Phys. Rev. Lett.*, vol. 111, no. 6, p. 068701, 2013.

[20] H. Cai and D. Y. Eun, "Crossing over the bounded domain: From exponential to power-law intermeeting time in mobile ad hoc networks," *IEEE/ACM Trans. Net.*, vol. 17, no. 5, pp. 1578–1591, Oct 2009.

[21] M. Molloy and B. Reed, "A critical point for random graphs with a given degree sequence," vol. 6, p. 161, 1995.