Path-based Epidemic Spreading in Networks

Wei Koong Chai, *Member, IEEE*, and George Pavlou, *Senior Member, IEEE*

***Abstract*—Conventional epidemic models assume omni-directional *contact*-based infection. This strongly associates the epidemic spreading process with node degrees. The role of the infection transmission medium is often neglected. In real-world networks, however, the infectious agent as the physical contagion medium usually flows from one node to another via specific directed routes (*i.e.*, *path*-based infection). Here, we use continuous-time Markov chain analysis to model the influence of the infectious agent and routing paths on the spreading behavior by taking into account the state transitions of each node individually, rather than the mean aggregated behavior of all nodes. By applying a mean field approximation, the analysis complexity of the path-based infection mechanics is reduced from exponential to polynomial. We show that the structure of the topology plays a secondary role in determining the size of the epidemic. Instead, it is the routing algorithm and traffic intensity that determine the survivability and the steady-state of the epidemic. We define an infection characterization matrix that encodes both the routing and traffic information. Based on this, we derive the critical path-based epidemic threshold below which the epidemic will die off, as well as conditional bounds of this threshold which network operators may use to promote/suppress path-based spreading in their networks. Finally, besides artificially generated random and scale-free graphs, we also use real-world networks and traffic, as case studies, in order to compare the behaviors of contact- and path-based epidemics. Our results further corroborate the recent empirical observations that epidemics in communication networks are highly persistent.**

***Index Terms*—Epidemic spreading, routing paths, Markov theory, mean field theory, complex networks.**

I. Introduction

ORIGINATED as part of epidemiology in biology studies for modelling disease spreading [1], epidemic theory has found applications in various scientific fields, ranging from natural networks (*e.g.*, hub protein and human brain structure [2], (online) social networks [3], *etc.*) to manmade infrastructures (*e.g.*, transportation systems [4], [5], power grid [6], telecommunication and computer networks [7], [8], [9], *etc.*). Epidemic theory, given its vast cross-disciplinary applicability, is now considered as part of network science.

In many real-world networks, the propagation of information follows specific paths. In computer networks, information messages are routed following routing protocol information from one host to another via a *path*. In the emerging information-centric networking (ICN) paradigm [10], content is cached along the path the content traverses (*e.g.*, [11], [12]). In cyber physical systems such as the smart grid, assessing the vulnerability of the power network requires understanding the path cascading failures will take when some nodes are attacked or fail (*e.g.*, [13], [14]). The information spreading process also forms paths in vehicular networks (*e.g.*, [15], [16]). Viral marketing/content spreading is another new area in which information is propagated from one "friend" to another in social media, following a self-perpetuating or time/distance diminishing spreading rate [17]. Finally, many networks (*e.g.*, delay-tolerant networks) are time-varying as not all nodes are active/connected at the same time, causing infection to spread in a path-like manner. In these cases, the current epidemic models, which assume contact-based diffusion, do not capture and thus, provide no explicit insights into the epidemic pathways driven by traffic flows.

Currently, theoretical epidemic models largely assume that infection propagation is based on contact in the sense that as long as there exists a link/contact between two nodes, there will be a fixed infection probability at all time. As such, each infected node constantly infects all its immediate neighbors even though not all nodes may be active at all time (*e.g.*, sensor nodes which often stay in "sleep" mode to save battery usage). Such a directionless reactive contact-based contagion process fails to capture two aspects of the spreading dynamics. First, as we mentioned, in many cases spreading follows certain paths and hence, each neighbor may be infected with different probabilities. Second, the reactionary infection process based on contacts does not take into account the need of an infectious agent to physically transfer the infection to another node. It implies that infection can still pass between nodes even when there are no actual interactions taking place.

Motivated by these observations, we model *path*-based information spreading by advancing the state of the art of epidemic theory to account for the directional effect caused by the paths constructed by different routing protocols as well as by the role played by the infectious agent[1] as the "infection carrier" that spreads the epidemic. Specifically, we first model the infectious agent by taking as input the network topology, routing protocol and traffic distribution. We then employ continuous time Markov chain analysis to model the path-based infection mechanics for one of the most representative epidemic models (*i.e.*, SIS model). We further apply a mean field approximation to reduce the overall analysis complexity from exponential to polynomial.

Our work advances the current contact-based epidemic modelling approach to additionally account for the above mentioned important factors. We focus on communication networks that transport data traffic via paths/routes. We consider that the infection must be carried by an infectious agent and explicitly model its role on the spreading dynamics. With this taken into account, the susceptible nodes in the network will possess different chances of getting infected, since now, the potential to be infected is governed by the amount of

W. K. Chai and G. Pavlou are with the Department of Electronic and Electrical Engineering, University College London, WC1E 7JE, Torrington Place, London, United Kingdom; e-mail: w.chai@ucl.ac.uk, g.pavlou@ucl.ac.uk.

[1] In biology, the term "pathogen" is often used in place of "infectious agent".

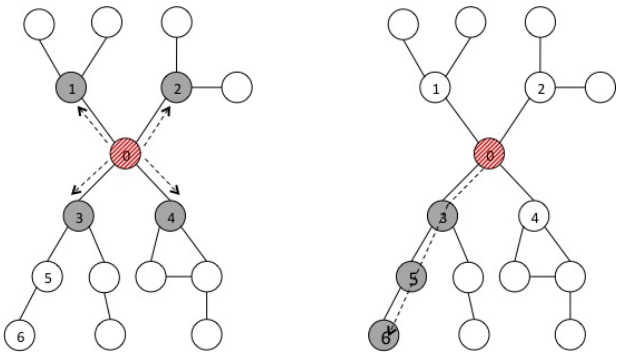


Fig. 1. (Color online) Contact-based *vs.* path-based: Node 0 is the source of infection. Grey nodes are susceptible nodes; (left) Contact-based epidemics only infect immediate neighbors on all directions; (right) Path-based epidemics infect all nodes along the paths where infectious agents traverse and neighbors having no interaction with the infected node are not proned to infection.

interactions in the system. A node having higher volume of infectious agents destined to or traversing it will proportionally have higher probability of getting infected. Fig. 1 provides a simple illustration comparing the contact-based and our path-based epidemic spreading process. In the contact-based model, with node 0 as the initial infected node, only nodes 1, 2, 3 and 4 are immediately susceptible to infection. Other nodes may be susceptible in the future, once they have at least one infected direct neighbor. In contrast, assuming interactions between nodes 0 and 6, the path-based model has a different set of susceptible nodes (*i.e.*, nodes 3, 5 and 6), determined by the information exchanges in the system. In this case, nodes 1, 2 and 4 are not in danger of infection albeit being the direct neighbors of the infected node.

The main contributions of this paper are four-fold.

- We model the spreading dynamics of information based on *paths* by taking into account the role of the infectious agent in the system. We contribute to the theoretical development of the general epidemic theory whereby we break from the conventional assumption of the contact-based infection process and account for the added dimension of *direction* of information flows. In our case, a host will still have non-zero probability of being infected even when it has no direct link to an infected node. Spreading is now based on whether a host lies in the routing path (usually the shortest path computed based on specific routing protocol) where infected nodes exist. Our modelling builds upon the analytical framework studied in [18], [19], [20].
- We characterize the path-based epidemic spreading via an infection characterization matrix that encodes both the information on traffic distribution and routing paths and find the critical epidemic threshold that determines the prevalence of the epidemic to be the inverse of the spectral radius of this matrix. We further derive conditional bounds of this threshold and provide the "control space" available in promoting or containing the spread.
- Our modelling approach provides a methodological basis for the study of various different epidemic models (*e.g.*, SIR, SEIS, SAIS, *etc.*) since the modelling approach is sufficiently general.
- Along with the insights gained from our work, our path-based epidemic analytical framework forms a set of tools for network stakeholders such as network operators to properly dimension or control their infrastructures to promote or suppress spreading of certain information or data objects depending on their needs and specific cases.

The rest of the paper is organized as follows. In Section II, we first review the basics of epidemic theory including the latest developments and some key relevant results. Then in Section III, we formalize the actual path-based spreading mechanics (Section III-A) and develop our analytical framework. We model the infectious agent in Section III-B in two ways; (1) by taking into account the routing protocol but without the knowledge of traffic distribution and (2) by assuming prior knowledge of the traffic via a traffic matrix. Our path-based spreading analytical framework is described next in Section III-C. Based on this framework, we investigate the epidemic threshold corresponding to the path-based spreading dynamics in Section IV. In Section V, a comparison between the contact- and path-based spreading dynamics is made. We then study the effects of network topology, routing protocol and traffic distribution on the epidemic spreading in Section VI and derive the bounds of the epidemic threshold with which one can use to determine the extent to which the epidemic can be controlled. We consider three use cases based on real networks and traffic in Section VII, showing the behavior of contact- and path-based epidemic spreading in these networks. A hypothetical epidemic that infects nodes via traceroute packets is studied using data collected in [21]. Finally, we conclude our work in Section VIII. Table I lists the notations used in this paper.

TABLE I
NOTATIONS

Symbol	Descriptions
A	Adjacency matrix representing the network topology
N	Number of nodes in the network
L	Number of links in the network
β	Infection probability
δ	Curing rate
d_{max}, $\bar{d}$, $\langle d^2 \rangle$	Maximum node degree, mean degree, second moment of network degree distribution
τ	Effective spreading rate
τ_c	Critical epidemic threshold
λ_n	Traffic generation rate of node n
μ^x_{max}	Spectral radius or largest eigenvalue of matrix x
b_{alg}	Algorithmic betweenness
R	Routing matrix
B	Matrix describing node involvement in forwarding packets
C	Infection characterization matrix
Γ	Traffic matrix
$i_n(t)$	Probability of node n in the infected state
$s_n(t)$	Probability of node n in the healthy state
ρ	Fraction of infected nodes in the network
Q	Infinitesimal generator of the continuous Markov chain

II. Background, Basics and Related Work

Recently, epidemic theory has been applied to computer networks in areas such as computer virus/malware propagation

and immunization (*e.g.*, [7]), information dissemination (*e.g.*, [8], [9]), protocol design (*e.g.*, [22]) and cascading network failures/faults and relevant protection strategies (*e.g.*, [23]).

The classical epidemic analytical framework involves the following two main aspects:

1) States – by compartmentalization, epidemic models break down a "disease" into distinct states (or stages) and each individual in the network is considered to be in one of the states at any given time. Two of the most common models are the SIS and SIR models [1], [24], [25] where the possible states are the following:
   - Susceptible (S) – Clean and healthy individuals who are not infected but prone to infection.
   - Infected (I) – Infected individuals who are at the same time infectious.
   - Removed (R) – Immune individuals who are neither susceptible to infection nor infectious.

   There exist a number of variants in the literature, such as SEIS/SEIR with an additional state where an individual is infected but not yet infectious [26], SAIS where an individual may be alerted and thus having less chance of getting infected [27], *etc.*
2) Infection mechanism – this describes how a disease is passed from one individual to another. Essentially, this refers to the transition of states. This transition is often related to an effective spreading rate, conventionally defined as $\tau = \beta/\delta$ where β is the infection probability (sometimes known as the transmission rate) and δ is the curing rate. However, for our case, this rate is additionally affected by the traffic in the system. Early work (*e.g.*, [1], [24]) mostly considers homogeneous mixing based on the law of mass action, where individuals have equal probability of being in contact with an infected individual, while more recent work has started to consider heterogeneous cases.

There exist already several key works on contact-based epidemic modelling for computer networks. In [28], the authors developed an homogeneous infection model for computer viruses in the Internet. In their work, they advanced the literature by considering the additional effect of directed links in a fixed network and discovered a critical threshold such that the epidemic will die off when the effective spreading rate is below the reciprocal of the mean degree, $1/\bar{d}$. In [29], [30], the authors observed from data that Internet viruses are more persistent than that predicted by the theoretical results for an homogeneous network and refined this critical threshold, still as a function of node degrees, as $\bar{d}/\langle d^2\rangle$ where $\langle d^2\rangle$ is the second moment of the network degree distribution. More recently, instead of relating the threshold directly to the network node degree, the authors in [18], [31], [32] found that the threshold is governed by the spectral radius of the adjacency matrix, A, representing the network topology. It is stated in these works that the critical epidemic threshold, τ_c, equals $1/\mu^A_{max}$ where μ^A_{max} is the largest eigenvalue of A. This threshold is further derived for generalized networks with heterogeneous infection rates in [33].

Since it is well-known that $\bar{d} \leq \mu^A_{max} \leq d_{max}$, we can also state that the bounds for the contact-based epidemic threshold are:

$$\frac{1}{d_{max}} \leq \tau_c \leq \frac{1}{\bar{d}} \tag{1}$$

where d_{max} is the maximum degree. For instance, $\tau_c = 1/d_{max}$ when the graph is d_{max}-regular. In our work, however, we will show that the threshold for path-based epidemic spreading is no longer directly bounded by the node degree or degree distribution of the network nodes. Furthermore, we are interested in finding the bounds of τ_c. Unlike contact-based epidemics which usually have a fixed system (*i.e.*, fixed network topology with constant infection/curing probabilities), with a path-based epidemic model, we have the possibility to "tune" the system based on τ_c. For instance, we can either encourage or control the epidemic spreading through design of different routing protocols or through traffic engineering techniques that change the traffic pattern in the network.

In one way or another, the known epidemic models in the literature employ some approximations or assumptions (*e.g.*, network size is assumed to be sufficiently large such that asymptotic regime behavior is reached) to ensure computational feasibility since the complexity to obtain an exact solution of an epidemic spread grows exponentially with the network size. In [34], the authors propose a pair-wise approximation *SIS* model that provides higher model accuracy but results in the need to consider $\binom{N}{2}$ number of pairs.

The nature of the exact solution has been studied in [18] by using a 2^N-state continuous-time Markov chain for the *SIS* model. By observing each node separately, the authors further introduced an N-intertwined model that reduces the complexity of exact solution from exponential $O(State^N)$ to polynomial $O(N)$ where $State$ is the number of possible states and N is the number of network nodes. This work forms the starting point of our work as we retain its reduced polynomial complexity feature. The approach has also been applied to the contact-based *SIR* epidemic model in [35].

In the literature, the incorporation of traffic dynamics into epidemic modelling was investigated in the form of a meta-population system in [36], [37] where the role of the infectious agent was considered. The authors departed from the previous epidemic studies that assumed infection will take place whenever a link (or contact) between two nodes exists. In [38], the authors compared pathogen spreading between the shortest paths of a fully and partially observable network. However, in that work, the authors still considered a contact-based infection mechanism with no specific destination nodes (stochastic process). In [39], the role of the data packet as infectious agent was modelled considering random source-destination pairs. The authors derived the critical threshold of such traffic-driven epidemic, given in Eq. 2, analogous to the previous work on contact-based studies that relates the threshold to the network degree

$$\tau_c = \frac{\langle b_{alg}\rangle}{\langle b^2_{alg}\rangle}\frac{1}{N} \tag{2}$$

where $\langle b_{alg}\rangle$ and $\langle b^2_{alg}\rangle$ are the mean and second moment of

the algorithmic betweenness respectively [40][2]. The algorithmic betweenness of a node is defined as the number of packets passing through that node when each node in the network sends one packet to every other node in the network. Using results from [39], the works in [42] and [43] investigated how to deter traffic-driven epidemic spreading by removing network links and altering routing protocol respectively. By exploiting the concept of algorithmic betweenness, these works took an implicit assumption that each network node has homogeneous interactions with all other nodes which unfortunately is often not the case in communication networks. Our work here does not rely on this assumption.

The critical epidemic threshold has now been considered as an important and fundamental quantity in describing epidemic dynamics. In our work, we derive the critical threshold that determines the survivability of a path-based epidemic. We find that this threshold relates to the spectral radius of an infection characterization matrix (detailed in Section III) which takes into account the effects of routing and traffic.

III. Path-based Spreading Model Development

A. General Path-based Spreading Process

Consider a 3-node line graph as an example. We use the Markov chain diagrams of *SI*, *SIS* and *SIR* models in Fig. 2 to illustrate the key departure of path-based spreading process from the conventional contact-based one. While the number of states remains the same, the transitions are not. Based on the 3-node line graph, since there is always only one valid route between any two nodes, Fig. 2 is representative for any routing protocol. A transition involving state changes to multiple nodes is possible (*e.g.*, state SSI to state III) while the conventional contact-based infection forbids this. Note that a direct transition from state SIS to state III is not possible for a line graph because the flow of packets and thus infection is *directional*. An infected node in the middle can only infect nodes either to its left or right at any time. However, if we consider a ring topology of the same size, then this transition from SIS to III is possible (illustrated with the dash arrows in Fig. 2) if the routing protocol chooses the longer path to deliver the packet. Therefore, it is already obvious that while the topology still plays a role in influencing the spread of the infection, it is the routing protocol that finally governs the actual infection dynamics.

Without loss of generality, for the rest of this paper we focus on the *SIS* model where an individual in the network can only be healthy (*i.e.*, susceptible) or infected. We model the spreading process that is based on the paths of information flows. For simplicity, we use *data packets* as the universal infectious agent although the "infection" can be transmitted by different agents depending on the specific application context (*e.g.*, content chunk in the case of in-network caching, software patch in the case of computer virus immunization, tweet in the context of gossip spreading in online social networks, *etc.*). The exact mechanics of the infection process are as follows:

[2]If the shortest paths are used, then it coincides with *topological* betweenness [41].

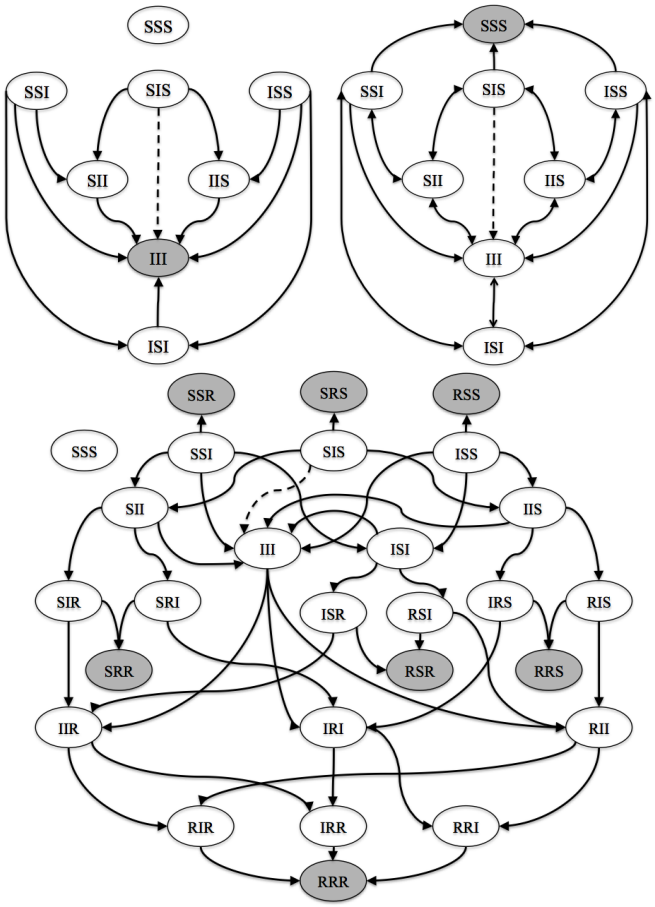


Fig. 2. The Markov chain state diagram of path-based epidemic spreading for a line graph with $N = 3$ for SI model with $2^3 = 8$ states (top-left), SIS model with $2^3 = 8$ states (top-right) and SIR model with $3^3 = 27$ states (bottom). The grey states indicate absorbing ones.

- A packet is infectious if it originates from an infected node. Otherwise, it is a *clean* packet.
- Packets traverse from one node to another via a path with certain traffic arrival rate, λ. We assume a Poisson packet arrival process with no routing delay.
- A clean packet is infected and thus becomes infectious when it traverses an infected node (*i.e.*, an infected node is infectious).
- A susceptible node can only be infected by an infectious packet. An infectious packet infects a node with probability β. A path-based spreading process may infect multiple nodes in one transmission. An infectious packet traversing a path of l hops length has the probability of β^l of infecting l nodes in one transition. Alternatively, an infected packet traversing a path has $1-(1-\beta)^l$ probability of infecting a node along that path.
- An infected node becomes susceptible again with a curing rate, δ. This is assumed to be a Poisson process independent of the traffic and infection rates. For the rest of the paper, we also assume $\delta = 1$.

B. Modelling the Infectious Agent

The state of a node (*i.e.*, either healthy or infected) is dependent on the number of infected packets that traverse

it or terminate there. This, in turn, is proportionate to the volume of traffic it carries (*i.e.*, the infection requires packets, as infectious agents, to spread).

Consider an undirected network, $G(V, E)$ with $V = v_1, ..., v_N$ nodes and $E = e_1, ..., e_L$ links where $N = |V|$ and $L = |E|$. G can be represented by A, the $N \times N$ symmetric adjacency matrix, with $a_{n,m} = 1$ if there exists a link between node n and m and 0 otherwise. Furthermore, we describe the effect of the routing protocol via an $N \times N(N-1)$ routing matrix[3], R. For our purpose, we depart from the conventional routing matrix that maps traffic to links (*e.g.*, [44]) and instead, encode the traffic to nodes it traverses or is destined to. Accordingly, we define the routing matrix as follows:

$$r_{n,k} = \begin{cases} 1 & \text{if traffic on path } k \text{ traverses across} \\ & \text{or is destined to } n, \\ 0 & \text{otherwise} \end{cases} \quad (3)$$

where k indexes routes (or paths) between all source-destination pairs in the network (*i.e.*, node pair $1 \rightarrow 2, 1 \rightarrow 3, \ldots, N \rightarrow (N-1)$). Note that matrix R is formed by concatenating N blocks of $N \times (N-1)$ matrices as follows:

$$R = \left[R^1 | R^2 | \ldots | R^N\right] \quad (4)$$

where R^n describe the node involvement in delivering the traffic originating from node n. Assuming traffic is not routed to itself, then all elements in the n^{th} row of R^n equal zero:

$$\forall k \in V : r^n_{n,k} = 0. \quad (5)$$

Given A and R, we construct an $N \times N$ matrix, B describing the probability of a node involved in delivering a packet originating from any other nodes in the network. In the context of this work, the destination node of the infected packets is also subjected to infection, thus it must be considered. Matrix B can then be constructed as in Eq. 6 below

$$b_{n,m} = \frac{\sum_{k=1+(m-1)(N-1)}^{m(N-1)} r_{n,k}}{N-1} \quad (6)$$

where $b_{n,m}$ denotes the probability of a packet originating from node m traverses across or destines to node n. Conceptually, $b_{n,m}$ resembles the notion of conditional betweenness centrality in [45] where the total node involvement in forwarding packet originating from source node, n, is computed, instead of all possible node pairs in the network[4].

The elements in B can further be weighted with the node specific traffic generation rate. If Λ is an $N \times 1$ vector whose entries, λ_n, denote the traffic generation rate of the nodes in G, then the total traffic node n is involved in can be computed as follows:

$$C = \text{diag}(\Lambda) \times B \quad (7)$$

where $\text{diag}(\Lambda)$ is the diagonal matrix with elements $\lambda_1, \lambda_2, \ldots, \lambda_N$ as its entries at the principal diagonal. This formulation however makes the implicit assumption that traffic distribution is uniform in the network (*i.e.*, all nodes send equal volume of traffic to all other nodes).

Often in practice, the traffic in a network is known or can be estimated/predicted (*e.g.*, [46]). This is usually represented via a traffic matrix. With this additional information, we can reformulate Eq. 7 above and model the traffic dynamics more precisely. Consider a stationary non-negative $N \times N$ traffic matrix[5], Γ where its entries, $\Gamma_{n,m}$, denote the traffic volume from node m to n. Since we do not consider self-traffic, the trace of the traffic matrix, $\text{tr}(\Gamma) = \sum_{n=1}^{N} \Gamma_{n,n} = 0$. The equivalent of Λ matrix can be computed by taking the column sum of Γ.

Further, we define a reduced Γ^* where these zero elements along the main diagonal are removed, resulting in a $(N-1) \times N$ matrix. Similar to the R matrix, Γ^* can be decomposed to the following form:

$$\Gamma^* = [\Gamma^{(*,1)} | \Gamma^{(*,2)} | \ldots | \Gamma^{(*,N)}] \quad (8)$$

where $\Gamma^{(*,n)}$ is the n^{th} column of Γ^* indicating the traffic volume originating from node n. Using the additional source-destination traffic information, we can therefore, alternatively, construct C as follows:

$$C = [R^1 \times \Gamma^{(*,1)} | R^2 \times \Gamma^{(*,2)} | \ldots | R^N \times \Gamma^{(*,N)}]. \quad (9)$$

We call the $N \times N$ matrix C as infection characterization matrix (discussed later in Section IV) whereby it conceptually signifies the overall level of involvement of the nodes in the graph in receiving and delivering infectious agents.

C. SIS *Path-based Spreading Model*

Let $X_n(t)$ be the state of node n at time t. For the *SIS* model, $X_n(t)$ can only be either "susceptible" or "infected". We further denote the probability of a node n be in the infected state at time t to be $i_n(t) = Pr[X_n(t) = 1]$ with "1" indicating the infected state and "0" the susceptible one. Hence, the probability of a node being in the healthy state is $s_n(t) = Pr[X_n(t) = 0] = 1 - i_n(t)$. By applying Markov theory, the infinitesimal generator $Q_n(t)$ of this two-state continuous Markov chain can be written as below:

$$Q_n(t) = \begin{bmatrix} -q_{1;n} & q_{1;n} \\ q_{2;n} & -q_{2;n} \end{bmatrix} \quad (10)$$

where the transitions involving the curing process are independent of the states of other nodes and thus, $q_{2;n} = \delta$ (See Section V for discussion.).

On the other hand, $q_{1;n}$ is a random variable dependent on the activities taking place in other nodes within the network. To proceed with the Markov analysis, the randomness of $q_{1;n}$ must be removed. One way to achieve this is to condition $q_{1;n}$ to all possible combinations of states for all nodes, $X_n, 1 \leq n \leq N$, resulting in the exact Markov chain solution of exponential complexity.

[3]We assume traffic is not destined to the source.

[4]In [45], the authors conditioned the betweenness metric using the destination node as oppose to the source node.

[5]Conventionally, the traffic matrix is often defined as the transpose of Γ (*e.g.*, [44]).

Here, we follow the approach of polynomial complexity discussed in [18][19] by applying a mean field approximation to account for the random infection rate, $q_{1;n}$, with an effective rate instead. Assuming that both the infection rate, β, and curing rate, δ, are constant, then we can average[6] over the states to obtain an expected rate as follows:

$$\begin{aligned} E[q_{1;n}] &= \beta \sum_{m=1}^{N} Pr[X_m(t)=1] c_{n,m} \\ &= \beta \sum_{m=1}^{N} i_m(t) c_{n,m} \text{ or } = \beta \sum_{m=1}^{N} i_m(t) \lambda_m b_{n,m} \end{aligned} \quad (11)$$

where $c_{n,m}$ is the element of the infection characterization matrix, C. We can then write the effective infinitesimal generator as follows:

$$\overline{Q_n(t)} = \begin{bmatrix} -E[q_{1;n}] & E[q_{1;n}] \\ \delta & -\delta \end{bmatrix}. \quad (12)$$

After the above steps, we can proceed with Markov theory using $\overline{Q_n(t)}$ by applying the Markov differential equation (See [47], Chapter 10, p. 182) for $X_n(t) = 1$ and obtain the following system of non-linear differential equations,

$$\frac{di_n(t)}{dt} = \beta \sum_{m=1}^{N} c_{n,m} i_m(t) - i_n(t) \left(\beta \sum_{m=1}^{N} c_{n,m} i_m(t) + \delta \right), \quad (13)$$

or

$$\begin{aligned} \frac{di_n(t)}{dt} &= \beta \sum_{m=1}^{N} \lambda_m b_{n,m} i_m(t) \\ &\quad - i_n(t) \left(\beta \sum_{m=1}^{N} \lambda_m b_{n,m} i_m(t) + \delta \right) \end{aligned} \quad (14)$$

depending on the knowledge of the traffic distribution in the network. This system of equations can then be solved in its matrix form as below.

$$\frac{dI(t)}{dt} = \beta C I(t) - \text{diag}(i_n(t))(\beta C I(t) + \delta u) \quad (15)$$

where u is a vector of all ones and $\text{diag}(i_n(t))$ is the diagonal matrix with elements $i_1(t), i_2(t), ..., i_N(t)$ at the principal diagonal.

Substituting $I(t) = \text{diag}(i_n(t)u)$ and rearranging the equation above, we get

$$\begin{aligned} \frac{dI(t)}{dt} &= (\beta \text{diag}(1 - i_n(t))C - \delta \mathbb{1}) I(t) & (16) \\ &= (\beta \text{diag}(1 - i_n(t)) \text{diag}(\Lambda) B - \delta \mathbb{1}) I(t) & (17) \end{aligned}$$

where $\mathbb{1}$ is the $N \times N$ identity matrix.

The instantaneous fraction of infected nodes in the network can then be written as

$$\rho(t) = \frac{1}{N} \sum_{n=1}^{N} i_n(t). \quad (18)$$

At steady-state, $\frac{di_n(t)}{dt}|_{t\to\infty} = 0$. Denote $i_{n\infty} = \lim_{t\to\infty} i_n(t)$, then from Eq. 13,

$$\begin{aligned} i_{n\infty} &= \frac{\beta \sum_{m=1}^{N} c_{n,m} i_{m\infty}}{\beta \sum_{m=1}^{N} c_{n,m} i_{m\infty} + \delta} \\ &= 1 - \frac{1}{1 + \tau \sum_{m=1}^{N} c_{n,m} i_{m\infty}} \end{aligned} \quad (19)$$

where $\tau = \beta/\delta$. From Eq. 19, $i_{n\infty} = 0$ is a trivial solution. This is also apparent by observing the Markov chain which is finite and possesses an absorbing state (*i.e.*, all nodes in healthy state) reachable by all other states. However, as studied in [48], for any networks with realistic size N, this true steady-state may be reached only after an extremely long time. In the meantime, the system converges exponentially fast to and remain for most time at a *metastable* state (as another positive solution of Eq. 19 besides the trivial one). In addition, [19] pointed out that this metastable state reflects more closely real world epidemics. As such, it is this metastable state that is of interest and for the rest of the paper, we focus on this state and refer to it as *the* steady state.

The ability to be able to compute $i_n(t)$ and $i_{n\infty}$ also lets us gain insights into the susceptibility of individual nodes in the network, rather than only observing the entire network as a whole.

Using Eq. 19, the steady state fraction of infected nodes in the network (*i.e.*, Eq. 18) can be rewritten as

$$\rho_\infty = \frac{1}{N} \sum_{n=1}^{N} i_{n\infty}. \quad (20)$$

The literature has shown evidence that pure random graphs such as Erdős-Rényi (ER) graph model [49], which has binomial degree distribution, and scale-free graphs [50], which have power-law degree distribution, exhibit very different epidemic behaviors. We use them here to show the predictive capacity of our analytical framework against Monte-Carlo simulations. We generate a sample set of graphs for each graph model above and for each graph, we pre-compute the routing paths for each and every node pair using Djikstra's algorithm, assuming non-weighted links. A set of ten randomly chosen seed nodes are set to be infected at time, $t = 0$. All other nodes are assumed healthy. At each time step, we generate λN packets. For each newly generated packet, a random source and destination pair is chosen and the packet is delivered following the pre-computed path of this node pair. The infection and curing process of each node then follows the description given in Section III-A.

Fig. 3 and Fig. 4 show two representative results of the instantaneous evolution of the infected fraction of population for $N = 100$ where we see close behavior for both cases. The infected fraction of the population stabilizes to a certain level which is dependent on τ. Furthermore, Fig. 5 shows the

[6]The implications of this approximation are discussed in [20].

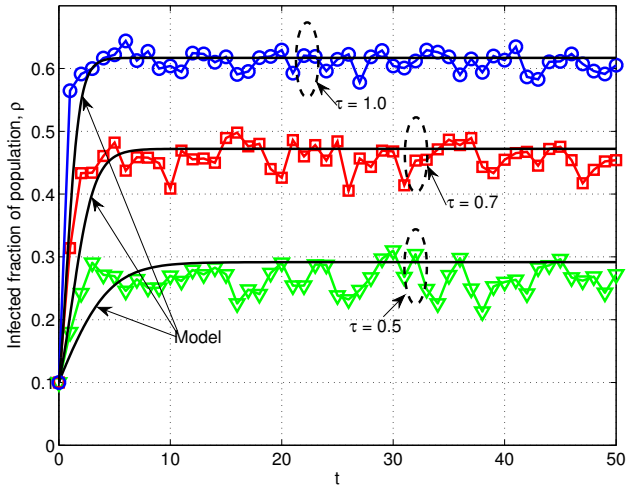


Fig. 3. (Color online) Instantaneous evolution of infected fraction of population for a random graph of size $N = 100$ with uniform traffic distribution for $\tau = \{0.5, 0.7, 1.0\}$. Solid black lines are computed based on Eq. 16 and colored lines with markers are results of Monte-carlo simulations.

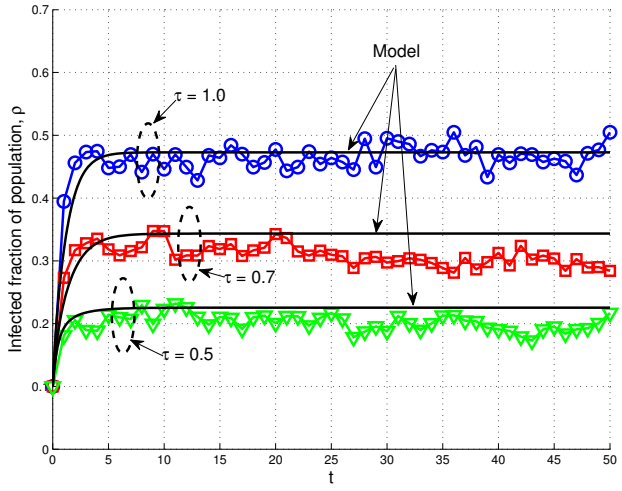


Fig. 4. (Color online) Instantaneous evolution of infected fraction of population for a scale-free graph of size $N = 100$ with uniform traffic distribution for $\tau = \{0.5, 0.7, 1.0\}$. Solid black lines are computed based on Eq. 16 and colored lines with markers are results of Monte-carlo simulations.

steady state for sample networks of different sizes obtained both from our model and simulation runs.

IV. Path-based Epidemic Threshold

As briefly mentioned in Section II, in previous studies (*e.g.*, [18]), a theoretical critical threshold, τ_c, has been found below which the epidemic will almost certainly die off and vice versa. However, it has to be mentioned here that the existence of such a threshold in real-world scenarios is argued against in several recent works [29], [30].

To investigate whether an epidemic will die off, we follow a similar approach as in [18]. We focus on the time when all nodes' infection probability, $i_n(t)$, is close to zero since the system is clear of infection only when $i_n = 0 : \forall n \in V$ (*i.e.*, all nodes remain healthy at all time; the absorbing state). At such condition and ignoring the non-linear term, we can rewrite Eq. 16 as follows:

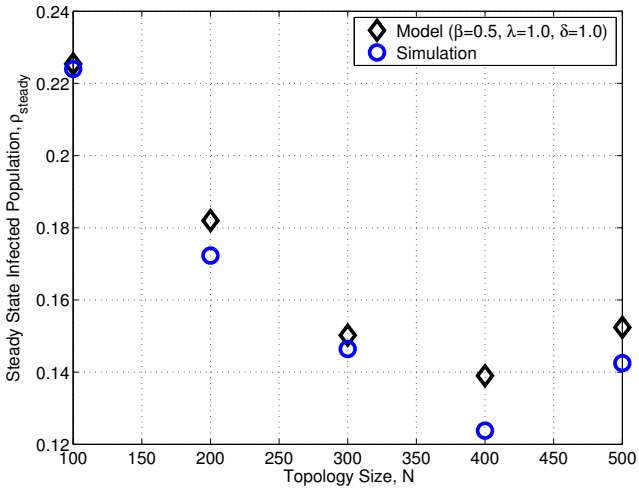


Fig. 5. (Color online) Steady state infected fraction of population for a set of sample topologies, $N = \{100, 200, 300, 400, 500\}$.

$$\frac{dI(t)}{dt} = (\beta C - \delta \mathbb{1})I(t). \tag{21}$$

Solving Eq. 21, we obtain the time evolution function of $I(t)$ below.

$$I(t) = e^{Ht} I(0) \tag{22}$$

where $H = \beta C - \delta \mathbb{1} = \beta \text{diag}(\Lambda) B - \delta \mathbb{1}$. By eigen decomposition,

$$H = U M^C U^T \tag{23}$$

where $M^C = \text{diag}(\mu_n^C)$ is the diagonal matrix with n-th eigenvalue of C as element at $M^C_{n,n}$ and U is the orthonormal matrix whose n-th column is the eigenvector corresponding to eigenvalue, μ_n^C. We then obtain

$$\begin{aligned} H &= \beta C - \delta \mathbb{1} \\ &= U(\beta M^C - \delta \mathbb{1}) U^T \\ &= U \text{diag}(\beta \mu_n^C - \delta) U^T. \end{aligned} \tag{24}$$

Substituting the Eq. 24 to Eq. 22, we get

$$I(t) = U \text{diag}(e^{(\beta \mu_n^C - \delta)t}) U^T I(0). \tag{25}$$

All eigenvalues must satisfy $\beta \mu_n^C - \delta \leq 0$ since $I(t)$ is a probability vector. The epidemic threshold can then be computed as follows:

$$\tau_c = \frac{\beta}{\delta} \leq \frac{1}{\mu^C_{max}}. \tag{26}$$

In other words, the epidemic will decay exponentially fast to zero when τ is equal or smaller than the reciprocal of the spectral radius of matrix C, μ^C_{max} (see Section V). Hence, C characterizes the spreading strength of the path-based epidemic.

In Fig. 6, we show the infected fraction of population for five random graphs of different sizes with $\tau = 0.5$ where

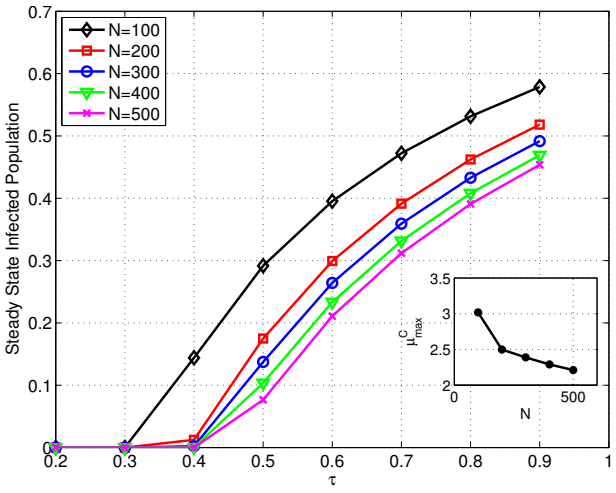


Fig. 6. (Color online) The size of epidemic at metastable steady state for random graphs of size, $N = \{100, 200, 300, 400, 500\}$. The infected fraction monotonically increases with the effective spreading rate, τ but only when $\tau > \tau_c$. Inset plot provides the spectral radius of C for the graphs.

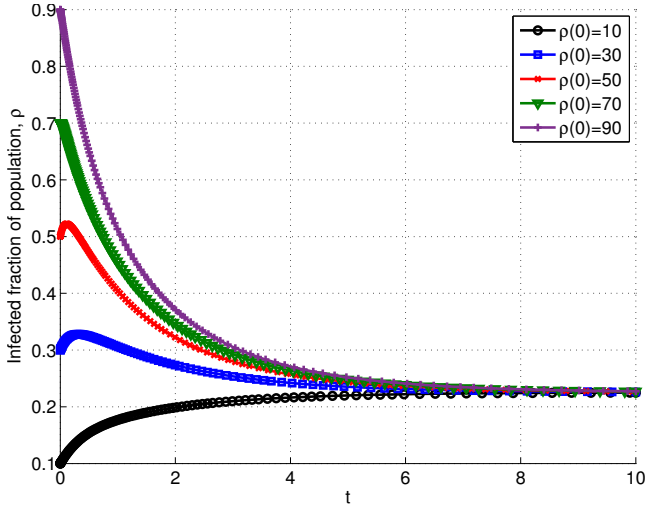


Fig. 7. (Color online) Instantaneous evolution of infected fraction of population for a network with $N = 100$ for $\rho(0) = \sum i_n(0) = \{10, 30, 50, 70, 90\}$. The number of initial infected nodes does not impact the metastable steady state of the infected fractions of population.

all nodes send the same amount of traffic to all other nodes. From the figure, we can see that the epidemic will not survive whenever $\tau < \tau_c$. We highlight that this critical threshold only defines the transition point between a surviving or dying epidemic but not the metastable steady state size of the epidemic above this threshold (*i.e.*, $\tau_c(C) > \tau_c(C')$ does not imply $\rho_\infty(C) > \rho_\infty(C')$ and vice versa).

From Eq. 26, we note that the critical threshold is independent of the initial state of the system. Furthermore, we show in Fig. 7 that regardless of the number of initial infected nodes, the system always converges to the same metastable steady state (*i.e.*, the stable infected population, ρ_∞, is also independent of the initial state).

At this point, it is interesting to look at the corresponding principal eigenvector, z^C_{max} of μ^C_{max} which is defined as follows:

$$\mu^C_{max}(z^C_{max})_n = \sum_{m=1}^{N} c_{n,m}(z^C_{max})_n \tag{27}$$

where $(z^C_{max})_n$ is n-th component of the principal eigenvector, z^C_{max}. From Eq. 27, we can observe that $(z^C_{max})_n$ is directly proportional to the level of involvement of node n in transporting traffic since $c_{n,m}$ is computed from R and Γ.

V. Path-based *vs.* Contact-based Spreading Dynamics

We begin our comparison of the two types of epidemic spreading based on their corresponding exact 2^N-state Markov chain of the network states. When we construct the exact 2^N-state Markov chain of network states via a binary representation of state space similar to that in Eq. 4 of [18], we can compare the infinitesimal generators, Q^{path} and $Q^{contact}$. Briefly, each state of the network is represented by an N-bit binary string with the n^{th} bit representing the n^{th} node in the network and "1" denoting the node being in the infected state while "0" indicating otherwise.

The network state as a whole in an *SIS* epidemic is determined by two processes: infection and curing. As the two processes are independent of each other, we can observe them separately. To facilitate this, it is convenient to decompose Q into the sum of three $N \times N$ matrices as follows:

$$Q = Q_{L\triangle} + Q_{U\triangle} + Q_{diag}$$

where $Q_{L\triangle}$ and $Q_{U\triangle}$ are the lower and upper triangular part of Q respectively while Q_{diag} takes the elements from the main diagonal of Q. Owing to the binary representation of the state space, $Q_{L\triangle}$ and $Q_{U\triangle}$ separately encode the curing (related to δ) and infection (related to β) transitions respectively. Since the curing process is identical for both contact- and path-based spreading and independent of the infection process, $Q^{path}_{L\triangle} = Q^{contact}_{L\triangle}$. They are also not influenced by A, R and Γ matrices. As such, theorem 1 in [18] stating that for $\beta = 0$, the eigenvalues of Q are $\mu^Q = -k\delta$ with multiplicity $\binom{N}{2}$ also applies for our path-based epidemic.

However, the same cannot be said for the upper triangular part of the Q matrices (*i.e.*, $Q^{path}_{U\triangle} \neq Q^{contact}_{U\triangle}$). While $Q^{contact}_{U\triangle}$ is determined by the A matrix, $Q^{path}_{U\triangle}$ is computed based on R and Γ. As briefly illustrated in Section II, there will be more possible state transitions in path-based spreading. Therefore, $Q^{path}_{U\triangle}$ will have more non-zero elements than $Q^{contact}_{U\triangle}$ and thus, Q^{path} is denser than $Q^{contact}$. Nevertheless, the largest eigenvalue for both Q matrices remains to be zero as $\det(Q)$ is still zero.

Further, comparing Eq. 16 and Eq. 17 of the path-based epidemic with the contact-based counterpart model (in [18], [20]), the systems of equations have similar form. The key difference of the models here is the absense of the adjacency matrix, A, as the direct influencer of the path-based epidemic spreading. In its place, we now have the characterization matrix, C, which takes into account the traffic intensity, Γ

and the routing protocol, R, which in fact is constrained by the connectivity of the topology, A.

Matrices A and C are both, by definition, non-negative matrices. The maximum eigenvalue of A of a connected graph is bounded between the average degree and the maximum degree of the vertices. So it follows that its maximum value is $N-1$, attained for the complete graph on N vertices. Hence, the bounds of Eq. 1 apply but this is not true for path-based epidemic spreading.

Since C is no longer surely symmetric, its spectral radius may be a complex number. For such matrices, the largest eigenvalue in magnitude is a real number and for this eigenvalue, the real part is the largest amongst all the eigenvalues [51]. Hence, C's spectral radius, $\mu^C_{max} = \mathbb{R}\mathrm{e}(\mu^C_{max})$. Also, for matrices such as C, it has already been established that the following spectral radius bounds apply:

$$\min_{1\le n\le N}\left(\sum_{m=1}^{N}|c_{n,m}|\right) \le \mu^C_{max} \le \max_{1\le n\le N}\left(\sum_{m=1}^{N}|c_{n,m}|\right). \tag{28}$$

Theorem 1 (General bounds of τ_c)**.** *Given a path-based epidemic characterized by C, its critical threshold can be bounded as follows:*

$$\frac{1}{\max\limits_{1\le n\le N}\left(\sum_{m=1}^{N}|c_{n,m}|\right)} \le \tau_c \le \frac{1}{\min\limits_{1\le n\le N}\left(\sum_{m=1}^{N}|c_{n,m}|\right)}. \tag{29}$$

Proof. This is direct result from Eq. 26 and Eq. 28. □

The physical interpretation of Theorem 1 is that τ_c is upper (lower) bounded by the node involved in carrying the lowest (highest) volume of traffic in the network. An example application of this theorem is that now, it is possible to formulate different traffic engineering optimization problems with a spreading-related constraint such that an epidemic will or will not occur based on the infinity-norm of C, $||C||_\infty$.

VI. Effect of Routing Protocol, Traffic and Network Topology

In this section, we investigate the role of the network topology (*i.e.*, A), the routing protocol (*i.e.*, R) and the traffic load in the system (*i.e.*, Γ) in determining the path-based spreading of an epidemic (*i.e.*, τ_c). We first establish the monotonicity of τ_c.

Theorem 2 (Monotonicity of τ_c)**.** *Given any two infection characterization matrices, C and C' where $0 \le C \le C'$ for which we define $C \le C'$ if $c_{n,m} \le c'_{n,m} : \forall n, m$, then*

$$\tau_c(C) \ge \tau_c(C').$$

Proof. As C and C' are non-negative square matrices, it follows from the Perron-Frobenius theorem that

$$\mu^C_{max} \le \mu^{C'}_{max} \text{ if } 0 \le C \le C'.$$

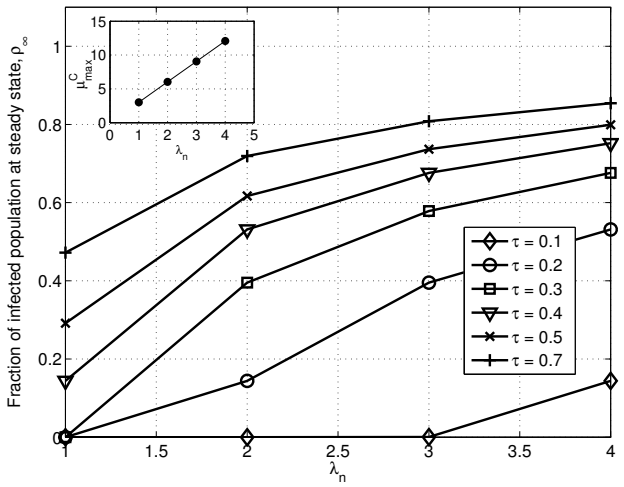


Fig. 8. The steady state of infected fraction of population monotonously increases when traffic is increased. Inset plot provides the spectral radius of C due to the change in $\lambda_n : \forall n$.

Since the epidemic threshold is inversely proportional to the spectral radius, then

$$\tau_c(C) = \frac{1}{\mu^C_{max}} \ge \tau_c(C') = \frac{1}{\mu^{C'}_{max}}.$$

Moreover, if C is primitive, then the monotonicity is strict. □

Theorem 2 shows that positive perturbation on C will inversely affect τ_c (*i.e.*, increment of any $c_{m,n}$ will monotonously lower τ_c and vice versa). Following this, in a network with a static topology and common routing protocol, higher traffic intensity will always lower the critical epidemic threshold and thus, promote and maintain the existence of the epidemic and conversely, the epidemic is more likely to die off when traffic intensity is lower. We show in Fig. 8 this monotonicity by increasing the aggregate load in the system by using an increasing λ for all nodes. Note that, however, this increase of ρ_∞ due to the change in λ is not linear.

However, the traffic load in a network is usually uncontrollable (or at best, partially controlled via traffic shaping/policing) as it depends, among many other aspects, on user behaviors. Conversely, the routing protocol is configured by the network operator and hence, controllable. We now investigate the effect of the routing protocol R. For this purpose, we leverage ER graphs with edge disorder (weighted network scenario) where non-uniform link weights are applied to the links independent of the degrees of the vertices involved. By using the same set of graphs, we fix the degree distribution for each one (*i.e.*, A unchanged) while by varying the disorder regime (through altering the link weight distribution), we obtain different R matrices and thus, the node involvement in handling traffic (*i.e.*, C) for the same graph.

Specifically, we consider non-negative independent and identically distributed (i.i.d) link weights in an additive setup to create different traffic distributions in the same graph by controlling the disorder of the graph. For this purpose, we

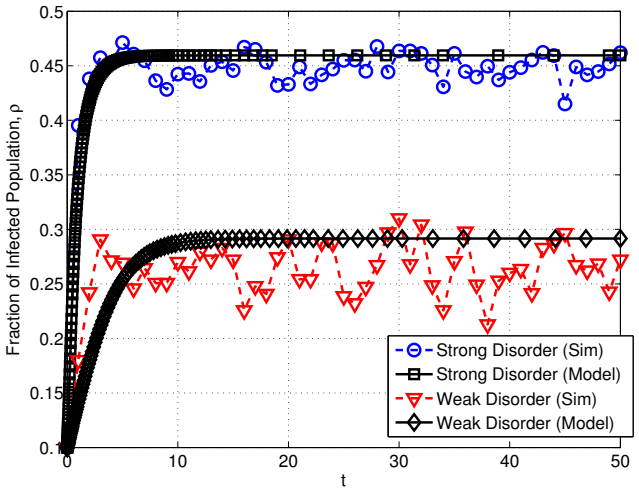


Fig. 9. (Color online) By changing the paths used for information delivery between node pairs, different level of steady state infected fraction is achieved in the same network.

follow [47] (Chapter 16) to use the polynomial link weight distribution.

$$F_w(x) = x^{\alpha}\mathbf{1}_{x\in[0,1]} + \mathbf{1}_{x\in(1,\infty)},\ \alpha > 0 \tag{30}$$

where $\mathbf{1}_x$ equals one if x is true and zero otherwise. When $\alpha \to 0$, the information delivery paths are mainly determined by the highest link weight of the constituent links. This corresponds to a strong disorder limit. In this disorder regime, each path between two nodes is characterized by the maximum link weight along that path and the shortest path is simply the path with the minimal maximum link weight between the two nodes. To create a weak disorder limit, we simply revert to constant unitary link weights (*i.e.*, non-weighted networks). In a weakly disordered system, most, if not all, of the links in a path contribute to the determination of the shortest path between two nodes. Essentially, changing the link weight distribution results in a different set of shortest paths for the same graphs and thus a different disorder limit is achieved. We can then study the impact of paths independent of the degree distribution.

We show in Fig. 9 the evolution of infected fraction over time for both strong and weak disorder regimes, whereby a higher infected fraction is expected for strong disorder limit. Because of the fact that the different fractions are obtained in the same ER graph, we also conclude that the degree distribution no longer directly determine the effective spreading of epidemic. This further confirms that the spreading is directly influenced by the delivery paths rather than the degree of the nodes.

Theorem 3 (Maximum achievable τ_c given A and Γ)**.** *When the network topology, A, and traffic load, Γ, are known, then*

$$\tau_c = \tau_c^{max} \text{ when } R = R^{\cup SPT}$$

where $R^{\cup SPT}$ is the routing matrix of the shortest paths by hop count between all possible node pairs in A.

Proof. Let R^* denote the binary routing matrix of an arbitrary routing protocol. We know that $\sum_{n=1}^{N}\sum_{k=1}^{N(N-1)} r^*_{n,k}$ is minimum *iff* $R^* = R^{\cup SPT}$. Conditioned by a fixed Γ, and after applying Eq. 9, we can observe the following:

$$\sum_{m=1}^{N} c_{n,m}^{\cup SPT} \leq \sum_{m=1}^{N} c^*_{n,m} : \forall n.$$

This implies that the total node involvement for delivering infectious agent in the network is inflated since by not using the shortest paths, more nodes are involved in delivering the same amount of infectious agents (*i.e.*, $\rho^{\cup SPT} \leq \rho^*$). Hence,

$$\tau_c^{max} = \tau_c^{\cup SPT} \geq \tau_c^*$$

where $\tau_c^{\cup SPT}$ denotes the critical threshold of the system when shortest path routing by hop count is used.

□

Theorem 3 defines the upper bound of τ_c for a specific workload in a network and this upper bound is achieved when the routing protocol uses only hop count as the metric to compute the shortest paths between all node pairs. However, routing in real networks does not always minimize hop count. For instance, although the Open Shortest Path First (OSPF) intra-domain routing protocol used in IP networks is based on Dijkstra's shortest path algorithm, it is often interfered by traffic engineering operations that uses link weights to change the resulting routes. It is worse for inter-domain routing where the routing protocol used (*i.e.*, Border Gateway Protocol (BGP)) is policy-based and does not even attempt to minimize any specific length criterion. As such, based on Theorem 3, it is often possible to decrease the spreading conduciveness of networks by changing the routing protocol such that $R^* \to R^{\cup SPT}$.

Theorem 4 (τ_c of different networks)**.** *For two different networks of size N denoted by A and A',*

$$\tau_c(A) \leq \tau_c(A') \tag{31}$$

when

$$\frac{1}{N}\sum_{n=1}^{N}\sum_{k=1}^{N(N-1)} r_{n,k} \geq \frac{1}{N}\sum_{n=1}^{N}\sum_{k=1}^{N(N-1)} r'_{n,k}$$

under the same load where $\tau_c(A)$ denotes the critical epidemic threshold of network A.

Proof. When Γ is equivalent for both networks, then according to Eq. 9, the determining factor of τ_c is R. However, the construction of R (*i.e.*, the computation of paths between node pairs) are constrained by the topology, A. Since A determines possible R matrices, from Theorem 3, we know that

$$\mu_{max}^{C} \propto \frac{1}{N}\sum_{n=1}^{N}\sum_{k=1}^{N(N-1)} r_{n,k}$$

i.e., the higher the average path lengths between all pairs of nodes, the higher the spectral radius of C. Consequently, the C of A having higher average path lengths will result in higher

magnitude of spectral radius, μ^C_{max}. Since the threshold is inversely proportional to μ^C_{max} and by the monotonicity of τ_c (*i.e.*, Theorem 2), this theorem is proven. □

This theorem is especially useful for cases where the network topology can be flexibly constructed either following certain requirements (*e.g.*, data center networks) or specific rules/guidelines (*e.g.*, self-organizing wireless sensor networks). Depending on the application scenario, the topology can be constructed to promote or suppress epidemic spreading.

For instance, in data center (DC) networking, the design of DC topology is a complex problem, already constrained by various factors (*e.g.*, resource fragmentation, oversubscription ratio, *etc.*). Theorem 4 allows the direct comparison of different DC topology designs with regards to the spreading capacity of the topologies. On the other hand, self-organizing sensor networks often operate in highly volatile conditions with uncertainties (*e.g.*, due to changing environment, intermittent connectivity, failures, power conservation requirements *etc.*), resulting in time varying topologies. In such a scenario, a network conducive to information spreading is often desirable to ensure high availability and persistence of information.

VII. Case Studies

In this section, we apply our path-based epidemic analytical framework to three real world Tier-1 networks (*i.e.*, Level-3 (AS1), Sprint (AS1239) and AT&T (AS7018) at point-of-presence (POP)-level based on the data from [21]) to investigate how conducive they are regarding path-based epidemic spreading. Table II outlines the relevant properties of these networks. Two sets of values are computed for parameters related to paths, (1) non-weighted and (2) weighted links. We can see from the table that contact-based epidemics have lower critical thresholds than path-based ones, implying that path-based epidemics are easier to die off. This may be slightly misleading. While for a contact-based epidemic, infection is always possible between neighboring nodes (*i.e.*, each infected node is infecting all its neighbors at all times), the path-based epidemic relies on the infectious agent to carry the infection. As such, increasing the traffic load in the system, Λ, will monotonically decrease τ_c (cf. Theorem 2) and at one point, the path-based epidemic will have lower τ_c than its counterpart. We also show in Fig. 10 the dependence of the threshold and the size of the epidemic on the traffic load and infection rate for the three networks. Increasing the traffic load and/or infection rate in the system will also increase the prevalence of the epidemic and decrease the critical epidemic threshold.

Furthermore, we see that for each case, routes computed via weighted graphs result in a more vulnerable network against a path-based epidemic. However, for all cases, even though not all shortest paths are used, the overall average path lengths are still relatively close [54] and the critical thresholds do not deviate significantly from the lower bound of τ_c (cf. Theorem 3). Table III compares the top ranked nodes for both contact- and path-based epidemics based on degrees and i_∞ (*i.e.*, the probability of the node be in the infected state at steady state).

It illustrates the vulnerability of the network at nodal-level. For a contact-based epidemic, the probability of a node being infected is strongly correlated with its degree (*i.e.*, compare columns 2 and 3). The set of top ranked nodes is almost identical with the nodes having the highest degrees. However, this relationship is weaker for path-based epidemic. For example, in the Sprint network, Tuckerton, London and Manasquan are three cities having low degrees but with relatively important role in the overall epidemic spread. This is especially highlighted by Tuckerton which has only four direct neighbors but has the highest probability of being infected based on the paths computed using the inferred weights. In this case, the operator of the Sprint network should "immunize" Tuckerton first when combating against path-based spreading in their weighted network while they should do the same to Chicago for contact-based spreading. For the Level-3 network, the operator should protect Washington, Denver and Indianapolis against contact-based, path-based unweighted and path-based weighted epidemics respectively. For the AT&T network, Chicago is the most important node both for contact-based and path-based epidemics (with uniform traffic distribution).

Going beyond uniform traffic distribution, we further constructed traffic matrices for each of the three networks based on the observed traceroute traffic in the dataset from [21] to investigate a hypothetical infection spreading via traceroute traffic. The respective {min, max, mean} values of the traffic matrices for Level-3, Sprint and AT&T networks are {2, 266295, 32275}, {2, 228201, 41556} and {2, 384754, 17690}. The top ranked cities based on their steady state infection probabilities are given in column 6 of Table III. The non-uniform traffic distribution again changes the infection probability of different nodes. For instance, Houston, only having the degree of two in the Level-3 network, is now among the most vulnerable nodes. On the other hand, New York emerges as the most vulnerable city for the AT&T network. With these traffic matrices, we further computed the corresponding critical thresholds, τ_c as 2.7522×10^{-6}, 2.2200×10^{-6} and 1.9899×10^{-6} for Level-3, Sprint and AT&T networks respectively. The very low thresholds further support the reported observations of [29], [30] whereby epidemics in real networks are highly persistent.

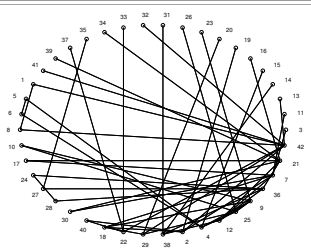
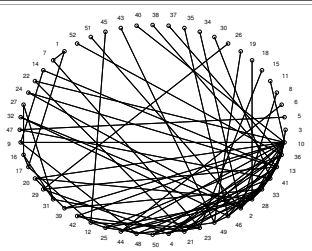
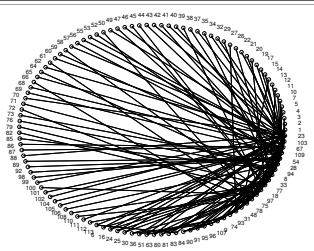
VIII. Conclusions

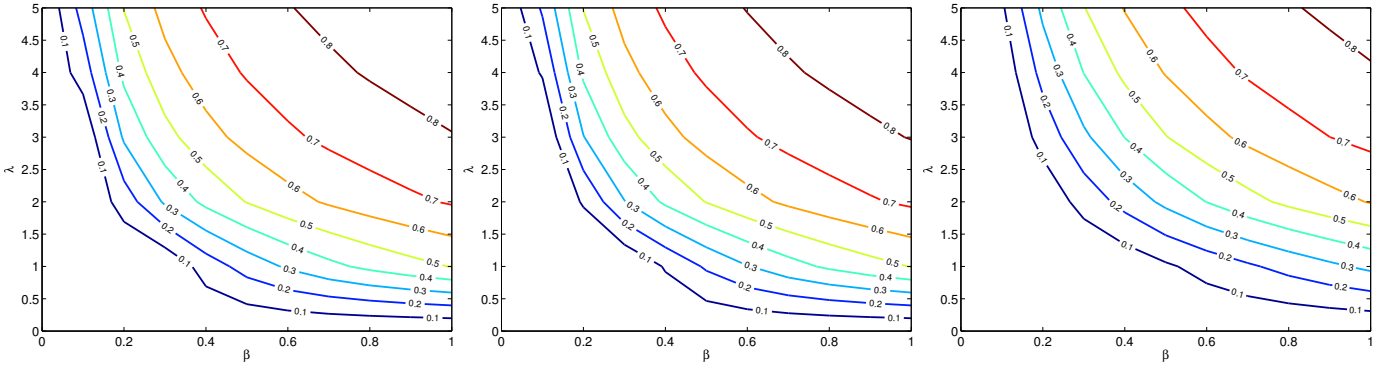
Many infection spreading phenomena follow paths. Infection passed from one node to another also relies on certain infectious agent as the physical transport medium. In this paper, we model such path-based epidemic spreading taking into account the volume and distribution of the infectious agent. Although our modeling methodology is general in nature, we focus our work in the context of communication networks and consider data packets as the infectious agent. Extending [18] as the modeling basis, our analytical framework considers each node individually rather than aggregating node behaviors and is of polynomial complexity. We express

[7] All properties relevant to C in this table assume $\lambda_n = 1 : \forall n \in V$.

[8] Bracketed values in columns 2-6 indicate the node degrees.

TABLE II
TOPOLOGICAL PROPERTIES OF SAMPLE REAL NETWORKS [21], [52], [53][7]

Properties	Level-3 (AS1)	Sprint (AS1239)	AT&T (AS7018)
			
N	42	52	113
d	2.6190	3.2308	2.6018
d_{max}	8	14	25
Average path length	3.7271 (unweighted) 3.9826 (weighted)	3.4721 (unweighted) 3.5765 (weighted)	3.3475 (unweighted) 3.4603 (weighted)
μ^A_{max}	3.9669	5.7166	6.9066
$\tau_c^{contact}$	0.2521	0.1749	0.1448
μ^C_{max}	3.1716 (unweighted) 3.4090 (weighted)	3.0252 (unweighted) 3.1123 (weighted)	2.7743 (unweighted) 2.8687 (weighted)
τ_c^{path}	0.3153 (unweighted) 0.2933 (weighted)	0.3306 (unweighted) 0.3213 (weighted)	0.3605 (unweighted) 0.3486 (weighted)



(a) Level-3 (AS1) (b) Sprint (AS1239) (c) AT&T (AS7018)

Fig. 10. (Color online) The fraction of infected nodes, ρ_∞, shown above as contour for Level-3, Sprint and AT&T networks (all using the weighted paths), driven by traffic conditions and infection rate. As traffic flows increases (λ_n), the size of epidemic increases while the critical threshold, τ_c, decreases.

the impact of traffic intensity and distribution in the network as well as the paths computed by the routing protocol via an epidemic characterization matrix C that is able to describe the epidemic behavior. We then find that the critical path-based epidemic threshold equals the reciprocal of C's spectral radius (*i.e.*, $\tau_c = 1/\mu^C_{max}$). Infection permeation in contact-based epidemic is largely determined by the topology structure, A. This is not the case for path-based epidemic as the primary factors for infection spreading are now related to the traffic load and the way this is routed to destinations. This provides us with two "tuning knobs" to control the behavior of the epidemic within the same network structure: (1) by modifying traffic intensity through traffic engineering, shaping/policing and admission control techniques and (2) by using different routing protocols to construct delivery paths. Based on these, we further derive conditional bounds for τ_c, subject to the availability of information regarding traffic load in the network and the routing algorithms, such that the network operator may use to control the epidemic as needed. In addition, since we consider each node separately, we can also easily identify/rank nodes within the network that are the most conducive to spreading the infection. Such nodal-level information may be used as a new centrality metric when designing immunization/protection schemes. We illustrate the applicability of our scheme to three real networks by using their inferred link weight sets and traceroute data. Based on our model, the critical epidemic thresholds are diminishingly small with λ and this re-affirms the observations reported in [29], [30] that epidemics in communication networks are extremely robust to extinction. Our modelling approach is general in nature and

TABLE III
TOP 10 NODES IN THE THREE NETWORKS RANKED IN DESCENDING ORDER BASED ON DEGREES (COLUMN 2) AND i_∞ (COLUMNS 3-6).[8]

AS	Degrees	Contact-based	Path-based Unweighted links, $\lambda_n = 1; \forall n$	Path-based Weighted links, $\lambda_n = 1; \forall n$	Path-based Weighted links, $\lambda_n \rightarrow$ traceroute data [21]
Level-3 (AS1)	Washington (8)	Washington (8)	Denver (5)	Indianapolis (4)	New York (5)
	Carrolton (7)	Carrolton (7)	Carrolton (7)	Chicago (6)	Boston (5)
	Los Angeles (7)	Chicago (6)	Atlanta (5)	Philadelphia (4)	Philadelphia (4)
	Chicago (6)	Denver (5)	Chicago (6)	Denver (5)	Chicago (6)
	San Jose (6)	Los Angeles (7)	Washington (8)	Washington (8)	Denver (5)
	Boston (5)	San Jose (6)	San Jose (6)	Carrolton (7)	San Jose (6)
	Atlanta (5)	Atlanta (5)	Indianapolis (4)	San Jose (6)	Indianapolis (4)
	New York (5)	New York (5)	Los Angeles (7)	Atlanta (5)	Washington (8)
	Denver (5)	Indianapolis (4)	Boston (5)	Los Angeles (7)	Carrolton (7)
	Indianapolis (4)	Boston (5)	Philadelphia (4)	New York (5)	Houston (2)
Sprint (AS1239)	Chicago (14)	Chicago (14)	Chicago (14)	Tuckerton (4)	Chicago (14)
	Dallas (9)	Pennsauken (8)	San Jose (8)	Relay (9)	Relay (9)
	Relay (9)	Dallas (9)	Relay (9)	San Jose (8)	New York (8)
	Pennsauken (8)	Relay (9)	Tuckerton (4)	Chicago (14)	Dallas (9)
	New York (8)	New York (8)	London (5)	London (5)	Atlanta (5)
	San Jose (8)	San Jose (8)	Dallas (9)	Manasquan (4)	Tuckerton (4)
	Anaheim (7)	Stockton (6)	Manasquan (4)	Anaheim (7)	San Jose (8)
	Stockton (6)	Atlanta (5)	New York (8)	Pennsauken (8)	Manasquan (4)
	Atlanta (5)	Anaheim (7)	Anaheim (7)	Dallas (9)	Anaheim (7)
	Kansas City (5)	Kansas City (5)	Pennsauken (8)	New York (8)	London (5)
AT&T (AS7018)	Chicago (25)	Chicago (25)	Chicago (25)	Chicago (25)	New York (18)
	St. Louis (18)	St. Louis (18)	Dallas (12)	Washington (16)	Philadelphia (8)
	New York (18)	New York (18)	New York (18)	New York (18)	San Francisco (11)
	Washington (16)	Washington (16)	Atlanta (10)	Dallas (12)	Chicago (25)
	Los Angeles (13)	Los Angeles (13)	Washington (16)	Atlanta (10)	Washington (16)
	Dallas (12)	Dallas (12)	St. Louis (18)	St. Louis (18)	Los Angeles (13)
	San Francisco (11)	San Francisco (11)	Los Angeles (13)	Cambridge (8)	Dallas (12)
	Atlanta (10)	Detroit (9)	Orlando (7)	Los Angeles (13)	Seattle (7)
	Detroit (9)	Atlanta (10)	Philadelphia (8)	Philadelphia (8)	St. Louis (18)
	Cambridge (8)	Seattle (7)	San Francisco (11)	Orlando (7)	Atlanta (10)

can be easily extended to model different epidemic models such as *SIR* (analogous to [35] for contact-based epidemic).

ACKNOWLEDGMENT

This work was partially funded by the Engineering and Physical Sciences Research Council (EPSRC) under the CHIST-ERA CONCERT (A Context-Adaptive Content Ecosystem Under Uncertainty), project number *I1402*. The authors would like to thank Faryad D. Sahneh for his helpful discussion prior to the conception of this work and Lorenzo Saino, Konstantinos V. Katsaros, Vasilis Sourlas and the reviewers for their constructive comments.

REFERENCES

[1] D. J. Daley and J. Gani, "Epidemic modelling: an introduction," Cambridge, UK, Cambridge Press, 1999.
[2] Y. Iturria-Medina, *et. al.*, "Epidemic spreading model to characterize misfolded proteins propagation in aging and associated neurodegenerative disorders," PLoS Computational Biology, 10(11), e1003956, 2014.
[3] H. Li, X. Cheng and J. Liu, "Understanding video sharing propagation in social networks: measurement and analysis," ACM Trans. Multimedia Comput. Commun. Appl., vol. 10, no. 4, pp. 33:1-33:20, Jun 2014.
[4] V. Colizza, *et. al.*, "The role of the airline transportation network in the prediction and predictability of global epidemics", Proc. of National Academy Science, USA, pp. 2015-2020, 2006.
[5] Z. Ruan, *et. al.*, "Risks of an epidemic in a two-layered railway-local area traveling network", the European Physical Journal B, 86:13, 2013.
[6] A. Bernstein, D. Bienstock, D. Hay, M. Uzunoglu and G. Zussman, "Power Grid Vulnerability to Geographically Correlated Failures - Analysis and Control Implications," IEEE INFOCOM, pp. 2634-2642, 2014.
[7] M. Garetto, W. Gong and D. Towsley, "Modeling malware spreading dynamics," IEEE INFOCOM, vol. 3, pp. 1869-1879, 2003.
[8] D. Chakrabarti, J. Leskovec, C. Faloutsos, S. Madden, C. Guestrin and M. Faloutsos, "Information survival threshold in sensor and p2p networks," IEEE INFOCOM, pp. 1316-1324, 2007.
[9] M. Vojnović, V. Gupta, T. Karagiannis and C. Gkantsidis, "Sampling strategies for epidemic-style information dissemination", *IEEE/ACM* Trans. on Networking, vol. 18, no. 4, Aug. 2010.
[10] G. Xylomenos, *et. al.*, "A Survey of Information-Centric Networking Research," in Communications Surveys & Tutorials, IEEE , vol. 16, no. 2, pp.1024-1049, 2014.
[11] W. K. Chai, D. He, I. Psaras and G. Pavlou, "Cache "less for more" in information-centric networks (Extended version)," Elsevier Computer Communications Journal, vol. 36, no. 7, pp. 758-770, 1 Apr. 2013.
[12] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. Briggs and R. Braynard, "Networking Named Content," Proceedings of the 5th ACM International Conference on Emerging Networking Experiments and Technologies (CoNEXT 2009); 2009 December 1-4; Rome, Italy. NY: ACM; 2009; 1-12.
[13] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley and S. Havlin, "Catastrophic cascade of failures in interdependent networks," Nature, vol. 464, no. 7291, pp. 1025-1028, 15 Apr. 2010.
[14] W. K. Chai, V. Kyritsis, K. V.Katsaros and G. Pavlou, "Resilience of Interdependent Communication and Power Distribution Networks against Cascading Failures," Proceedings of the 15th IFIP Networking, Vienna, Austria, 17-19 May 2016.
[15] T. Spyropoulos, K. Psounis and C. S. Raghavendra, "Efficient Routing in Intermittently Connected Mobile Networks: The Single-Copy Case," *IEEE/ACM* Trans. on Networking, vol. 16, no. 1, pp. 63–76, Feb. 2008.

[16] T. Spyropoulos, K. Psounis and C. S. Raghavendra, "Efficient Routing in Intermittently Connected Mobile Networks: The Multiple-Copy Case," *IEEE/ACM* Trans. on Networking, vol. 16, no. 1, pp. 77–90, Feb. 2008.
[17] T. N. Dinh, H. Zhang, D. T. Nguyen and M. T. Thai, "Cost-effective viral marketing for time-critical campaigns in large-scale social networks," *IEEE/ACM* Trans. on Networking, vol. 22, no. 6, pp. 2001-2011, Dec. 2014.
[18] P. Van Mieghem, J. Omic and R. Kooij, "Virus spread in networks," *IEEE/ACM* Trans. on Networking, vol. 17, no. 1, Feb. 2009.
[19] P. Van Mieghem, "The N-intertwined SIS epidemic network model," *Computing*, 93(2):147-169, 2011.
[20] F. Darabi Sahneh, C. Scoglio and P. Van Mieghem, "Generalized epidemic mean-field model for spreading processes over multi-layer complex networks," *IEEE/ACM* Trans. on Networking, vol. 21, no. 5, pp. 1609-1620, Oct. 2013.
[21] http://research.cs.washington.edu/networking/rocketfuel/. Last accessed: 11-Nov-2015.
[22] I. Gupta, A.-M. Kermarrec and A. J. Ganesh, "Efficient and adaptive epidemic-style protocols for reliable and scalable multicast," IEEE Trans. on Parallel and Distributed Systems, vol. 17, no. 7, pp. 593-605, 2006.
[23] Y. Li and J. Lui, "Epidemic attacks in network-coding-enabled wireless mesh networks: detection, identification, and evaluation," *IEEE/ACM* Trans. on Networking, vol. 12, no. 11, pp. 2219-2231, Nov. 2013.
[24] W. O. Kermack and A. G. McKendrick, "A Contribution to the Mathematical Theory of Epidemics", Proc. of the Royal Society A: Mathematical, Physical and Engineering Sciences 115 (772): 700.
[25] P. Whittle, "The outcome of a stochastic epidemic – a note on Bailey's Paper," *Biometrika*, vol. 42, p. 116-122, 1955.
[26] R. M. Anderson and R. M. May"Infectious Diseases of Humans", Oxford: Oxford University Press, 1991.
[27] F. Darabi Sahneh and C. Scoglio, "Epidemic spread in human networks," Proc. of IEEE Conference on Decision and Control, Dec. 2011.
[28] J. O. Kephart and S. R. White, "Measuring and modelling computer virus prevalence," IEEE Symposium on Security and Privacy, 1993.
[29] R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," Physical Review Letters, vol. 86, no. 14, 3200-3203, 2001.
[30] M. Boguñá, R. Pastor-Satorras and A. Vespignani, "Absence of epidemic threshold in scale-free networks with degree correlations", Physical Review Letters, vol. 90, no. 2, 17 Jan. 2003.
[31] Y. Wang, D. Chakrabarti, C. Wang and C. Faloutsos, "Epidemic spreading in real networks: an eigenvalue viewpoint," *Proc.* 22^{nd} *Int'l. Symp. Reliable Distributed Systems (SRDS)*, Oct. 2003, pp. 25-34.
[32] D. Chakrabarti, Y. Wang, C. Wang, J. Leskovec and C. Faloutsos, "Epidemic spreading in real networks," ACM Trans. on Information and System Security, 10(4)(2008), pp. 1-26.
[33] C. Peng, X. Jin and M. Shi, "Epidemic threshold and immunization on generalized networks," Physica A, vol. 389, pp. 549-560, 2010.
[34] Z. Nikoloski, N. Deo and L. Kucera, "Correlation model of worm propagation on scale-free networks," *Complexus Network Modelling*, vol. 3, pp. 169-182, 2006.
[35] M. Youssef and C. Scoglio, "An individual-based approach to SIR epidemics in contact networks," *Journal of Theoretical Biology*, vol. 283, no. 1, pp. 136-144, 2011.
[36] V. Colizza and A. Vespignani, "Epidemic modeling in metapopulation systems with heterogeneous coupling pattern: Theory and simulations", Journal of Theoretical Biology 251, pp. 450-467, 2008.
[37] Q. Xuan, F. Du, L. Yu and G. Chen, "Reaction-diffusion processes and metapopulation models on duplex networks", Physics Review E vol. 87, no. 3, 032809, 2013
[38] J-P Onnela and N. A. Christakis, "Spreading paths in partially observed social networks," Phys. Rev. E, vol. 85, no. 3, pp. 036106, Mar. 2012.
[39] S. Meloni, A. Arenas and Y. Moreno, "Traffic-driven epidemic spreading in finite-size scale-free networks," Proc. National Academy of Sciences (PNAS), vol. 106, no. 40, 16897-16902.
[40] R. Guimerá, A. Díaz-Guilera, F. Vega-Redondo, A. Cabrales and A. Arenas, "Optimal network topologies for local search with congestions," Physics Review Letter 89:248701, 2002.
[41] S. Wassermann and K. Faust, "Social Network Analysis: Methods and Applications," Cambridge, Cambridge University Press, 1994.
[42] H.-X. Yang, Z.-X. Wu and B.-H. Wang, "Suppressing traffic-driven epidemic spreading by edge-removal strategies," Physical Review E 87, 064801, 2013.
[43] H.-X. Yang and Z.-X. Wu, "Suppressing traffic-driven epidemic spreading by use of the efficient routing protocol," Journal of Statistical Mechanics: Theory and Experiment, no. 3, 1742-5468/14/P03018.
[44] P. Tune and M. Roughan, "Internet traffic matrices: A primer," *Recent Advances in Networking*, Vol. 1. ACM SIGCOMM, pp. 108-163, 2013.
[45] P. Pantazopoulos, M. Karaliopoulos and I. Stavrakakis, "Centrality-driven scalable service migration," Proc. International Teletraffic Congress (ITC), 2011.
[46] Cisco White Paper, "Building accurate traffic matrices with demand deduction," http://www.cisco.com/c/en/us/products/collateral/routers/wan-automation-engine/white_paper_c11-728552.pdf, 2013. Last accessed: 11-Nov-2015.
[47] P. Van Mieghem, "Performance analysis of communications systems and networks," Cambridge University Press, Cambridge, 2006.
[48] A. Ganesh, L. Massoulié, D. Towsley, "The effect of network topology on the spread of epidemics," IEEE INFOCOM, pp. 1455-1466, 2005.
[49] P. Erdős and A. Rényi, "On random graphs I," Publicationes Mathematicae no. 6, pp. 290-297, 1959.
[50] A. L. Barabasi and R. Albert, "Emergence of scaling in random networks," Science, vol. 286, no. 5439, pp. 509-512, Oct. 1999.
[51] A. Berman, R. J. Plemmons, "Nonnegative matrices in the mathematical sciences," Society of Industrial Mathematics, 1994.
[52] N. Spring, R. Mahajan and D. Wetherall, "Measuring ISP Topologies with Rocketfuel," Proc. of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '02), pp. 133-145, 2002.
[53] R. Mahajan, N. Spring, D. Wetherall and T. Anderson, "Inferring Link Weights Using End-to-end Measurements," ACM SIGCOMM Workshop on Internet Measurement (IMW '02), pp. 231-236, 2002.
[54] N. Spring, R. Mahajan and T. Anderson, "Quantifying the causes of path inflation," ACM SIGCOMM, 2003.

Wei Koong Chai received the B.Eng. degree in electrical engineering from the Universiti Teknologi Malaysia, Johor Bahru, Malaysia, in 2000, and both the M.Sc. (Distinction) and the Ph.D. degrees from the University of Surrey, Surrey, U.K., in 2002 and 2008, respectively. He is currently a Senior Research Associate at the Department of Electronic and Electrical Engineering, University College London, London, U.K. His research spans across heterogeneous networks including wired/wireless networks and cyber physical systems. His current research interests include information-centric networking, smart grid communication and network science. He has in the past involved in research on quality of service, resource management (e.g., for satellite networks and wireless mesh networks), cross-layer design (specifically on interaction of protocols at different layers), traffic engineering, and network optimization.

George Pavlou received the Diploma degree in engineering from the National Technical University of Athens, Athens, Greece, and the M.Sc. and Ph.D. degrees in computer science from University College London, London, U.K. He is a Professor of communication networks in the Department of Electronic and Electrical Engineering, University College London, where he coordinates research activities in networking and network management. His research interests include networking and network management, including aspects such as traffic engineering, quality of service management, autonomic networking, information-centric networking, grid networking, and software-defined networks. He has been instrumental in a number of European and U.K. research projects that produced significant results with real-world uptake and has contributed to standardization activities in ISO, ITU-T, and IETF. He has been on the editorial board of a number of key journals in these areas and he is the Chief Editor of the bi-annual IEEE Communications Network and Service Management Series. In 2011 he received the IFIP/IEEE Daniel Stokesbury Award for distinguished technical contributions to the growth of the network management field.