LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-TR-498747

Modeling the Dynamics of Compromised Networks

B. Soper, D. M. Merl

September 12, 2011

Disclaimer

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

MODELING THE DYNAMICS OF COMPROMISED NETWORKS

BRADEN SOPER AND DAN MERL

1. Introduction

Accurate predictive models of compromised networks would contribute greatly to improving the effectiveness and efficiency of the detection and control of network attacks. Compartmental epidemiological models have been applied to modeling attack vectors such as viruses and worms [1]. We extend the application of these models to capture a wider class of dynamics applicable to cyber security. By making basic assumptions regarding network topology we use multi-group epidemiological models and reaction rate kinetics to model the stochastic evolution of a compromised network. The Gillespie Algorithm is used to run simulations under a worst case scenario in which the intruder follows the basic connection rates of network traffic as a method of obfuscation.

2. SIR Model

The standard SIR model for infectious diseases is defined in terms of the susceptible, S, infected, I, and removed, R, compartments of a population of size N. If the population is closed we have $N = S + I + R$. Letting β be the contact rate between susceptible and infected individuals and ν be the removal rate of infected individuals, the dynamics of the system are given by the following system of ODES.

$$\begin{aligned}\frac{dS}{dt} &= -\beta SI/N \\ \frac{dI}{dt} &= \beta SI/N - \nu I \\ \frac{dR}{dt} &= \nu I\end{aligned}$$

3. SLIR Model

We modify and extend the standard SIR model to include a latently infected group, L. This group contains compromised computers capable of "infecting" other computers yet are not known to be compromised. We use the standard incidence of transmission, but with $L + I$ infecting agents. Latently infected computers are discovered at a rate of d and overtly infected machines are removed from the network at a rate of r. We assume there

Date: September 12, 2011.

is a maximum rate, ρ, at which computers can be repaired and returned to the network. We will consider two possible functions which limit the repair rate to the threshold ρ. The first of these is simply $f(R) = \frac{R}{N}$ and the second is $g(R) = 1 - e^{-\gamma R}$ where γ is a threshold parameter.

3.1. **Threshold $f(R)$.** Given a repair rate threshold $f(R) = \frac{R}{N}$, the SLIR dynamics are defined as follows.

$$\begin{aligned} \frac{dS}{dt} &= -\beta(L+I)S/N + \rho R/N \\ \frac{dL}{dt} &= \beta(L+I)S/N - dL \\ \frac{dI}{dt} &= dL - rI \\ \frac{dR}{dt} &= rI - \rho R/N \end{aligned} \tag{1}$$

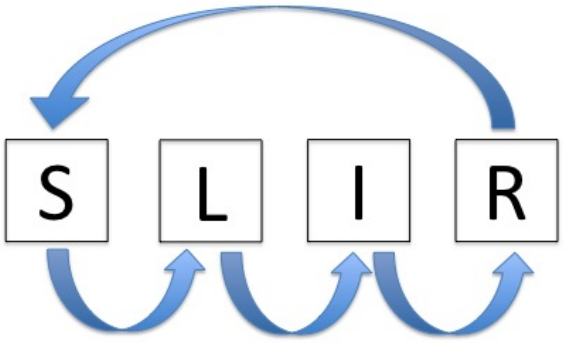

FIGURE 1. SLIR Dynamics

We assume the population is closed with $N = S+L+I+R$. Furthermore, all parameters are assumed to be positive. Starting with one latently infected node and $N-1$ susceptible nodes, we wish to find the threshold value R_0, the expected number of new infections due to a single infected node. The time spent covertly infected is roughly $\frac{1}{d}$ and the time spent overtly infected is roughly $\frac{1}{r}$. Thus the average time a single node is infected is $\frac{r+d}{rd}$. If we keep $L+I$ fixed at one we obtain $S(t) = (N-1)e^{-\frac{\beta}{N}t}$. If N is large then we assume $N \approx N-1$ and the expected number of new infections, R_0, due to a single infected node is as follows.

$$R_0 = S(0) - S\left(\frac{r+d}{rd}\right) = N - 1 - (N-1)e^{-\frac{\beta}{N}(\frac{r+d}{rd})}$$
$$= (N-1)(1 - e^{-\frac{\beta}{N}(\frac{r+d}{rd})}) \approx N\left(\frac{\beta}{N}\right)\left(\frac{r+d}{rd}\right) = \beta\left(\frac{r+d}{rd}\right)$$

Because the system is closed we have $R = N - S - L - I$ and we need only consider S, L, and I. System (1) then reduces to

$$\frac{dS}{dt} = -\beta(L+I)S/N + \rho(N - S - L - I)/N$$
$$\frac{dL}{dt} = \beta(L+I)S/N - dL$$
$$\frac{dI}{dt} = dL - rI.$$

Clearly $(N, 0, 0)$ is a steady state of the system. Suppose there exists a steady state (S^*, L^*, I^*) with $S^* > 0, L^* > 0$ and $I^* > 0$. Any such steady state will be determined by

$$\beta(L^* + I^*)S^*/N = \rho(N - S^* - L^* - I^*)/N = dL^* = rI^*.$$

From these equations one obtains the following.

$$S^* = \frac{Nrd}{\beta(r+d)} = \frac{N}{R_0}$$
$$L^* = \frac{r\rho N}{Nrd + \rho(r+d)}\left(1 - \frac{rd}{\beta(r+d)}\right) = \frac{r\rho N}{Nrd + \rho(r+d)}\left(\frac{R_0 - 1}{R_0}\right)$$
$$I^* = \frac{d\rho N}{Nrd + \rho(r+d)}\left(1 - \frac{rd}{\beta(r+d)}\right) = \frac{d\rho N}{Nrd + \rho(r+d)}\left(\frac{R_0 - 1}{R_0}\right)$$

It is clear that $R_0 > 1$ is a necessary condition for an endemic equilibrium point to exist in the first octant while $R_0 = 1$ reduces (S^*, L^*, I^*) to $(N, 0, 0)$. Thus we suspect $R_0 = 1$ is a bifurcation threshold.

To characterize the fixed points we linearize the system around them using the Jacobian. If $\frac{dS}{dt} = f(S, L, I)$, $\frac{dL}{dt} = g(S, L, I)$ and $\frac{dI}{dt} = h(S, L, I)$, then the Jacobian is defined as the matrix

$$J_{(S^*, L^*, I^*)} = \begin{pmatrix} f_S & f_L & f_I \\ g_S & g_L & g_I \\ h_S & h_L & h_I \end{pmatrix}$$

where subscripts denote differentiation and each derivative is evaluated at the fixed point (S^*, L^*, I^*). The Jacobian for system (1) is

$$J_{(S^*,L^*,I^*)} = \begin{pmatrix} -\frac{\beta}{N}(L^*+I^*) - \frac{\rho}{N} & -\frac{\beta}{N}S^* - \frac{\rho}{N} & -\frac{\beta}{N}S^* - \frac{\rho}{N} \\ \frac{\beta}{N}(L^*+I^*) & \frac{\beta}{N}S^* - d & \frac{\beta}{N}S^* \\ 0 & d & -r \end{pmatrix}$$

For the fixed point $(N,0,0)$ we have

$$J_{(N,0,0)} = \begin{pmatrix} -\frac{\rho}{N} & -\beta - \frac{\rho}{N} & -\beta - \frac{\rho}{N} \\ 0 & \beta - d & \beta \\ 0 & d & -r \end{pmatrix}$$

The characteristic equation for this matrix is

$$(\frac{\rho}{N} + \lambda)[\lambda^2 + (r+d-\beta)\lambda - (\beta(r+d) - dr)] = 0.$$

Thus one eigenvalue is given by $\lambda_1 = -\frac{\rho}{N}$ and the other two are given by

$$\lambda_{2,3} = \frac{1}{2}\left[-(r+d-\beta) \pm \sqrt{(r+d-\beta)^2 + 4(\beta(r+d) - dr)}\right].$$

The discriminant of this polynomial can be rewritten as $(r-d)^2+2(r+d)N\beta+\beta^2N^2 > 0$, hence all eigenvalues are real (i.e. no periodic or spiraling solutions exists locally around this fixed point). If $R_0 = 1$ then $\beta(r+d)-dr = 0$ and the characteristic polynomial reduces to $\lambda(\frac{\rho}{N} + \lambda)(\lambda + r + d - \beta) = 0$ giving a zero eigenvalue. Furthermore since $\beta = \frac{rd}{r+d}$ and $\beta, r, d > 0$ we must have $r+d-\beta > 0$. So locally the fixed point at $(N,0,0)$ is a degenerate attracting fixed point when $R_0 = 1$. If $R_0 < 1$ then $\beta(r+d) - dr < 0$ and we will obtain two positive eigenvectors. If $R_0 > 1$ then $\beta(r+d) - dr > 0$ and there will be one positive and one negative eigenvalue. In either case it is a type of saddle point where we again see R_0 acting as a threshold value, this time controlling a bifurcation of the qualitative nature of the fixed point at $(N,0,0)$.

The Jacobian for the fixed point with $L^*, I^* > 0$ is

$$J_{(S^*,L^*,I^*)} = \begin{pmatrix} -\frac{\beta\rho(R_0-1)}{N\beta+\rho R_0} - \frac{\rho}{N} & -\frac{\beta}{R_0} - \frac{\rho}{N} & -\frac{\beta}{R_0} - \frac{\rho}{N} \\ \frac{\beta\rho(R_0-1)}{N\beta+\rho R_0} & \frac{\beta}{R_0} - d & \frac{\beta}{R_0} \\ 0 & d & -r \end{pmatrix}$$

The characteristic polynomial for this matrix is

$$\left(\frac{\beta\rho(R_0-1)}{N\beta+\rho R_0} + \frac{\rho}{N} + \lambda\right)\left[\left(\frac{\beta}{R_0} - d - \lambda\right)(r+\lambda) + \frac{d\beta}{R_0}\right] - \frac{\beta\rho(R_0-1)}{NR_0}(r+d+\lambda) = 0$$

Let $\phi = \frac{\beta\rho(R_0-1)}{N\beta+\rho R_0} + \frac{\rho}{N}$. Then we have

$$(\phi+\lambda)\left(\frac{\beta}{R_0} - d - \lambda\right)(r+\lambda) + \frac{d\beta}{R_0}(\phi+\lambda) - \frac{\beta\rho(R_0-1)}{NR_0}(r+d+\lambda) = 0.$$

If we write the characteristic polynomial as $A\lambda^3 + B\lambda^2 + C\lambda + D = 0$ we have the following.

$$A = -1$$
$$B = \frac{\beta}{R_0} - (r + d) - \phi$$
$$C = (\phi + r)(\frac{\beta}{R_0} - d) - r\phi + \frac{r\beta}{R_0} - \frac{\beta\rho}{N}\frac{R_0 - 1}{R_0}$$
$$D = -\frac{rd\rho}{N}(R_0 - 1)$$

Though possible, determining the roots in terms of the above parameters using the cubic formula may be a bit cumbersome, and at this point we have not embarked on this task. Thus further work is needed to determine the local stability of the endemic equilibrium.

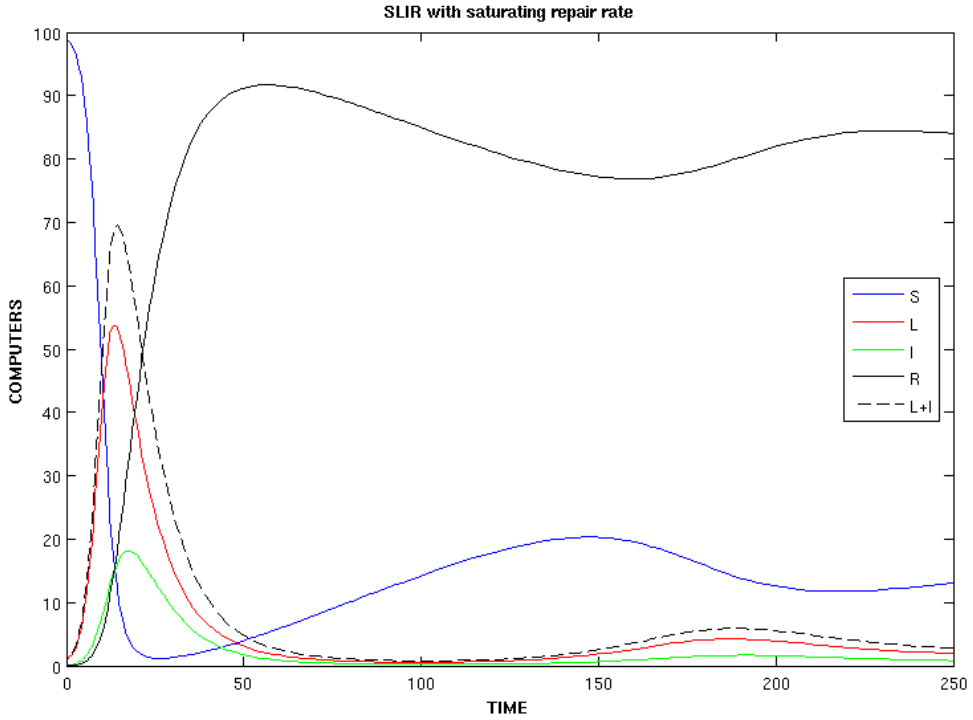

FIGURE 2. SLIR Dynamics with $N = 100$, $\beta = 0.5$, $\rho = 0.3$, $r = 0.25$, $d = 0.1$ and repair threshold $f(R) = \frac{R}{N}$

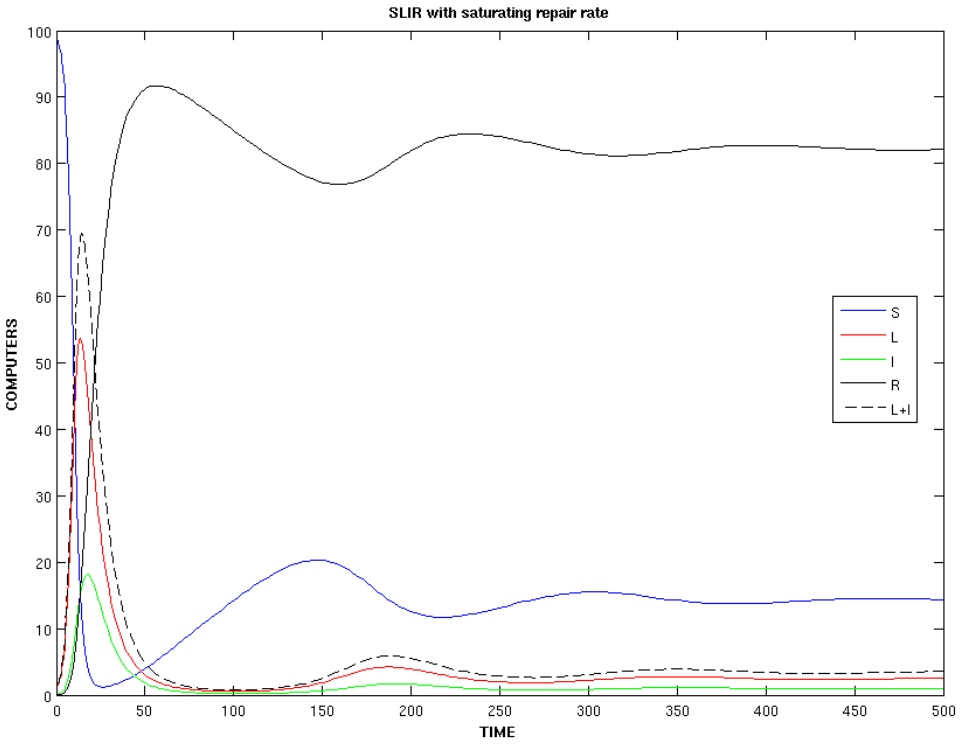

FIGURE 3. SLIR Dynamics with $N = 100$, $\beta = 0.5$, $\rho = 0.3$, $r = 0.25$, $d = 0.1$ and repair threshold $f(R) = \frac{R}{N}$

3.2. **Threshold $g(R)$.** To obtain a different probabilistic interpretation of the repair process we consider the repair rate threshold $g(R) = 1 - e^{-\gamma R}$. The SLIR dynamics then become

$$
\begin{aligned}
\frac{dS}{dt} &= -\beta(L+I)S/N + \rho(1-e^{-\gamma R}) \\
\frac{dL}{dt} &= \beta(L+I)S/N - dL \\
\frac{dI}{dt} &= dL - rI \\
\frac{dR}{dt} &= rI - \rho(1-e^{-\gamma R})
\end{aligned} \tag{2}
$$

Still assuming a closed population the system reduces to

$$
\begin{aligned}
\frac{dS}{dt} &= -\beta(L+I)S/N + \rho(1-e^{-\gamma(N-S-L-I)}) \\
\frac{dL}{dt} &= \beta(L+I)S/N - dL \\
\frac{dI}{dt} &= dL - rI
\end{aligned} \tag{3}
$$

We find the steady states for system (2) in a similar way. Again $(N,0,0)$ is a steady state and any non-zero steady state (S^*, L^*, I^*) will be determined by

$$\beta(L^*+I^*)S^*/N = \rho(1-e^{-\gamma(N-S^*-L^*-I^*)}) = dL^* = rI^*.$$

From $\beta(L^*+I^*)S^*/N = rI^*$ and $dL^* = rI^*$ we obtain $S^* = \frac{Nrd}{\beta(r+d)}$ from which it follows

$$
\begin{aligned}
\rho - rI^* &= \rho e^{-\gamma(N-S^*-L^*-I^*)} \\
\rho - rI^* &= \rho e^{-\gamma N + \gamma\frac{Nrd}{\beta(r+d)} + \gamma\frac{r}{d}I^* + \gamma I^*} \\
(\rho - rI^*)\, e^{-\gamma\frac{r+d}{d}I^*} &= \rho e^{-\gamma N(1-\frac{rd}{\beta(r+d)})}.
\end{aligned}
$$

Multiplying both sides by $\gamma\frac{r+d}{rd}e^{\gamma\rho\frac{r+d}{rd}}$ gives

$$
\begin{aligned}
\gamma\frac{r+d}{rd}(\rho - rI^*)\, e^{\gamma\rho\frac{r+d}{rd} - \gamma\frac{r+d}{d}I^*} &= \gamma\rho\frac{r+d}{rd}e^{\gamma\rho\frac{r+d}{rd} - \gamma N(1-\frac{rd}{\beta(r+d)})} \\
\gamma\frac{r+d}{rd}(\rho - rI^*)\, e^{\gamma\frac{r+d}{rd}(\rho - rI^*)} &= \gamma\rho\frac{r+d}{rd}e^{\gamma\rho\frac{r+d}{rd} - \gamma N(1-\frac{rd}{\beta(r+d)})}.
\end{aligned}
$$

Let $W(z)$ denote the Lambert W function (i.e. the inverse of the function $f(z) = ze^z$). Because the left hand side is of the form ze^z and the right hand side is positive, we can write

$$\gamma\frac{r+d}{rd}(\rho - rI^*) = W\left(\gamma\rho\frac{r+d}{rd}e^{\gamma\rho\frac{r+d}{rd} - \gamma N\left(1-\frac{rd}{\beta(r+d)}\right)}\right).$$

Rearranging we finally obtain

$$I^* = \frac{\rho}{r} - \frac{d}{\gamma(r+d)}W\left(\gamma\rho\frac{r+d}{rd}e^{\gamma\rho\frac{r+d}{rd} - \gamma N\left(1-\frac{rd}{\beta(r+d)}\right)}\right).$$

It follows that $L^* = \frac{\rho}{d} - \frac{r}{\gamma(r+d)} W\left(\gamma\rho\frac{r+d}{rd}e^{\gamma\rho\frac{r+d}{rd}-\gamma N\left(1-\frac{rd}{\beta(r+d)}\right)}\right)$. The steady state solutions can be rewritten in terms of the basic reproduction number, R_0.

$$\begin{aligned} S^* &= N/R_0 \\ L^* &= \frac{\rho}{d} - \frac{\beta}{d\gamma R_0} W\left(\frac{\gamma\rho}{\beta}R_0 e^{\frac{\gamma\rho}{\beta}R_0-\gamma N\left(\frac{R_0-1}{R_0}\right)}\right) \\ I^* &= \frac{\rho}{r} - \frac{\beta}{r\gamma R_0} W\left(\frac{\gamma\rho}{\beta}R_0 e^{\frac{\gamma\rho}{\beta}R_0-\gamma N\left(\frac{R_0-1}{R_0}\right)}\right) \end{aligned}$$

If $R_0 = 1$ then $W\left(\frac{\gamma\rho}{\beta}R_0 e^{\frac{\gamma\rho}{\beta}R_0-\gamma N\left(\frac{R_0-1}{R_0}\right)}\right) = W\left(\frac{\gamma\rho}{\beta}R_0 e^{\frac{\gamma\rho}{\beta}R_0}\right) = \frac{\gamma\rho}{\beta}R_0$ and (S^*, L^*, I^*, R^*) reduces to $(N, 0, 0, 0)$. When $R_0 < 1$ we have $S^* > N$, which is not possible. Furthermore, for any $x, a > 0$ we have $xe^{x+a} > xe^x$ and applying the Lambert W function to both sides we obtain $W(xe^{x+a}) > W(xe^x) = x$. Thus $W\left(\frac{\gamma\rho}{\beta}R_0 e^{\frac{\gamma\rho}{\beta}R_0-\gamma N\left(\frac{R_0-1}{R_0}\right)}\right) > \frac{\gamma\rho}{\beta}R_0$ from which it follows that $I^* < 0$ and $L^* < 0$. On the other hand, when $R_0 > 1$, $S^* < N$ and $W\left(\frac{\gamma\rho}{\beta}R_0 e^{\frac{\gamma\rho}{\beta}R_0-\gamma N\left(\frac{R_0-1}{R_0}\right)}\right) < \frac{\gamma\rho}{\beta}R_0$ implying that $I^* > 0$ and $L^* > 0$. Thus R_0 is again the endemic threshold.

The Jacobian for the fixed point $(N, 0, 0)$ is

$$J_{(N,0,0)} = \begin{pmatrix} -\gamma\rho & -\beta-\gamma\rho & -\beta-\gamma\rho \\ 0 & \beta-d & \beta \\ 0 & d & -r \end{pmatrix}$$

A similar analysis as in system (1) yields equivalent results regarding the nature of this fixed point. Letting $\mathbb{W} = W\left(\frac{\gamma\rho}{\beta}R_0 e^{\frac{\gamma\rho}{\beta}R_0-\gamma N\left(\frac{R_0-1}{R_0}\right)}\right)$ and $\Phi = S^* + L^* + I^* = \frac{N}{R_0} + \frac{\rho}{\beta}R_0 + \frac{1}{\gamma}\mathbb{W}$ we can write the Jacobian of the fixed point (S^*, L^*, I^*) as

$$J_{(S^*,L^*,I^*)} = \begin{pmatrix} -(\rho R_0 - \frac{\beta}{\gamma}\mathbb{W})/N - \gamma\rho e^{-\gamma(N-\Phi)} & -\frac{\beta}{R_0} - \rho e^{-\gamma(N-\Phi)} & -\frac{\beta}{R_0} - \rho e^{-\gamma(N-\Phi)} \\ (\rho R_0 - \frac{\beta}{\gamma}\mathbb{W})/N & \frac{\beta}{R_0} - d & \frac{\beta}{R_0} \\ 0 & d & -r \end{pmatrix}$$

The above matrix is of a similar form to that of the endemic equilibrium of system (1). Again we run into the problem of algebraic complexity in determining the roots of the characteristic polynomial and further work is needed to determine the local stability. It would be interesting to explore the possibility of constructing a Lyupunov Function to demonstrate global stability. It is also of practical interest to demonstrate that the region in the first octant bounded by the plane $S + L + I = N$ is positively invariant.

4. Heterogeneous Networks

4.1. **Multi-Group SLIR.** One assumption mass-action models such as the SLIR model makes is that the population is homogeneous in terms of individual contacts. This is not a realistic assumption in many cases. In particular it is not often true for computer networks. To deal with contact heterogeneity we consider a multi-group SLIR model where the network is divided into n subnets, each of which is internally homogeneous with regards to contact dynamics. This is accomplished by coupling n SLIR models. Let the the number of susceptibles, latently infected, overtly infected and removed computers in each subnet be given by S_k, L_k, I_k, R_k respectively. Let $N_k = S_k + L_k + I_k + R_k$ and $N = \Sigma_{k=1}^{n} N_k$. The parameters r_k, d_k and ρ_k are the removal, discovery and repair rates in the kth subnet and β_{jk} denotes the rate at which computers in the jth subnet contact computers in the kth subnet.

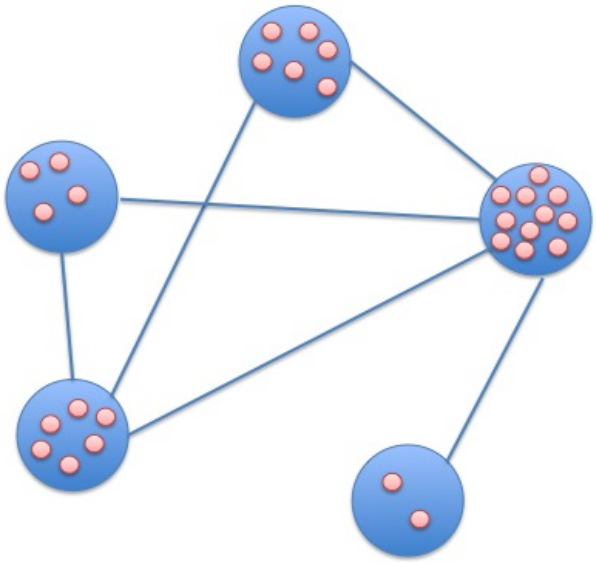

Figure 4. Example of a multi-group SLIR network

The dynamics of the kth subnet are defined as follows.

$$
\begin{aligned}
\frac{dS_k}{dt} &= -\Sigma_{j=1}^{n}\beta_{jk}(L_j + I_j)S_k/N_k + \frac{\rho_k}{N}\Sigma_{j=1}^{n}R_j \\
\frac{dL_k}{dt} &= -\Sigma_{j=1}^{n}\beta_{jk}(L_j + I_j)S_k/N_k - d_kL_k \\
\frac{dI_k}{dt} &= d_kL_k - r_kI_k \\
\frac{dR_k}{dt} &= r_kI_k - \frac{\rho_k}{N}\Sigma_{j=1}^{n}R_j
\end{aligned} \tag{4}
$$

If each subnet remains closed the kth system reduces to

$$
\begin{aligned}
\frac{dS_k}{dt} &= -\Sigma_{j=1}^{n}\beta_{jk}(L_j + I_j)S_k/N_k + \frac{\rho_k}{N}\Sigma_{j=1}^{n}(N_j - S_j - L_j - I_j) \\
\frac{dL_k}{dt} &= -\Sigma_{j=1}^{n}\beta_{jk}(L_j + I_j)S_k/N_k - d_kL_k \\
\frac{dI_k}{dt} &= d_kL_k - r_kI_k \\
\frac{dR_k}{dt} &= r_kI_k - \frac{\rho_k}{N}\Sigma_{j=1}^{n}(N_j - S_j - L_j - I_j)
\end{aligned} \tag{5}
$$

The alternative multi-group SLIR model becomes

$$
\begin{aligned}
\frac{dS_k}{dt} &= -\Sigma_{j=1}^{n}\beta_{jk}(L_j + I_j)S_k/N_k + \rho_k(1 - e^{\Sigma_{j=1}^{n}(N_j - S_j - L_j - I_j)}) \\
\frac{dL_k}{dt} &= -\Sigma_{j=1}^{n}\beta_{jk}(L_j + I_j)S_k/N_k - d_kL_k \\
\frac{dI_k}{dt} &= d_kL_k - r_kI_k \\
\frac{dR_k}{dt} &= r_kI_k - \rho_k(1 - e^{\Sigma_{j=1}^{n}(N_j - S_j - L_j - I_j)})
\end{aligned} \tag{6}
$$

4.2. **Global Stability.** Provided we can find a Lyupunov function for the single group SLIR model, we should be able to construct a Lyupunov function for the multi-group model based on the work by Li and Shuai [2], thus demonstrating the global stability of steady states.

5. Stochastic SLIR

If the number of computers in each subnet is not large the mass-action assumption of deterministic models may not be a reliable approximation. In this case we want to discretize the states of the system and proceed with a probabilistic interpretation. It seems reasonable to assume that the evolution of the system depends only on its current state. We therefore model the system as a Markov Jump Process and the parameters in our model become event probabilities per unit time rather than event rates. For the single-group SLIR model

we have four possible events. Let T_i be the transition probability per unit time for event i to occur and associate the following events with each T_i.

$$\begin{aligned} T_1 &: S \longrightarrow L \\ T_2 &: L \longrightarrow I \\ T_3 &: I \longrightarrow R \\ T_4 &: R \longrightarrow S \end{aligned}$$

Given a closed population let the state of the system be given by (s, l, i) where s is the current number of susceptibles, l is the current number of latently infected and i is the current number of overtly infected. Interpreting the parameters as probabilities per unit time we have

$$\begin{aligned} T_1(s, l, i) &= \beta(l + i)s/N \\ T_2(s, l, i) &= dl \\ T_3(s, l, i) &= ri \\ T_4(s, l, i) &= \rho(N - s - l - i)/N. \end{aligned}$$

Let $P(s, l, i, t)$ be the probability of being in state (s, l, i) at time t. Then we can write

$$\begin{aligned} P(s, l, i, t + \Delta t) = (1 - (T_1 + T_2 + T_3 + T_4)\Delta t)P(s, l, i, t) + T_1 P(s + 1, l - 1, i, t)\Delta t \\ + T_2 P(s, l + 1, i - 1, t)\Delta t + T_3 P(s, l, i + 1, t)\Delta t \\ + T_4 P(s - 1, l, i, t)\Delta t + o(\Delta t) \end{aligned}$$

Multiplying out the first term, dividing by Δt and taking $\Delta t \to 0$ we obtain the Master Equation for the stochastic SLIR model.

$$\begin{aligned} \frac{\partial P(s, l, i, t)}{\partial t} = \frac{\beta}{N}(l + i - 1)(s + 1)P(s + 1, l - 1, i, t) + d(l + 1)P(s, l + 1, i - 1, t) \\ + r(i + 1)P(s, l, i + 1, t) + \frac{\rho}{N}(N + 1 - s - l - i)P(s - 1, l, i, t) \\ - (\beta(l + i - 1)(s + 1)/N + d(l + 1) + r(i + 1) + \rho(N + 1 - s - l - i)/N)P(s, l, i, t) \end{aligned}$$

To generalizing the above system to an n-group stochastic SLIR model let the state of the system be given by the vector $\mathbf{x} = (s_1, l_1, i_1, ..., s_n, l_n, i_n)$ and let the probability of being in this state at time t be given by $P(\mathbf{x}, t)$. Define the following state vectors.

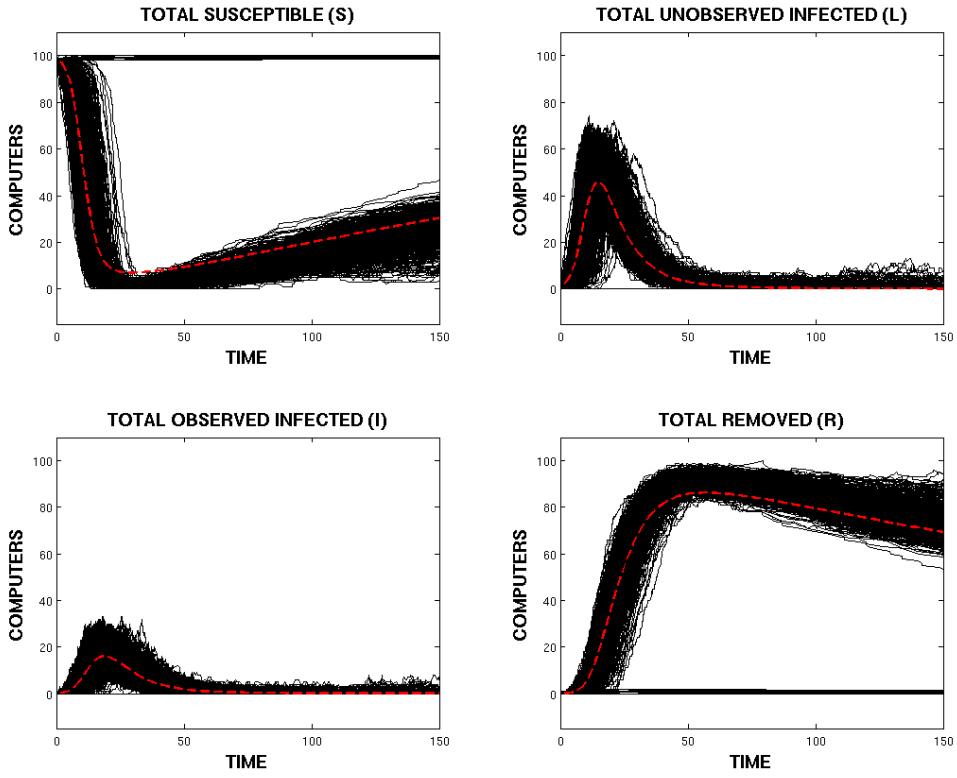

FIGURE 5. One thousand runs of the single-group Stochastic SLIR with $N = 100$, $\beta = 0.5$, $\rho = 0.3$, $r = 0.25$, and $d = 0.1$

$$
\begin{aligned}
\mathbf{x} &= (s_1, l_1, i_1, ..., s_n, l_n, i_n) \\
\mathbf{x_1^k} &= (s_1, l_1, i_1, ..., s_k + 1, l_k - 1, i_k, ..., s_n, l_n, i_n) \\
\mathbf{x_2^k} &= (s_1, l_1, i_1, ..., s_k, l_k + 1, i_k - 1, ..., s_n, l_n, i_n) \\
\mathbf{x_3^k} &= (s_1, l_1, i_1, ..., s_k, l_k, i_k + 1, ..., s_n, l_n, i_n) \\
\mathbf{x_4^k} &= (s_1, l_1, i_1, ..., s_k - 1, l_k, i_k, ..., s_n, l_n, i_n)
\end{aligned}
$$

A similar derivation as above yields the n-group SLIR Master Equation.

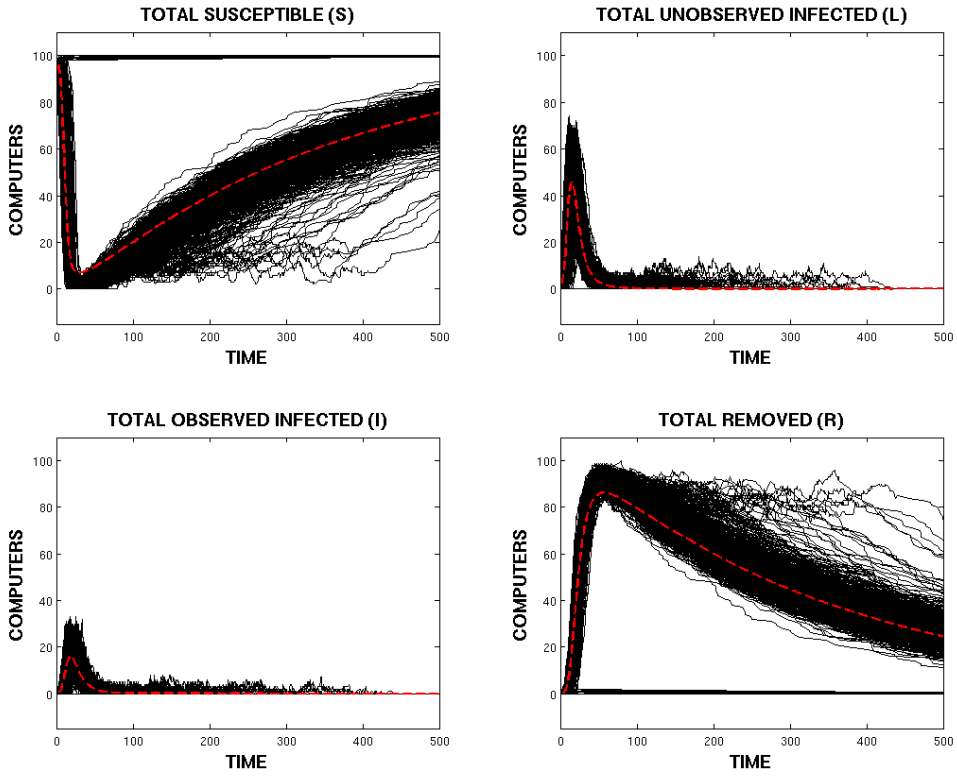

FIGURE 6. One thousand runs of the single-group Stochastic SLIR with $N = 100$, $\beta = 0.5$, $\rho = 0.3$, $r = 0.25$, and $d = 0.1$

$$\begin{aligned}\frac{\partial P(\mathbf{x},t)}{\partial t} &= \Sigma_{j\neq k}\frac{\beta_{jk}}{N_k}(l_j+i_j)(s_k+1)P(\mathbf{x_1^k},t) + \Sigma_{k=1}^{n}\frac{\beta_{kk}}{N_k}(l_k+i_k-1)(s_k+1)P(\mathbf{x_1^k},t)\\ &+ \Sigma_{k=1}^{n}d_k(l_k+1)P(\mathbf{x_2^k},t) + \Sigma_{k=1}^{n}r_k(i_k+1)P(\mathbf{x_3^k},t)\\ &+ \Sigma_{k=1}^{n}\frac{\rho_k}{N_k}(N_k+1-s_k-l_k-i_k)P(\mathbf{x_4^k},t)\\ &- (\Sigma_{j\neq k}\frac{\beta_{jk}}{N_k} + \Sigma_{k=1}^{n}\frac{\beta_{kk}}{N_k}(l_k+i_k-1)(s_k+1) + \Sigma_{k=1}^{n}d_k(l_k+1) + ...\\ &... + \Sigma_{k=1}^{n}r_k(i_k+1) + \Sigma_{k=1}^{n}\frac{\rho_k}{N_k}(N_k+1-s_k-l_k-i_k))P(\mathbf{x},t)\end{aligned}$$

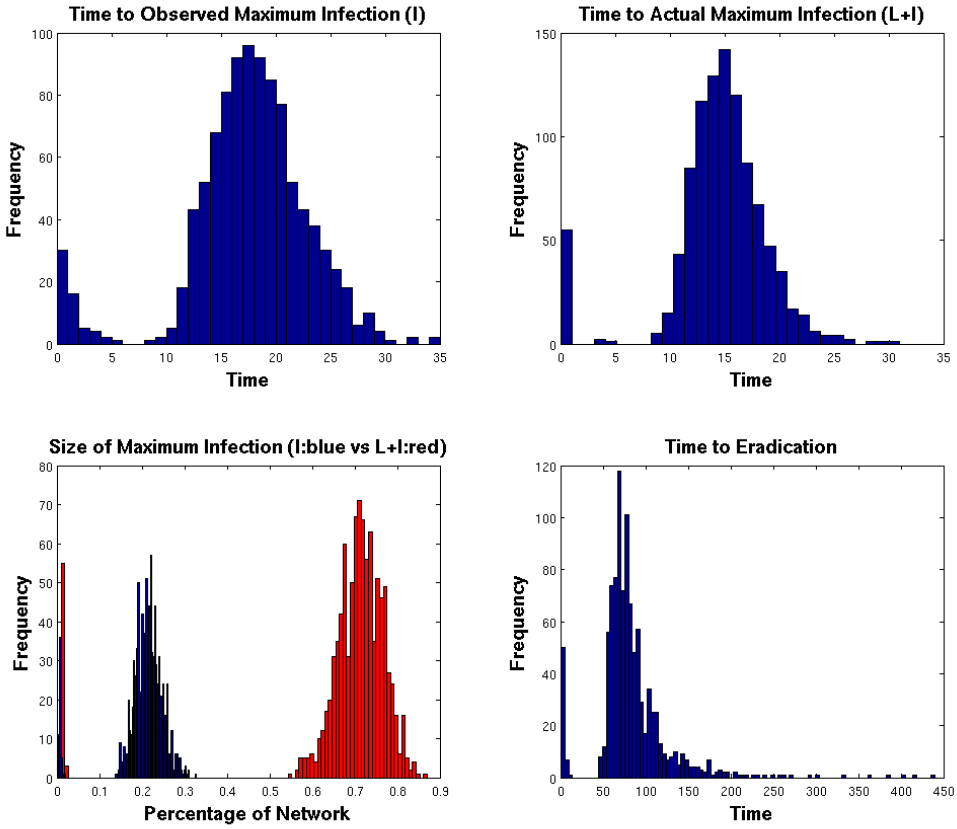

FIGURE 7. Distributions of some critical metrics for 1000 runs of the Stochastic SLIR model.

To simulate the evolution of this stochastic process we used the Gillespie Algorithm [3]. Notice in Figure 6 the long term evolution of the stochastic systems. Given the non-zero probability of eradicating the network intruder, the stochastic system fluctuates around the endemic equilibrium for a finite time. Eventually the intruder is eradicated leading to the "disease-free" equilibrium. Compare this to the endemic equilibrium approached by the deterministic system in Figure 3. Many useful statistical properties can be obtained from these stochastic simulations. Here we present the distributions of some critical metrics in figure 7 as well as the evolution of the distribution of susceptibles in figure 8.

6. Alternative Models and Future Work

6.1. **SLIRP Model.** There are many modifications of the basic compartmental epidemiological models that may be useful for describing different scenarios. One possible extension

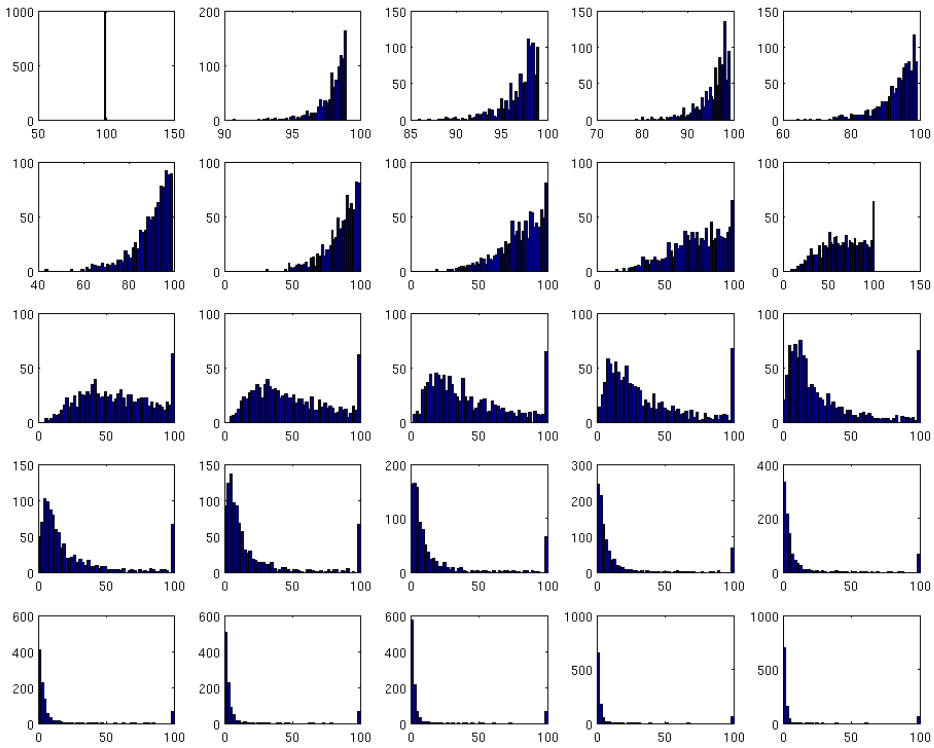

FIGURE 8. Evolution in unit time increments of the distribution of susceptible computers for 100 runs of the Stochastic SLIR model: $0 \leq t \leq 24$.

is to consider a patched group, P, which contains computers that have been patched with appropriate software as to make them, permanently or temporarily, immune to infection. We may consider a birth and death parameter λ which represents the rate at which computers break down or become obsolete and are replaced. Software patches sent out by network administrators may be downloaded and installed at a rate of ρ_s while the patches themselves fail at a rate of ψ. Denoting the repair rate by ρ_r and the threshold function by $f(R)$ we can consider the following much more complex system.

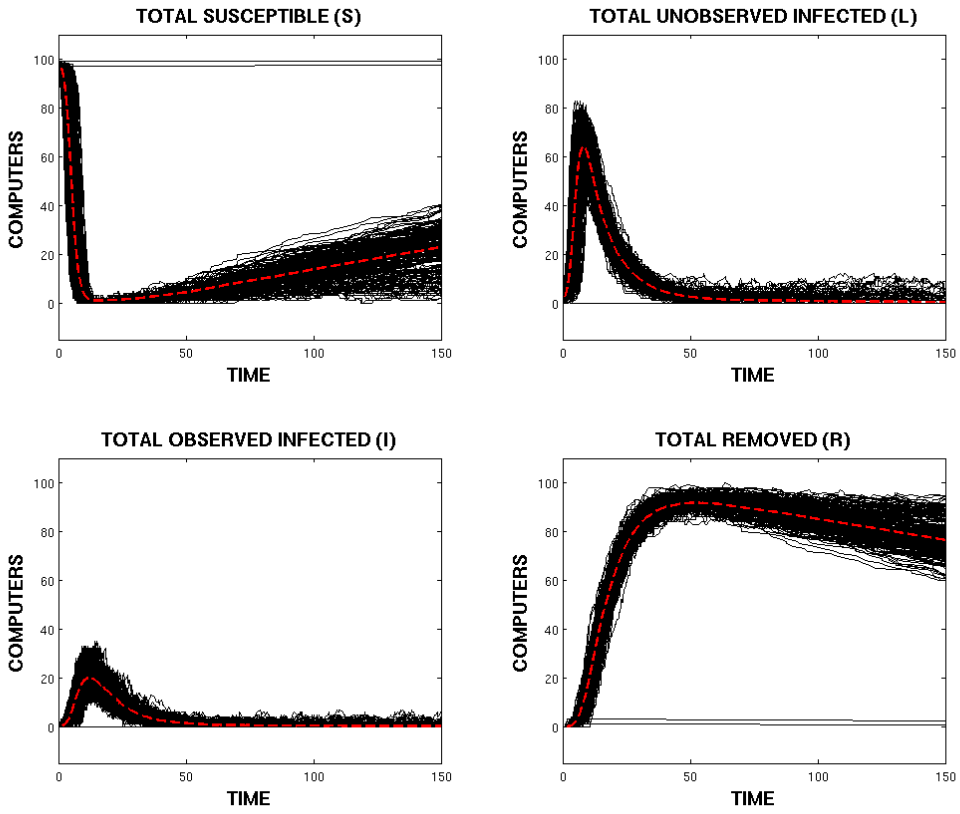

FIGURE 9. 250 runs of a 10-subnet Stochastic SLIR with $N_k = 10$, $\beta_{kk} = 0.51$, $\beta_{jk} = 0.01(j \neq k)$, $\rho_s = 0.05$, $\rho_s = 0.15$, $r = 0.25$, and $d = 0.1$. Red dashed line is the mean.

$$\begin{aligned}
\frac{dS}{dt} &= \psi P + \lambda\,(1 - S/N) - \beta(L + I)S/N - \rho_s S \\
\frac{dL}{dt} &= \beta(L + I)S/N - (d + \lambda/N)L \\
\frac{dI}{dt} &= dL - (r + \lambda/N)I \\
\frac{dR}{dt} &= rI - \rho_r f(R) - \lambda R/N \\
\frac{dP}{dt} &= \rho_s S + \rho_r f(R) - (\psi + \lambda/N)P
\end{aligned}$$

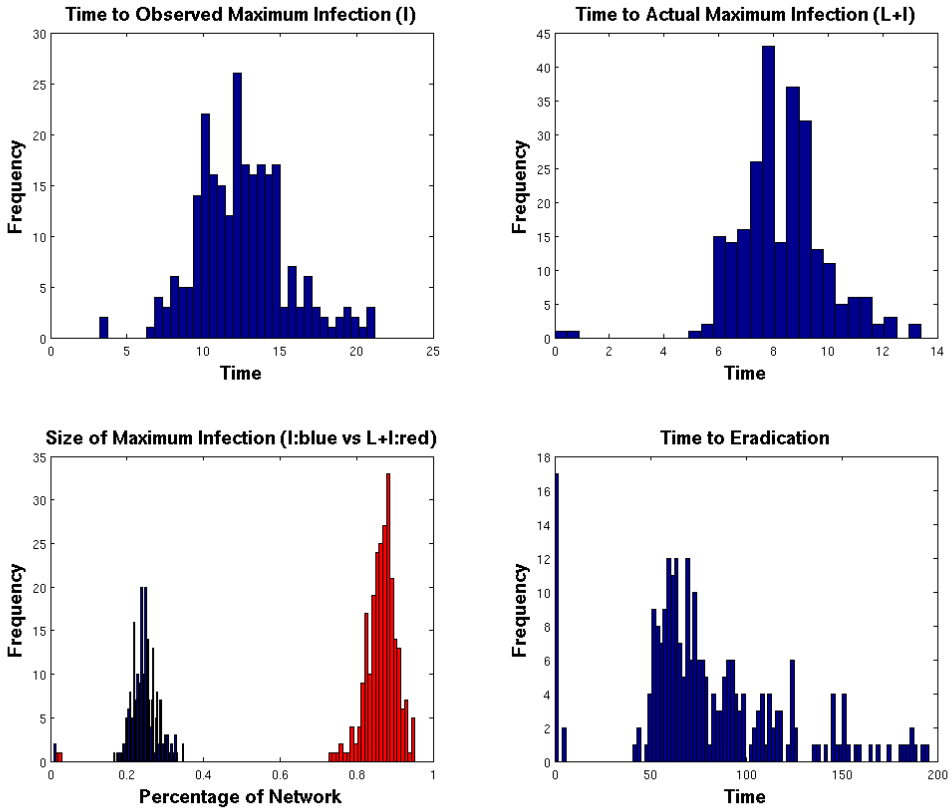

FIGURE 10. Distributions of some critical metrics for 250 runs of the multi-group Stochastic SLIR model.

Extending these models to the multi-group systems and incorporating stochasticity into the dynamics presents a wide range of possible research.

6.2. **Contact Network Epidemiology.** Though coupling systems of ODEs into multi-group epidemiological models takes some degree of contact heterogeneity into account, it still relies on mass-action assumptions that may not be realistic. The use of percolation theory and random graphs in Contact Network Epidemiology can dispose of the mass-action assumptions by using arbitrary distributions of a networks edges among nodes, giving the network more realistic topologies which may greatly affect the final outcome of a disease [4]. One shortcoming of these models was the fact that they did not take into account the dynamics of the disease over time, however more recently progress has been made along these lines [5]. Applying the techniques from Contact Network Epidemiology to our current modeling efforts may yield very useful results.

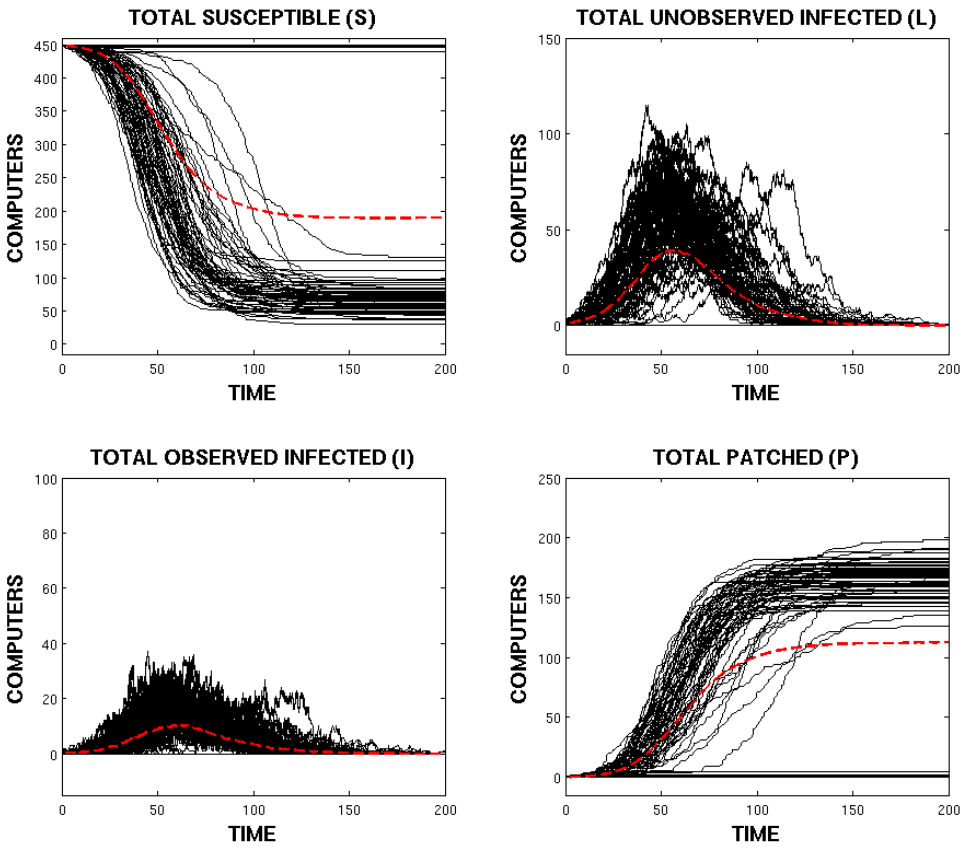

FIGURE 11. One hundred runs of a 15-subnet Stochastic SLIRP with $N_k = 30$, $\beta_{kk} = 0.51$, $\beta_{jk} = 0.01(j \neq k)$, $\rho_s = 0.05$, $\rho_s = 0.15$, $r = 0.25$, and $d = 0.1$. Red dashed line is the mean.

6.3. **Control Theory.** Once an appropriate model is developed we would like to study the optimal control of a compromised network. Control parameters such as the discovery rate and removal rate are integral parts of network defense. By determining the associated cost with each defense tactic, a cost function could be created to determine the optimal control strategy which minimizes cost of defense and maximizes productivity of the network.

6.4. **Game Theory.** The adversarial nature of network attacks lends itself to game theoretic analysis. Framing our models of network intrusion in the language of game theory and developing optimal strategies could provide meaningful insights to network defense strategies.

6.5. **Network Data.** Stochastic simulation provides a convenient testing environment for the optimal control of a compromised network. Obtaining parameter values based on observed network data flow would provide our models with more realistic network topology. Defense parameters such as detection rate, patching rate and removal rate can be altered to test for optimal response methods. Estimates of critical values may be obtained such as average time to maximum intrusion, average total time of intrusion, and average number of compromised machines.

References

[1] Kephart, J.O., White, S.R.: Directed-Graph Epidemiological Models of Computer Viruses In *IEEE Symposium on Security and Privacy*. (1991) 343-361

[2] Li, M. Y., Shuai, Z.: Global-stability for coupled systems of differential equations on networks, *Journal of Differential Equations*. 248 (2010) 1-20.

[3] Gillespie, D.T.: Exact Stochastic Simulation of Coupled Chemical Reactions, *Journal of Physical Chemistry* 81 (1977) 2340-2361.

[4] Newman, M.E.J.: The Spread of Epidemic Disease on Networks *Physical Review E* 66 (2002) 016128.

[5] Volz, E.: SIR Dynamics in Structured Populations with Heterogeneous Connectivity *Journal of Mathematical Biology* 56 (2005) 293-310.

Department of Applied Mathematics and Statistics, University of California, Santa Cruz

Applied Statistics Group, Lawrence Livermore National Laboratory