Analytical Lifecycle Modeling and Threat Analysis of Botnets

Masood Khosroshahy

Ph.D. Thesis Defence

Electrical and Computer Engineering Department
Concordia University
Montreal, Canada

Outline

Outline

What is a botnet and how is it constructed?

Botnet:

- Network of (ro)bots
- An overlay network of compromised computers

Initial Infection

- E-mail attachments
- File sharing sites
- P2P networks
- Windows vulnerabilities
- Web browser vulnerabilities

Joining the Botnet

Centralized: connect to the C&C (IRC) server

Peer-to-peer: find other peers to join the botnet

Botnet in Operation

Node receives commands of the botmaster for:

- taking part in illicit activities
- updating/managing the malware

Botnets are being used for a host of illicit activities

- sending e-mail spams:
  - November 2008: takedown of few botnets led to an instant drop of 80% in e-mail spam volume.
- launching Distributed Denial-of-Service (DDoS) attacks:
  - The country of Estonia came under a DDoS attack in April 2007 which knocked off critical infrastructure and the media.
- engaging in click fraud against syndicated search engines:
  - Google reports having detected a botnet of 100,000 nodes committing click fraud.

Outline

Analytical Botnet Models: Common Assumptions

- Ignoring the details of infection inside a single machine *(node)*.
- Considering the node to be in one of few *stages*, e.g., *Infected*, *Susceptible*, *Immune*, etc.
- Abstraction of the details of viral transmission. A probability per unit time is used based on which:
  - an infected node will infect a susceptible node.
  - an infected node will get disinfected.
  - etc.

Development History of Analytical Lifecycle Models

- 1st generation: epidemiological (theoretical biology) models:
  - Developed during the 19th and 20th centuries.
  - Capturing the flow of people/patients between stages.
  - Models such as SIS, i.e., *Susceptible* to *Infected* and back.
- 2nd generation: computer virus propagation models:
  - Development started in early 1990's.
  - Epidemiological models adapted to computer virus propagation.
- 3rd generation: Botnet expansion/lifecycle models:
  - Development started in the last few years.
  - Computer virus propagation models adapted to botnet lifecycle.

Analytical Botnet Lifecycle Models: Current Shortcomings

Current models suffer from one, or more, of these shortcomings:

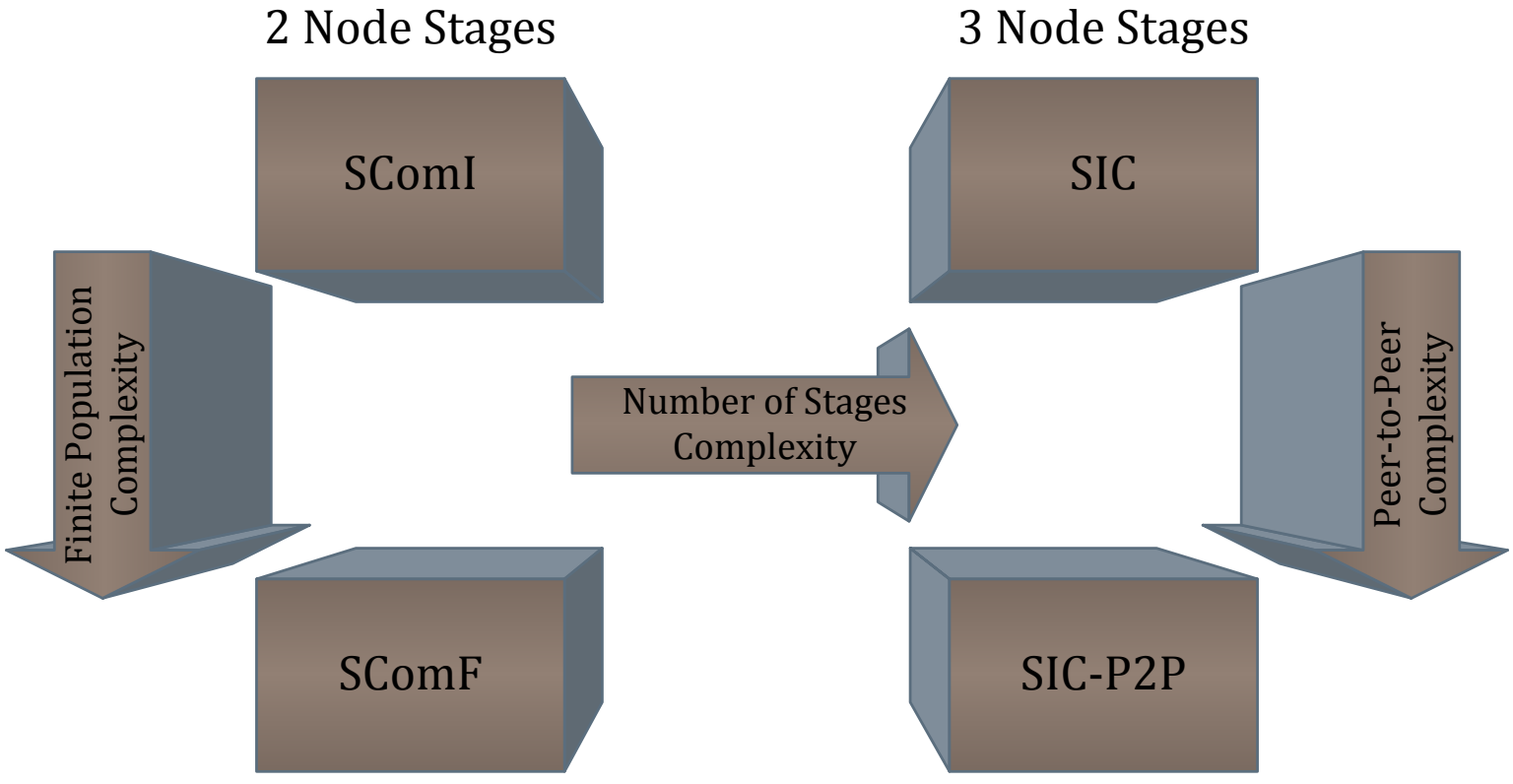
- Not defining proper *node stages* relevant to botnet dynamics.
- Not defining proper *transitions* and/or *transition rates* between node stages relevant to botnet dynamics.
- If deterministic model:
  - the modeling approach is dismissive of the stochastic nature of population size changes.
  - the model cannot provide information about probabilities of botnet's steep expansion or demise.

Outline

Modeling Techniques and Assumptions

- Nodes go through different stages in the lifetime of the botnet: *Susceptible*, *Infected* and *Connected*.
- State of the system: number of nodes in each stage.
- System modeled by Continuous-Time Markov Chain (CTMC).
- From the CTMC models, we derive:
  - either the probability distribution of number of nodes in each stage – *more difficult*.
  - or at least the mean/variance of number of nodes in each stage directly and without the probability distribution derivation – *easier*.

Botnet Models: The Big Picture



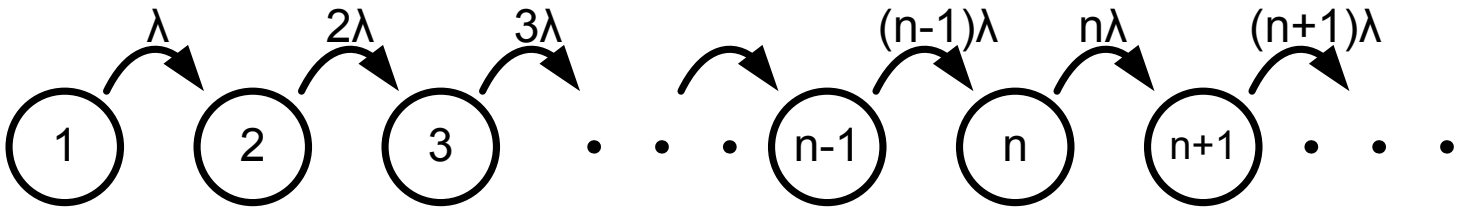
Outline

SComI: Unhindered Expansion - Infinite Population Size

- Node stages considered:
  - **S**usceptible: a node is susceptible to be compromised.
  - **Com**promised: the node is part of the botnet now.
- Infinite population size assumption: considering the total number of devices that are connected to the Internet.
- Model is therefore suitable for a botnet that can expand throughout the Internet.
- State of the system: number of nodes that are in the botnet (nodes in *Compromised* stage).

SComI: Unhindered Expansion - Infinite Population Size

State-transition-rate Diagram (1-dimensional pure-birth CTMC):



Rate of change of probability at any state = difference of probability flows into and out of that state:

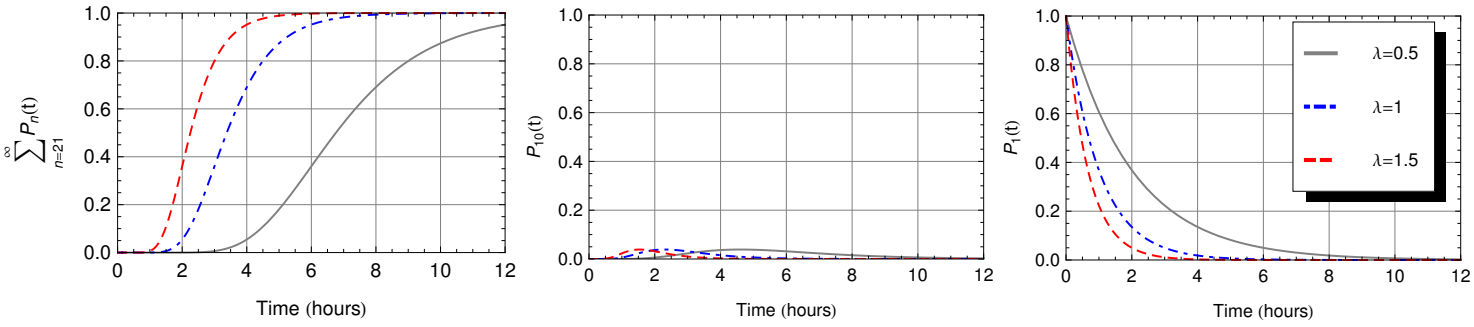
$$\frac{dP_n(t)}{dt} = (n-1)\lambda P_{n-1}(t) - n\lambda P_n(t) \qquad n \geq 1$$

Probability distribution can be derived:

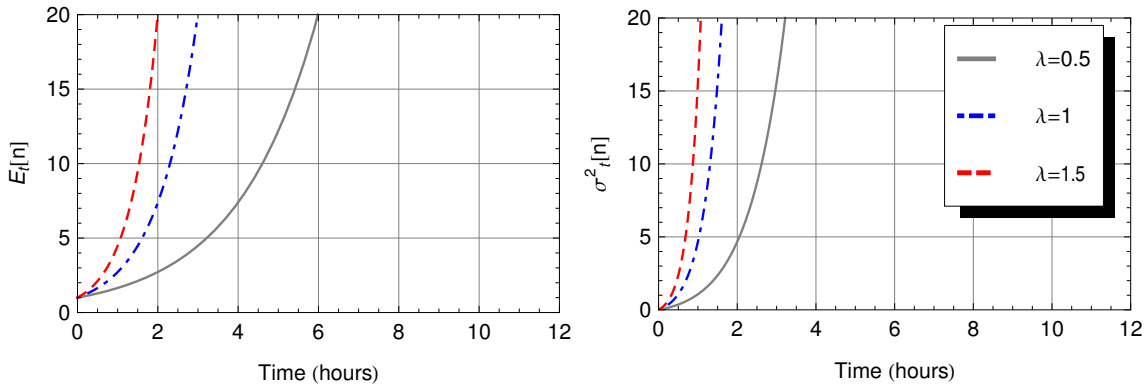
$$P_n(t) = e^{-\lambda t}(1 - e^{-\lambda t})^{n-1} \qquad n \geq 1$$

SComI: Numerical Results

- Probabilities of the no. of *Compromised* nodes (botnet size):



- Mean and variance of the no. of *Compromised* nodes:

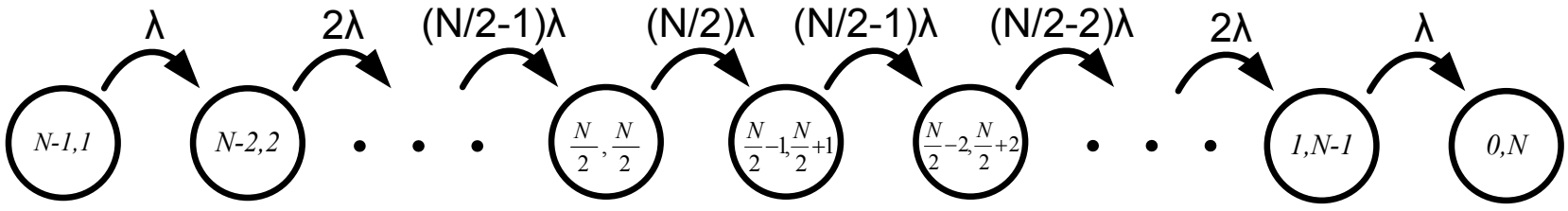


SComF: Unhindered Expansion - Finite Population Size

- Node stages considered: **S**usceptible and **Com**promised.
- Finite population size assumption: model suitable for a botnet that can expand throughout a segment of Internet or a local/wide area network.
- State of the system: number of nodes that are in the botnet (nodes in *Compromised* stage).
- Number of nodes that are in *Susceptible* stage is automatically obtained due to finite total population.

SComF: Unhindered Expansion - Finite Population Size

State-transition-rate Diagram (2-dimensional CTMC):



- Expansion rate continues to increase up to the point where half of the susceptible population has left this stage, afterwards, it decreases linearly.
- Probability flow equations:

$$\begin{cases} \frac{dP_1(t)}{dt} = -\lambda P_1(t) & n = 1 \\ \frac{dP_n(t)}{dt} = (n-1)\lambda P_{n-1}(t) - n\lambda P_n(t) & 2 \leq n \leq \frac{N}{2} \\ \frac{dP_n(t)}{dt} = (N-n+1)\lambda P_{n-1}(t) - (N-n)\lambda P_n(t) & \frac{N}{2}+1 \leq n \leq N \end{cases}$$

SComF: Unhindered Expansion - Finite Population Size

Probability distribution can be derived:

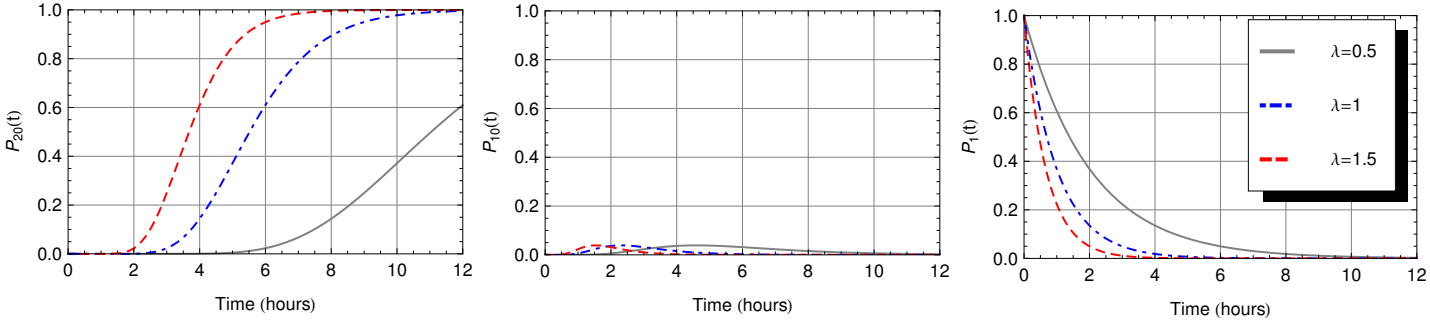
$$P_n(t) = \begin{cases} e^{-\lambda t} & n = 1 \\ \sum_{k=0}^{n-1} \left((-1)^k \binom{n-1}{k} e^{-(k+1)\lambda t} \right) & 2 \le n \le \frac{N}{2} \\ \sum\limits_{\substack{k=1 \\ k \notin [N-n, \frac{N}{2}-1]}}^{\frac{N}{2}} \left(\frac{T_1}{T_2} e^{-k\lambda t} \right) + \sum\limits_{k \in [N-n, \frac{N}{2}-1]}^{\frac{N}{2}-1} \left(\frac{T_1}{T_2} t e^{-k\lambda t} + \left. \frac{d(\frac{T_1}{T_3})}{ds} \right|_{s=-k\lambda} e^{-k\lambda t} \right) & \frac{N}{2}+1 \le n < N \\ \frac{T_1}{T_2|_{k=0}} + \sum_{k=1}^{\frac{N}{2}-1} \left(\frac{T_1}{T_2} t e^{-k\lambda t} + \left. \frac{d(\frac{T_1}{T_3})}{ds} \right|_{s=-k\lambda} e^{-k\lambda t} \right) + \frac{T_1}{T_2|_{k=\frac{N}{2}}} e^{-\frac{N}{2}\lambda t} & n = N \end{cases}$$

where T_1, T_2 and T_3 are given as follows:

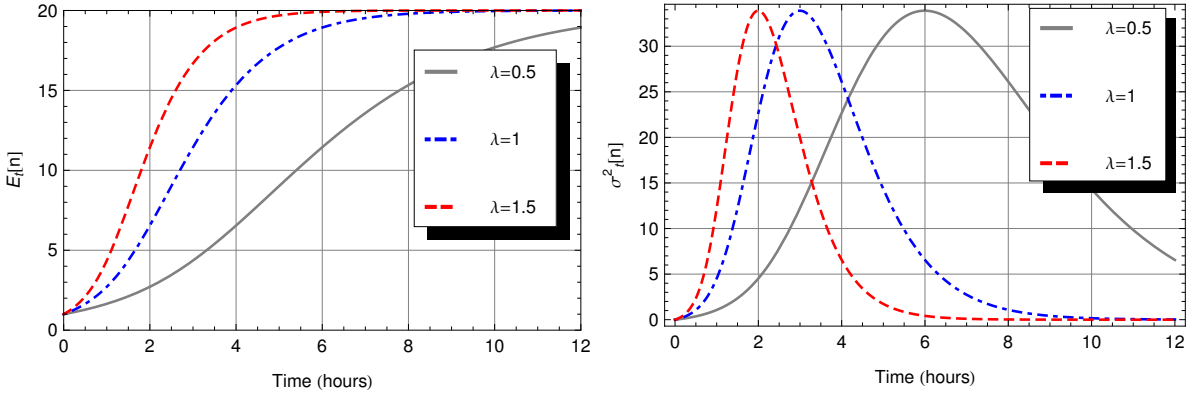
$$\begin{aligned} T_1 &= \frac{\frac{N}{2}!}{(N-n)!} \lambda^{(n-\frac{N}{2})} (\tfrac{N}{2}-1)! \lambda^{\frac{N}{2}-1} \\ T_2 &= \prod_{\substack{i=1 \\ i \neq k}}^{\frac{N}{2}} (i-k)\lambda \prod_{\substack{j=N-n \\ j \neq k}}^{\frac{N}{2}-1} (j-k)\lambda \\ T_3 &= \prod_{\substack{i=1 \\ i \neq k}}^{\frac{N}{2}} (s+i\lambda) \prod_{\substack{j=N-n \\ j \neq k}}^{\frac{N}{2}-1} (s+j\lambda) \end{aligned}$$

SComF: Numerical Results

- Probabilities of the no. of *Compromised* nodes (botnet size):



- Mean and variance of the no. of *Compromised* nodes:

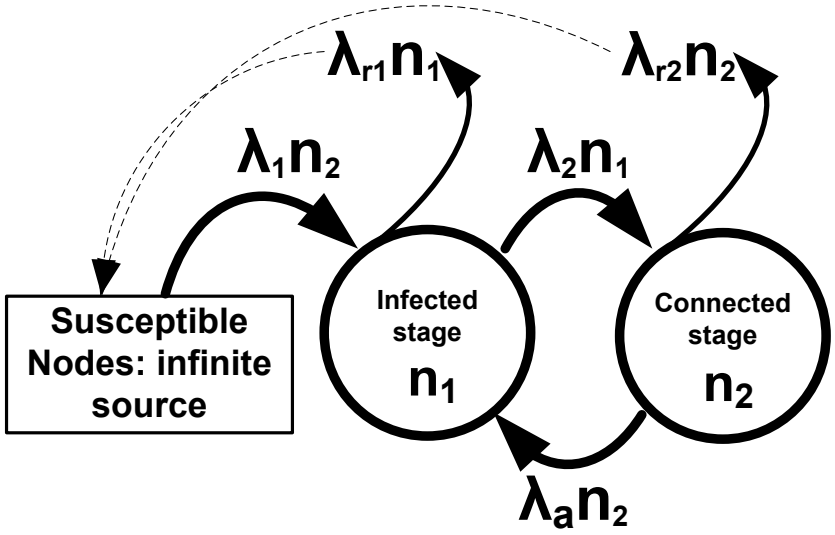


Outline

SIC: Susceptible-Infected-Connected

2-dimensional birth-death process: inter-stage-rate diagram

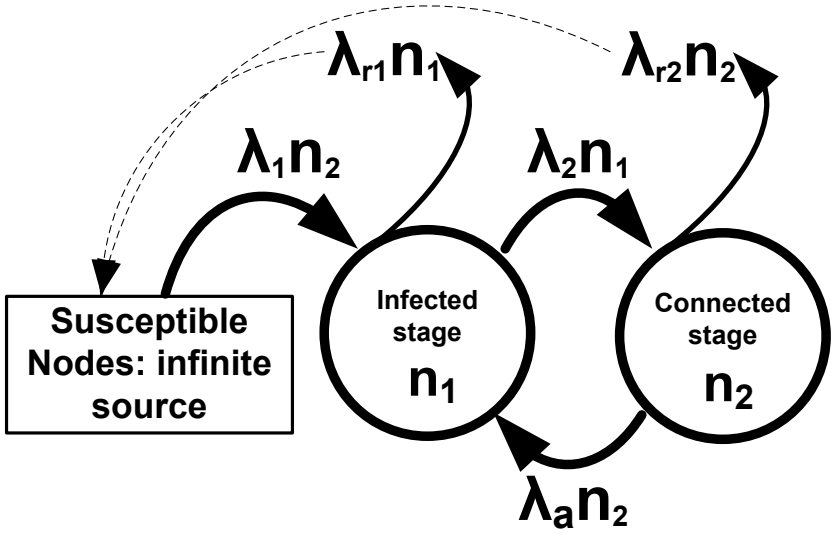
- Node stages considered:
  - **S**usceptible: a node is susceptible to be infected.
  - **I**nfected: the node has been infected, but it is not infectious.
  - **C**onnected:
    - The infected node has joined the botnet and is infectious now.
    - Botnet size = number of nodes that are in Connected stage.



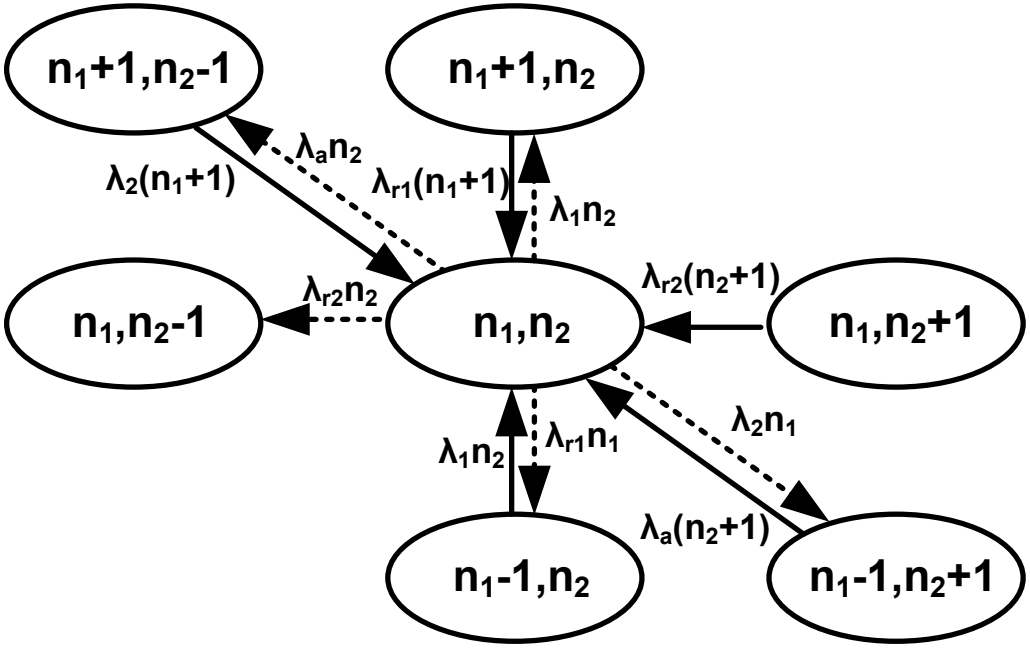
SIC: Susceptible-Infected-Connected

2-dimensional birth-death process: inter-stage-rate diagram

- SIC model incorporates both botnet mitigation strategies:
  - Removal rates from two stages due to disinfection of nodes.
  - Attacks on botnets: nodes lose the ability to communicate (they might be able to reconnect again).



SIC: State-transition-rate Diagram



- n_1: number of nodes in *Infected* stage.
- n_2: number of nodes in *Connected* stage.
- State of the system: number of nodes that are in *Infected* and *Connected* stages.

SIC: Probability Flow Equations

Rate of change of probability at any state = difference of probability flows into and out of that state:

$$
\begin{cases}
\frac{dP_{n_1,n_2}(t)}{dt} = \lambda_1 n_2 P_{n_1-1,n_2}(t) + \lambda_{r1}(n_1+1)P_{n_1+1,n_2}(t) \\
\qquad + \lambda_{r2}(n_2+1)P_{n_1,n_2+1}(t) + \lambda_2(n_1+1)P_{n_1+1,n_2-1}(t) & \langle n_1 > 0, n_2 > 0 \rangle \ (a) \\
\qquad + \lambda_a(n_2+1)P_{n_1-1,n_2+1}(t) \\
\qquad - (\lambda_1 n_2 + \lambda_{r1} n_1 + \lambda_{r2} n_2 + \lambda_2 n_1 + \lambda_a n_2)P_{n_1,n_2}(t) \\
\frac{dP_{0,n_2}(t)}{dt} = \lambda_{r1} P_{1,n_2}(t) + \lambda_{r2}(n_2+1)P_{0,n_2+1}(t) + \lambda_2 P_{1,n_2-1}(t) & \langle n_1 = 0, n_2 > 0 \rangle \ (b) \\
\qquad - (\lambda_1 n_2 + \lambda_{r2} n_2 + \lambda_a n_2)P_{0,n_2}(t) \\
\frac{dP_{n_1,0}(t)}{dt} = \lambda_{r1}(n_1+1)P_{n_1+1,0}(t) + \lambda_{r2} P_{n_1,1}(t) + \lambda_a P_{n_1-1,1}(t) & \langle n_1 > 0, n_2 = 0 \rangle \ (c) \\
\qquad - (\lambda_{r1} n_1 + \lambda_2 n_1)P_{n_1,0}(t) \\
\frac{dP_{0,0}(t)}{dt} = \lambda_{r1} P_{1,0}(t) + \lambda_{r2} P_{0,1}(t) & \langle n_1 = 0, n_2 = 0 \rangle \ (d)
\end{cases}
$$

SIC: Direct Mean Derivation

Relationship between the PGF and the probability distribution:

$$P(z_1, z_2, t) = \sum_{n_1=0}^{\infty} \sum_{n_2=0}^{\infty} P_{n_1,n_2}(t) z_1^{n_1} z_2^{n_2}$$

Derived PDE of the PGF:

$$(\lambda_{r1} + \lambda_2 z_2 - \lambda_{r1} z_1 - \lambda_2 z_1) \frac{\partial P(z_1,z_2,t)}{\partial z_1}$$
$$+(\lambda_1 z_1 z_2 + \lambda_{r2} + \lambda_a z_1 - \lambda_1 z_2 - \lambda_{r2} z_2 - \lambda_a z_2) \frac{\partial P(z_1,z_2,t)}{\partial z_2} - \frac{\partial P(z_1,z_2,t)}{\partial t} = 0$$

This PDE has remained unsolved (an open problem):

- The PDE transforms to this unsolvable 2nd order ODE (a Lienard equation): $\frac{d^2 z_1}{ds^2} + (A + B z_1) \frac{dz_1}{ds} + C z_1^2 + D z_1 + E = 0$
- Means/variances derived directly from the PDE.

SIC: Closed-form Formulas for the Means

$$\begin{cases} \frac{dE_1(t)}{dt} + (\lambda_2 + \lambda_{r1})E_1(t) - (\lambda_1 + \lambda_a)E_2(t) = 0 \\ \frac{dE_2(t)}{dt} - \lambda_2 E_1(t) + (\lambda_{r2} + \lambda_a)E_2(t) = 0 \end{cases}$$

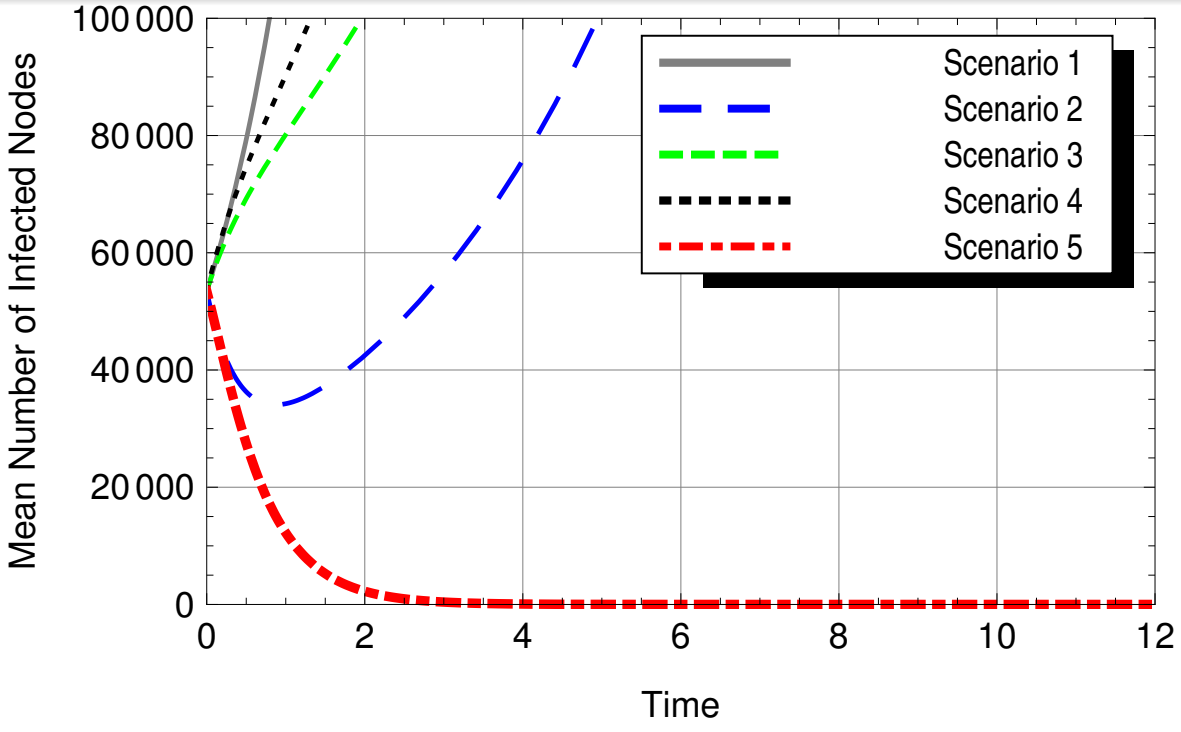
$$\begin{aligned} E_1(t) = \Big[& \exp\left(-\frac{1}{2}t\left(\lambda_{T3} + \lambda_{T1}\right)\right)\left(\bar{k_1}\lambda_2\left(-\exp\left(t\lambda_{T3}\right)\right)\right. \\ & + \left(\bar{k_1}\lambda_a - \bar{k_1}\lambda_{r1} + \bar{k_1}\lambda_{r2} + \bar{k_1}\lambda_{T3} + 2\lambda_1\bar{k_2}\right)\exp\left(t\lambda_{T3}\right) \\ & + 2\bar{k_2}\lambda_a\exp\left(t\lambda_{T3}\right) + \bar{k_1}\lambda_{T3} + \bar{k_1}\lambda_2 - \bar{k_1}\lambda_a + \bar{k_1}\lambda_{r1} \\ & \left. - \bar{k_1}\lambda_{r2} - 2\lambda_1\bar{k_2} - 2\bar{k_2}\lambda_a\right)\Big] / (2\lambda_{T3}) \end{aligned}$$

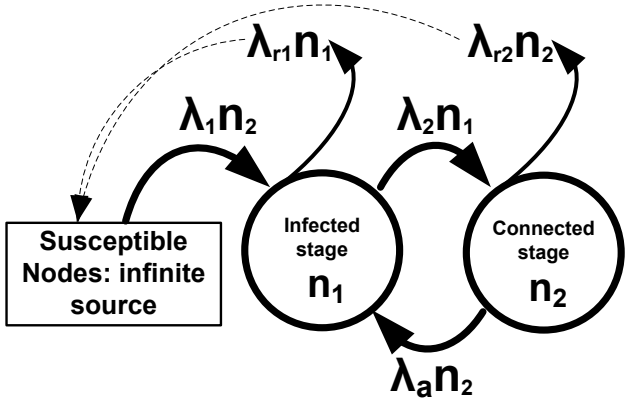
$$\begin{aligned} E_2(t) = \Big[& \exp\left(-\frac{1}{2}t\left(\lambda_{T3} + \lambda_{T1}\right)\right)\left(2\bar{k_1}\lambda_2\exp\left(t\lambda_{T3}\right)\right. \\ & + \left(\lambda_2\bar{k_2} - \bar{k_2}\lambda_a + \bar{k_2}\lambda_{r1} - \bar{k_2}\lambda_{r2} + \bar{k_2}\lambda_{T3}\right)\exp\left(t\lambda_{T3}\right) \\ & - 2\bar{k_1}\lambda_2 + \bar{k_2}\lambda_{T3} - \lambda_2\bar{k_2} + \bar{k_2}\lambda_a - \bar{k_2}\lambda_{r1} \\ & \left. + \bar{k_2}\lambda_{r2}\right)\Big] / (2\lambda_{T3}) \end{aligned}$$

where, $\lambda_{T1} = \lambda_2 + \lambda_a + \lambda_{r1} + \lambda_{r2}$, $\lambda_{T2} = -\lambda_1\lambda_2 + \lambda_{r2}\left(\lambda_2 + \lambda_{r1}\right) + \lambda_a\lambda_{r1}$, and $\lambda_{T3} = \sqrt{{\lambda_{T1}}^2 - 4\lambda_{T2}}$.

SIC: Comparison of Mitigation Strategies

Mean number of nodes in *Infected* stage (all scenarios)

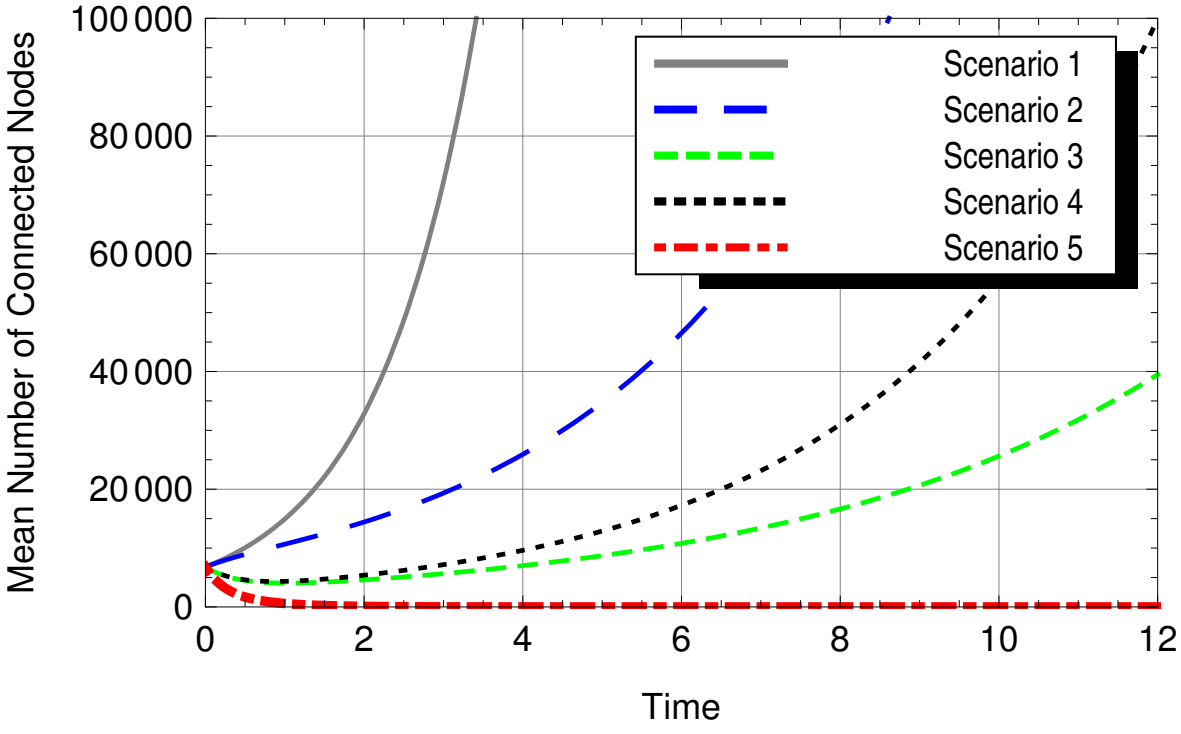


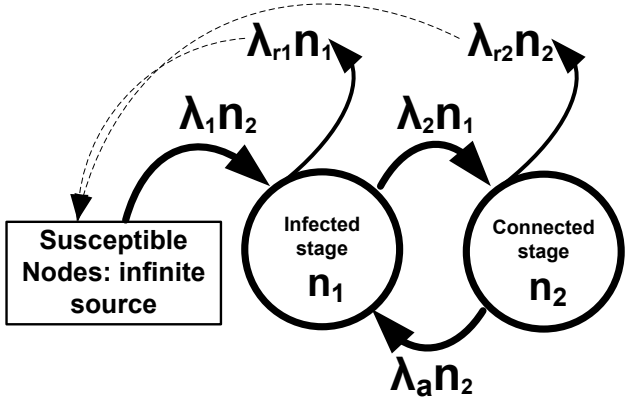


Scenario 1: unhindered expansion ($\lambda_{r1} = 0, \lambda_{r2} = 0, \lambda_a = 0$);
Scenario 2: only removal of Infected nodes ($\lambda_{r1} = 2, \lambda_{r2} = 0, \lambda_a = 0$);
Scenario 3: only removal of Connected nodes ($\lambda_{r1} = 0, \lambda_{r2} = 2, \lambda_a = 0$);
Scenario 4: only attack on botnet ($\lambda_{r1} = 0, \lambda_{r2} = 0, \lambda_a = 2$);
Scenario 5: three strategies simultaneously ($\lambda_{r1} = 2, \lambda_{r2} = 2, \lambda_a = 2$).

SIC: Comparison of Mitigation Strategies

Mean number of nodes in *Connected* stage (all scenarios)





Scenario 1: unhindered expansion ($\lambda_{r1} = 0, \lambda_{r2} = 0, \lambda_a = 0$);
Scenario 2: only removal of Infected nodes ($\lambda_{r1} = 2, \lambda_{r2} = 0, \lambda_a = 0$);
Scenario 3: only removal of Connected nodes ($\lambda_{r1} = 0, \lambda_{r2} = 2, \lambda_a = 0$);
Scenario 4: only attack on botnet ($\lambda_{r1} = 0, \lambda_{r2} = 0, \lambda_a = 2$);
Scenario 5: three strategies simultaneously ($\lambda_{r1} = 2, \lambda_{r2} = 2, \lambda_a = 2$).

SIC: Comparison of Mitigation Strategies

Conclusions from the numerical analysis

Most *effective measure* to contain/dismantle the botnet

- Removal/disinfection from *Connected* stage (λ_{r2}).
- Given that all other parameters are the same in all scenarios.

Most *economical way* to contain/dismantle the botnet

- Implementing all three measures at the same time: we can choose moderate rates.
- Concentrating on a single measure (disinfection or attack) = having to choose a very high rate = high cost

SIC: Comparison of Mitigation Strategies

Conclusions from the numerical analysis

Most *effective measure* to contain/dismantle the botnet

- Removal/disinfection from *Connected* stage (λ_{r2}).
- Given that all other parameters are the same in all scenarios.

Most *economical way* to contain/dismantle the botnet

- Implementing all three measures at the same time: we can choose moderate rates.
- Concentrating on a single measure (disinfection or attack) = having to choose a very high rate = high cost

SIC: Derivation of Variance

- We take the 2nd derivatives of the PDE of the PGF with respect to z_1 and z_2, separately.
- Further, we take the derivative of the PDE with respect to z_1 and then with respect to z_2.
- By setting $z_1 = z_2 = 1$ in each equation, we arrive at a set of ODEs solution of which leads to the derivation of variances.
- $\sigma_1^2(t) = E_t[n_1^2] - (E_1(t))^2$
- $E_t[n_1^2] = \frac{\partial^2 P(z_1,z_2,t)}{\partial z_1^2} \mid_{z_1=z_2=1} + \frac{\partial P(z_1,z_2,t)}{\partial z_1} \mid_{z_1=z_2=1}$
- $\psi_1(t) \triangleq \frac{\partial^2 P(z_1,z_2,t)}{\partial z_1^2} \mid_{z_1=z_2=1}$

$$\begin{cases} \frac{d\psi_1(t)}{dt} = 2(\lambda_1 + \lambda_a)\psi_{12}(t) - 2(\lambda_{r1} + \lambda_2)\psi_1(t) \\ \frac{d\psi_2(t)}{dt} = 2\lambda_2\psi_{12}(t) - 2(\lambda_{r2} + \lambda_a)\psi_2(t) \\ \frac{d\psi_{12}(t)}{dt} = -(\lambda_{r1} + \lambda_2 + \lambda_{r2} + \lambda_a)\psi_{12}(t) + \lambda_2\psi_1(t) \\ \qquad + \lambda_1 E_2(t) + (\lambda_1 + \lambda_a)\psi_2(t) \end{cases}$$

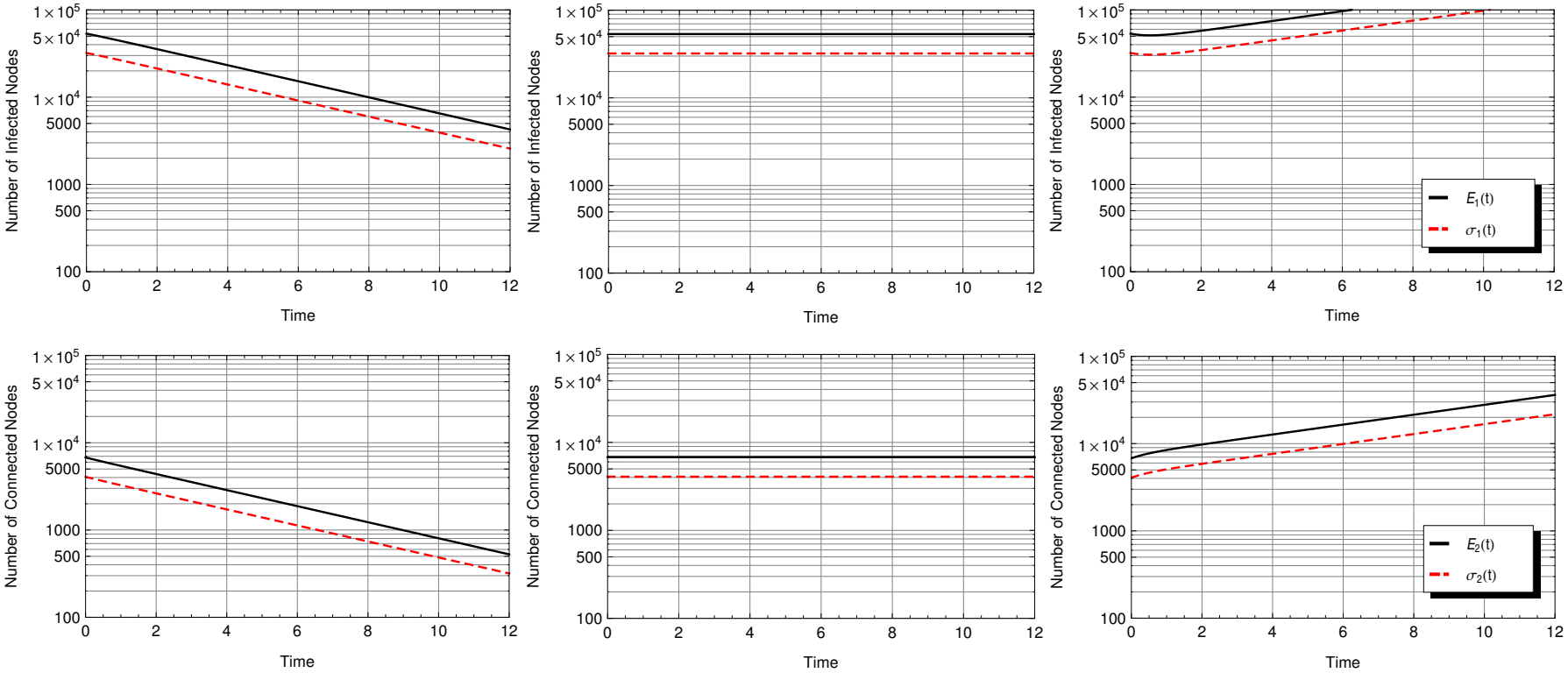
SIC: Derivation of Epidemiological Threshold

- In epidemiology, specific epidemic parameters are used in determining the outbreak or disappearance of disease.
- Basic Reproduction Number (R_0): the mean number of infections that any single botnet node can cause among the population of susceptible nodes.
- Based on differential equations of means, R_0 can be derived in terms of various SIC model's rates using the "Next Generation Matrix" method as follows:

$$R_0 = \sqrt{\frac{\lambda_2(\lambda_1 + \lambda_a)}{(\lambda_{r2} + \lambda_a)(\lambda_2 + \lambda_{r1})}}$$

- If $R_0 < 1$, botnet will eventually disappear with probability one.
- If $R_0 > 1$, however, there is a probability that the botnet size will continue to increase exponentially.

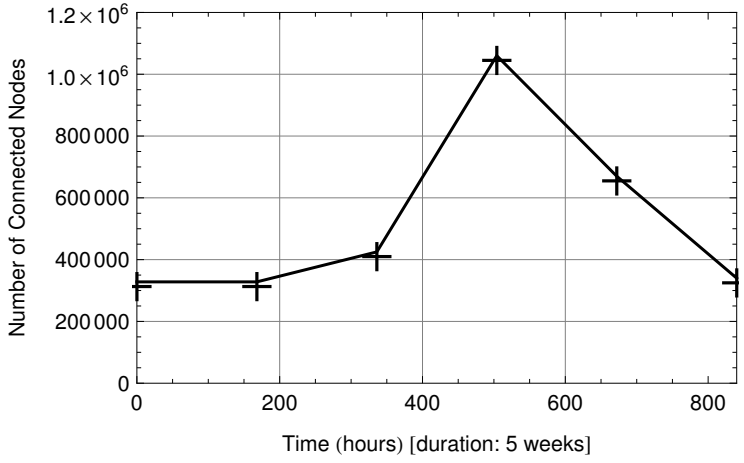
SIC: Variance and Epidemiological Threshold

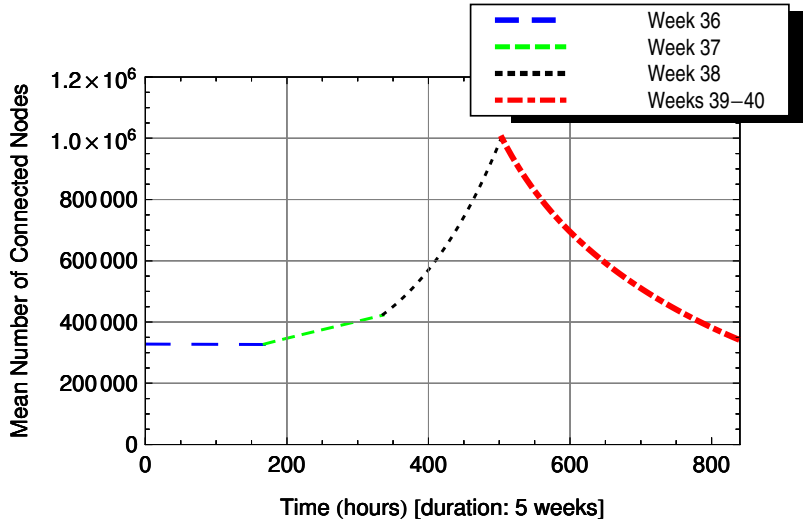


The higher the variance/standard dev. gets, the less should be the importance of the precise value of the mean in our interpretations.

SIC Model vs. Reported Botnet Measurements

FourLakeRiders: botnet mitigation strategies analyzed using the SIC model





–Left: weekly botnet size evolution reported by Damballa corporation.
–Right: botnet size evolution reconstructed using the SIC Model.

–During Week 36, the botnet size has reached an equilibrium. During Week 37, the mitigation strategies weaken and, during Week 38, they completely disappear. During Weeks 39 and 40, all mitigation strategies are employed.

–During both expansion & shrinkage, SIC results follow well the reported data.

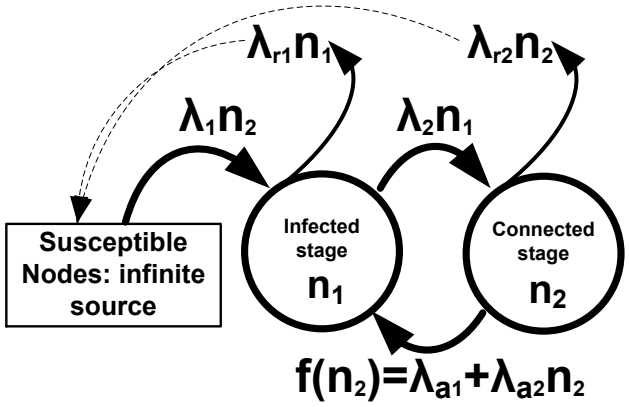
Mitigation Strategies of P2P Botnets

- Mitigation strategies of Distributed Hash Table (DHT)-based P2P botnets include *index poisoning* and *sybil attack*.
- Index poisoning: poisoning some targeted keys in the DHT.
  - Consists of injecting bogus content under the same keys associated with the original content (botmaster's commands).
- Sybil attack: numerous clean nodes (sybils) are injected into the botnet, posing themselves as "legitimate" botnet nodes.
  - Sybils then try to re-route, block, and corrupt the C&C traffic.

SIC-P2P: Focusing on Mitigation Strategies of P2P Botnets

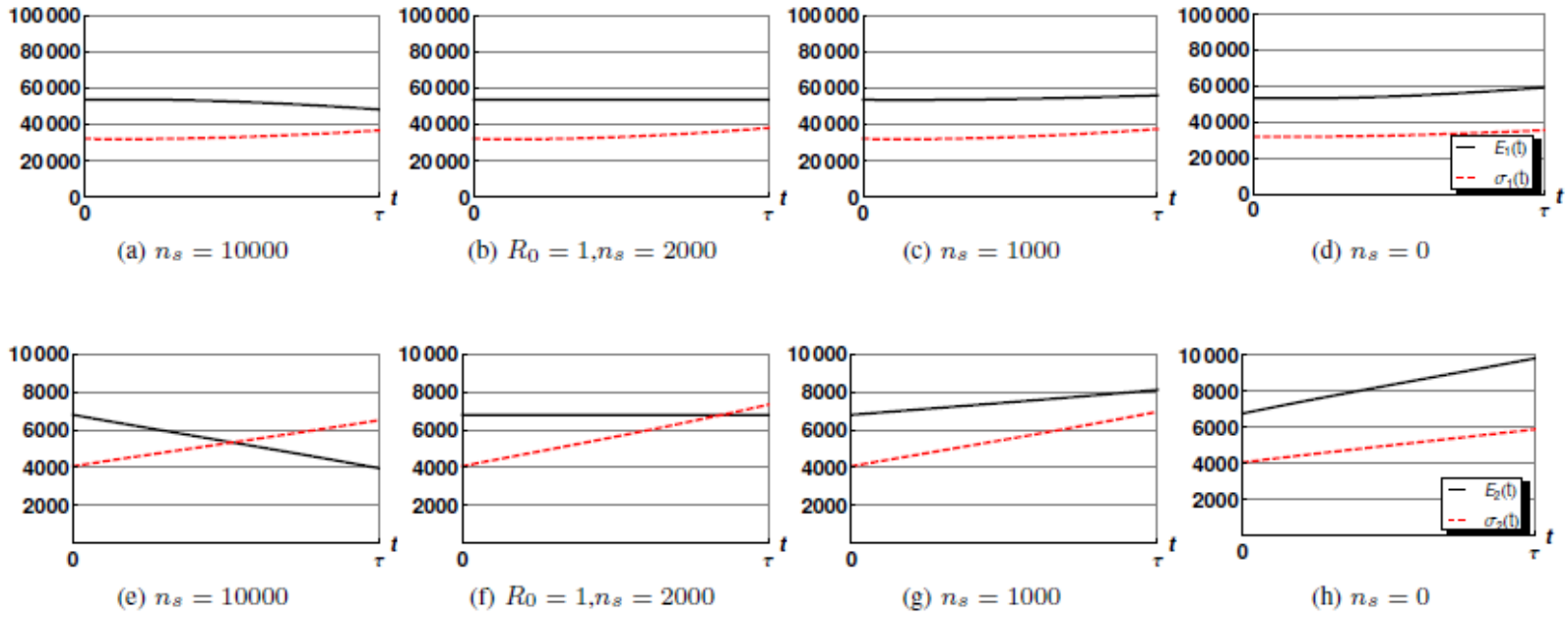
- Development of a link between lifecycle models (e.g., the SIC model) and the P2P botnet mitigation strategies.
- We treat the case of random sybil attack here.
- $P_s = \left(1 - \frac{n_s}{n_s+n}\right)^{\frac{\log_2(n_s+n)}{b}}$ [Ping Wang *et al.*, 2009]
  - P_s: the probability that a node obtains a real command.
  - If botnet operates without any interference, then $P_s = 1$.
  - If, however, the botnet is under attack, then $P_s < 1$.

SIC-P2P: Attack Rate | Derivations Similar to SIC



- Based on P_s, we define an attack rate (transition rate from Connected stage to Infected stage).
- We use Taylor series approximation to arrive at a linear function for the attack rate (i.e., $\lambda_{a1} + \lambda_{a2} n_2$).
- We have verified numerically that the first 2 terms of Taylor series are enough.
- Similar to the SIC model, for the SIC-P2P model, we have derived mean, variance, and basic reproduction number.

SIC-P2P: Numerical Analysis – Random Sybil Attack



(a) $n_s = 10000$ (b) $R_0 = 1, n_s = 2000$ (c) $n_s = 1000$ (d) $n_s = 0$

(e) $n_s = 10000$ (f) $R_0 = 1, n_s = 2000$ (g) $n_s = 1000$ (h) $n_s = 0$

Mean and standard deviation of number of nodes in Infected stage (top) and Connected stage (bottom) – various no. of sybil nodes.

Outline

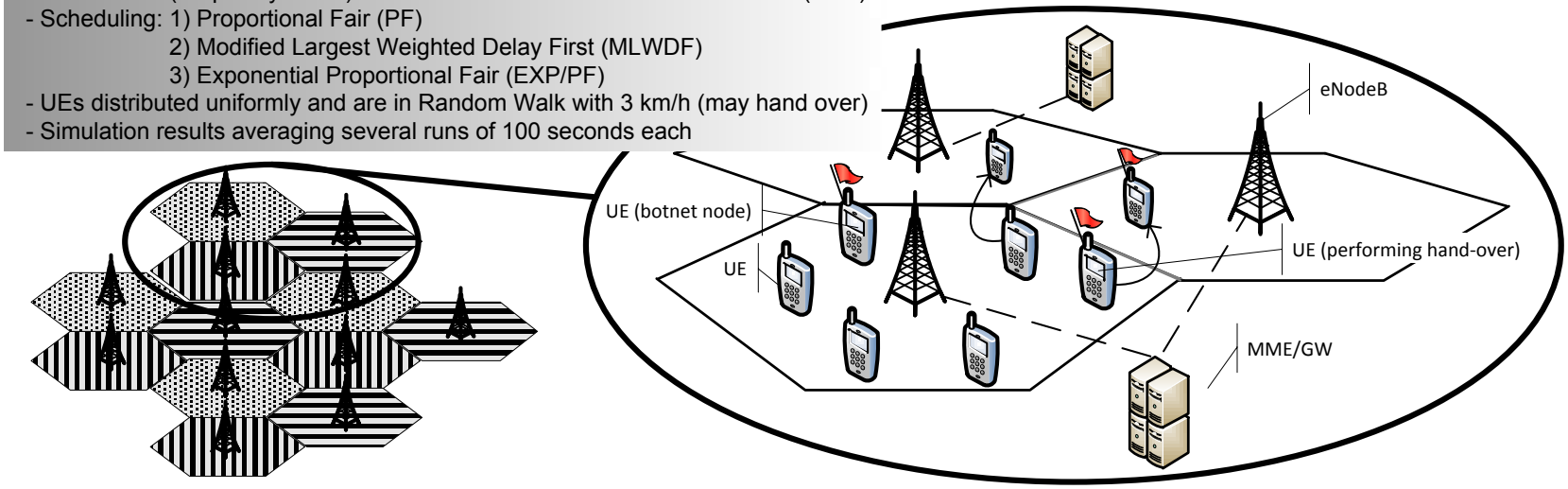
Botnets in 4G Cellular Networks

- As the convergence of Internet and traditional telecommunication services is underway, the threat of botnets is looming over essential basic communication services.
- We analyze the threat of botnets in the 4G cellular networks.
- We identify the vulnerability of the air interface, i.e. the Long Term Evolution (LTE), which allows a successful botnet-launched DDoS attack against it.
- Through simulation using an LTE simulator, we determine the number of botnet nodes per cell that can significantly degrade the service availability of such cellular networks.

Simulation Scenario

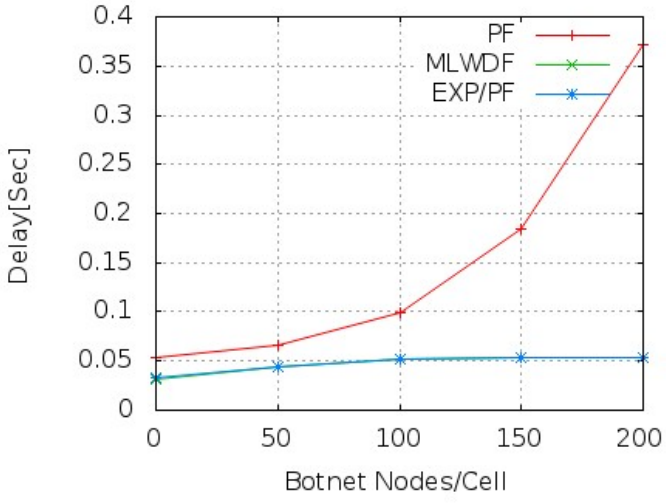
Simulation Scenario:

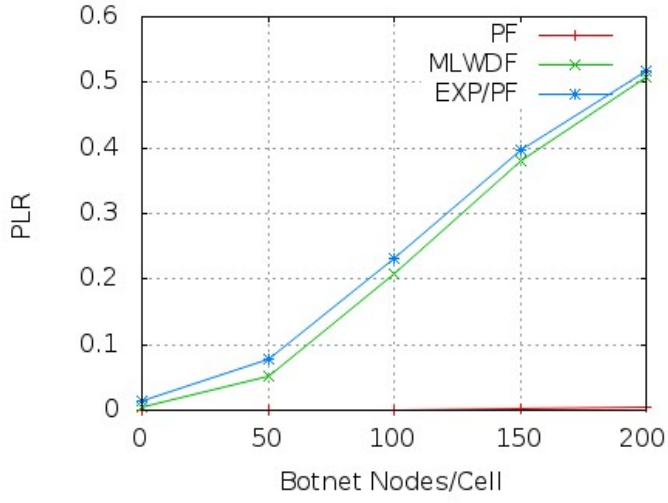
- User Equipment (UE) connected to eNodeB of each cell with radius of 1 km
- eNodeBs connected to Mobility Management Entity/Gateway (MME/GW)
- Cluster size (frequency reuse) of 3 cells with 5 MHz downlink in each cell (FDD)
- Scheduling: 1) Proportional Fair (PF)
  2) Modified Largest Weighted Delay First (MLWDF)
  3) Exponential Proportional Fair (EXP/PF)
- UEs distributed uniformly and are in Random Walk with 3 km/h (may hand over)
- Simulation results averaging several runs of 100 seconds each



- Attack scenario: botmaster instructing the botnet nodes to start downloading dummy data to overwhelm the air interface.
- Creation of extreme congestion is simple to implement: botmaster does not need any inside knowledge about network.

Simulation Results

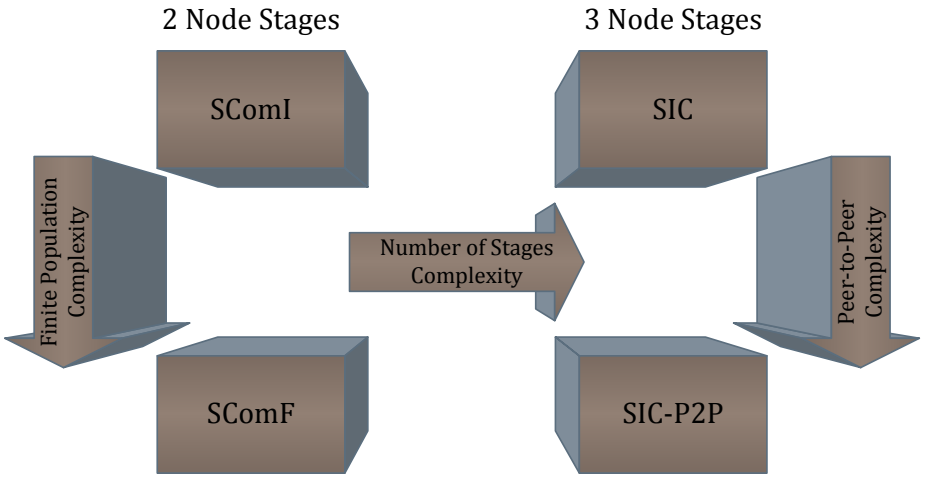




- Cell capacity is around 100 VoIP users ($\approx$ 3,300 subscribers).
- At capacity, we add an increasing number of botnet nodes:
  - PF scheduler: PLR acceptable, delay large.
  - MLWDF and EXP/PF schedulers: PLR large, delay acceptable.
- 200 botnet nodes (6% of subscribers) cause voice quality Mean Opinion Score (MOS) value of 1.

Outline

Botnet Models: Summary and Conclusions



- Main aspects of the developed botnet models:
  - SComI/SComF: 1) Initial expansion; 2) Probability distribution
  - SIC/SIC-P2P: 1) Full lifecycle analysis; 2) Mean/variance
- Time-dependent (transient) closed-form expressions for derived probability distributions and means/variances.
- Values for model parameters can come from measurements.

Outline

Publications

Two papers accepted, two more papers under review/submission

- "*SComF and SComI Botnet Models: The Cases of Initial Unhindered Botnet Expansion*", 25th Annual Canadian Conference on Electrical and Computer Engineering (CCECE12), Montreal, Canada, April 29-May 2, 2012
- "*The SIC Botnet Lifecycle Model: A Step Beyond Traditional Epidemiological Models*", Accepted paper to appear in Computer Networks (Elsevier), Special Issue on Botnet Activity: Analysis, Detection and Shutdown, DOI: 10.1016/j.comnet.2012.07.020
- "*SIC-P2P: A Lifecycle Model for the Evaluation of Mitigation Strategies Against P2P Botnets*", Under submission.
- "*Botnets in 4G Cellular Networks: Platforms to Launch DDoS Attacks Against the Air Interface*", Submitted.

Outline

Future Work

- Derivation of probability distributions for SIC & SIC-P2P:
  - The considerable efforts made were not successful due to certain cases of differential equations remaining unsolved.
  - By monitoring developments in this branch of mathematics, one could ultimately obtain closed-form solutions.
- Extension of the work done with regard to the threat of botnet in 4G cellular networks in two directions:
  - Investigation of the potential mitigation techniques in order to reduce and possibly eliminate the threat of air interface falling victim to a DDoS attack (e.g., enhancement of the CAC)
  - Determining how a botnet could attack a core network element in 4G systems (e.g., Home Subscriber Server of IMS).