A Compartmental Model for Transmission Dynamics of Distributed Attack of Malicious Codes on the Targeted Network: Effect of Firewall Security

B.Tech Project Presentation

Group Number -22

Durgesh Kumar Soni (2012IPG-032)
Palash Jain (2012IPG-105)
Ashish Bhargava (2012IPG-123)

September 29, 2015

Contents

INTRODUCTION

- Malicious codes are programs that can get into networks and spread. It may delete or corrupt files that are stored on the system. Malicious code are of various types: virus, worm, Trojan horse, etc..

- Malicious codes can replicate themselves and a recognizable degradation in the performance could be observed in a computer.

- Malicious codes propagation is epidemic in nature.

- Due to continuous emergence of new types of attacks there is a need to enhance the existing propagation models.

LITERATURE REVIEW

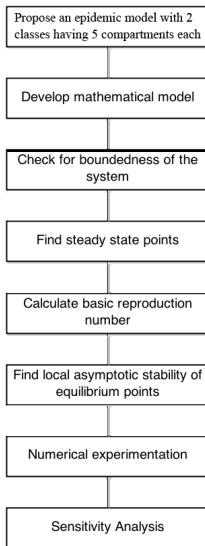| Author	Paper Title	Publication Details	Salient Points
Kephart, Jeffrey O and White, Steve R.	Measuring and modeling computer virus prevalence.	Research in Security and Privacy, 1993. Proceedings., 1993 IEEE Computer Society Symposium.	Kill signal idea.
Misra, AK and Verma, Maitri and Sharma, Anupama.	Capturing the interplay between malware and anti-malware in a computer network.	Applied Mathematics and Computation, 2014.	To assess the potency of anti-malware softwares in protecting a network from malicious attack.
Yang, Xiaofan and Yang, Lu-Xing.	Towards the epidemiological modeling of computer viruses.	Discrete Dynamics in Nature and Society, 2012.	Identify flaws of previous models and propose a generic SLBS epidemic model.
Wang, Fangwei and Yang, Yong and Zhao, Dongmei and Zhang, Yunkai.	A Worm Defending Model with Partial Immunization and Its Stability Analysis.	Journal of Communications, 2015.	Proposes a novel epidemic SVEIR model with partial immunization and give a theoretical foundation for controlling internet worms.

LITERATURE REVIEW

| Author	Paper Title	Publication Details	Salient Points
Brady, Oliver J and Godfray, H Charles J and Tatem.	Adult vector control, mosquito ecology and malaria transmission.	International health, 2015.	Idea of reducing the lifespan of adult mosquitoes is taken in this paper.
Mishra, Bimal Kumar and Prajapati, Apeksha.	Mathematical Model on Attack by Malicious Objects Leading to Cyber War.	International Journal of Nonlinear Science, 2014.	Impact of two recovered and infection classes has taken into consideration.
A.A.M. ARAFA, M. KHALIL and A. HASSAN.	Fractional order E-Epidemic Model with highly Infectious Nodes.	December, 2014.	A SIJR epidemic model of fractional order is proposed.
Sun, Mei and Li, Dandan and Han, Dun and Jia,Changsheng.	Impact of anti-virus software on computer virus dynamical behavior.	International Journal of Modern Physics C, 2014.	The effect of antivirus software and disconnecting rate on the spreading of virus are analyzed. SLBV model is proposed.

PROBLEM STATEMENT AND OBJECTIVE

- ▶ The main objective of our work is to propose an epidemic model for propagation of malicious codes in computer networks. This model is developed to enhance the previous work done in this area.

- ▶ To achieve this goal, we have developed a model which considers two classes of population named targeted and attacker classes, and these classes are sub-divided into five compartments each(viz., Susceptible-Latent-Breaking out-Recovered-Antidotal). We have also taken into consideration the effect of firewall security coefficient 'm' to analyze its effect on malicious code propagation.

WORKFLOW CHART

```
┌─────────────────────────────────┐
│ Propose an epidemic model with 2│
│ classes having 5 compartments each│
└─────────────────────────────────┘
                 │
┌─────────────────────────────────┐
│   Develop mathematical model    │
└─────────────────────────────────┘
                 │
┌─────────────────────────────────┐
│  Check for boundedness of the   │
│            system               │
└─────────────────────────────────┘
                 │
┌─────────────────────────────────┐
│     Find steady state points    │
└─────────────────────────────────┘
                 │
┌─────────────────────────────────┐
│   Calculate basic reproduction  │
│            number               │
└─────────────────────────────────┘
                 │
┌─────────────────────────────────┐
│ Find local asymptotic stability of│
│      equilibrium points         │
└─────────────────────────────────┘
                 │
┌─────────────────────────────────┐
│    Numerical experimentation    │
└─────────────────────────────────┘
                 │
┌─────────────────────────────────┐
│      Sensitivity Analysis       │
└─────────────────────────────────┘
```

Schematic Flow of Proposed Compartmental Model
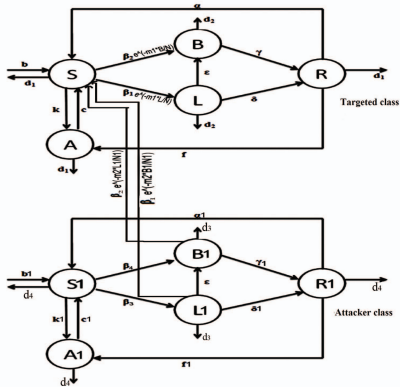
Parameters Description of Proposed Compartmental Model

Parameters	Description
b, b_1	Recruitment rates
d_1, d_2	Natural death rate of attacker and targeted population nodes
β_1, β_3	rate of contact from susceptible class to latent class;(without firewall security)
β_2, β_4	rate of contact from susceptible class to breaking-out class;(without firewall security)
γ, γ_1	Recovery rate of breaking-out nodes
δ, δ_1	Recovery rate of latent nodes
d_3, d_4	Death rate of nodes in infected class(death due to infection and natural death)
ϵ, ϵ_1	Rate of breaking-out of viruses in latent class
f, f_1	Rate of conversion of recovered nodes into antidotal nodes
c, c_1	Rate of conversion of antidotal nodes into susceptible nodes
k, k_1	Rate of conversion of susceptible nodes into antidotal nodes
α, α_1	Rate of conversion of recovered nodes into susceptible nodes
$m_1, \ m_2$	firewall security coefficients

Table: Parameters Description

Model Development

For targeted nodes:

$$\frac{d\tilde{S}}{d\tilde{t}} = b - \tilde{\beta}_2 e^{-m_1 \frac{\tilde{B}}{N}} \tilde{S} \frac{\tilde{B}}{N} - \tilde{\beta}_1 e^{-m_1 \frac{\tilde{L}}{N}} \tilde{S} \frac{\tilde{L}}{N} - \tilde{k}\tilde{S}\tilde{A} + \tilde{c}\tilde{A} - \tilde{d}_1 \tilde{S}$$
$$+ \tilde{\alpha}\tilde{R} - \tilde{\beta}_2 e^{-m_2 \frac{\tilde{B}_1}{N_1}} \tilde{S} \frac{\tilde{B}_1}{\tilde{N}_1} - \tilde{\beta}_1 e^{-m_2 \frac{\tilde{L}_1}{N_1}} \tilde{S} \frac{\tilde{L}_1}{\tilde{N}_1},$$

$$\frac{d\tilde{B}}{d\tilde{t}} = \tilde{\beta}_2 e^{-m_1 \frac{\tilde{B}}{N}} \tilde{S} \frac{\tilde{B}}{N} - \tilde{d}_2 \tilde{B} + \tilde{\epsilon}\tilde{L} - \tilde{\gamma}\tilde{B} + \tilde{\beta}_2 e^{-m_2 \frac{\tilde{B}_1}{N_1}} \tilde{S} \frac{\tilde{B}_1}{\tilde{N}_1},$$

$$\frac{d\tilde{L}}{d\tilde{t}} = \tilde{\beta}_1 e^{-m_1 \frac{\tilde{L}}{N}} \tilde{S} \frac{\tilde{L}}{N} - \tilde{d}_2 \tilde{L} - \tilde{\epsilon}\tilde{L} - \tilde{\delta}\tilde{L} + \tilde{\beta}_1 e^{-m_2 \frac{\tilde{L}_1}{N_1}} \tilde{S} \frac{\tilde{L}_1}{\tilde{N}_1},$$

$$\frac{d\tilde{R}}{d\tilde{t}} = \tilde{\gamma}\tilde{B} + \tilde{\delta}\tilde{L} - \tilde{f}\tilde{R} - \tilde{\alpha}\tilde{R} - \tilde{d}_1 \tilde{R},$$

$$\frac{d\tilde{A}}{d\tilde{t}} = \tilde{f}\tilde{R} - \tilde{d}_1 \tilde{A} + \tilde{k}\tilde{S}\tilde{A} - \tilde{c}\tilde{A}.$$

For attacker nodes:

$$\frac{d\tilde{S}_1}{d\tilde{t}} = b_1 - \tilde{\beta}_4 \tilde{S}_1 \tilde{B}_1 - \tilde{\beta}_3 \tilde{S}_1 \tilde{L}_1 - \tilde{k}_1 \tilde{S}_1 \tilde{A}_1 + \tilde{c}_1 \tilde{A}_1 - \tilde{d}_3 S_1 + \tilde{\alpha}_1 \tilde{R}_1,$$

$$\frac{d\tilde{B}_1}{d\tilde{t}} = \tilde{\beta}_4 \tilde{S}_1 \tilde{B}_1 - \tilde{d}_4 \tilde{B}_1 + \tilde{\epsilon}_1 L_1 - \tilde{\gamma}_1 B_1,$$

$$\frac{d\tilde{L}_1}{d\tilde{t}} = \tilde{\beta}_3 \tilde{S}_1 \tilde{L}_1 - \tilde{d}_4 \tilde{L}_1 - \tilde{\epsilon}_1 L_1 - \tilde{\delta}_1 L_1,$$

$$\frac{d\tilde{R}_1}{d\tilde{t}} = \tilde{\gamma}_1 \tilde{B}_1 + \tilde{\delta}_1 \tilde{L}_1 - \tilde{f}_1 \tilde{R}_1 - \tilde{\alpha}_1 \tilde{R}_1 - \tilde{d}_3 \tilde{R}_1,$$

$$\frac{d\tilde{A}_1}{d\tilde{t}} = \tilde{f}_1 \tilde{R}_1 - \tilde{d}_3 \tilde{A}_1 + \tilde{k}_1 \tilde{S}_1 \tilde{A}_1 - \tilde{c}_1 \tilde{A}_1.$$

- Boundedness of the system is examined for both the attacker and targeted classes and the observed results are:
  For targeted class : it is seen that, for arbitrarily small $k > 0$, given simply connected compact set is invariant.

$$\Omega_k = \{(\tilde{S}, \tilde{L}, \tilde{B}, \tilde{R}, \tilde{A}) \in R_+{}^5 : \tilde{S} + \tilde{L} + \tilde{B} + \tilde{R} + \tilde{A} \leq \frac{b}{d} + k\},$$

For attacker class :

$$\Omega_{k_1} = \{(\tilde{S_1}, \tilde{L_1}, \tilde{B_1}, \tilde{R_1}, \tilde{A_1}) \in R_+{}^5 : \tilde{S_1} + \tilde{L_1} + \tilde{B_1} + \tilde{R_1} + \tilde{A_1} \leq \frac{b_1}{d_1} + k_1\},$$

- Steady States and their Stability : Sixteen equilibrium states are observed out of which four are malicious-codes free and rest are endemic equilibrium states.

- Basic Reproduction Number : It is defined as the expected number of secondary cases produced by a single infection in a completely susceptible population. Observed basic reproduction number for this model is :

$$R_0 = max\left\{\frac{S(1+\beta_1)}{1+d_2+\delta+\varepsilon-A}, \frac{S_1(1+\beta_3)}{1+d_3+\delta_1+\varepsilon_1-A_1}, \frac{S(1+\beta_2)}{1+d_2+\gamma-A}, \frac{S_1(1+\beta_4)}{1+d_3+\gamma_1-A_1}\right\},$$

- ▶ Local Asymptotic Stability : The local stability of malicious codes free and endemic equilibrium is verified by the eigen values of the variational matrix J_0. It is observed that any equilibrium state will be locally asymptotically stable when all the eigen values are negative or having negative real parts. If $R_{01} < 1$, then all the eigen values will have negative real parts. Hence, the malicious codes free equilibrium is locally asymptotically stable, if $R_{01} < 1$, and unstable otherwise.

- ▶ Numerical Simulation : The feasibility of steady states for different parameter sets along with basic reproduction number for malicious codes free equilibrium states are calculated, a steady state is feasible if all the classes have non-negative values at this point.

Parameters	Set 1	Set 2
β_1	0.6	0.6
β_2	0.5	0.5
k	0.06	0.06
c	0.03	0.03
α	0.05	0.05
d_2	0.04	0.08
ϵ	0.3	0.3
γ	0.045	0.45
δ	0.025	0.25
f	0.02	0.02
β_3	0.4	0.4
β_4	0.3	0.3
f_1	0.15	0.15
k_1	0.05	0.05
c_1	0.01	0.01
α_1	0.04	0.04
d_3	0.05	0.05
γ_1	0.035	0.35
δ_1	0.02	0.2
ϵ_1	0.25	0.25
feasible SS	E_9, E_{10}	E_1, E_2, E_3, E_4
$\mathcal{R}_{01}$	5.8803	0.9523
$\mathcal{R}_{02}$	5.88034	0.9523
$\mathcal{R}_{03}$	3.52822	0.8000
$\mathcal{R}_{04}$	2.94421	0.4767

Feasible steady states and basic reproduction number for different parameter set in the model

NUMERICAL SIMULATION
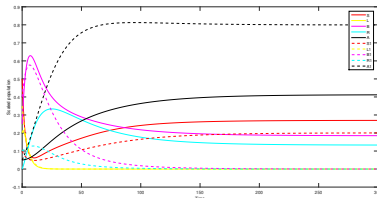
fig:3.1 Node Density vs. Time for set 1 initial point(0.5 0.2 0.25 0 0.05 0.1 0.35 0.4 0.1 0.05)
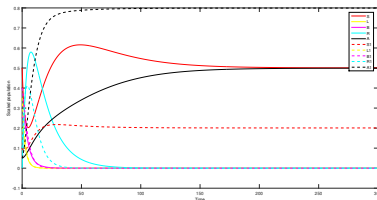
fig:3.2 Feasible steady states and basic reproduction number for different parameter set in the model)

▶ Figure 3.1 is plotted with parameter Set 1 and initial point $(0.5, 0.2, 0.25, 0, 0.05, 0.1, 0.35, 0.4, 0.1, 0.05)$. In this figure at steady state, node density of S, B, R, A and S_1 classes are greater than zero and possible feasible states are E_9 and E_{10}. Since all the reproduction number is greater than 1, hence we can conclude from the fig. 3.1 that E_{10} is the stable steady state.

▶ Similarly, figure 3.2 is plotted with parameter Set 2 and initial point $(0.5, 0.2, 0.25, 0, 0.05, 0.1, 0.35, 0.4, 0.1, 0.05)$ and from the figure we can conclude that E_1, E_2, E_3 and E_4 are the feasible steady states and E_4 is the stable steady state.

Estimation of firewall security coefficient 'm'

▶ The objective of the use of firewall security is to create rules and policies which allows only particular connections. We define a way for measuring the value m of firewall security as,

$$m = -\log_e(a + b - ab),$$

where, b measures the response of the files to the defined security rules. For our work we can add certain rules by monitoring the behavior of attacker class. When the files will be received in targeted class, they will be checked according to the rules defined in the firewall rule base. If they response correctly to all these rules then b=0 and if they dont match any of the rules then b=1 and it is assumed that the malware propagation rate can be reduced by fraction a, when all received files abide the defined security rules.

fig:3.3 Effect of m on L when $R_0 = 0.9523 < 1$
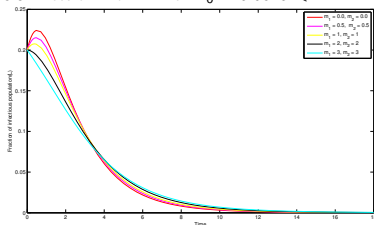
fig:3.4 Effect of m on B when $R_0 = 1.58846 > 1$
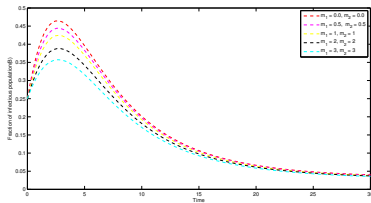
SENSITIVITY ANALYSIS

► Normalized forward sensitivity index is used for the sensitivity analysis of basic reproduction number. Sensitivity indices enables us to measure the relative change in a state variable with respect to a small change in the system parameter. Estimation and measurement of highly sensitive parameter should be done carefully, because a small change in the parameter will lead to relatively huge quantitative change. With respect to each parameter, we derived analytical expressions for sensitivity index of R_0. We observed most sensitive parameters for Basic Reproduction Number which are shown in the table below,

Parameters	$\Upsilon_{y_j}^{\mathcal{R}_{01}}$ Set 1	$\Upsilon_{y_j}^{\mathcal{R}_{01}}$ Set 2	$\Upsilon_{y_j}^{\mathcal{R}_{01}}$ Set 3	$\Upsilon_{y_j}^{\mathcal{R}_{01}}$ Set 4	$\Upsilon_{y_j}^{\mathcal{R}_{01}}$ Set 5	$\Upsilon_{y_j}^{\mathcal{R}_{01}}$ Set 6
β_1	0	0.999	0	0	0	0
β_2	0.999	0	0	0.999	0.999	0.9999
k	0	0	0	0	0	0
c	0	0	0	0	0	0
α	0	0	0	0	0	0
d_2	-0.47	-0126	0	-0.499	-0.446	-0.72
ϵ	0	-0.476	0	0	0	0
γ	0.529	0	0	0.499	0.553	0.285
δ	0	-0.396	0	0	0	0
f	0	0	0	0	0	0
β_3	0	0	0	0	0	0
β_4	0	0	0.99	0	0	0
f_1	0	0	0	0	0	0
k_1	0	0	0	0	0	0
c_1	0	0	0	0	0	0
α_1	0	0	0	0	0	0
d_3	0	0	-0.499	0	0	0
γ_1	0	0	-0.499	0	0	0
δ_1	0	0	0	0	0	0
ϵ_1	0	0	0	0	0	0

Normalized sensitivity indices w.r.t. R_{01}

Basic Reproduction Number	Most Sensitive Parameters
R_{01}	$\beta_1, \beta_2, \beta_4$
R_{02}	β_1, β_2
R_{03}	$\beta_2, \beta_3, \beta_4, k, c$
R_{04}	β_1, β_2, k, c

Most sensitive parameters for Basic Reproduction Number

- For the proposed model sixteen equilibrium states are calculated out of which four are malicious codes free equilibrium and rest are endemic in nature. Basic reproduction number for the malicious codes free equilibrium states has been observed and it has been found that the malicious code free equilibrium is stable, if $R_0 < 1$ and, the endemic equilibrium is stable, if $R_0 > 1$. Local asymptotic stability is used as a mathematical tool to verify the stability of the system

- We have observed that the basic reproduction number R_0 is not affected by the coefficient of firewall security 'm' and hence the qualitative features of the model don't change.

- We conclude that the use of firewall security rule base helps to mitigate the problem of malicious code propagation in the network by minimizing the level of infected nodes at steady state

- Future Scope: This work can be extended by considering a time delay for outbreak and time variant birth rate. "Kill Signal" idea can be implemented in the proposed model.

📄 Kephart, Jeffrey O., and Steve R. White. "Measuring and modeling computer virus prevalence." Research in Security and Privacy, 1993. Proceedings., 1993 IEEE Computer Society Symposium on. IEEE, 1993.

📄 Misra, A. K., Maitri Verma, and Anupama Sharma. "Capturing the interplay between malware and anti-malware in a computer network." Applied Mathematics and Computation 229 (2014): 340-349.

📄 Yang, Xiaofan, and Lu-Xing Yang. "Towards the epidemiological modeling of computer viruses." Discrete Dynamics in Nature and Society 2012 (2012).

📄 Wang, Fangwei, et al. "A Worm Defending Model with Partial Immunization and Its Stability Analysis." Journal of Communications 10.4 (2015).

📄 Kermack, William O., and Anderson G. McKendrick. "A contribution to the mathematical theory of epidemics." Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences. Vol. 115. No. 772. The Royal Society, 1927.

📄 Mishra, Bimal Kumar, and Apeksha Prajapati. "Mathematical Model on Attack by Malicious Objects Leading to Cyber War." International Journal of Nonlinear Science 17.2 (2014): 145-153.

📄 Sun, Mei, et al. "Impact of anti-virus software on computer virus dynamical behavior." International Journal of Modern Physics C 25.05 (2014): 1440010.

📄 Brady, Oliver J., et al. "Editor's choice: Adult vector control, mosquito ecology and malaria transmission." International health 7.2 (2015): 121.

📄 Sahu, Govind Prasad, and Joydip Dhar. "Dynamics of an SEQIHRS epidemic model with media coverage, quarantine and isolation in a community with pre-existing immunity." Journal of Mathematical Analysis and Applications 421.2 (2015): 1651-1672.

📄 Mishra, Bimal Kumar, and Dinesh Kumar Saini. "SEIRS epidemic model with delay for transmission of malicious objects in computer network." Applied Mathematics and Computation 188.2 (2007): 1476-1482.