Ecological Modelling 383 (2018) 91–97

Contents lists available at ScienceDirect

Ecological Modelling

journal homepage: www.elsevier.com/locate/ecolmodel

The intrinsic vulnerability of networks to epidemics

G. Strona[a,*], C.J. Carstens[b], P.S.A. Beck[a], B.A. Han[c]

[a] European Commission, Joint Research Centre, Directorate D – Sustainable Resources – Bio-Economy Unit, 21027 Ispra, VA, Italy
[b] University of Amsterdam, Korteweg de Vries Instituut, 1098 XG Amsterdam, The Netherlands
[c] Cary Institute of Ecosystem Studies, Millbrook, NY 12545, USA

ARTICLE INFO

Keywords:
Contact networks
Disease ecology
Emerging infectious diseases
Epidemic model
Immunization

ABSTRACT

Contact networks are convenient models to investigate epidemics, with nodes and links representing potential hosts and infection pathways, respectively. The outcomes of outbreak simulations on networks are driven both by the underlying epidemic model, and by the networks' structural properties, so that the same pathogen can generate different epidemic dynamics on different networks. Here we ask whether there are general properties that make a contact network intrinsically vulnerable to epidemics (that is, regardless of specific epidemiological parameters). By conducting simulations on a large set of modelled networks, we show that, when a broad range of network topologies is taken into account, the effect of specific network properties on outbreak magnitude is stronger than that of fundamental pathogen features such as transmission rate, infection duration, and immunization ability. Then, by focusing on a large set of real world networks of the same type (potential contacts between field voles, *Microtus agrestis*), we showed how network structure can be used to accurately assess the relative, intrinsic vulnerability of networks towards a specific pathogen, even when those have limited topological variability. These results have profound implications for how we prevent disease outbreaks; in many real world situations, the topology of host contact networks can be described and used to infer intrinsic vulnerability. Such an approach can increase preparedness and inform preventive measures against emerging diseases for which limited epidemiological information is available, enabling the identification of priority targets before an epidemic event.

1. Introduction

Network analysis is a powerful approach for investigating epidemics, with nodes representing anything from individuals to countries, and links mapping transmission routes that pathogens can exploit to spread from one node to another (Newman, 2002; Keeling and Eames, 2005; Strona and Castellano, 2018). This general framework permits simulating different epidemiological scenarios over the same network (Pastor-Satorras et al., 2015), yielding disease-specific outcomes that could be important for informing management and intervention strategies (Rushmore et al., 2013; Yamin et al., 2014; Sun et al., 2014; Herrera et al., 2016). Although each scenario has its own characteristics and is expected to lead to specific outcomes, those are also constrained by network structure. Understanding to what extent such constraints can attenuate differences between different epidemiological scenarios may offer important insights into the ecology and dynamics of infectious disease spread (Keeling, 2005).

Common models that investigate epidemics in networks are based on identifying distinct categories (i.e., compartments) that define the health status of a host, and a set of specific rules dictating the probability of transition from one status to another. In a typical implementation of epidemic models, nodes can be in one of three different states at any given time: susceptible to the infection, S; infected, I; and recovered/removed from the system, R (following complete immunization or death). Different epidemic models are then formulated by varying the rules that permit hosts to transition from one state to another. For example, a very common model is the *SI*, where nodes can pass only from S to I. In the *SIS* models, infected nodes are allowed to roll back to the susceptible state without gaining immunity ($I \rightarrow S$) according to a certain probability, which enables a disease to cycle in a host population by re-infecting individuals that have recovered from a previous infection. Simulating individuals gaining permanent or temporary immunity requires the addition of a third compartment that sees nodes removed from the network ($I \rightarrow R$), which creates more complex models, such as the *SIR* and the *SIRS* (note that, besides immunization, the R status may indicate the death of a node) (Pastor-Satorras et al., 2015).

The classic compartmental epidemic models are flexible and simple,

* Corresponding author.
E-mail address: giovanni.strona@ec.europa.eu (G. Strona).

https://doi.org/10.1016/j.ecolmodel.2018.05.013
Received 30 July 2017; Received in revised form 15 May 2018; Accepted 15 May 2018
Available online 26 May 2018

but moving beyond these particular formulations to establish more general topology-vulnerability relationships has been difficult, in part because they depict specific and distinct scenarios. As a result, the effects of network structure on disease outcomes are usually investigated by focusing on a particular type of network and pathogen whose features combine to determine disease dynamics (Pastor-Satorras et al., 2015). While precise, these constraints on model formulation limit our ability to compare dynamical outcomes across different networks configurations and across different pathogen types.

In an attempt to overcome these issues, we introduce here a generalization of classic compartmental models, which we named the 'Synthetic Network Epidemic Spread' (*SNES*) model. Despite its simple formulation, the *SNES* model permits the investigation of a wide range of epidemic scenarios in a continuous and controlled way, through tuning three parameters quantifying fundamental pathogen features: (1) the pathogen's transmission rate, τ; (2) the duration of infection (i.e., survival time of the pathogen in the host), ρ; and (3) the pathogen's immunization effect on hosts over repeated infections, ι. Such parameters (all bounded in [0, 1]) offer a straightforward way to perform comparisons across different epidemic scenarios.

Here we take advantage of this by applying the *SNES* model to a large set of simulated networks (representative of many different real world situations), and to a set of animal contact networks (representing potential encounters between field voles obtained from a mark/recapture study, Davis et al., 2015), with the aim to investigate to what extent network structure affects the outcome of an epidemic.

We found that, when a broad range of network topologies is taken into account, the epidemiological parameters of the model are in many cases less important than network structure in determining the magnitude of an epidemic outbreak. Of course, when similar networks are considered, as in the case of the field vole contact networks, epidemic parameters (and particularly transmission rate) became fundamental to determine epidemic magnitude. Nevertheless, even in the case of similarly structured networks, topological properties still permit an accurate assessment of relative network vulnerability towards a given class of pathogens (i.e. to pathogens whose spread can be modelled using similar epidemic parameters). These findings can help improve preparedness when limited epidemiological information is available and a fast response (for example in terms of prioritization) is needed, a situation that is expected to become ever more common in the future, due to the growing globalization, and the rapid emergence of new diseases.

2. Materials and methods

2.1. The Synthetic Network Epidemic Spread model (SNES)

At each time step, any node i can be infected by nodes pointing towards (or, in the case of an undirected network, connected to) it according to a given probability $\tau \times S_i$, with τ being the pathogen's transmission rate, and S_i being individual host susceptibility to the infection.

Concurrently, each node recovers with probability R_i, controlled by a parameter ρ, varying in [0, 1], and increasing with time since infection: $R_i = (1 - 1/(1 + t)^{\rho})$. Due to the purely theoretical nature of this study, the choice of the R_i function is arbitrary. This formulation of R_i, however, permits a smooth transition from situations where the probability of recovery increases very slowly with time (when ρ is close to 0), to opposite scenarios of fast recovery (when ρ is close to 1). It is intuitive that the concept behind the *SNES* model allows for maximum flexibility in the choice of $R_i(t)$ function, making it possible to accommodate specific situations. Yet, to avoid adding further complexity to our analyses (and possibly complicating the interpretation of results), we used the above formulation in all of our epidemic simulations.

The susceptibility of a node following infection becomes $S_i = S_i \times \iota$, with ι being equal for all individuals (since theoretically dependent on the pathogen) and varying in [0, 1]. This accounts for a general property of immunizing diseases where individuals who have been infected and who have recovered are less likely to be re-infected, which is the basis of vaccination (though we note there is variation with respect to immunity which is unaccounted for in these models; e.g., waning immunity; Scherer and McLean, 2002). Interestingly, analogies can be drawn for very different contexts, such as that of information spread in social networks. The probability that a person will share a piece of information will rapidly decrease when receiving the same piece of information again. In the following, we will refer to this process as 'immunization', but it may also represent the path towards removal/death of an individual, corresponding to real world situations where repeated infections can be fatal. As in the case of $R_i(t)$, $S_i(\iota)$ can also be adjusted to fit specific hypotheses.

The parameters ρ and ι combine to control disease behavior, for instance, the extent of disease spread in terms of number of infected nodes. These parameters also permit the model to be tuned to reflect typical epidemiological models such as *SI* (when $\rho = 0$, $\iota = 1$), *SIS* (when $\rho > 0$, $\iota = 1$), *SIR*(*S*) (when $\rho > 0$ and $\iota \leq 1$), or to explore epidemic scenarios in a continuous and controlled way. For example, the *SNES* framework makes it possible to track how epidemic outcomes compare between the *SI* scenario to a typical *SIS* scenario (Pastor-Satorras et al., 2015) by progressively increasing the probability that a host will recover and become susceptible again. Additionally, the *SNES* model can also be easily adapted to more specific scenarios. For example, the addition of a simple rule controlling the lapse between the time a node is infected and the time it becomes infectious enables the *SNES* to emulate compartment models that include latency (such as the *SEIRS*, which includes an 'exposed' class).

We note that the *SNES* is conceptually similar to a *SIRS* model were the transition probabilities $S \rightarrow I$, $I \rightarrow R$, and $R \rightarrow S$ are adjusted to particular values. Nevertheless, by departing from the typical compartmental scheme, the formulation of *SNES* offers some advantages in terms of clarity. In particular, while the different, typical compartmental models (and possibly a 'tunable' *SIRS*) focus on the possibility (and probability) of a host's transition from a health status to another, and use this constraint to identify different epidemic categories on the basis of permitted and forbidden transitions, the *SNES* attempts to remove the boundaries between different models. Those, in fact, simply represent different regions of an ideal, continuous three-dimensional space defined by ρ, ι and τ.

2.2. Generation of simulated networks

We tested our model on 10,000 simulated networks. To grow each network, we selected at random a model between four different well-known ones (configuration model; Erdos Renyi, *ER*; Barabasi–Albert, *BA*; and Watts–Strogatz, *WS*) (Strogatz, 2001). To build networks using the configuration model (Békéssy et al., 1972), we selected a random exponent for the power law degree distribution varying between 2 and 3. In *ER* networks we set the number of nodes (V) to a random integer in [50, 500] and the number of edges to a random integer in [V, 1000]. In *BA* networks, we set the number of nodes to a random integer in [500, 1000], and the number of outgoing edges generated for each node to ($V \times r \times 0.01 + 1$), with V being the number of nodes, and r being a random real number in [0, 1]. In *WS* networks, we set the dimension of the lattice to 1, the size of the lattice along all dimensions to a random integer in [50, 250], the distance within two nodes are connected to a random integer in [2, 10], and the rewiring probability to a random real number in [0, 1]. In this way, we obtained networks with a good variation in number of edges, nodes, connectance, clustering, and diameter (Fig. 1).

2.3. Reciprocity

Instead of focusing on directed and undirected networks separately,