ANALYSIS OF MALICIOUS CODE DYNAMICS WITH TARGET AND ATTACKER NODES USING MATHEMATICAL MODEL

Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)

ATAL BIHARI VAJPAYEE INDIAN INSTITUTE OF INFORMATION TECHNOLOGY AND MANAGEMENT

20-09-2017

Contents

ABV-IIITM Gwalior

Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)

Introduction

ABV-IIITM Gwalior
Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)

- Malicious code is any code intentionally integrated, converted or cut out from a software system to damage or debase the system's predetermined function, e.g., Virus, Worms, Ransom-Ware.
- Propagation of malicious codes is epidemic in nature.
- To predict the behavior of cyber threats and to make the secure cyber system, it is necessary to study and find out the different types of malicious objects.

Literature Review

Author	**Paper Title**	**Publishing Details**	**Salient Features**
A. K. Misra, M. Verma and A. Sharma	Capturing the interplay between malware and anti-malware in a computer network	Applied Mathematics and Computation 2014	Effect of antivirus over a system [5]

Literature Review

ABV-IIITM Gwalior
Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)

Author	**Paper Title**	**Publishing Details**	**Salient Features**
Bhargava, D.Soni, P.jain, J.Dhar	Dynamics of attack of malicious codes on the targeted network	ICRTIT, IEEE 2016	Malicious code dynamics and effect of firewall[1]
G. P. Sahu,J. Dhar	SEIQHRS epidemic model with media coverage, quarantine and isolation in a community with pre-existing immunity	J. Mathematical Analysis and Applications, Elsevier 2015	An epidemic model SEQIHRS is proposed with quarantine and isolation control strategies [6]

Literature Review

Author	**Paper Title**	**Publishing Details**	**Salient Features**
A. Grey et. al.	A stochastic differential equation SIS epidemic model	SIAM J. Applied Mathematics 2011	Analysis of stochastic SIS model [3]
Kribs-Zaleta and Velasco-Hernandez	A simple vaccination model with multiple endemic states	Mathematical biosciences 2002	Effect of vaccination on basic reproduction number for a large population [4]

Problem Statement and Objective

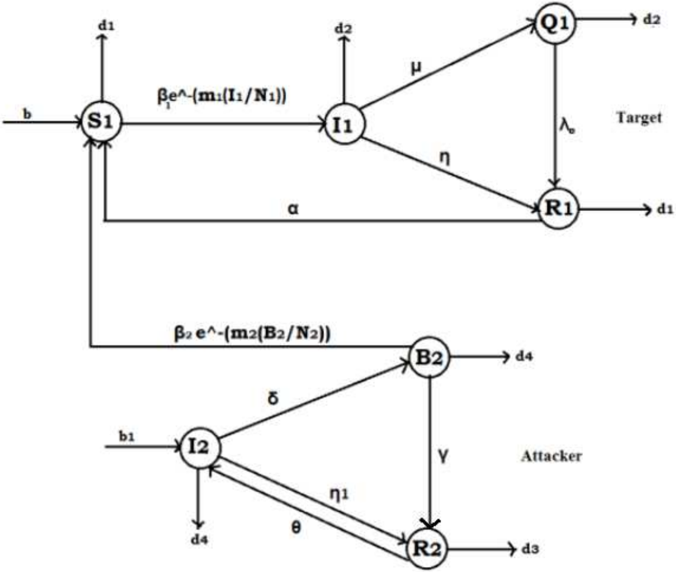
Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)

The objective of this project is to analyze the malicious code dynamics with the target and attacker nodes using a mathematical model.

Schematic Flow of Proposed Compartmental Model

ABV-IIITM Gwalior

Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)



Parameters Descriptions

Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)

Parameters	Description
b, b_1	Recruitment rates of target and attacker classes
d_1 , d_3	Natural death rate of targeted and attacker population node
β_1	Contact rate from susceptible class to infected class
β_2	Contact rate from breaking-out to susceptible class
γ	Rate of recovery of computers with malicious codes in breaking-out state
η, η_1	Rate of recovery of computers with malicious codes in infected state
d_2	Death rate in infected target classes(death due to infection and natural death)
λ_0	Rate of recovery of computers with malicious codes in quarantine state
δ	Rate of change of malicious nodes from infected to breaking-out state
θ	Rate of change of recovered nodes into infected nodes
d_4	Death rate in infected attacker classes(death due to infection and natural death)
α	Rate of change of recovered nodes into susceptible nodes
m_1 , m_2	Infection controlling coefficients
μ	Rate of change of malicious nodes from infected to quarantine state

Table: Description of Parameters

ABV-IIITM Gwalior

Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)

Proposed mathematical model

For targeted nodes:

$$
\begin{aligned}
\frac{d\tilde{S}_1}{d\tilde{t}} &= b - d_1\tilde{S}_1 + \tilde{\alpha}\tilde{R}_1 - \tilde{\beta}_1 e^{-m_1\left(\frac{\tilde{I}_1}{\tilde{N}_1}\right)}\left(\frac{\tilde{I}_1}{\tilde{N}_1}\right)\tilde{S}_1 - \tilde{\beta}_2 e^{-m_2\left(\frac{\tilde{B}_2}{\tilde{N}_2}\right)}\left(\frac{\tilde{B}_2}{\tilde{N}_2}\right)\tilde{S}_1 \\
\frac{d\tilde{I}_1}{d\tilde{t}} &= \tilde{\beta}_1 e^{-m_1\left(\frac{\tilde{I}_1}{\tilde{N}_1}\right)}\left(\frac{\tilde{I}_1}{\tilde{N}_1}\right)\tilde{S}_1 + \tilde{\beta}_2 e^{-m_2\left(\frac{\tilde{B}_2}{\tilde{N}_2}\right)}\left(\frac{\tilde{B}_2}{\tilde{N}_2}\right)\tilde{S}_1 - (\tilde{d}_2 + \tilde{\eta} + \tilde{\mu})\tilde{I}_1 \\
\frac{d\tilde{Q}_1}{d\tilde{t}} &= \tilde{\mu}\tilde{I}_1 - \tilde{d}_2\tilde{Q}_1 - \tilde{\lambda}_0\tilde{Q}_1 \\
\frac{d\tilde{R}_1}{d\tilde{t}} &= \tilde{\lambda}_0\tilde{Q}_1 - \tilde{\alpha}\tilde{R}_1 - d_1\tilde{R}_1 + \tilde{\eta}\tilde{I}_1
\end{aligned}
$$

For attacker nodes:

$$
\begin{aligned}
\frac{d\tilde{I}_2}{d\tilde{t}} &= b_1 - \tilde{d}_4\tilde{I}_2 - \tilde{\delta}\tilde{I}_2 + \tilde{\theta}\tilde{R}_2 - \tilde{\eta}_1\tilde{I}_2 \\
\frac{d\tilde{B}_2}{d\tilde{t}} &= \tilde{\delta}\tilde{I}_2 - \tilde{d}_4\tilde{B}_2 - \tilde{\gamma}\tilde{B}_2 \\
\frac{d\tilde{R}_2}{d\tilde{t}} &= \tilde{\gamma}\tilde{B}_2 - d_3\tilde{R}_2 - \tilde{\theta}\tilde{R}_2 + \tilde{\eta}_1\tilde{I}_2
\end{aligned}
$$

Boundedness of the system

ABV-IIITM Gwalior
Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)

- For targeted population,

$$\Omega_k = \{(\tilde{S}_1, \tilde{I}_1, \tilde{Q}_1, \tilde{R}_1) \in {R_+}^4 : \tilde{S}_1 + \tilde{I}_1 + \tilde{Q}_1 + \tilde{R}_1 \leq b/d\}$$

  And for Attacker population

$$\Omega_{k1} = \{(\tilde{I}_2, \tilde{B}_2, \tilde{R}_2) \in {R_+}^3 : \tilde{I}_2 + \tilde{B}_2 + \tilde{R}_2 \leq b_1/d_1\}$$

- Steady States and their Stability : Two equilibrium states are observed out of which one is malicious-codes free and another is endemic equilibrium states.

Proposed mathematical model(Non- Dimensional)

ABV-IIITM Gwalior
Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)

Due to complicated nature of the equations, the equations are non-dimensionalized for the above system using:

$$S_1 = \frac{\tilde{S}_1}{\tilde{N}_1}, \quad I_1 = \frac{\tilde{I}_1}{\tilde{N}_1}, \quad Q_1 = \frac{\tilde{Q}_1}{\tilde{N}_1} \quad R_1 = \frac{\tilde{R}_1}{\tilde{N}_1},$$

$$I_2 = \frac{\tilde{I}_2}{\tilde{N}_2}, \quad B_2 = \frac{\tilde{B}_2}{\tilde{N}_2}, \quad R_2 = \frac{\tilde{R}_2}{\tilde{N}_2}, \quad t = \tilde{d}_1 \tilde{t},$$

$$N_1 = \frac{\tilde{N}_1}{\tilde{N}_1{}^0}, \quad N_2 = \frac{\tilde{N}_2}{\tilde{N}_2{}^0}, \quad \tilde{N}_1{}^0 = \frac{b}{\tilde{d}_1}, \quad \tilde{N}_2{}^0 = \frac{b_1}{\tilde{d}_3}$$

ABV-IIITM Gwalior
Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)

For targeted nodes:

$$\begin{aligned}\frac{dS_1}{dt} &= \frac{(1-S_1)}{N_1} + \alpha R_1 - \beta_1 e^{-m_1 I_1} I_1 S_1 - \beta_2 e^{-m_2 B_2} B_2 S_1 - S_1 + S_1^2 \\ &+ d_2 I_1 S_1 + d_2 Q_1 S_1 + R_1 S_1\end{aligned}$$

$$\begin{aligned}\frac{dI_1}{dt} &= \beta_1 e^{-m_1 I_1} I_1 S_1 + \beta_2 e^{-m_2 B_2} B_2 S_1 - (d_2 + \eta + \mu) I_1 - \frac{I_1}{N_1} + d_2 I_1^2 \\ &+ I_1 S_1 + d_2 Q_1 I_1 + I_1 R_1\end{aligned}$$

$$\frac{dQ_1}{dt} = \mu I_1 - d_2 Q_1 - \lambda_0 Q_1 - \frac{Q_1}{N_1} + d_2 Q_1^2 + d_2 I_1 Q_1 + Q_1 S_1 + Q_1 R_1$$

$$\frac{dR_1}{dt} = \lambda_0 Q_1 - \alpha R_1 - R_1 + \eta I_1 - \frac{R_1}{N_1} + R_1^2 + d_2 I_1 R_1 + d_2 Q_1 R_1 + R_1 S_1$$

For attacker nodes:

$$\begin{aligned}\frac{dI_2}{dt} &= \frac{(1-I_2)}{N_2} - d_4 I_2 - \delta I_2 + \theta R_2 - \eta_1 I_2 + d_4 I_2^2 + d_4 I_2 B_2 + I_2 R_2 \\ \frac{dB_2}{dt} &= \delta I_2 - d_4 B_2 - \gamma B_2 - \frac{B_2}{N_2} + d_4 B_2^2 + d_4 I_2 B_2 + B_2 R_2 \\ \frac{dR_2}{dt} &= \gamma B_2 - R_2 - \theta R_2 + \eta_1 I_2 - \frac{R_2}{N_2} + R_2^2 + d_4 I_2 R_2 + d_4 B_2 R_2\end{aligned}$$

Basic Reproduction Number

ABV-IIITM Gwalior
Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)

Basic Reproduction Number : It is defined by the expected number of secondary cases produced by a single infection in a completely susceptible population..

Observed basic reproduction number for this model is calculated by using F and V matrices with the infectious nodes (I_1, Q_1, I_2, B_2),

$$\mathcal{F} = \begin{bmatrix} \beta_1 e^{-m_1 I_1} I_1 S_1 - \beta_2 e^{-m_2 B_2} B_2 N_2 S_1 \\ Q_1 S_1 \\ 0 \\ 0 \end{bmatrix}$$

$$\mathcal{V} = \begin{bmatrix} (d_2 + \eta + \mu) I_1 + \frac{I_1}{N_1} - d_2 I_1^2 - I_1 S_1 - d_2 Q_1 I_1 - I_1 R_1 \\ -\mu I_1 + d_2 Q_1 + \lambda_0 Q_1 + \frac{Q_1}{N_1} - d_2 Q_1^2 - d_2 I_1 Q_1 - Q_1 R_1 \\ -\frac{(1-I_2)}{N_2} + d_4 I_2 + \delta I_2 - \theta R_2 + \eta_1 I_2 - d_4 I_2^2 - d_4 I_2 B_2 - I_2 R_2 \\ -\delta I_2 + d_4 B_2 + \gamma B_2 + \frac{B_2}{N_2} - d_4 B_2^2 - d_4 I_2 B_2 - B_2 R_2 \end{bmatrix}$$

Contd..

ABV-IIITM Gwalior
Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)

Now, calculating Jacobian of $\mathcal{F}$ and $\mathcal{V}$ as F and V respectively,
F=

$$\begin{bmatrix} (\beta_1+1)S_1 & 0 & 0 & \beta_2 S_1 \\ 0 & S_1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

V=

$$\begin{bmatrix} (d_2+\eta+\mu+1) & 0 & 0 & 0 \\ -\mu & (d_2+\lambda_0+1) & 0 & 0 \\ 0 & 0 & (1+d_4+\delta+\eta_1) & 0 \\ 0 & 0 & -\delta & (d_4+\gamma+1) \end{bmatrix}$$

Then, the dominant eigenvalue of FV^{-1} is the basic reproduction number R_0.

$$R_0 = max\{\frac{(\beta_1+1)S_1}{(d_2+\mu+\eta+1)}, \frac{S_1}{(d_2+\lambda_0+1)}\}$$

Dynamic Behavior and Results

Malicious-code free equilibrium E_1 is stable if the reproduction number $R_0 < 1$. Endemic equilibrium E_2 is stable if $R_0 > 1$.

Dynamic Behavior and Results

The local stability of malicious codes free and endemic equilibrium is verified by the eigenvalues of the variational matrix. If all the eigenvalues have negative real part, then the equilibrium point is said to be asymptotically stable.

$$J = \begin{bmatrix} -2+2S_1 & a_{12} & d_2 S_1 & \alpha + S_1 & 0 & -\beta_2 S_1 & 0 \\ 0 & a_{22} & 0 & 0 & 0 & \beta_2 S_1 & 0 \\ 0 & \mu & a_{33} & 0 & 0 & 0 & 0 \\ 0 & \eta & \lambda_0 & a_{44} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a_{55} & 0 & \theta \\ 0 & 0 & 0 & 0 & \delta & -1-d_4-\gamma & 0 \\ 0 & 0 & 0 & 0 & \eta_1 & \gamma & -2-\theta \end{bmatrix}$$

Where,

$$\begin{aligned} a_{12} &= d_2 S_1 - \beta_1 S_1 \\ a_{22} &= -1 - d_2 - \eta - \mu + \beta_1 S_1 + S_1 \\ a_{33} &= -1 - d_2 - \lambda_0 + S_1 \\ a_{44} &= -2 + \alpha + S_1 \\ a_{55} &= -1 - d_4 - \eta_1 - \delta \end{aligned}$$

Numerical Experimentation (Feasible States)

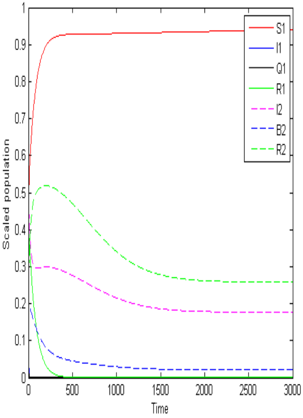
ABV-IIITM Gwalior

Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)

Possible steady states with respect to the reproduction number for different parameter set(Dimensional and non-dimensional) in the model.

Parameters (Non-Dimensional)	Set A	Set B	Parameters (With Dimensions)	Set C	Set D
b	7.5	7.5	b	1	75
d_1	0.003	0.003	d_1	0.3	0.3
β_1	0.001	0.01	$\tilde{\beta}_1$	0.5	2.5
β_2	0.006	0.30	$\tilde{\beta}_2$	0.6	0.6
μ	0.003	0.003	$\tilde{\mu}$	0.3	0.3
λ_0	0.008	0.0008	$\tilde{\lambda}_0$	0.8	0.8
d_4	0.075	0.0075	$\tilde{d}_4$	10	2.5
b_1	7.5	7.5	$\tilde{b}_1$	75	75
d_3	0.02	0.02	$\tilde{d}_3$	2.0	2.0
η	0.004	0.0004	$\tilde{\eta}$	0.4	0.4
η_1	0.175	0.0175	$\tilde{\eta}_1$	17.5	7.5
α	0.010	0.0005	$\tilde{\alpha}$	1.0	1.0
d_2	0.4	0.004	$\tilde{d}_2$	0.4	0.4
γ	0.0005	0.01	$\tilde{\gamma}$	0.75	0.75
δ	0.009	0.027	$\tilde{\delta}$	1.9	0.9
θ	0.10	0.20	$\tilde{\theta}$	10	10
m_1	2	2	m_1	6	2
m_2	3	2	m_2	6	2
Feasible SS	E_1	E_2	Feasible SS	E_1	E_2
R_{01}	0.0098	1.2500			
R_{02}	0.0073	0.3846	$\tilde{R}_0$	0.4545	2.2727

Simulation



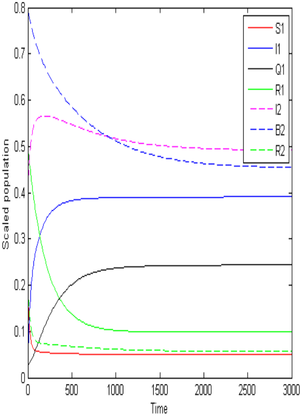


Figure: Node density vs Time for set A (left) and set B (right)

Numerical Experimentation(No Security)

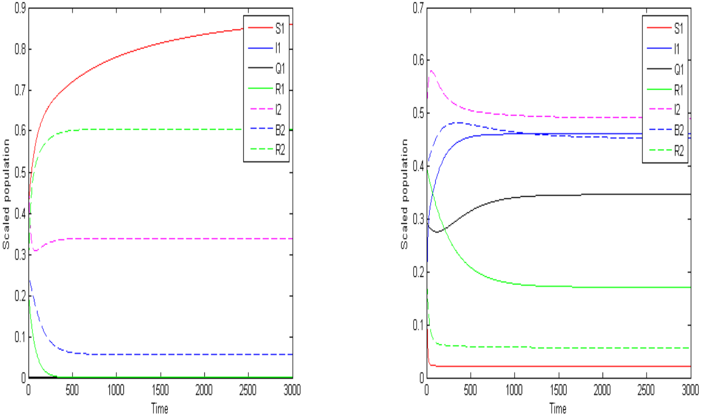
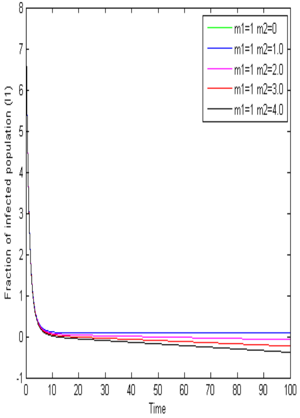


Figure: Node density vs Time for set A (left) and set B(right)

Analysis of firewall coverage



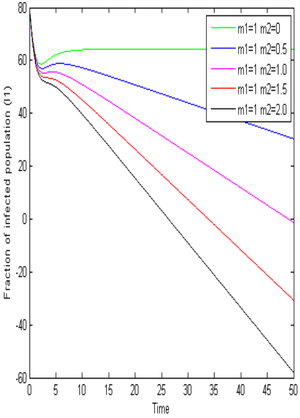


Figure: Effect of m_2 (firewall coefficient) on $\tilde{I}_1$ when $\tilde{R}_0 < 1$ (left) and $\tilde{R}_0 > 1$(right)

Sensitivity analysis of the system parameters

- Sensitivity indices enables us to measure the relative change in a state variable with respect to a small change in the system parameter [2].
- 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 the most significant reproduction number R_{01}. We observed most sensitive parameters for Basic Reproduction Numbers which are shown in the table.

Sensitivity Analysis

ABV-IIITM Gwalior

Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)

Parameters (y_j)	Sensitivity $\Upsilon_{y_j}^{R_{01}}$	$\Upsilon_{y_j}^{R_{01}}$ Set 1	$\Upsilon_{y_j}^{R_{01}}$ Set 2
b	0	0	0
d_1	0	0	0
β_1	$\frac{\beta_1}{\beta_1+1}$	0.000999	0.0099
β_2	0	0	0
μ	$-\frac{\mu}{d_2+\mu+\eta+1}$	-0.002	-0.00298
λ_0	0	0	0
d_4	0	0	0
b_1	0	0	0
d_3	0	0	0
η	$-\frac{\eta}{d_2+\mu+\eta+1}$	-0.0028	-0.000397
η_1	0	0	0
α	0	0	0
d_2	$-\frac{d_2}{d_2+\mu+\eta+1}$	-0.28	-0.00397
γ	0	0	0
δ	0	0	0
θ	0	0	0

Table: Distributed sensitivity indices concerning R_{01}

d_2, β_1, μ and η are moderately sensitive and rest are independent of R_{01}.

Conclusion

ABV-IIITM Gwalior
Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)

- β_1 was found as decisive parameter for the reproduction number.
- Malicious code free equilibrium is stable, when $R_0 < 1$ and, the endemic equilibrium achieved stability when $R_0 > 1$.
- The coefficient of firewall security m can be defined as

$$m = -log_2(a + b - ab).$$

- The basic reproduction number R_0 is not affected by the coefficient of firewall security and hence the features related to quality of the model don't change.

Conclusion

ABV-IIITM Gwalior

Alok Singh (2014IPG-009)
Neha Singh (2014IPG-059)
Saurabh Sharma (2014IPG-078)

Type of Analysis	**Bhargava, Palash, Soni, Dhar**	**Proposed Model**
Total equilibrium states	16	2
Malicious code free equilibrium	4	1
Endemic equilibrium	12	1
Highly sensitive parameters	2 to 4	0
Moderately sensitive parameters	3 to 5	2 to 4

Table: Comparison Table

Future Scope

- The analysis can be extended by considering time variant recruitment rate.
- Using some antidotal nodes.
- The idea of quarantined nodes can also help an individual of an organization to get rid of some new computer network attacks like Ransom-ware etc.
- The idea of kill signals can be implemented.

References I

[1] Bhargava, A., Soni, D. K., Jain, P. and Dhar, J.: 2016, Dynamics of attack of malicious codes on the targeted network: Effect of firewall, *International Conference on Recent Trends in Information Technology (ICRTIT), 2016*, IEEE, pp. 1–6.

[2] Chitnis, N., Hyman, J. M. and Cushing, J. M.: 2008, Determining important parameters in the spread of malaria through the sensitivity analysis of a mathematical model, *Bulletin of Mathematical Biology* **70**(5), 1272–1296.

[3] Gray, A., Greenhalgh, D., Hu, L., Mao, X. and Pan, J.: 2011, A stochastic differential equation sis epidemic model, *SIAM Journal on Applied Mathematics* **71**(3), 876–902.

References II

[4] Kribs-Zaleta, C. M. and Velasco-Hernandez, J. X.: 2000, A simple vaccination model with multiple endemic states, *Mathematical Biosciences* **164**(2), 183–201.

[5] Misra, A. K., Verma, M. and Sharma, A.: 2014, Capturing the interplay between malware and anti-malware in a computer network., *Applied Mathematics and Computation* **229**, 340–349.

[6] Sahu, G. P. and Dhar, J.: 2015, 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), 1651–1672.

Thank You