Open Access Library Journal
2023, Volume 10, e10174
ISSN Online: 2333-9721
ISSN Print: 2333-9705

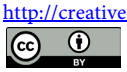
An Analytical Model Modifications and Adaptations for Malware Spread and Containment in Communication Networks

Moses Okechukwu Onyesolu[1], Charles Okechukwu Ugwunna[2]

[1]Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria
[2]Department of Computer Science, Federal University of Agriculture, Abeokuta, Nigeria
Email: mo.onyesolu@unizik.edu.ng

How to cite this paper: Onyesolu, M.O. and Ugwunna, C.O. (2023) An Analytical Model Modifications and Adaptations for Malware Spread and Containment in Communication Networks. *Open Access Library Journal*, **10**: e10174.
https://doi.org/10.4236/oalib.1110174

Received: April 21, 2023
Accepted: July 28, 2023
Published: July 31, 2023



Abstract

Due to the escalating wave of malware in communication networks, continuous/discrete differential equations have been used in traditional analytical models to better understand the patterns of malware spread. Networks for local area networks, networks for metropolitan areas, and broad area networks were all utilized in this study. In particular, we developed the vulnerable-latent-contagious-recovery-inoculation (VLCR-I) model as well as built its computational equivalents in MathLab simulator. From the mathematical results, the VLCR-I model predicted increases in the latent (L), contagious (C), and inoculated (I) compartments and a decrease in the vulnerable (V) compartment. With the initial set of data, where V nodes are 100 and L is 2, this is accurate. A decrease in the aforementioned compartments was observed when the V and L nodes were increased to 1050 and 2500, respectively. At V = 100 and L = 2, there were increases in the L, C, I, and R compartments for the second set of data. There was a decrease in these nodes due to the addition of 1050 V, 2500 L, and 25 L nodes.

Subject Areas

Computer and Network Security

Keywords

Epidemic, Containment, Malware, Production Number, and Analytic

1. Introduction

The repercussions of malware proliferation, have been disastrous to organiza-

tions and enterprises, with even more lethal evidence being revealed as a result; cybercrime's sinister shift toward preying on schools, municipal agencies, and other persistently underfunded and overcrowded public organizations [1]. Unknown virus detection has become a new difficulty [2]. In addition to anti-malware software, epidemic models have been employed to examine the methods by which malware spreads and to lessen ongoing cyberattacks on ICT infrastructure [3]. Epidemic techniques have their roots in public health and epidemiology, where infectious outcomes of populations are analyzed to better understand transmission patterns. Researchers in cyber security have discovered significant parallels between disease-causing pathogens in biological networks and malware in communication networks.

Classical analytical models in the form of continuous/discrete differential equations have been utilized in recent times to define malicious code propagation in networks [4] [5]. The analytical models are developed to represent compartments (or groups) such as S, E, I, R, and V stand for susceptible, exposed, infectious, recovered, and immunized (V). Examples of these models include SEIR, SEI, SEIR-V, and others. Of course, these analytical models originated from the SIR epidemic model of [6]. Both infectious disease epidemics and malware epidemics can be predicted using spatial and temporal factors, and this field of study has remained active in recent years. Forecasting approaches applying these models are dubbed causal methods (or mechanistic methods) since they are based on the causation mechanisms of infectious illnesses [7]. The underlying epidemiological models are analytical compartmental models (CM) or agent-based models (ABM). Here, compartmentalization allows the population to be divided into a number of classifications, primarily Susceptible (S), Exposed (E), Infectious (I) and Recovered (R). Additionally, a system of differential equations represents the changes/dynamics of each class as a result of disease spread and progression mathematical modeling of epidemic spread since the Bernolli era has experienced evolvements that transverse beyond diverse spheres of mathematical biology and other disciplines such as Applied Mathematics, Non-linear Sciences, Statistical Physics, Computer Science and Network Security. From literature, it appears that classical models (the basic SIR compartments) are referred to as models that are treated by the acclaimed work of [8]. Mishra and Singh [9] were of the opinion that the proliferation of harmful agents is similar to the propagation of epidemics in the microbial system. This discovery led to the development of computer simulations for worm/virus spread utilizing epidemiological modeling, which compartmentalizes diseases according to their severity. Relating the epidemic triad concept to cyberspace, nodes/computer terminals; worms/virus/trojan horse and networked environment (computer network, wireless sensor networks, etc.) can be likened to the host, agent, and environment respectively.

The results of modeling mathematical models may be perceptive and clear. For network managers in real organizations with security issues that must be

fixed to guarantee a malware-free online environment, there are significant benefits. However, the mathematical models examined in this paper did not take into account how to slow down the rate of infection propagation from latent nodes or the infectivity contact rate. This is crucial because worm attacks can infect any machine and lead to nodes becoming established in the infectious compartment. These issues are properly addressed with the VLCRI method.

2. Review of Related Literature

For the vertical transmission of worms through communications systems, Mishra and Pandey [10] developed the e-epidemic SEIRS model. The stability of the result was characterized by the altered reproduction number. They showed that for the asymptotical stabilization of the worm-free condition, Rv must be both smaller than and bigger than one., whose component of infective is zero, and they also created an analytical expression for the altered regenerative number Rv. Figure 1 displays the schematic diagram of how they constructed their model.

There are four subclasses of the population size $N(t)$, which reflects the total number of nodes in the computer network: susceptible, exposed (contaminated but not yet contagious), infectious, and recovered. These subclasses are identified by the sizes $S(t)$, $E(t)$, $I(t)$, and $R(t)$, respectively. Those differential equations that follow are shown in Equation (2.1);

$$\left.\begin{aligned} \dot{S} &= b - \lambda IS - \rho bE - qbI - dS + \zeta R \\ \dot{E} &= \lambda IS - \rho bE - qbl - \varepsilon E - dE \\ \dot{I} &= \varepsilon E - \gamma I - dI - \eta I \\ \dot{R} &= \gamma I - \zeta R - dR \end{aligned}\right\} \tag{2.1}$$

where, b, d, λ are positive constants and ε, η, γ, ζ are non-negative constants. The constants b represents the rate at which vulnerable nodes are added to the computer network, d represents the rate at which nodes crash for reasons other than worm attacks, and is the rate Consistent for nodes leaving exposed nodes. In class I, class E is the disease-related mortality rate (i.e., the rate constant for nodes collapsing owing to worm attack), and class R is the rate constant for nodes becoming susceptible again after recovering. The proportionality constant

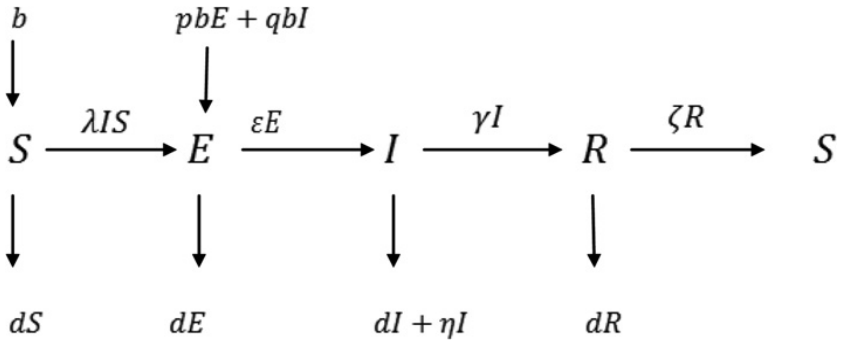


Figure 1. Diagram of a computer network worm [10].

for nodes leaving the contagious class I for the recovered class R equals class E for the infectious class I.

Mishra and Keshri [11] considered an SEIQRS model for the dissemination of harmful objects in a network. With regard to cyber mass action incidence, thresholds, equilibria, and their stability are also discovered. A viable zone is an asymptotic stability region for the endemic equilibrium state if Rcq > 1 and the infected fraction remains. If Rcq < 1, the infected fraction of the nodes disappears and the disease dies out. Analysis was also done on the impact of quarantine on recovered nodes. Figure 2 shows the schematic diagram of their model formulation.

In this model a given population of size $N(t)$ is separated into subcategories of nodes that are susceptible, exposed (infected but not yet infectious), infectious, quarantined, and recovered using the sizes $S(t)$, $E(t)$, $I(t)$, $Q(t)$, and $R(t)$, respectively. A cyber mass action occurrence, as defined by the SEIQRS model is presented in Equation (2.2):

$$\left.\begin{aligned} \dot{S} &= A - \beta SI - dS + \eta R \\ \dot{E} &= \beta SI - (\delta + \mu) E \\ \dot{I} &= \mu E - (d + \alpha + \gamma + \delta) I \\ \dot{Q} &= \delta I - (d + \alpha + \varepsilon) Q \end{aligned}\right\} \tag{2.2}$$

where A, d, β are positive constants, and μ, γ, δ, ε, η, α, are nonnegative constants, respectively. According to the parameters A and d, nodes leave the exposed class E for contaminated compartment, crash for reasons other than being attacked by malicious objects, and join the computer network at various rates. Are indeed the disease-related mortality rates (crashing of nodes due to the attack of malicious objects) constant in the compartments I and Q; are the disease-related recovery rates (temporary recovery after using anti-malware software and return to recovered class R from compartments I and Q, respectively); and are the immunity loss rate constants g [9].

To safeguard the Internet from many types of dangerous goods, the SIjRS Multi-Group Model, also known as the SI1I2I3RS (Susceptible, Infectious Due to Worm, Infectious Due to Virus, Infectious Due to Trojan Horse, Recovered and

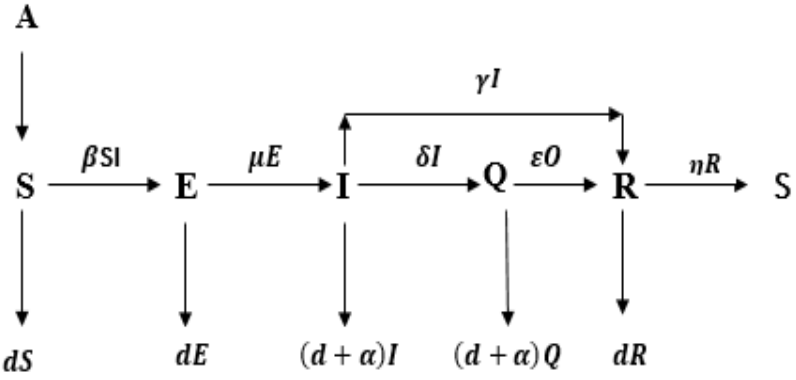


Figure 2. Schematic diagram for the flow of malicious objects in SEIQRS model [11].

Susceptible) model, was created. Simple mass action incidence's threshold, equilibrium, and stability are all explained. Numerical approaches have been used to solve and simulate the differential equation system, which has improved our understanding of the behavior of malicious entities that invade computer networks as well as the efficiency of antivirus software. Figure 3 illustrates schematically how they built their model.

Let $S(t)$ become the quantity of vulnerable nodes, $I(t)$, $I(t)$, and $I(t)$ be the numbers of nodes infected by worm, virus, and trojan horse, accordingly, $R(t)$ be the recover nodes after the run of anti-malicious software, and $N(t)$ be the size of the general population, according to the SI1I2I3RS. The differential equations for the model are shown Equation (2.3):

$$\left.\begin{aligned} \frac{\mathrm{d}s}{\mathrm{d}t} &= \mu\left(A-S\right)-a_j\sum_{j=1}^{3}\beta_j I_j S+\delta R \\ \frac{\mathrm{d}I}{\mathrm{d}t} &= a_j\sum_{j=1}^{3}\beta_j I_j S-\left(\mu+\alpha_j+\gamma_j\right)I_j \quad j=1,2,3 \\ \frac{\mathrm{d}R}{\mathrm{d}t} &= \sum_{j=1}^{3}\gamma_j I_j-\left(\mu+\delta\right)R \end{aligned}\right\} \tag{2.3}$$

where q_j is the likelihood that an infected node will join group I_j from the susceptible class. A represents the recruitment of susceptible nodes into the computer network, while B and C represent the rates at which nodes leave the infectious classes I_1, I_2, and I_3 and enter the recover class, respectively.

This study developed the Vulnerable-Latent-Contagious-Recovery-Inoculation (VLCR-I) for computer networks, which is analogous to the model proposed by [11] with the quarantine compartment removed and the vaccination compartment added. To put it another way, it is the model's addition of the immunization compartment [10]. The presumptions include adding new nodes to the network and removing (or killing) nodes due to worm attacks or hardware or

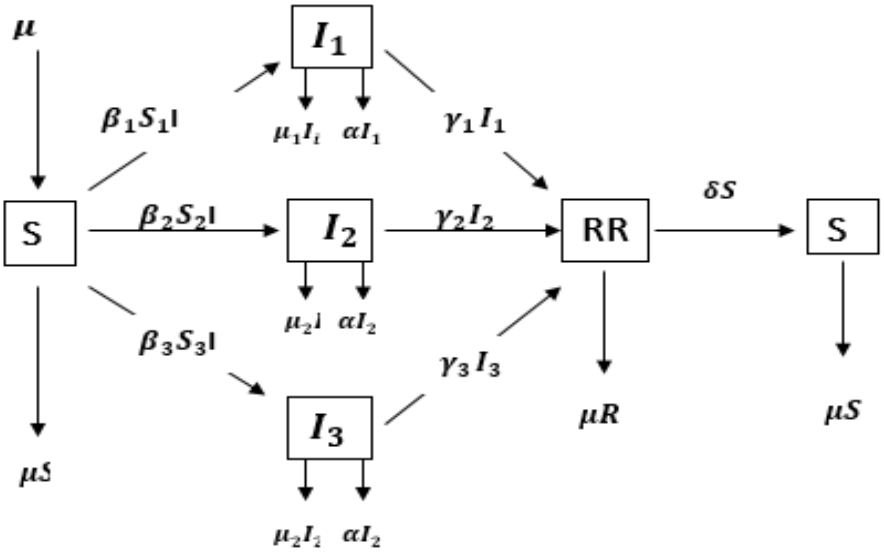


Figure 3. Schematic diagram for the flow of malicious objects in computer network [9].

software malfunctions. All computers are susceptible to worm attacks and eventually become infected. Some computers are in the Exposed (latent) phase before they transmit the infection; during this time, the worm is inactive and the nodes are unable to do so. Yet, because there are several worm varieties in cyberspace, computers never develop a permanent immunity against worm infection and instead become more vulnerable over time. Additional factors include the percentage of computers included in the population of computer networks, is the speed at which infected nodes spread from exposed nodes to recovered nodes, the speed at which infected nodes immunize susceptible computers, and the speed at which infection travels from the immunization compartment to the susceptible computer. The rate of contact for infectiousness, the mortality rate (or fatality rate) of nodes due to software or hardware malfunctions, the speed of crashing as a result of an attack by malicious objects (in this example, worms), and the rate at which exposed nodes become infectious are some of these variables.

3. Methodology

The modeling and assessment of dynamical systems is a technique that will be used to accomplish the objectives of this study. Networks are seen as dynamical systems in the modeling and analysis of cyber defense systems, which paves the way for the creation of standard analytical (equation-based) models [12]. By dynamic systems we mean systems that are not homogeneous and whose state changes over time as a result of input signals or external disturbances (sensitivity analysis). This methodology aids in analyzing and projecting how models will behave if particular model parameters are altered. The models created using this methodology take the forms of block diagrams, transfer functions, input-output differential equations, and state-variable equations. When using this methodology, it is possible to use the Laplace transform, Jacobian matrix method, Lyapunov's theorem, Kutta-Fehlberg orders 4 and 5, among other tools, to achieve various analytical goals and solutions. On MATLAB, computer solutions are built. The networked system is represented as a distributed system with exact solution by analysts using this approach. More research is done on the endurance of the exact solution [5]. This section presents decisions that will affect the suggested model considerations and the desired results. It should be noted that to show how quickly computer network parameters fluctuate over a period of time, mathematical expressions were used. **Figure 4** shows the architecture of the VLCR-I model, which illustrates the strategy for attaining the main objective of the study. This technique begins with the specification of model parameters/the formation of a set of differential equations. The Basic Replication Number and the solution is obtained will be found by using Mathematica to solve the differential equations. This is followed by sensitivity analysis in MathLab, which is done by altering some of the model parameters. Following that, the created result will be verified and validated. **Figure 5** depicts the process flow for the VLCR-I model. The detailed steps/stages of this methodology are discussed.

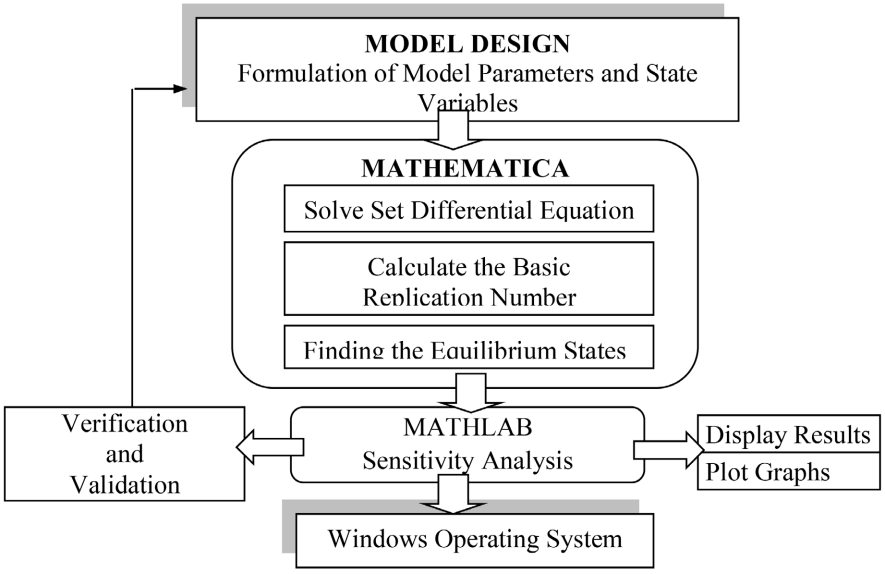


Figure 4. Architecture of the VLCR-I model.

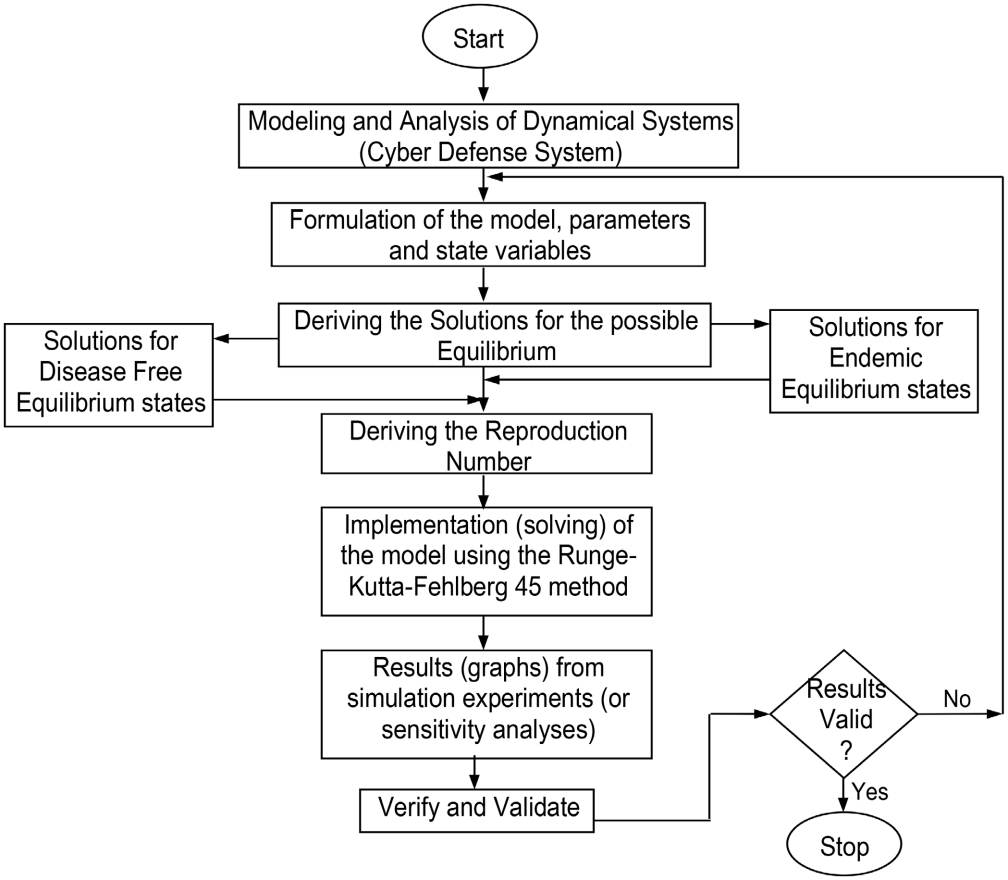


Figure 5. Flowchart for the analytical model modifications and adaptations.

1) Model Formulation

The first step in developing mathematical (deterministic) or simulation (stochastic) models, according to [13], is to thoroughly research and get to know the

operational reality of the system to be represented, if one is available, or the system whose behavior is most similar to it, if not. We looked at relevant data on threats (worms, viruses, and trojans), in addition to the body of literature on the transmission of threats and infections in networks, in light of this assertion. With the relevant information, using the VLCR-I input parameters specification as shown in Table 1, the system would then be simplified to a system of differential equations, first as a graphical representation (continuing equation). The system of differential equations would indeed be resolved using the Runge-Kutta-Fehlberg order 4 and 5 techniques, an effective numerical technique for dealing with initial value (IVP) problems.

In fact, the Runge-Kutta-Fehlberg order 4 and 5 approach is an efficient numerical method for solving initial value (IVP) problems. As stated earlier, this method is used in this study to solve the system of differential equations. The only way to ensure correctness in an I.V.P. solution using this approach is to solve the issue twice using different step sizes and then comparing the results at the grid positions correlating to the higher step size. The lower step size, however, necessitates a large amount of calculation, and this process must be redone if the agreement is found to be insufficient. The step size is increased if the solutions agree to more significant digits than necessary. For the model formulation, the overall population is indicated by the letters $V(t)$, $L(t)$, $C(t)$, $R(t)$, and I, is made up of all the nodes in the computer system. Vulnerable, Latent, Contagious, Recovered, and Inoculated nodes make up the remainder of the population (t). This suggests that

$$V(t), L(t), C(t), R(t), I(t), = N.(t). \tag{2.4}$$

The VLCR-I Model for the Propagation of Worms in Computer Networks is schematically depicted in Figure 6.

Table 1. VLCR-I input parameters specification.

Specification	Name	Explanation
λ	Lambda	Node inclusion rate in the population of the computer network
β	Beta	Contact rate for infection
τ	Tau	number of nodes that have died due to hardware or software failures
ω	Omega	Speed decline brought by malicious object attacks (in this case worm)
θ	Theta	How quickly infected nodes exposed to infection spread
ν	Nu	Recovery rate
φ	Phi	Rate of infection susceptibility of recovered nodes
ρ	Rho	Vaccination rate for vulnerable computer networks
ξ	Xi	Transmission speed between the vaccinated and susceptible compartments

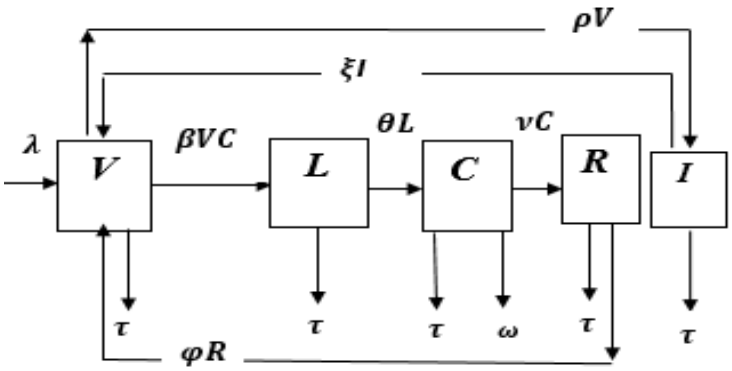


Figure 6. Schematic diagram of the VLCR-I model for the flow of worms in computer networks.

Furthermore, VLCR-I model is represented thus, Equation (2.5):

$$\left.\begin{aligned}
\dot{V} &= \lambda - \beta VC - \tau L - \rho V + \varphi R + \xi I \\
\dot{L} &= \beta VC - \tau L - \theta L \\
\dot{C} &= \theta L - \tau C - \omega C - \upsilon C \\
\dot{R} &= \upsilon C - \tau R - \varphi R \\
\dot{I} &= \rho V - \tau I - \xi I
\end{aligned}\right\} \tag{2.5}$$

where $\dot{V} = \mathrm{d}V/\mathrm{d}t$, $\dot{L} = \mathrm{d}L/\mathrm{d}t$, $\dot{C} = \mathrm{d}C/\mathrm{d}t$, $\dot{R} = \mathrm{d}R/\mathrm{d}t$ and $\dot{I} = \mathrm{d}I/\mathrm{d}t$. Using this analytical model, a corresponding agent model can also be developed.

2) Identification of the Equilibrium States

It has long been standard practice to demonstrate the existence of two steady state, namely Disease Free Equilibrium and Endemic Stability, while examining the spread of illness [14] [15]. Disease Free stability, also known as infection-free equilibrium, uses the same formulated mathematical model to explain the exclusion of infection, disease, or threat in the network, whereas endemic stabilization uses the same mathematical model to explain the existence of infection, disease, or threat in the network. Remember that only susceptible individuals/nodes will make up the whole population in the disease-free equilibrium, with all infected classes being zero.

3) Deriving the Basic Reproduction Number

The next step following model formulation is to determine the fundamental replication number. This phase is essential because the basic replication number, which is unquestionably "the most significant greatest and most important insights that mathematical thought has brought to epidemiological theory [16], is a measurement of the propensity for diseases transmitted in a population. It reflects the typical amount of additional cases that an infected person would cause if they were transferred to a susceptible community lacking disease resistance and there were no treatments to manage the illness. If Ro < 1, an infected person often infects fewer beyond one new person during the length of his infection period. In this situation, the infection can eventually go. On the other side, if Ro > 1, the virus can spread throughout a community since each sick individual often

causes more than one new infection.

4) Sensitivity Analysis and Numerical Results/Responses

This requires gradually altering the model parameters and assessing how it affects the simulation result. It is impossible to overstate the value of sensitivity analysis in terms of models. The sensitivity analysis of a model can be used to assess the comparative impact of model parameters on model conclusions. In other words, the goal of sensitivity testing is to determine whether a little change in the parameter values will have a large impact on the model's output or internal dynamics. Consequently, it would be necessary to change a few parameters one at a time during the model's sensitivity analysis to examine the outcomes. In this case, perturbations (simulation experiments) on the proposed model using various values for the various rates will produce responses that are understood. Table 2 shows initial values of the compartments while Table 3 and Table 4 show first and second set of data for sensitivity analysis In this case, perturbations (simulation experiments) on the conceptual scheme using various values for the various rates will produce results that are understood.

Table 2. Initial values of the compartments.

Compartments	Initial Values	Initial Values	Initial Values
Vulnerable	100	1050	2500
Exposed	2	25	25
Infectious	0	0	0
Recovered	0	0	0
Vaccinated	0	0	0

Table 3. First set of data for testing the model.

Notations	Name	Values	Indicating
σ	sigma	0.3	Availability density
r_0^2	r	1	range of transmission
λ	lambda	0.33	Nodes' rate of incorporation into the population of the network
β	beta	0.1	Contact rate for infection
τ	tau	0.003	Number of nodes dying due to hardware or software issues
ω	omega	0.07	Rate decline brought on by malware attack
θ	theta	0.25	Rate of transmission of latent nodes
ν	nu	0.4	Recovery speed
φ	phi	0.3	How quickly healed nodes are exposed to infection
ρ	rho	0.3	Vaccination frequency for sensitive sensor nodes
ξ	zeta	0.06	Transmission speed from the immune segment to the vulnerable segment

4. Test Data and Actual Experiments

During the experiment the values of the V (Vulnerable) nodes and that of the L (Latent) nodes were perturbed, while the actual values for testing the experiment (analytic model) in this study were culled from [17] [10] and [5] as can be seen in Table 2 and Table 3.

5. Simulation Experiments for the VLCRI Model

Simulation experiments were carried out utilizing the time history of [5] and the initial values of Table 2 and Table 3 as follows. Figures 7-12 display the chronology of the analysis-related compartments over time. In order to solve the initial value problems IVP, the Runge-Kutta-Fehlberg order 4 and 5 approach would be utilized with a set of differential equations for the simulation trials. The system of differential equations is solved using an integrated function of MatLab called ode45. The following section has the pseudocode for utilizing this integrated function for simulation purposes.

Pseudocode for the Analytic Model VLCR-1 (Adapted from [12])

1) Open Mfile and give it the name VLCRL 1.

2) The entry point is dy = VLCRI 1(t,y).

3) Set the Column Vector.

4) State the data values for the VLCR-I input parameters as follows: Lambda = 0.33, Beta = 0.1, Tau = 0.03, Omega = 0.07, Theta = 0.25, Nu = 0.4, Phi = 0.3, Rho = 0.3, and Xi = 0.06.

5) The vulnerable input differential equation (dy(1))

6) Latent Node Input Differential Equation (dy(2))

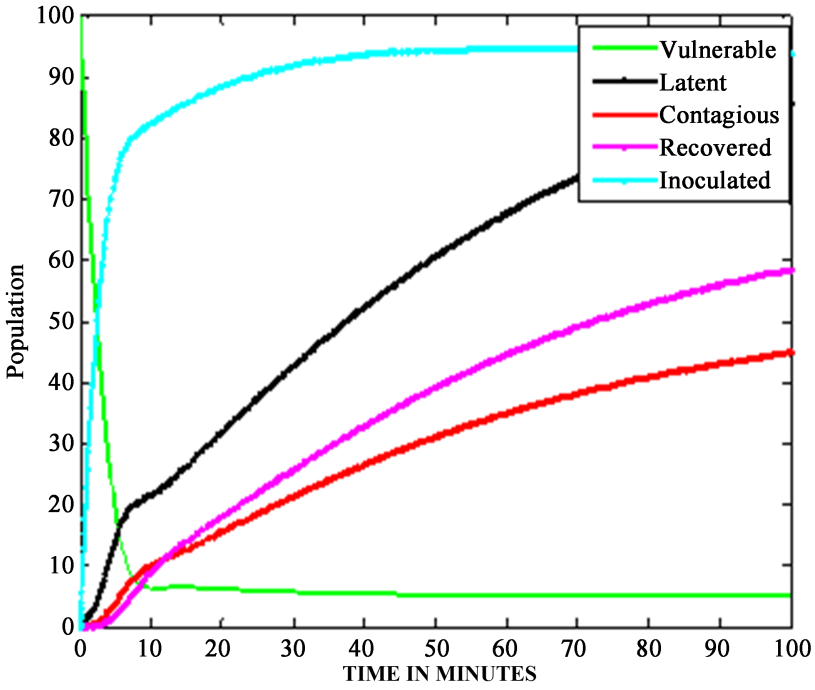


Figure 7. Time history at V = 100 and L = 2 with first set of data.

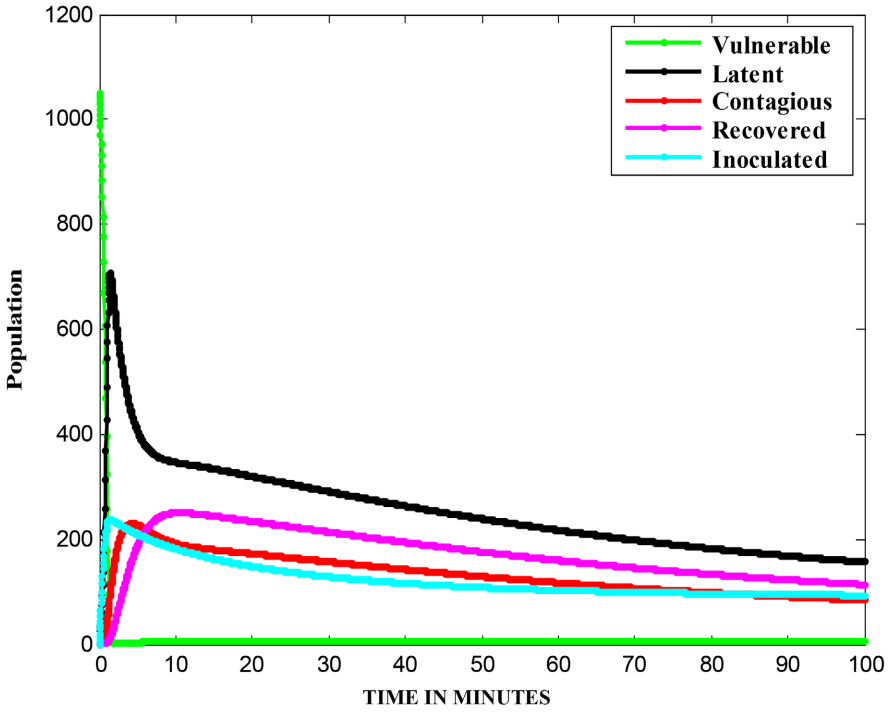


Figure 8. Time history at V = 1050 and L = 25 with first set of data.

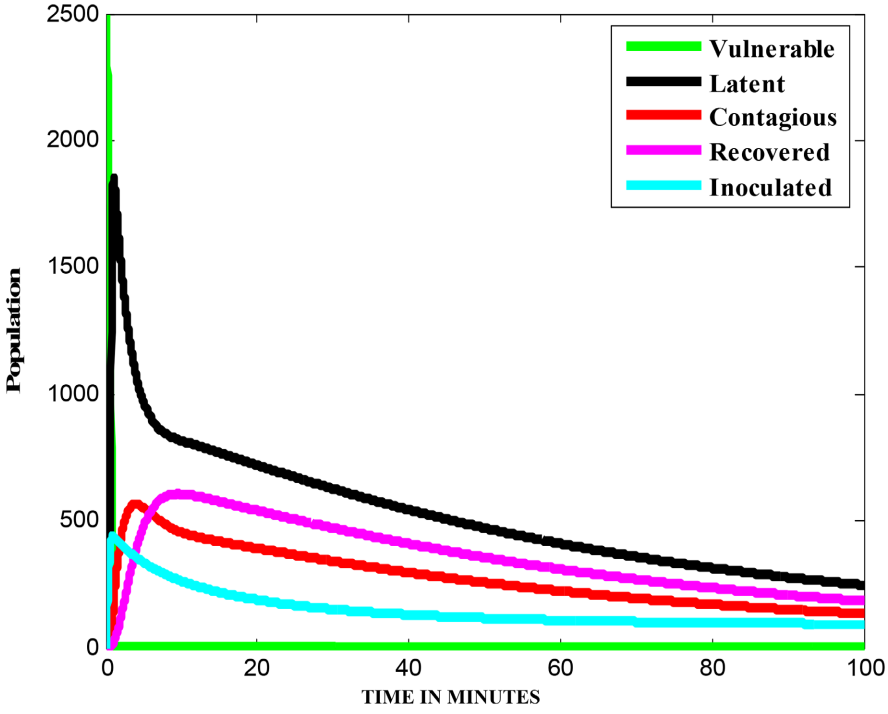


Figure 9.Time history at V = 2500 and L = 25 with first set of data.

7) Contagious nodes input differential equation (dy(3))
8) The Recovered Nodes' Input Differential Equation (dy(4))
9) Input differential equation for vaccinated nodes (dy(5))
10) Launch a command prompt

11) Enter the solution syntax for the equation [x,] = (@VLCR-I, tspan, yo)

12) Display the outcome in the form of graphs

Please take note of the dynamic response of the simulations' figures with different propagation and distribution densities from [5's time history] values. It is clear from the simulation that the latent, infectious, and immunized compartments

Table 4. Second set of data for testing the model.

Notations	Name	Values	Indicating
σ	sigma	0.3	Availability density
r_0^2	r	1	range of transmission
λ	lambda	0.33	Nodes' rate of incorporation into the population of the network
β	beta	0.48	Contact rate for infection
τ	tau	0.003	Number of nodes dying as a result of hardware or software issues
ω	omega	0.07	Rate decline brought on by malware attack
θ	theta	0.57	Rate of transmission of latent nodes
ν	nu	0.50	Recovery speed
φ	phi	0.3	How quickly healed nodes are exposed to infection
ρ	rho	0.49	Vaccination frequency for sensitive sensor nodes
ξ	zeta	0.06	Transmission speed from the immune segment to the vulnerable segment

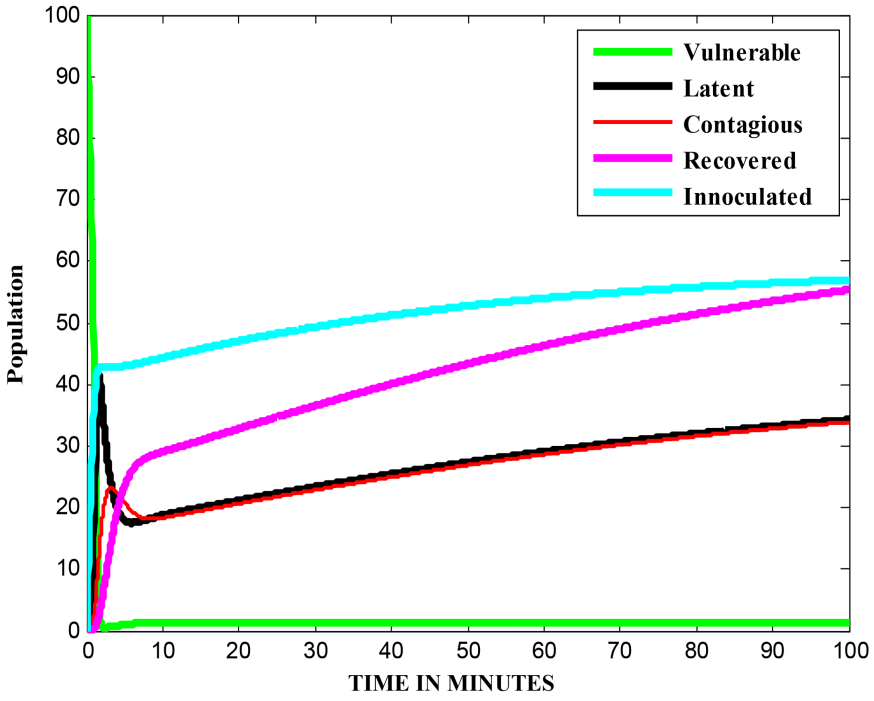


Figure 10. Time history at V = 100 and L = 2 with second set of data.

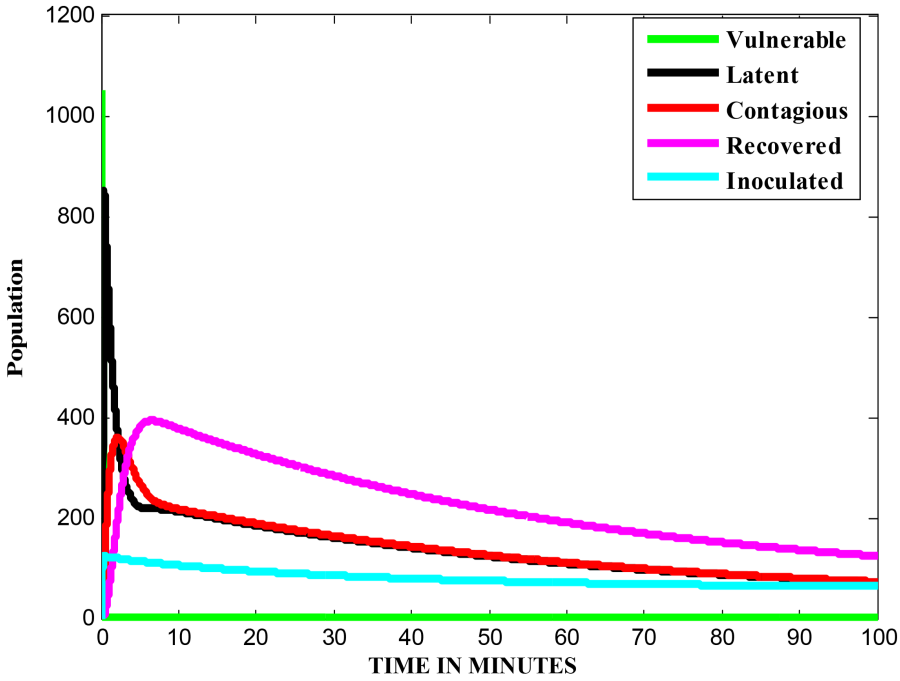


Figure 11. Time history at V = 1050 and L = 25 with second set of data.

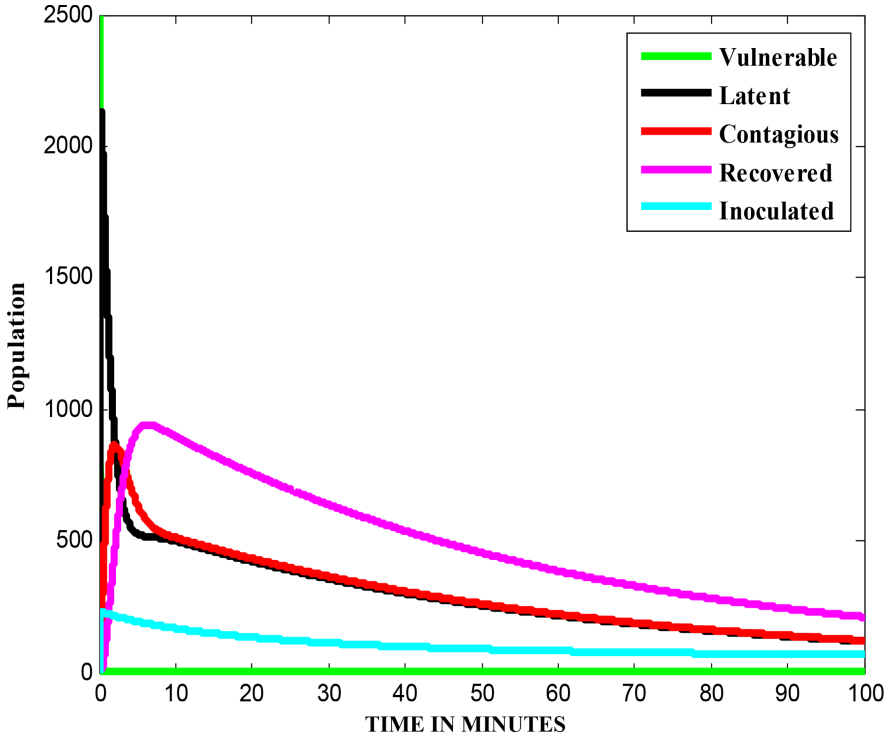


Figure 12. Time history at V = 2500 and L = 25 with first set of data.

all increased, while the vulnerable compartment decreased.

6. Research Findings and Implications

The VLCRI model depicted increases for latent (L), contagious (C) and inocu-

lated (I) compartments and a reduction in the vulnerable (V) compartment (Figure 7). This is true for the first set of data, where V nodes is 100 and L is 2. Increasing the V nodes to 1050 and 2500; and L nodes to 25 showed a reduction in the aforementioned compartments (Figure 8 and Figure 9). These results were generated using Table 3.

Using Table 4, which contains the second set of data, there was increases in the L, C, I, R compartments at V = 1 = 00 and L = 2, depicted in Figure 10. By increasing the number of V nodes to 1050 and 2500 and L to 25, there was a reduction in these nodes. The results of the simulation show the impact of the V and L nodes are shown in Figures 7-9. It is clear that from Figures 9-12, the model demonstrated an increase in the latent, contagious, and immunized compartments as well as a decrease in the vulnerable compartment

Table 3 and Table 4 infectivity contact rate, latent node contagiousness rate, recovery rate, and rate of inoculation for V sensor nodes are examples of tables where the model parameters may vary. The consequences of the model parameter changes were shown by the accompanying simulations.

7. Conclusion

The study was able to demonstrate the development of an analytical model for malware spread/containment in communication networks, which was one of its key goals. Deriving the Basic Reproduction Number Sensitivity Analysis and Numerical Results/Responses Producing exact reproduction ratios, as well as implementing simulation tests utilizing the VLCRI model (in MatLab) were all completed for specific goals. It is important to highlight that this study addressed rates and time frames of susceptibility, exposure to malware infection, infectiousness, isolation, recovery, and vaccination as extremely relevant factors in characterizing malware spread/containment in communication networks using mathematical models. The modified models employed in this study are derived from the literature on malware epidemiology for computer networks, specifically computer virus and worm epidemic models.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] CrowdStrike (2020) 2020 Global Threat Report. https://www.newcastle.edu.au/__data/assets/pdf_file/0006/616875/2020_Global-Threat-Report.pdf

[2] Lu, X.F., Zhou, X., Jiang, F.S., Yi, S.W. and Sha, J. (2018) ASSCA: API Based Sequence and Statistics Features Combined Malware Detection Architecture. *Procedia Computer Science*, **129**, 248-256. https://doi.org/10.1016/j.procs.2018.03.072

[3] Nwokoye, C.H., Umeugoji, C. and Umeh, I. (2020) Evaluating Degrees of Differential Infections on Sensor Networks' Features Using the SEjIjR-V Epidemic Model. *Egyptian Computer Science Journal*, **44**, 86-97.

http://ecsjournal.org/Archive/Volume44/Issue3/6.pdf

[4] Mishra, B.K. and Saini, D.K. (2007) SEIRS Epidemic Model with Delay for Transmission of Malicious Objects in Computer Network. *Applied Mathematics and Computation*, **188**, 1476-1482. https://doi.org/10.1016/j.amc.2006.11.012

[5] Mishra, B.K. and Keshri, N. (2013) Mathematical Model on the Transmission of Worms in Wireless Sensor Network. *Applied Mathematical Modelling*, **37**, 4103-4111. https://doi.org/10.1016/j.apm.2012.09.025

[6] Kermack, W.O. and McKendrick, A.G. (1991) Contributions to the Mathematical Theory of Epidemics—I. 1927. *Bulletin of Mathematical Biology*, **53**, 33-55.

[7] Wang, L., Chen, J. and Marathe, M. (2018) TDEFSI: Theory-Guided Deep Learning-Based Epidemic Forecasting with Synthetic Information. *ACM Transactions on Spatial Algorithms and Systems*, **6**, 1-39. https://doi.org/10.1145/3380971

[8] Kermack, W.O. and McKendrick, A.G. (1927) A Contribution to the Mathematical Theory of Epidemics. *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character*, **115**, 700-721. https://doi.org/10.1098/rspa.1927.0118

[9] Mishra, B.K. and Singh, A.K. (2012) SIjRS E-Epidemic Model with Multiple Groups of Infection in Computer Network. *International Journal of Nonlinear Science*, **13**, 357-362.

[10] Mishra, B.K. and Pandey, S.K. (2011) Dynamic Model of Worms with Vertical Transmission in Computer Network. *Applied Mathematics and Computation*, **217**, 8438–8446. https://doi.org/10.1016/j.amc.2011.03.041

[11] Mishra, B.K. and Jha, N. (2010) SEIQRS Model for the Transmission of Malicious Objects in Computer Network. *Applied Mathematical Modelling*, **34**, 710-715. https://doi.org/10.1016/j.apm.2009.06.011

[12] Nwokoye, C. and Umeh, I. (2018) Analytic-Agent Cyber Dynamical Systems Analysis and Design Method for Modeling Spatio-Temporal Factors of Malware Propagation in Wireless Sensor Networks. *MethodsX*, **5**, 1373-1398. https://doi.org/10.1016/j.mex.2018.10.005

[13] Wagner, H.M. (1989) Principles of Operational Research with Application in Management Decision. Prentice Hall, Hoboke.

[14] Haldar, K. and Mishra, B.K. (2014) A Mathematical Model for a Distributed Attack on Targeted Resources in a Computer Network. *Communications in Nonlinear Science and Numerical Simulation*, **19**, 3149-3160. https://doi.org/10.1016/j.cnsns.2014.01.028

[15] Mishra, B.K. and Tyagi, I. (2014) Defending against Malicious Threats in Wireless Sensor Network: A Mathematical Model. *International Journal of Information Technology and Computer Science*, **6**, 12-19. https://doi.org/10.5815/ijitcs.2014.03.02

[16] Heesterbeek, J.A.P. and Dietz, K. (1996) The Concept of R_o in Epidemic Theory. *Statistica Neerlandica*, **50**, 89-110. https://doi.org/10.1111/j.1467-9574.1996.tb01482.x

[17] Tang, S. and Mark, B.L. (2009) Analysis of Virus Spread in Wireless Sensor Networks: An Epidemic Model. 2009 7*th International Workshop on Design of Reliable Communication Networks*, Washington DC, 25-28 October 2009, 86-91. https://doi.org/10.1109/DRCN.2009.5340022