Optimal Control for Antivirus Routing in Epidemiological-Based Heterogeneous Computer Network Clusters

Shuangge Wang[†,1], Zhilin He[†,2], Zihao Xu[†,2], Cymra Haskell[2], Bhaskar Krishnamachari[3]

***Abstract*— Maintaining productivity in computer networks under virus threats has been an ongoing research. Existing works have adopted epidemiological-based ordinary differentiation equations (ODEs) to model virus and antivirus propagation. However, these models tend to oversimplify by not accounting for the heterogeneity among different computer network clusters and ignoring real-world protocol constraints, e.g., nodes cannot communicate simultaneously with nodes in different groups. In this work, we develop a novel model that acknowledges these constraints and incorporates heterogeneity. We first propose a single-cluster ODE model in which both the virus and antivirus propagate. We then generalize this single-cluster model to a model for networks with heterogeneous clusters. Leveraging these models, we formulate the maximum productivity objective as an optimization problem that could be solved using quasi-Newton methods. We also numerically formalize the optimal control's validity in the single-cluster model through Pontryagin's Maximum Principle (PMP). By experimentation and simulation, we find that the optimal control policy follows a bang-bang structure and performs guided prioritization for the heterogeneity of clusters.**

I. Introduction

Amid advancing computer technology and growing internet use, we enjoy being in an interconnected network and accessing information despite geographic constraints. Characterized by their scalability, performance, and flexibility, computer networks provide a wide range of benefits, including resource sharing, remote collaboration, and centralized management, all contributing to improved productivity.

In certain computer networks, nodes within a roaming area all receive information from the sender. These communication schemes suffer less from bandwidth limitations thanks to Multiple Access Techniques [1], allowing each node to communicate with infinite nodes under a constrained spectrum of communication medium.

This extensive connectivity, however, allows computer viruses to attack devices and cause various damages at a higher rate. Through the internet, each node can send a malicious packet to others [2]–[4]. The infection of computer viruses may cause the leak of private information. Moreover, they may rapidly propagate through nodes and invade databases or services, leading to their malfunction and resulting in reduced productivity. Therefore, the dynamic modeling of network antivirus routing is crucial to understand virus propagation and help maintain computer productivity.

Although innately different, it has been suggested that computer and biological viruses spread similarly due to their network structures [5]. For biological viruses, the classical Susceptible-Infected-Recovered (SIR) model was first introduced in [6] and has been used extensively to model epidemic dynamics [7]–[10]. The SIR model, defined by a system of deterministic ordinary differential equations (ODEs), divides the population into three distinct groups: the susceptible, the infected, and the recovered. The infected group infects the susceptible, and the infected group automatically recovers from the virus over time. Based on the SIR model, [11]–[14] incorporates antivirus routing, showing the pattern of virus invasion in computer networks and exhibiting the validity of endemic virus equilibrium.

Despite advancing measures in modeling virus propagation and antivirus routing, they assume homogeneity within the network and overlook the heterogeneity of each network cluster. Such heterogeneity can be prevalent in real-world scenarios as different network clusters may have their distinct transmission rates, resource capacities, and levels of criticality. Current approaches also attempt to prevent virus propagation in hardware systems by manually adding antivirus nodes. In the context of Artificial Immune Systems [15], where immunity can be passed autonomously in the network, existing model designs also fail to realize that recovered nodes can actively broadcast their antivirus to others, making the system self-healing. Moreover, existing works have yet to incorporate the constrained availability of network resources observed in real-world scenarios. For instance, nodes from distinct clusters might require different communication protocols, which inhibits nodes from simultaneously contacting others across multiple clusters.

This work, therefore, proposes an epidemiological-based model that describes antivirus routing in computer network clusters with resource constraints under both single-cluster and heterogeneous-cluster network settings. The model assumes that each recovered node carries the antivirus and will pass it to other non-recovered nodes through communications to imitate biological self-healing. Our key contributions are two-fold. Firstly, we propose a novel single-cluster model (Fig. 1), which we later generalize to a model for multiple heterogeneous network clusters in Section IV. Secondly, motivated by the objective of maximum productivity in virus-exposed computer systems, we introduce an optimal control

[†]Shuangge Wang, Zhilin He, and Zihao Xu contributed equally.

[1]Shuangge Wang is with the Department of Computer Science, Yale University, New Haven, CT, 06511 USA. Email: shuangge.wang@yale.edu

[2]Zhilin He, Zihao Xu, and Cymra Haskell are with the Department of Mathematics, University of Southern California, Los Angeles, CA, 90089 USA. Emails: {zhilinhe, xuzihao, chaskell}@usc.edu

[3]Bhaskar Krishnamachari is with the Ming Hsieh Department of Electrical and Computer Engineering, University of Southern California, Los Angeles, CA, 90089 USA. Email: bkrishna@usc.edu

Preprint. To be published at ACC 2024

strategy for nodes that carry the antivirus to spread the virus through the single and heterogeneous network clusters. We also provide a satisfying intuition of the optimal control strategy and its implications in the single cluster case. As we will show in later sections, this work is non-trivial because of the communication protocol and procedure constraints.

II. Related Work

Epidemiological-based ODEs have been used extensively to model the dynamics of antivirus routing in network clusters. [16] uses a Susceptible-Infected (SI) ODE model to examine the impact of an active viral cyber threat targeting high-availability network clusters by seeking the average number of infected nodes. Based on the SIR model, [17] introduces a tripartite-cluster graph model, concluding that substantial heterogeneity will lead to fewer infected nodes. Although models derived from the above methods are generally applicable, they inadequately represent cluster interactions. Such interactions, determined by the heterogeneity of each cluster, affect node migration within and across clusters and, therefore need to be further investigated.

Existing works on Epidemic Routing aim to showcase the interaction among nodes, focusing on forwarding packets from packet-carrying nodes to those that have not received them yet [18]. Following this topic, [19]–[20] attempts to maximize the transmission efficiency by limiting the average delay or delivery probability of nodes in the network. [21]–[22] expands the dissemination scenario from a single group of nodes into heterogeneous groups. [23] considers a weighted priority between nodes and models on multiple groups transmission, maximizing the number of nodes receiving packets with a preference for one cluster over another. In our work, rather than allocating priorities to nodes, we assign priorities to the entire cluster and investigate how antivirus dissemination, within and across clusters, affects the network's productivity.

Works in optimal control have focused thus far on improving the deployment of antivirus routing in network clusters, including infection containment [24], optimal resource allocation [25]–[27], and operational cost minimization [28]–[29]. Optimal control theory, particularly Pontryagin's Maximum Principle (PMP) [30]–[33], has been widely used to solve non-linear optimal control problems. Such works include designing optimal congestion management in large-scale networks [34] and protecting communication networks from malware attacks [35]–[36]. To our best knowledge, our work is the first to combine epidemiological-based and epidemic routing approaches to construct ODEs for antivirus routing in network clusters. Furthermore, we formulate this problem as an optimal control problem via PMP, aiming to maximize productivity in heterogeneous computer network clusters.

III. Single-Cluster Network

We first model the propagation of the virus and antivirus in a single network cluster based on the classical SIR model, in which nodes are categorized into either the susceptible, infected, or recovered group, whose population in proportion at time t are $S(t)$, $I(t)$, and $R(t)$, respectively.

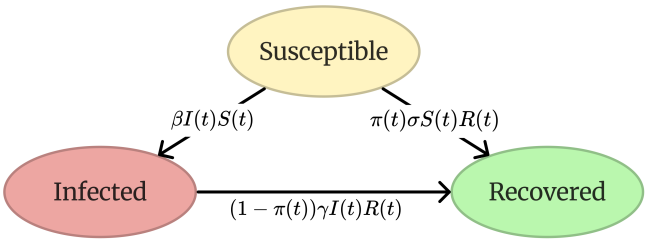


Fig. 1: Single-Cluster Model

Susceptible nodes have yet to catch the virus and are thus susceptible to the virus; infected nodes have caught the virus and are capable of infecting susceptible nodes; recovered nodes have recovered from the virus thanks to having the antivirus and are capable of passing the antivirus to the susceptible and infected nodes. By receiving the virus and antivirus, nodes migrate among these three groups. The full chain of migration is illustrated in Fig. 1.

Before defining the model ODEs, we will make some mild assumptions. The first assumption is that, in alignment with common approaches in mathematical epidemiology [37]–[38], the virus is potent enough to require infected nodes to recover if and only if they possess antivirus in the self-healing process. Secondly, from the design of Scale-Free Networks [39], which allows for nodes having unlimited degrees of connectivity, we assume there is no limit on how many nodes a single node could communicate to since each group-wise communication shares a unique spectrum. Therefore, virus and antivirus transmission rates between the two groups are proportional to their respective population and a contact parameter that embodies factors like roaming area, contact time, and loss. Lastly, we assume that, due to protocol constraints in computer networks and data transmission rate limitations in node communication procedures as suggested in [23] and [40], recovered nodes cannot communicate with susceptible and infected nodes simultaneously. To facilitate the interaction of recovered nodes exclusively with either susceptible or infected nodes, we introduce $\pi(t) \in [0, 1]$ as a control variable to describe the probability that recovered nodes pass their antivirus to susceptible nodes. Thus, the probability that recovered nodes pass their antivirus to infected nodes is $1 - \pi(t)$.

A. Model

As the total number of nodes in the network increases, the system's ODEs asymptomatically approach

$$\begin{bmatrix} \dot{S}(t) \\ \dot{I}(t) \\ \dot{R}(t) \end{bmatrix} = \begin{bmatrix} -\beta I(t)S(t) - \pi(t)\sigma S(t)R(t) \\ \beta I(t)S(t) - (1-\pi(t))\gamma I(t)R(t) \\ \pi(t)\sigma S(t)R(t) + (1-\pi(t))\gamma I(t)R(t) \end{bmatrix} \tag{1}$$

with constraints

$$\begin{aligned} S(0) + I(0) + R(0) &= 1 \\ \beta, \sigma, \gamma, S(0), I(0), R(0) &> 0 \end{aligned} \tag{2}$$

where β, σ, and γ are contact parameters between susceptible and infected nodes, susceptible and recovered nodes, and infected and recovered nodes, respectively.

Thanks to (1) and (2), we have

$$\begin{aligned} S(t), I(t), R(t) > 0, \forall t \in [0, T] \\ S(t) + I(t) + R(t) = 1, \forall t \in [0, T] \end{aligned} \tag{3}$$

which reduces the ODEs into

$$\dot{x}(t) = \begin{bmatrix} \dot{S}(t) \\ \dot{I}(t) \end{bmatrix} = \begin{bmatrix} -\beta I(t) S(t) - \pi(t) \sigma S(t)(1 - S(t) - I(t)) \\ \beta I(t) S(t) - (1 - \pi(t)) \gamma I(t)(1 - S(t) - I(t)) \end{bmatrix} \tag{4}$$

without loss of information about the system.

B. Optimal Control

We aim for maximum computer productivity in a given time frame $[0, T]$, so we minimize the time integration of the unproductive population, i.e., the infected nodes. The optimization problem is therefore formulated as

$$\min_{\pi(t)} \int_0^T I(t) dt \tag{5a}$$

$$\text{s.t.} \quad x(0) = \begin{bmatrix} S(0) & I(0) \end{bmatrix}^T \tag{5b}$$

$$\dot{x}(t) = \begin{bmatrix} \dot{S}(t) & \dot{I}(t) \end{bmatrix}^T \tag{5c}$$

$$0 \leq \pi(t) \leq 1 \tag{5d}$$

which can be solved using quasi-Newton methods like the L-BFGS-B algorithm [41]–[42].

After solving for the control, we adopt the PMP to verify its optimality. The Hamiltonian function is constructed as

$$H\left(x(t), \pi(t), \lambda(t), t\right) = I(t) + \lambda^T(t) \dot{x}(t) \tag{6}$$

where the adjoint function, $\lambda(t)$, is the solution to this ODE

$$-\dot{\lambda}(t) = -\begin{bmatrix} \lambda_a(t) \\ \lambda_b(t) \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} + J\lambda(t) \tag{7}$$

in which J is

$$\begin{bmatrix} -\beta I(t) - \sigma\pi(t)(1 - I(t) - 2S(t)) & \beta I(t) + \gamma(1 - \pi(t)) I(t) \\ -\beta S(t) + \sigma\pi(t) S(t) & \beta S(t) - \gamma(1 - \pi(t))(1 - S(t) - 2I(t)) \end{bmatrix} \tag{8}$$

with final conditions $\lambda(T) = \begin{bmatrix} 0 & 0 \end{bmatrix}^T$.

By PMP, the optimal control, $\pi^*(t)$, follows

$$\pi^*(t) = \arg\min_{\pi(t) \in \mathbb{U}} H\left(x^*(t), \pi(t), \lambda^*(t), t\right) \tag{9}$$

in which * denotes optimaility.

Due to (2) and (3), we can further simplify (9) to

$$\pi^*(t) = \arg\min_{\pi(t) \in \mathbb{U}} \pi(t)(\lambda_b^*(t) \gamma I^*(t) - \lambda_a^*(t) \sigma S^*(t)) \tag{10}$$

where optimality of $\lambda_a(t)$, $\lambda_b(t)$, $I(t)$ and $S(t)$ will be achieved for the optimization problem (5) and the minimization objective on the right-hand side is linear with respect to the control variable, hinting that $\pi^*(t)$ follows a bang-bang control policy where the control clips to either maximum or minimum values depending on the sign of the switching function,

$$\phi(t) = \lambda_b^*(t) \gamma I^*(t) - \lambda_a^*(t) \sigma S^*(t). \tag{11}$$

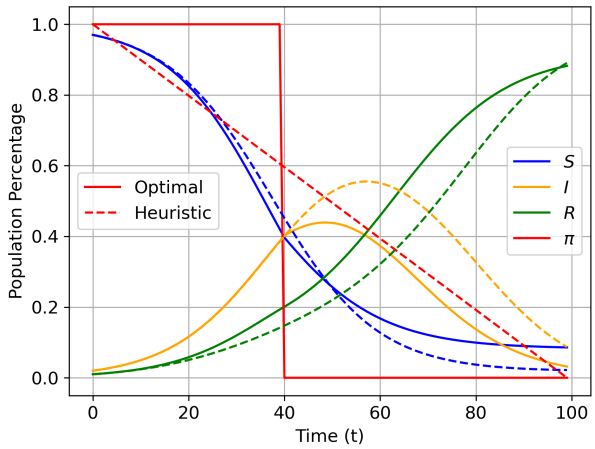


Fig. 2: Two control policies and their associated states, with the solid line being optimal and the dashed line being heuristic.

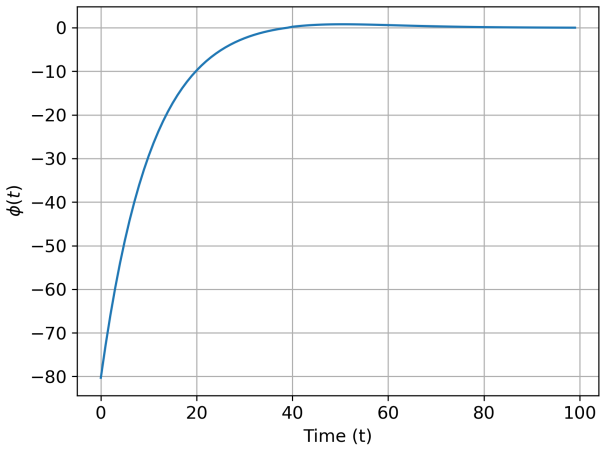


Fig. 3: Switching Function

After obtaining $\pi^*(t)$ and its associated $x^*(t)$ through optimization, we solve for $\lambda^*(t)$ by propagating it backwards in time starting from T. By PMP, we can then leverage (10) to verify our solution's global optimality.

C. Experiment

We simulate a case with contact parameters $\beta = \sigma = \gamma = 0.1$, $S(0) = 0.2$, and $R(0) = 0.97$. We set $T = 100$ and discretize the dynamics with a time granularity of 1. We also include a linearly decreasing control policy as a heuristic comparison. Fig. 2 includes the two control policies and their respective states. The bang-bang control policy generates an overall smaller $I(t)$ curve than the heuristic policy does, showing that the virus is better contained for maximum node productivity. Moreover, we can see from Fig. 3 that $\pi(t) = 1$ when $\phi(t) < 0$ and $\pi(t) = 0$ when $\phi(t) > 0$, verifying that our solution is optimal.

D. Discussion

We also hope to give some insights into why the optimal control takes such shape. Although ours is a finite horizon problem, as T approaches ∞, the structure of the optimal control policy reflects a phenomenon similar to the Most Rapid Approach Path (MRAP) [43], where the control allows the system to approach its steady state as quickly as possible. In fact, [43] and [44] proved that, for any problem whose augmented objective integrand can be written as

$$W(x(t), \dot{x}(t)) = M(x(t)) + N(x(t))\dot{x}(t) \tag{12}$$

where M and N are differentiable functions, the problem fits into the general class of MRAP problems, where x follows an MRAP to the optimal steady state defined by

$$\frac{\partial W(x(t), \dot{x}(t))}{\partial t} = 0 \tag{13}$$

In our case where $W(x(t), \dot{x}(t)) = I(t)$, we assign $M(x(t)) = I(t)$ and $N(x(t)) = 0$, reducing (13) to $\dot{I}(t) = 0$. According to Fig. 2, we see that there exists $\tau \geq 0$ that segments $I(t)$ into two monotonic intervals, $[0, \tau]$ and $[\tau, \infty]$, where the former is increasing and latter is decreasing. Therefore, the solution to (13) are τ and ∞.

In the first interval, $[0, \tau]$, $\pi(t)$ is initially set to 1 for prioritizing the retention of $I(t)$ so that it increases as fast as possible to approach $I(\tau)$. As $I(t)$ gets greater, the contribution from $S(t)$ to $I(t)$ decreases. Therefore, to help $I(t)$ approach its maximum faster, we need to reduce its gradient as fast as possible, so the policy shifts to decrease its rate of increase by migrating $I(t)$ to $R(t)$, hence setting $\pi(t) = 0$. In the second interval, $[\tau, \infty]$, $\pi(t)$ is simply set to 0 to prioritize the decrease of $I(t)$ so that $\dot{I}(t) = 0$ is achieved as quickly as possible, although it would practically take infinite time to reach.

Together, these two intervals comprise the first-susceptible-then-infected control policy, which shares the same intuition as *vaccination before quarantine* in disease control, *reinvestment before consumption* in asset value generation [45], and *education before employment* in human resource management [43].

IV. Heterogeneous-Cluster Network

We now proceed to formulate a new multi-cluster model that describes virus and antivirus propagation in a network with heterogeneous clusters. The motivation behind introducing heterogeneity lies in each cluster's different transmission rates, node densities, resource capacity, and importance.

In this configuration, we assume the virus still spreads within the same cluster (intra-cluster), but the antivirus could be communicated across different clusters (inter-cluster). This assumption is largely based on how each cluster usually has its inter-cluster firewall to filter out malicious files from other clusters [46]–[47]. We also assume that the state of a node is opaque to nodes not in the same cluster, so recovered nodes could not target a specific group, i.e., the susceptible or the infected group, during inter-cluster communication.

A. Model

For Cluster i, the model ODEs are defined as

$$\begin{aligned}\dot{x}_i(t) &= \begin{bmatrix}\dot{S}_i(t)\\ \dot{I}_i(t)\end{bmatrix} \\ &= \begin{bmatrix}-\beta_i I_i(t) S_i(t) - \omega_i(t)\sigma_i S_i(t)(1 - S_i(t) - I_i(t))\\ \beta_i I_i(t) S_i(t) - \epsilon_i(t)\gamma_i I_i(t)(1 - S_i(t) - I_i(t))\end{bmatrix} \\ &\quad - \sum_{j=1, j\neq i}^{n} p_{ji}(t)(1 - S_i(t) - I_i(t)) \begin{bmatrix}\tau_{ji} S_i(t)\\ \phi_{ji} I_i(t)\end{bmatrix}\end{aligned} \tag{14}$$

with constraints

$$\begin{aligned} S_i(0) + I_i(0) + R_i(0) &= 1 \\ \beta_i, \sigma_i, \gamma_i, \tau_{ji}, \phi_{ji}, S_i(0), I_i(0), R_i(0) &> 0\end{aligned} \tag{15}$$

where β_i, σ_i, and γ_i are intra-cluster contact parameters defined in Section III, τ_{ji} and ϕ_{ji} are inter-cluster contact parameters from recovered nodes in Cluster j to susceptible nodes and infected nodes in Cluster i respectively. $\omega_i(t)$. and $\epsilon_i(t)$ are probabilities of the recovered nodes passing antivirus to the susceptible and infected nodes in the same cluster. $p_{ji}(t)$ is the probability that a recovered node in Cluster j passes its antivirus to Cluster i. The new control parameter $\pi_i(t)$ for Cluster i is therefore

$$\pi_i(t) = \begin{bmatrix}\omega_i(t)\\ \epsilon_i(t)\\ p_{i1}(t)\\ \vdots\\ p_{in}(t)\end{bmatrix}^T \begin{bmatrix}\mathbf{I}_{i+1} & \mathbf{O}_{n-i,i+2}\\ \mathbf{O}_{i+1,n-i+1} & \mathbf{I}_{n-i}\end{bmatrix} \tag{16}$$

with constraints

$$\pi_i(t) \in \mathbb{U}_i = \left\{\pi_i(t) \in \mathbb{R}_+^{n+1}, \|\pi_i(t)\|_1 = 1\right\} \tag{17}$$

B. Optimal Control

We first release constraints (17) to turn our problem into an unconstrained optimization. For cluster i, we define an unconstrained space $\tilde{\pi}_i(t) \in \mathbb{R}^{n+1}$ that satisfies this mapping

$$\pi_i(t) = \frac{e^{\tilde{\pi}_i(t)}}{\sum_{j=1}^{n+1} e^{\tilde{\pi}_{ij}(t)}} \tag{18}$$

Due to the heterogeneity in clusters' computing power, security, and operation cost, we should assign different weights to different clusters' productivity. The minimization objective now becomes a linear combination, characterized by $w \in \mathbb{R}^n$, of the time integration of the infected population. The optimization problem can then be formulated as

$$\begin{bmatrix}\tilde{\pi}_1(t) & \dots & \tilde{\pi}_n(t)\end{bmatrix} \min \int_0^T w^T \begin{bmatrix}I_1(t)\\ \vdots\\ I_n(t)\end{bmatrix} dt \tag{19a}$$

$$\text{s.t.} \quad x_i(0) = \begin{bmatrix}S_i(0) & I_i(0)\end{bmatrix}^T, \quad \forall i \in \mathbb{Z}_{\leq n}^+ \tag{19b}$$

$$\dot{x}_i(t) = \begin{bmatrix}\dot{S}_i(t) & \dot{I}_i(t)\end{bmatrix}^T, \quad \forall i \in \mathbb{Z}_{\leq n}^+ \tag{19c}$$

$$\pi_i(t) = \frac{e^{\tilde{\pi}_i(t)}}{\sum_{j=1}^{n+1} e^{\tilde{\pi}_{ij}(t)}}, \quad \forall i \in \mathbb{Z}_{\leq n}^+ \tag{19d}$$

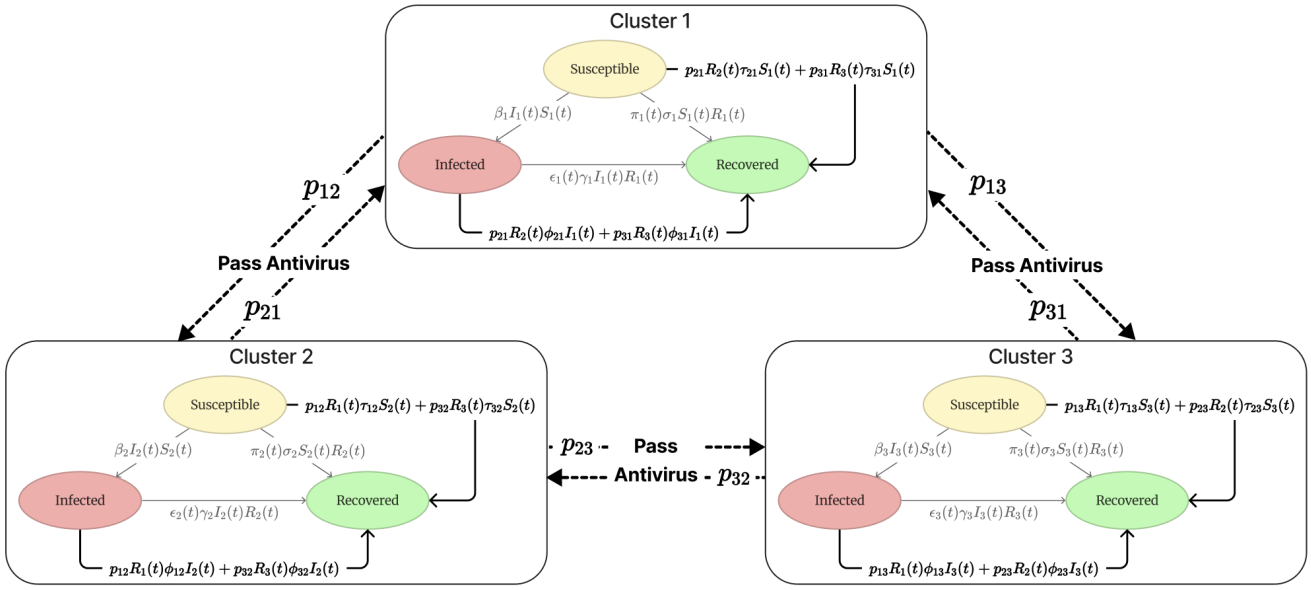


Fig. 4: Heterogeneous-Cluster Model: This particular configuration is comprised of 3 clusters, in which each cluster's intra-cluster node migration is indicated in light texts. Additionally, we also included the inter-cluster node migration (bold solid line), which resulted from inter-cluster communication (bold dashed line).

Parameters	Values
$\begin{bmatrix} S_1(0) & S_2(0) & S_3(0) \\ I_1(0) & I_2(0) & I_3(0) \end{bmatrix}$	$\begin{bmatrix} 0.97 & 0.97 & 0.97 \\ 0.01 & 0.01 & 0.01 \end{bmatrix}$
β $(Scenario\ I)$	$\begin{bmatrix} 0.1 & 0.15 & 0.2 \end{bmatrix}$
β $(Scenario\ II)$	$\begin{bmatrix} 0.2 & 0.2 & 0.2 \end{bmatrix}$
σ	$\begin{bmatrix} 0.2 & 0.2 & 0.2 \end{bmatrix}$
γ	$\begin{bmatrix} 0.2 & 0.2 & 0.2 \end{bmatrix}$
τ $(Scenario\ I)$	$\begin{bmatrix} 0.15 & 0.15 & 0.15 \\ 0.15 & 0.15 & 0.15 \\ 0.15 & 0.15 & 0.15 \end{bmatrix}$
τ $(Scenario\ II)$	$\begin{bmatrix} 0.1 & 0.1 & 0.1 \\ 0.1 & 0.1 & 0.1 \\ 0.1 & 0.1 & 0.1 \end{bmatrix}$
ϕ $(Scenario\ I)$	$\begin{bmatrix} 0.15 & 0.15 & 0.15 \\ 0.15 & 0.15 & 0.15 \\ 0.15 & 0.15 & 0.15 \end{bmatrix}$
ϕ $(Scenario\ II)$	$\begin{bmatrix} 0.1 & 0.1 & 0.1 \\ 0.1 & 0.1 & 0.1 \\ 0.1 & 0.1 & 0.1 \end{bmatrix}$
w $(Scenario\ I)$	$\begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$
w $(Scenario\ II)$	$\begin{bmatrix} 1 & 2 & 3 \end{bmatrix}$

TABLE I: Simulation Initial Conditions and Parameters

which can be solved using the L-BFGS algorithm. After obtaining the solution, we transform the optimization space using (18) to recover the control policy.

V. Simulation

We now proceed to simulate our models. We assume a centralized optimization scheme in which all information of all clusters is available to the solver. The scenarios we study below are mere arbitrary choices, and the simulation software we provide is easily adjustable for studying other wide ranges of scenarios. Here, we simulate two scenarios, both with 3 clusters, and set the simulation parameters as in TABLE I.

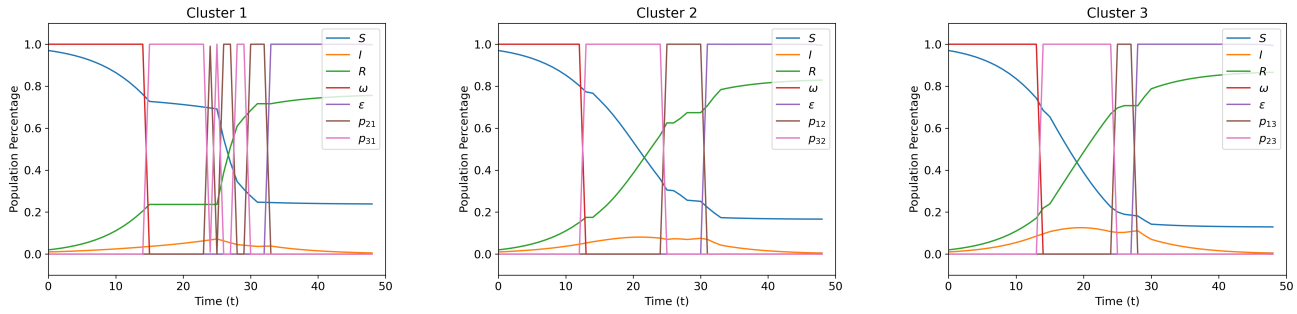
A. Scenario I: Different Intra-Cluster Transmission Rate

For the first scenario, we consider the case where all clusters are equally important in terms of productivity. However, the infectiousness of viruses may be amplified in certain clusters due to different β, resulting in a more substantial infection count in different clusters. Therefore, the minimization objective has equal weight on all clusters, but each cluster has a different β. In this experiment, we set $\beta = \begin{bmatrix} 0.1 & 0.15 & 0.2 \end{bmatrix}$.

Fig. 5 contains the states and control parameters of each cluster. The optimal control policy mostly follows a bang-bang structure, in which the control clips to either the maximum or minimum value. Contrary to the single cluster case where the control is monotonic, the solution to the heterogeneous cluster problem may undergo multiple switches. We can see that Cluster 3 has the largest area under the $I(t)$ curve, and Cluster 1 has the smallest, which corresponds with our experiment design and goal. As $I(t)$ increases, $\omega(t)$ clips from maximum to minimum in all clusters, and inter-cluster resources are gathered towards Cluster 3. Then, as $I(t)$ reaches its maximum, inter-cluster resources start to distribute more evenly with a slight focus on Cluster 2. Finally, $\epsilon(t)$ clips from minimum to maximum, enabling the regulation of intra-cluster virus control until the infection diminishes completely. The observed trend in this simulation aligns with our objective design, which prioritizes Cluster 3 over Cluster 2, and Cluster 2 over Cluster 1.

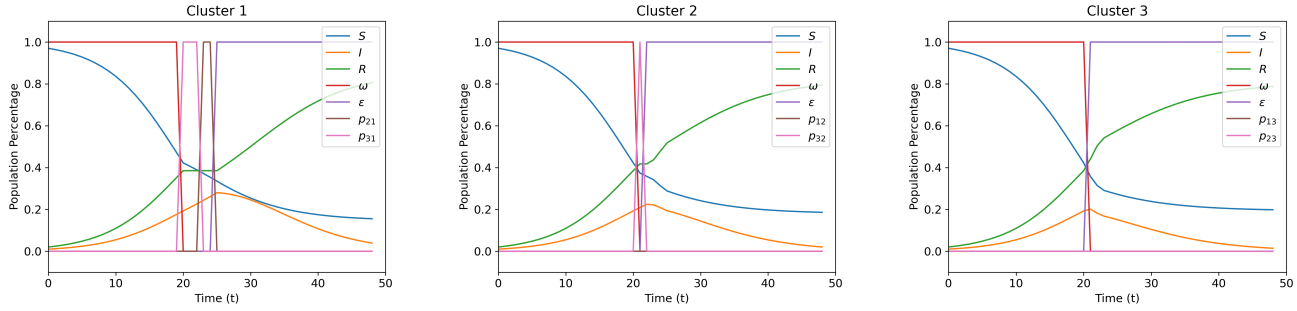
B. Scenario II: Different Cluster Weight With Lower Inter-Cluster Transmission Rate

Certain clusters, such as large cloud computing platforms, may warrant prioritization over other clusters. In the event of a virus outbreak, it is imperative to prioritize resource



(a) Cluster 1 States and Controls (b) Cluster 2 States and Controls (c) Cluster 3 States and Controls

Fig. 5: Scenario I: Different Intra-Cluster Transmission Rate



(a) Cluster 1 States and Controls (b) Cluster 2 States and Controls (c) Cluster 3 States and Controls

Fig. 6: Scenario II: Different Cluster Weight With Lower Inter-Cluster Transmission Rate

allocation to these pivotal clusters to safeguard their functionality and data integrity. Therefore, for the second scenario, we consider clusters that are assigned weights that signify their relative significance in aspects such as productivity. In specific, we assign $w = \begin{bmatrix}1 & 2 & 3\end{bmatrix}$. We make the assumption that each cluster has an identical disease transmission rate, hence we assign $\beta = \begin{bmatrix}0.2 & 0.2 & 0.2\end{bmatrix}$. Furthermore, nodes in different clusters may have a lower rate of interaction than nodes within a cluster, often due to the imposition of security policies that limit cross-cluster communications. Therefore, we configure the inter-cluster transmission rates, denoted as τ and ϕ, to be lower compared to the intra-cluster transmission rates, i.e., σ and γ.

Fig. 6 contains the states and control parameters of each cluster. Again, the optimal control policy follows a bang-bang structure. Similar to Scenario I, $\omega(t)$ clips from maximum to minimum in all clusters as $I(t)$ increases. However, inter-cluster resources in this case no longer target the prioritized Cluster 3. As a result, in Cluster 3, the inter-cluster control policy remains at a constant minimum, while the intra-cluster control policy becomes monotonic. This could be attributed to lower inter-cluster transmission rates, signifying a reduced capability of inter-cluster resources to aid across different clusters. Under such conditions, the system utilizes intra-cluster resources for virus control to enhance efficiency. As $I(t)$ in Cluster 3 reaches its maximum, $\omega(t)$ clips from maximum to minimum, and $\epsilon(t)$ clips from minimum to maximum within the same cluster. Meanwhile, inter-cluster resources begin to distribute across Cluster 1 and Cluster 2 along with the clip of their respective $\omega(t)$. This observation is consistent with our objective that prioritizes Cluster 3 over Cluster 2, and Cluster 2 over Cluster 1.

VI. Conclusions

In this work, we present a novel epidemiological-based approach to model virus propagation and antivirus routing in computer networks. We present the single-cluster model and then generalize it to a model for multiple heterogeneous network clusters. By incorporating a control variable, we aim to maximize computer productivity, for which we then apply L-BFGS-based algorithms to solve. We also include an approach to verify the solution's optimality using PMP and an intuitive insight into the first-susceptible-then-infected (bang-bang) control policy in the single-cluster case. Our simulations of heterogeneous cluster routing also demonstrate this bang-bang structure. Besides, the control policies perform a routing priority over the heterogeneity of clusters and overall objective weights.

Future works could focus on providing analytical guarantees for the control structure, decentralizing the optimization to each cluster under the framework of partially observable Markov decision processes, and adopting learning-based methods to transform the history-dependent objective into a memoryless value function, which can be solved by using polynomial-time algorithms.

REFERENCES

[1] D. Torrieri, *Principles of spread-spectrum communication systems*. Springer, 2005, vol. 1.

[2] F. Cohen, "Computer viruses: theory and experiments," *Computers & security*, vol. 6, no. 1, pp. 22–35, 1987.

[3] R. Ball, "Computer viruses, computer worms, and the self-replication of programs," in *Viruses in all Dimensions: How an Information Code Controls Viruses, Software and Microorganisms*. Springer, 2023, pp. 73–85.

[4] G. Kaur, E. Kaur, H. Jindal, and N. Gautam, "Computer viruses: Security risks and solution," *i-Manager's Journal on Software Engineering*, vol. 17, no. 4, p. 29, 2023.

[5] J. Boase and B. Wellman, "A plague of viruses: biological, computer and marketing," *Current sociology*, vol. 49, no. 6, pp. 39–55, 2001.

[6] W. O. Kermack and A. G. McKendrick, "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*, vol. 115, no. 772, pp. 700–721, 1927.

[7] K. Rock, S. Brand, J. Moir, and M. J. Keeling, "Dynamics of infectious diseases," *Reports on Progress in Physics*, vol. 77, no. 2, p. 026602, 2014.

[8] M. Saeedian, M. Khalighi, N. Azimi-Tafreshi, G. Jafari, and M. Ausloos, "Memory effects on epidemic evolution: The susceptible-infected-recovered epidemic model," *Physical Review E*, vol. 95, no. 2, p. 022409, 2017.

[9] D. J. Earn, "A light introduction to modelling recurrent epidemics," in *Mathematical epidemiology*. Springer, 2008, vol. 1945, pp. 3–16.

[10] D. Acemoglu, V. Chernozhukov, I. Werning, M. D. Whinston *et al.*, *A multi-risk SIR model with optimally targeted lockdown*. National Bureau of Economic Research Cambridge, MA, 2020, vol. 2020.

[11] K. Chinnadurai and S. Athithan, "Effect of anti-virus in computer network: A mathematical model in deterministic and stochastic approach," *Annals of the Romanian Society for Cell Biology*, vol. 25, no. 2, pp. 3501–3512, 2021.

[12] M. López, A. Peinado, and A. Ortiz, "An extensive validation of a sir epidemic model to study the propagation of jamming attacks against iot wireless networks," *Computer Networks*, vol. 165, p. 106945, 2019.

[13] S. Noinang, M. Munawar, M. A. Zahoor Raja, Z. Sabir, T. Botmart, W. Weera, and P. Junsawang, "Numerical assessments employing neural networks for a novel drafted anti-virus subcategory in a nonlinear fractional-order sir differential system," *IEEE Access*, vol. 10, pp. 114 192–114 202, 2022.

[14] J. R. C. Piqueira, B. F. Navarro, and L. H. A. Monteiro, "Epidemiological models applied to viruses in computer networks," *journal of computer science*, vol. 1, no. 1, pp. 31–34, 2005.

[15] F. Hosseinpour, K. A. Bakar, A. H. Hardoroudi, and N. Kazazi, "Survey on artificial immune system as a bio-inspired technique for anomaly based intrusion detection systems," pp. 323–324, 2010.

[16] A. Altameem, M. Al-Ma'aitah, V. Kovtun, and T. Altameem, "A computationally efficient method for assessing the impact of an active viral cyber threat on a high-availability cluster," *Egyptian Informatics Journal*, vol. 24, no. 1, pp. 61–69, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1110866522000706

[17] W. Pan and Z. Jin, "Edge-based modeling of computer virus contagion on a tripartite graph," *Applied Mathematics and Computation*, vol. 320, pp. 282–291, 2018.

[18] A. Vahdat, D. Becker *et al.*, "Epidemic routing for partially connected ad hoc networks," 2000.

[19] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: an efficient routing scheme for intermittently connected mobile networks," in *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*, 2005, pp. 252–259.

[20] A. Lindgren, A. Doria, and O. Schelén, "Probabilistic routing in intermittently connected networks," *ACM SIGMOBILE mobile computing and communications review*, vol. 7, no. 3, pp. 19–20, 2003.

[21] S. Ioannidis, L. Massoulie, and A. Chaintreau, "Distributed caching over heterogeneous mobile networks," in *Proceedings of the ACM SIGMETRICS international conference on Measurement and modeling of computer systems*, 2010, pp. 311–322.

[22] K. Moghadam, M. Sathiamoorthy, B. Krishnamachari, and F. Bai, "Dynamic online storage allocation for multi-content dissemination in two-tier hybrid mobile vehicular networks," in *IEEE Vehicular Networking Conference*, 2013.

[23] S. Wang, M. Khouzani, B. Krishnamachari, and F. Bai, "Optimal control for epidemic routing of two files with different priorities in delay tolerant networks," in *2015 American Control Conference (ACC)*, 2015, pp. 1387–1392.

[24] X. Liang, Y. Pei, and Y. Lv, "Modeling the state dependent impulse control for computer virus propagation under media coverage," *Physica A Statistical Mechanics and its Applications*, vol. 491, pp. 516–527, Feb. 2018.

[25] L. Long, K. Zhong, and W. Wang, "Malicious viruses spreading on complex networks with heterogeneous recovery rate," *Physica A: Statistical Mechanics and its Applications*, vol. 509, pp. 746–753, 2018.

[26] X. Chen, T. Zhou, L. Feng, J. Liang, F. Liljeros, S. Havlin, and Y. Hu, "Non-trivial resource amount requirement in the early stage for containing fatal diseases," *arXiv preprint arXiv:1611.00212*, 2016.

[27] X. Chen, W. Wang, S. Cai, H. E. Stanley, and L. A. Braunstein, "Optimal resource diffusion for suppressing disease spreading in multiplex networks," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2018, no. 5, p. 053501, 2018.

[28] E. Gubar, V. Taynitskiy, and Q. Zhu, "Optimal control of heterogeneous mutating viruses," *Games*, vol. 9, no. 4, p. 103, 2018.

[29] W. Liu and S. Zhong, "Web malware spread modelling and optimal control strategies," *Scientific reports*, vol. 7, no. 1, p. 42308, 2017.

[30] V. G. Boltyanskii, R. V. Gamkrelidze, and L. S. Pontryagin, "On the theory of optimal processes," in *Dokl. Akad. Nauk SSSR*, vol. 110, no. 1, 1956, pp. 7–10.

[31] L. S. Pontryagin, *Mathematical theory of optimal processes*. Routledge, 2018.

[32] R. V. Gamkrelidze, "On the theory of optimal processes in linear systems," in *Dokl. Akad. Nauk SSSR*, vol. 116, no. 1, 1957, pp. 9–11.

[33] L. Pontryagin, "Some mathematical problems arising in connection with the theory of optimal automatic control systems," in *Proc. Conf. on Basic Problems in Automatic Control and Regulation*, 1957.

[34] A. Aalipour, H. Kebriaei, and M. Ramezani, "Analytical optimal solution of perimeter traffic flow control based on mfd dynamics: A pontryagin's maximum principle approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 9, pp. 3224–3234, 2019.

[35] X. Yan and Y. Zou, "Optimal internet worm treatment strategy based on the two-factor model," *ETRI journal*, vol. 30, no. 1, pp. 81–88, 2008.

[36] M. Khouzani, S. Sarkar, and E. Altman, "Maximum damage malware attack in mobile wireless networks," *IEEE/ACM Transactions on Networking*, vol. 20, no. 5, pp. 1347–1360, 2012.

[37] F. Brauer, P. Van den Driessche, J. Wu, and L. J. Allen, *Mathematical epidemiology*. Springer, 2008, vol. 1945.

[38] J. El Karkri and M. Benmir, "Some key concepts of mathematical epidemiology," in *Mathematical Analysis of Infectious Diseases*. Elsevier, 2022, pp. 137–162.

[39] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *science*, vol. 286, no. 5439, pp. 509–512, 1999.

[40] D. F. Macedo, A. L. dos Santos, L. H. Correia, J. M. Nogueira, and G. Pujolle, "Transmission power and data rate aware routing on wireless networks," *Computer Networks*, vol. 54, no. 17, pp. 2979–2990, 2010.

[41] C. Zhu, R. H. Byrd, P. Lu, and J. Nocedal, "Algorithm 778: L-bfgs-b: Fortran subroutines for large-scale bound-constrained optimization," *ACM Transactions on mathematical software (TOMS)*, vol. 23, no. 4, pp. 550–560, 1997.

[42] R. H. Byrd, P. Lu, J. Nocedal, and C. Zhu, "A limited memory algorithm for bound constrained optimization," *SIAM Journal on scientific computing*, vol. 16, no. 5, pp. 1190–1208, 1995.

[43] M. Spence and D. Starrett, "Most rapid approach paths in accumulation problems," *International Economic Review*, pp. 388–403, 1975.

[44] J. E. Wilen, "Bioeconomics of renewable resource use," in *Handbook of natural resource and energy economics*. Elsevier, 1985, vol. 1, pp. 61–124.

[45] M. I. Kamien and N. L. Schwartz, *Dynamic optimization: the calculus of variations and optimal control in economics and management*. courier corporation, 2012.

[46] Y. Chang and T. Lin, "Cloud-clustered firewall with distributed sdn devices," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2018, pp. 1–5.

[47] B. Khan, K. Dombrowski, M. Saad, K. McLean, S. Friedman *et al.*, "Network firewall dynamics and the subsaturation stabilization of hiv," *Discrete dynamics in nature and society*, vol. 2013, 2013.