Ανάλυση Κοινωνικών Δικτύων Και Εφαρμογές

Επιδημιολογικά Μοντέλα

Συμεών Παπαβασιλείου (papavass@mail.ntua.gr)
Βασίλειος Καρυώτης (vassilis@netmode.ntua.gr)

Πέμπτη, 2 Ιουνίου 2022

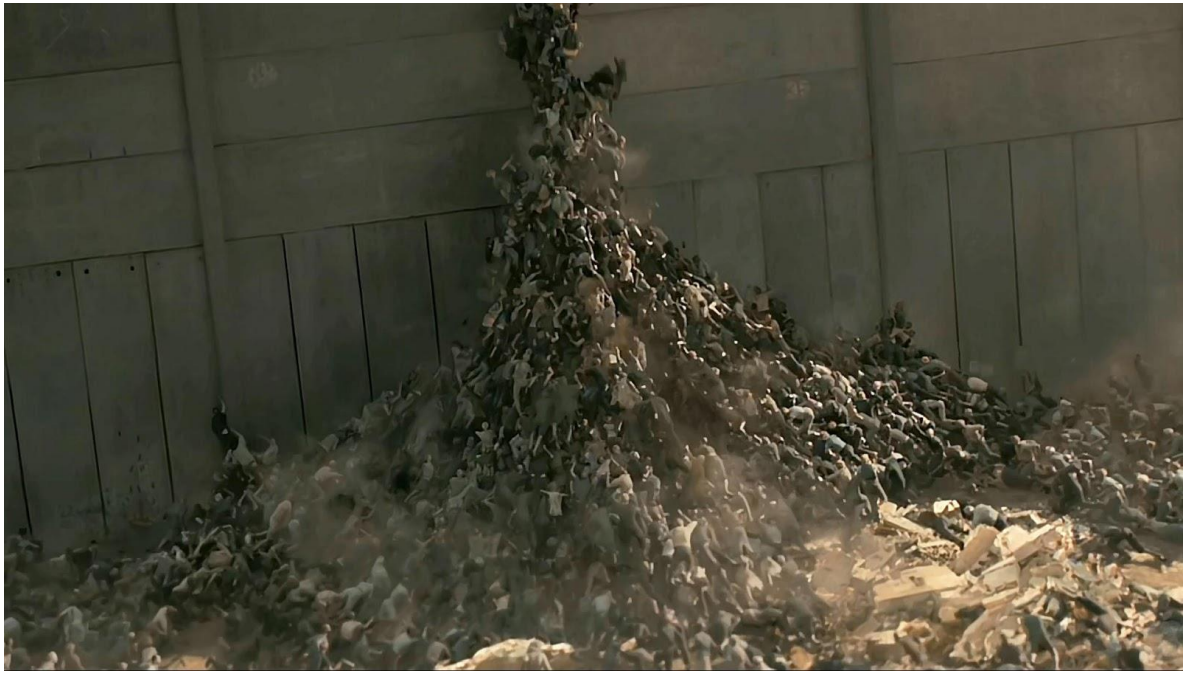
Outline

- Examples of epidemics
- Node infection paradigms
- Epidemic models
  - SI
  - SIR
  - SIRD
  - SIS
  - General epidemic model
- Comparison of epidemic models
- Examples from computer malware area
  - Application to information diffusion

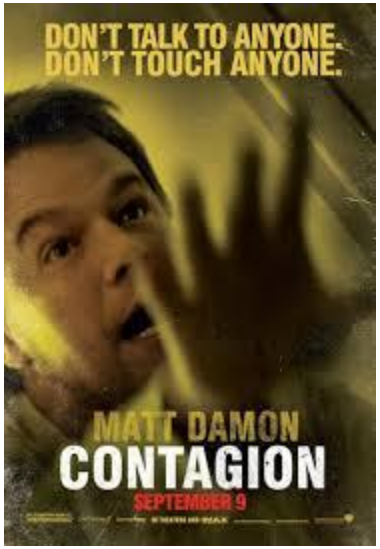
Examples of Epidemics

- Athens plague: 429-426BC (75-100k)
- Black plague – 1300s (30-70% of Europe's population)
- Cocoliztli (hemorrhagic fever): 1500s (50-80% of Mexico's population)
- HIV – AIDS: 1960s (up to now more than 30mil.)
- Ebola
- Blaster
- Slammer
- Love
- CodeRed
- "Fascinating" list of epidemics in:
  - https://en.wikipedia.org/wiki/List_of_epidemics
  - https://en.wikipedia.org/wiki/Comparison_of_computer_viruses

Not Scared Yet?



So Where's the Thin Red Line of Reality?



Epidemics

- Epidemics: from «επί» + «δήμος»
- Studies the rapid spread of “agents” on “populations”
- In network science → cross-section of biology with sociology, computer science, etc.
  - Populations
  - Contagious “modules”
    - Viruses
    - Diseases
    - Malware (malicious software)
  - Infection model
  - Objective: outcome of epidemic
- Form of network dynamics process
  - Studies propagation dynamics over interacting actors
  - Other structure-dependent network processes can be studied similarly

SNA and Epidemics

- Resemblance to diffusion of ideas, news, etc.
  - Example of "social contagion"
- Point-by-point contagion
- Fundamental difference:
  - Contagion: no decision-making → spreading of agent (random)
  - Social contagion: decision-making → propagation of agent
- ***Spreading*** vs. ***propagative*** networks
- Various models to describe such behaviors
  - Will be studied in the sequel
- Various outcomes as well:
  - Pandemic
  - Endemic
  - Distinction

Epidemics & Malware

- Various types of malware (malicious software)
- Also called outbreaks, threats, attacks, etc.
- Both spreading and propagative nature
- Different contamination types
  - Point-to-point or group infections

Threat	Malware type	Contamination type
Worms	propagation	point-to-point/group
Botnets	propagation/spreading	point-to-point
Trojan horses	spreading	point-to-point
Sinkhole/wormhole	spreading	point-to-point
Spyware	spreading	point-to-point
Trapdoors/Backdoors	spreading	point-to-point/group
DoS/DDoS	spreading	group/point-to-point
Phising	spreading	point-to-point
WiFi viruses	propagation	point-to-point/group
Bluetooth viruses	propagation	point-to-point
Smartphone viruses	spreading/propagation	point-to-point
Socialnet application viruses	spreading	group

Computers, Networks and Epidemics

- Malware started with individual computers – via floppy disks, only in universities
- Bloomed in networks when the latter proliferated
- Different scope and severity

Malware Type	Notable attacks	Severity
Worms	Blaster,Welchia	Highest
Botnets	SDBot,RBot,Agobot,Spybot,Mytob	High
Rabbit	Fork bomb	Average
Logic bombs	Medco Health Solutions, Fannie Mae, CSOC	Average
Trojan horse	Netbus,Sub7,Back Orifice,Beast,Zeus	High
Sinkhole/wormhole	Styx EK, SweetOrange EK	High
Spyware	CoolWebSearch, WinTools, Zango, Zlob	Average
Adware	Typhoid	Low
Trapdoors/Backdoors	Sobig, Mydoom, Skynet, MD5	Average
DoS	Teardrop, Smurf, SYN flood, Sockstress	High
Zombies (DDoS)	SPEWS, Blue frog and smartphone attacks	Average
Phishing	AOHell, warez, Heartbleed	High
Viruses (boot-sector, file, macro)	CodeRed,Sasser,Melissa,Conficker	High
WiFi viruses	Chameleon (experimental virus)	High
Bluetooth viruses	Cabir,Ronie,Commwarrior	Average
Smartphone viruses	Cabir, Duts, Skulls, Commwarrior, Ikee	High
Socialnet app viruses	Net-Worm.Win32.Koobface.a/b	High
Hybrid and blended	Storm worm, Klez, Bobax, CIH	High

Node States in Epidemics

- Node state: one of possible conditions a legitimate node lies in
- Types of states
  - Susceptible, ***S(t)***: prone to receive a disease
  - Infected, ***I(t)***: node that already received a disease
  - Removed, ***R(t)***: infected and removed from a disease
  - Dead, ***D(t)***: completely immune – removed from a network
  - Passive immunity
  - Exposed

Node State	Symbol	Interpretation
Susceptible	S	non-infected node
Infected/infectious	I	infected node
Removed	R	recovering node (temporarily removed)
Dead	D	node not considered anymore (completely removed)
Susceptible-r	Sr	non-infected node with recharging capabilities
Infected-r	Ir	infected node with recharging capabilities
Removed-r	Rr	recovering node with recharging capabilities
Dead-r	Dr	completely removed node with recharging capabilities

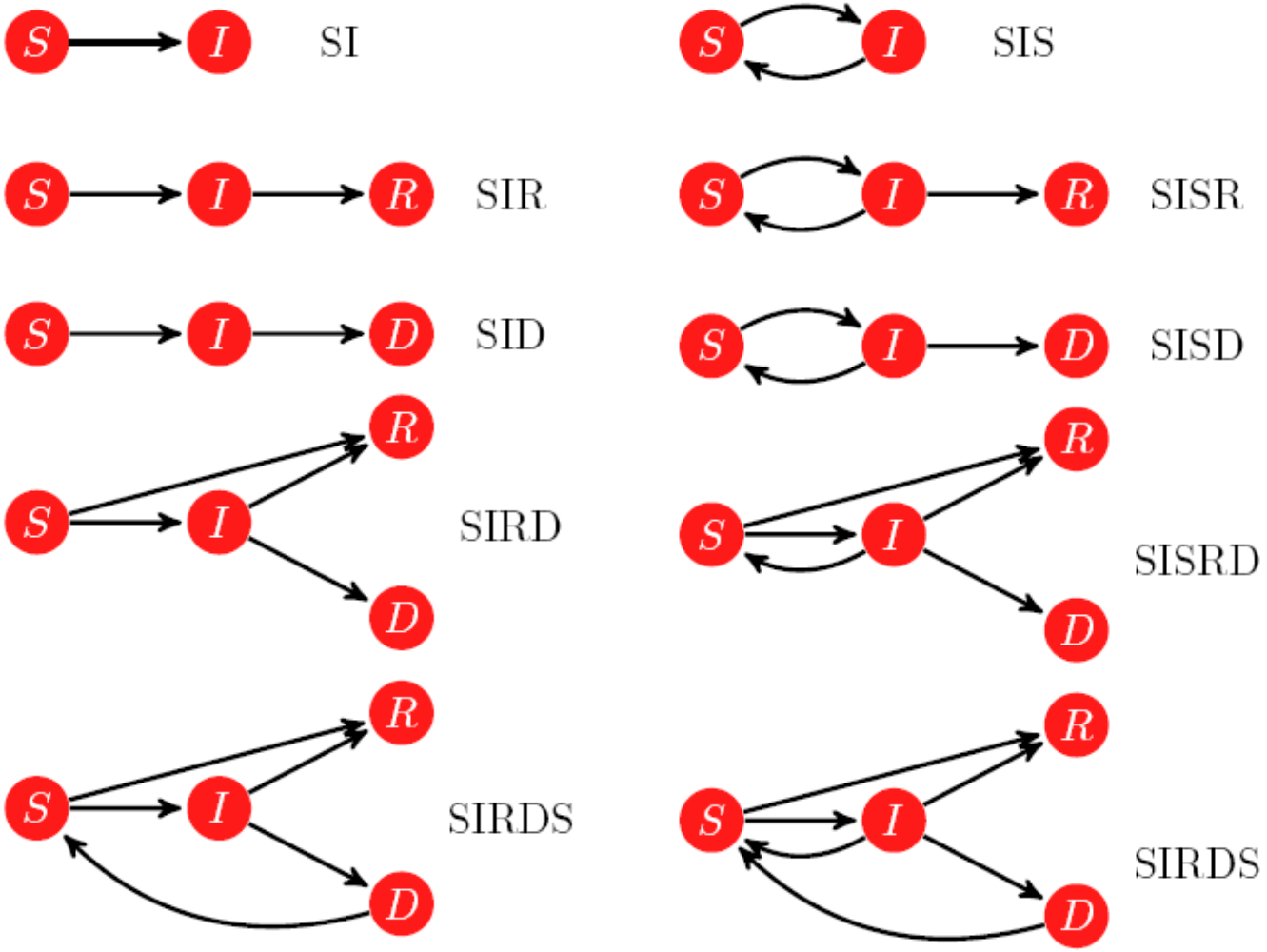
Node Infection Models

- Infection model: defines the specific states that legitimate nodes can be in, with respect to malware diffusion
- Describes generically the transitions of users between their possible states, due to malware-relate reasons, for various malware types and network paradigms, structures, operations, etc.
- Basic feature
  - Macroscopic vs. specific threat modeling

Infection model	Infection model	Malware types
SI	simple epidemic spreading	p2p or group spreading
SIR	epidemic spreading with patching	p2p or group spreading
SIRD	epidemic spreading with patching and killing	p2p or group spreading
SIS	macroscopic epidemic propagation	p2p or group propagation
SISR	macroscopic epidemic propagation with patching	p2p or group propagation

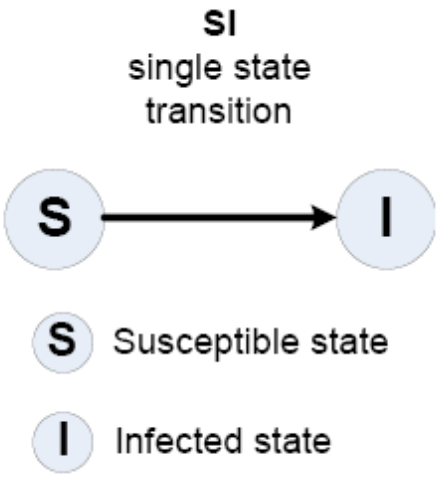
Examples of Node Infection Models

Some of them will be analyzed in the sequel



SI Model

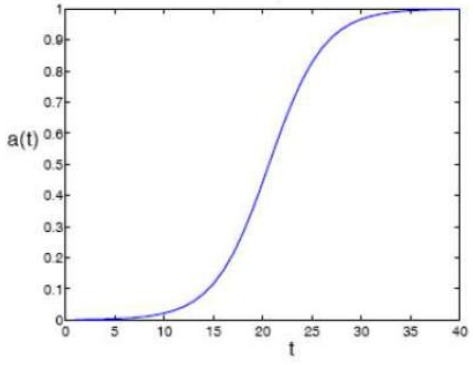
- **SI: Susceptible-Infected**
  - Simple epidemic model
- Single transition from S to I state
- Models specific & single threats
- One differential (nonlinear) equation:
  - where β is the contact rate of actors



$$\frac{dI(t)}{dt} = \beta I(t)S(t) = \beta I(t)[N - I(t)]; \qquad \alpha(t) = I(t)/N$$

$$\frac{d\alpha(t)}{dt} = k\alpha(t)[1 - \alpha(t)]; \qquad \beta = \gamma N$$

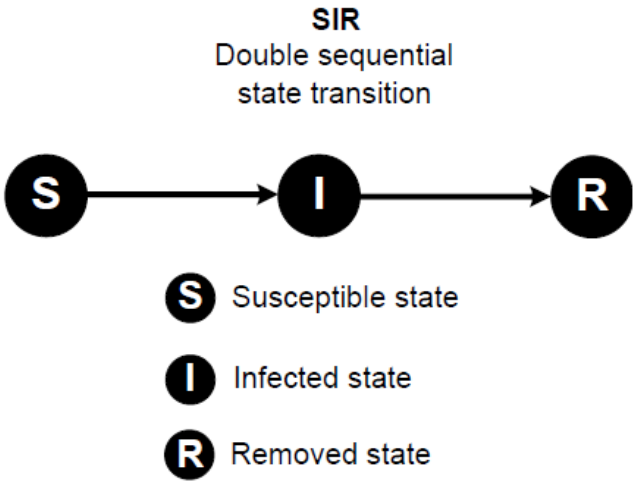
$$\frac{dS(t)}{dt} = -\beta I(t)S(t) = -\beta S(t)[N - S(t)]. \qquad N = S(t) + I(t)$$



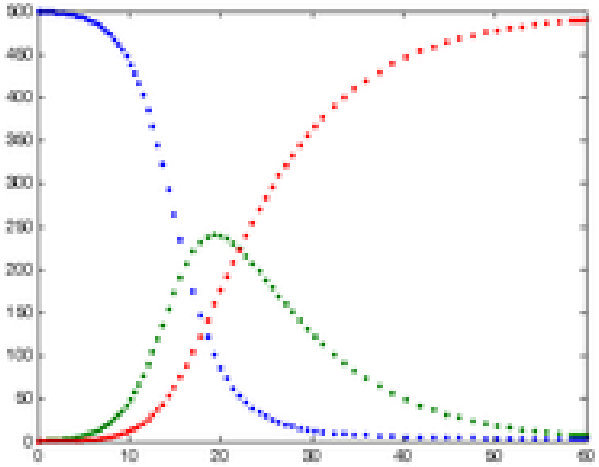
$$I(t) = \frac{I_0}{I_0 + (1 - I_0)e^{-\gamma t}}, \qquad I(0) = I_0 \qquad S(0) = N - I_0$$

SIR Model

- **SIR: Susceptible-Infected-Removed**
  - Also Kermack-McKendrick model
- Models specific & single threats
- 2 state transitions for nodes
  - S to I to R
- System of ODEs necessary
  - γ is the mean recovery (healing) rate



$$\frac{dS(t)}{dt} = -\frac{\beta S(t) I(t)}{N};$$
$$\frac{dI(t)}{dt} = \frac{\beta S(t) I(t)}{N} - \gamma I(t);$$
$$\frac{dR(t)}{dt} = \gamma I(t);$$
$$N = S(t) + I(t) + R(t),$$



- Nonlinear ODEs with no generic solution

SIR Features

- SIR is a good & simple model for many infectious diseases including measles, mumps and rubella
- Also a good initial model for worm viruses, e.g. CodeRed
- Basic reproduction number $R_0 = \frac{\beta}{\gamma}$
  - Expected # of new infections
- If $R_0 < \frac{N}{S(0)},$ then $\frac{dI}{dt}(0) < 0,$ and the outbreak tends to distinction
- Force of infection: $F = \beta I,$
  - transition rate from the susceptible individuals to infectious individuals

SIR Model with Birth-Deaths

- A more realistic modeling: assume a population characterized by a death rate μ and birth rate Λ:

$$\frac{dS}{dt} = \Lambda - \mu S - \beta IS$$

$$\frac{dI}{dt} = \beta IS - (\gamma + \mu) I$$

$$\frac{dR}{dt} = \gamma I - \mu R$$

- Disease-free equilibrium $(S(t), I(t), R(t)) = \left(\frac{\Lambda}{\mu}, 0, 0\right).$
- Basic reproduction number with threshold properties: $R_0 = \frac{\beta \Lambda}{\mu(\mu + \gamma)},$

$$R_0 \leq 1 \Rightarrow \lim_{t \to \infty} (S(t), I(t), R(t)) = \text{DFE} = \left(\frac{\Lambda}{\mu}, 0, 0\right)$$

$$R_0 > 1, I(0) > 0 \Rightarrow \lim_{t \to \infty} (S(t), I(t), R(t)) = \text{EE} = \left(\frac{\gamma + \mu}{\beta}, \frac{\mu}{\beta}(R_0 - 1), \frac{\gamma}{\beta}(R_0 - 1)\right).$$

Dynamic Quarantine

- Similarly to 2-factor model, some nodes are quarantined
  - Quarantined nodes are removed from the epidemic dynamics
- The quarantine on a host under alarm is released after a quarantine time T
  - a falsely quarantined but otherwise healthy host will only be quarantined for a short time
  - the worm anomaly detection program can be set more sensitive to a worm's activities
- Parameter λ_1 denotes the quarantine rate of infectious hosts
- Parameter λ_2 is the quarantine rate of susceptible hosts (false alarm rate of the anomaly detection program used in the system)
- The values of λ_1 and λ_2 are determined by the desired performance (and sensitivity) of the detection program

Dynamic Quarantine II

- Number of infectious hosts removed $R(t) = \int_{t-T}^{t} [I(\tau) - R(\tau)]\lambda_1 d\tau,$
- Interactions between $[I(t) - R(t)]$ $[S(t) - Q(t)]$

$$\frac{dI(t)}{dt} = \beta[I(t) - R(t)][S(t) - Q(t)] = \beta', I(t)[N - I(t)]$$

$$p_1' = \frac{\lambda_1 T}{1+\lambda_1 T} \qquad p_2' = \frac{\lambda_2 T}{1+\lambda_2 T}$$

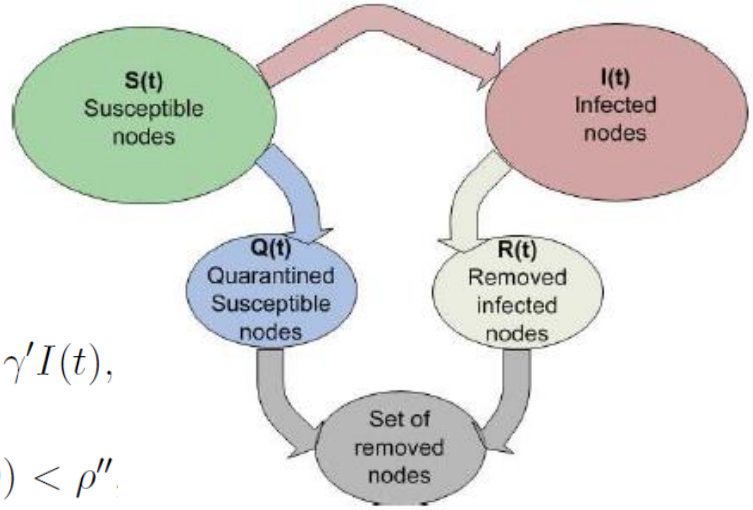
$$\beta' = (1 - p_1')(1 - p_2')\beta$$

$$Q(t) = p_2' S(t) \qquad R(t) = \int_{t-T}^{t} [I(\tau) - R(\tau)]\lambda_1 d\tau - \int_{t-T}^{t} \gamma R(\tau) d\tau$$

$$R(t) = q_1' I(t) \qquad q_1' = \frac{\lambda_1 T}{1+(\lambda_1+\gamma)T} \qquad q_2' = p_2' = \frac{\lambda_2 T}{1+(\lambda_2+\gamma)T}$$

$$dI(t)/dt = \beta[I(t) - R(t)][S(t) - Q(t)] - \gamma I(t) = \beta'' I(t) S(t) - \gamma I(t),$$

$$\beta'' = (1-q_1')(1-q_2')\beta \qquad \rho' = \gamma/\beta'' = \frac{1}{(1-q_1')(1-q_2')}\rho.$$



- all infectious hosts have an equal probability to be removed, if not:

$$\frac{dI(t)}{dt} = \beta[I(t) - R(t)][S(t) - Q(t)] - \gamma R(t) = \beta'' I(t) S(t) - \gamma' I(t),$$

$$\gamma' = q_1'\gamma \qquad \rho'' = \gamma'/\beta'' = \frac{q_1}{(1-q_1')(1-q_2')}\rho, \qquad S(0) < \rho''$$

SIRD Model

- Instantaneous fractions of susceptible, infective, recovered and dead nodes at time *t, S(t), I(t), D(t)*
- Infective nodes spread the malware during communication with susceptible nodes
- Each pair of infective-susceptible nodes initiates communication at rate $\hat{\beta}$ $\beta = \lim_{N\to\infty} N\hat{\beta}$

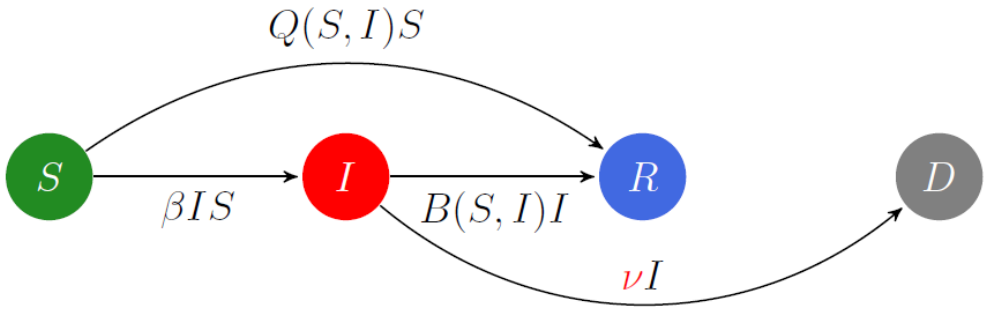
$$\dot{S}(t) = -\beta I(t)S(t) - Q\left(S(t), I(t)\right) S(t) \qquad S(0) = 1 - I_0$$

$$\dot{I}(t) = \beta I(t)S(t) - B\left(S(t), I(t)\right) I(t) - \nu(t)I(t) \qquad I(0) = I_0$$

$$\dot{D}(t) = \nu(t)I(t) \qquad D(0) = 0.$$

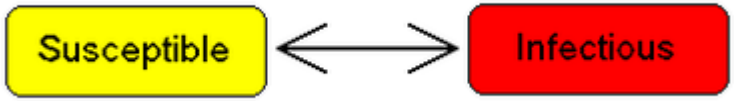
$$0 \le S(t), I(t), D(t)$$

$$S(t) + I(t) + D(t) \le 1.$$



SIS Model

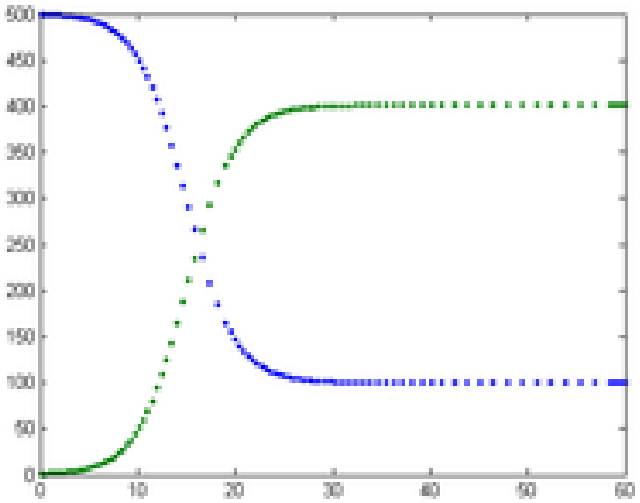
- SIS: Susceptible-Infected-Susceptible
- Examples are common cold & flu
- Macroscopic malware modeling
- No immunity after recovery



$$\frac{dS}{dt} = -\frac{\beta SI}{N} + \gamma I$$

$$\frac{dI}{dt} = \frac{\beta SI}{N} - \gamma I$$

$$\frac{dS}{dt} + \frac{dI}{dt} = 0 \Rightarrow S(t) + I(t) = N$$



- The dynamics of infectious is ruled by a logistic equation:

$$\frac{\beta N}{\gamma} \leq 1 \Rightarrow \lim_{t \to +\infty} I(t) = 0$$

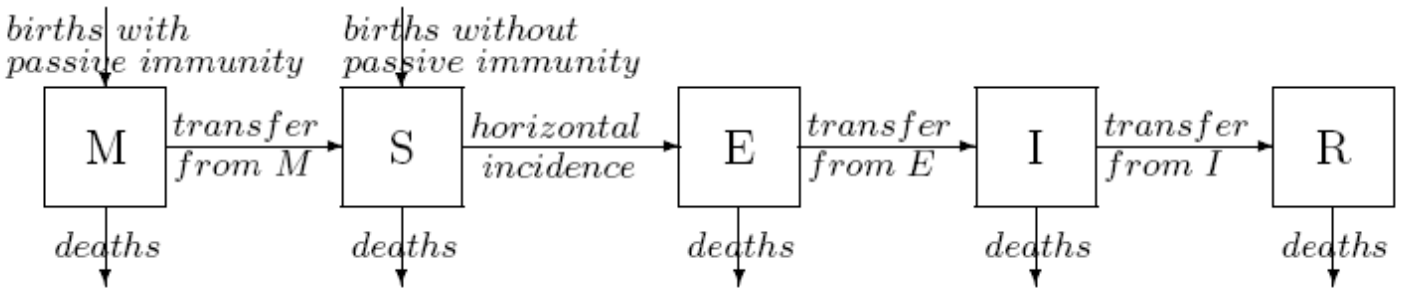
$$\frac{\beta N}{\gamma} > 1 \Rightarrow \lim_{t \to +\infty} I(t) = \frac{\beta N - \gamma}{\beta}$$

$$I(t) = \frac{I_\infty}{1 + Ve^{-\chi(t-t_0)}} \qquad I_\infty = \chi N/\beta \qquad \chi = \beta - \gamma$$

$$V = I_\infty / I_0 - 1$$

General Node Infection Model

- Also known as compartmental model
- MSEIR model
- M: passive immunity state
  - member of the population is born with antibodies
- E: exposed state
  - there exists an adequate contact of a susceptible with an infective
- Apart from time, it can also include age as a model factor



Compartmental Models

- SEIS model

$$\frac{dS}{dT} = B - \beta SI - \mu S + \gamma I \qquad \frac{dE}{dT} = \beta SI - (\epsilon + \mu)E \qquad \frac{dI}{dT} = \varepsilon E - (\gamma + \mu)I$$

- SEIR model

$$\frac{dS}{dT} = B - \beta SI - \mu S \qquad \frac{dE}{dT} = \beta SI - (\varepsilon + \mu)E \qquad \frac{dI}{dT} = \varepsilon E - (\gamma + \mu)I \qquad \frac{dR}{dT} = \gamma I - \mu R$$

- MSIR model

$$\frac{dM}{dT} = B - \delta M - \mu M \qquad \frac{dS}{dT} = \delta M - \beta SI - \mu S \qquad \frac{dI}{dT} = \beta SI - \gamma I - \mu I \qquad \frac{dR}{dT} = \gamma I - \mu R$$

- MSEIR model

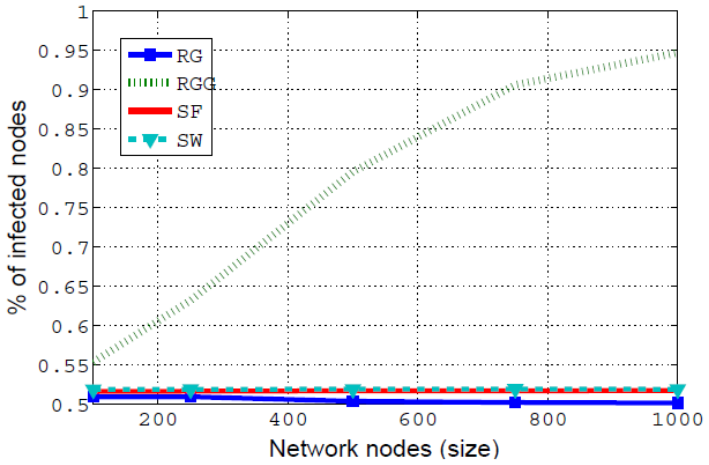
$$\frac{dM}{dT} = B - \delta M - \mu M \qquad \frac{dS}{dT} = \delta M - \beta SI - \mu S \qquad \frac{dI}{dT} = \varepsilon E - (\gamma + \mu)I \qquad \frac{dE}{dT} = \beta SI - (\varepsilon + \mu)E \qquad \frac{dR}{dT} = \gamma I - \mu R$$

- MSEIRS model
  - Similar to the MSEIR, but the immunity in the R class would be temporary, so that individuals would regain their susceptibility when the temporary immunity ended

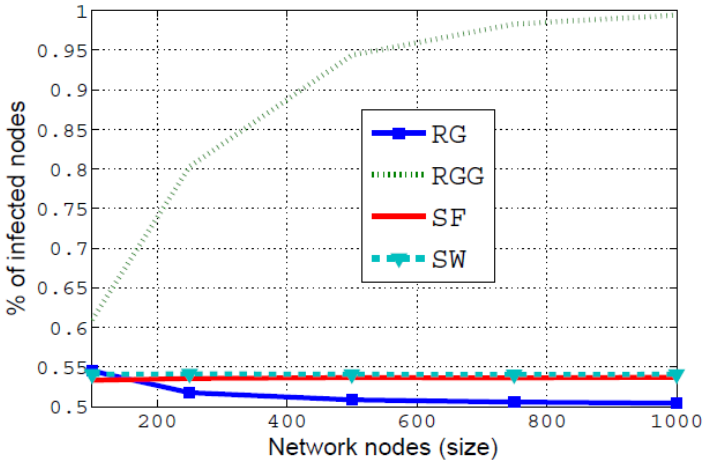
Random Attacks in SIS Complex Networks

- Examples of robustness analysis for complex spreading networks under the SIS infection paradigm
- Robustness analysis: average # of infected nodes in the long-term
- Random attacks employed
  - Homogeneous populations – attackers have contacts infecting nodes at random
- Parameter J/c_0 indicates the capabilities of the network (for a model)

sparse regime



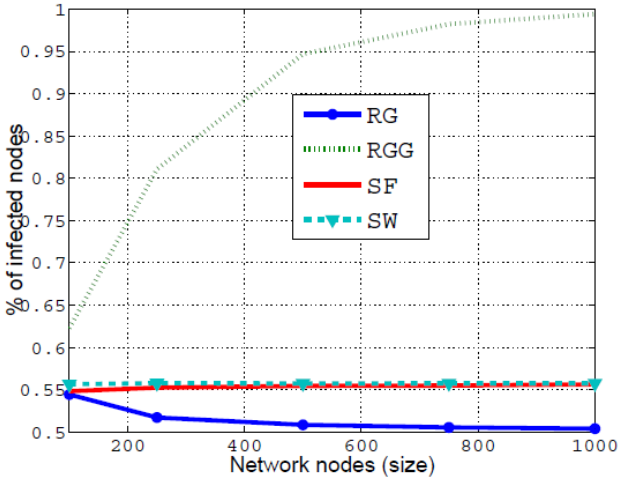
(a) Scaling for $J/c_0 = 0.005$.



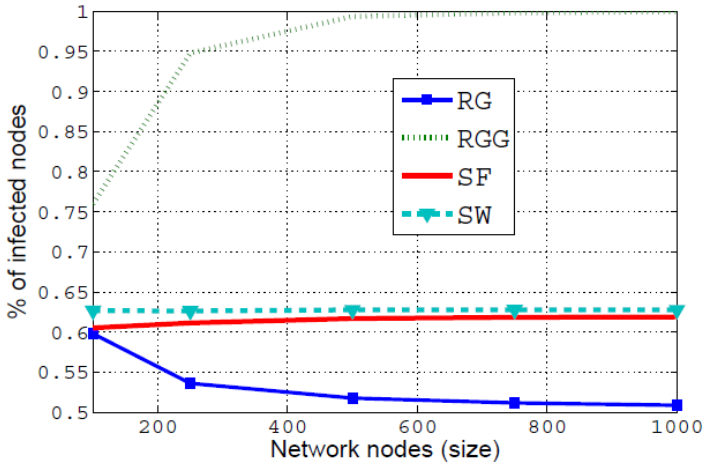
(b) Scaling for $J/c_0 = 0.01$.

Robustness Analysis

moderate regime

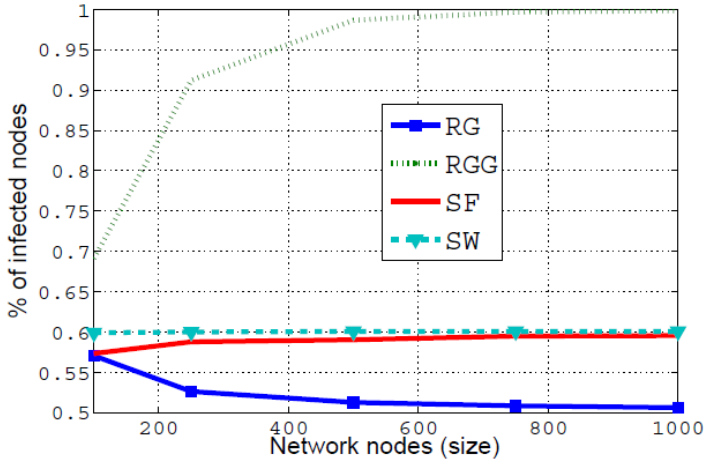


(a) Scaling for $J/c_0 = 0.005$.

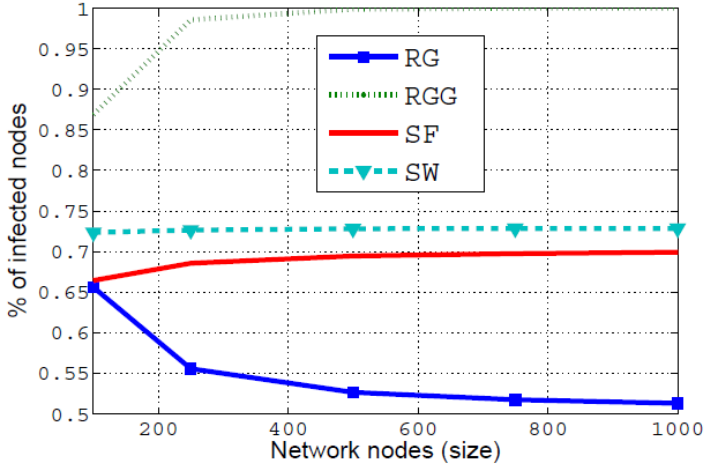


(b) Scaling for $J/c_0 = 0.01$.

dense regime



(a) Scaling for $J/c_0 = 0.005$.



(b) Scaling for $J/c_0 = 0.01$.

Overall Comments

- Deterministic models of population interaction dynamics
- Spreading and propagation networks
- Fixed or varying populations in the general case
- Macroscopic or no immunity modeling: SIS
- Specific threat modeling or immunity: SIR
- Homogeneous mixing of the population was assumed in all cases
  - What if heterogeneous mixing? A tough open problem
- Robustness analysis under random attacks
  - What if attacks become more intelligent? Optimal control (maybe next lecture….)
- Algebraic models not presented but yield ‘nice’ epidemic thresholds
- The Season 1 episode "Vector" (2005) of the television crime drama NUMB3RS features SIR models