J Comb Optim
DOI 10.1007/s10878-006-8903-1

Resource allocation for restoration of compromised systems

Qunwei Zheng · Sibabrata Ray* · Xiaoyan Hong

Published online: 27 June 2006

Abstract Computer systems are constantly under the threats of being attacked and in many cases these attacks succeed. Today's networked systems are thus built to be intrusion tolerant. In a large scale, the progresses of compromising the networked system and recovering the damage will carry on in parallel, allowing services to be continued (at a degraded level). One of the key problems in the restoration procedure regards to the resource allocation strategies and the cost associated with, specifically, a minimal cost is desired. In this paper we model the cost as a sum of service loss and resource expense that incur during the restoration procedure. We investigate the achievable minimal total cost and corresponding resource allocation strategy for different situations. The situations include both constant rates and time-variant rates in terms of the speed of compromising and recovering. We also consider the fact that the restoration rate is constrained by the resource allocated. The relationship can be either linear or obeying *the law of diminishing marginal utility*. We present both analytical and numerical results in the paper. The results show the impact from various system parameters on the critical conditions for a successful system restoration and on the minimal cost.

Keywords Cost analysis · Intrusion tolerance · Resource allocation · System restoration · Internet worm

1. Introduction

Research in Internet security has three main directions, namely, intrusion prevention, detection, and tolerance. Traditional security prevention mechanisms are firewalls, cryptography

*Dr. Ray is currently with Google Inc., 604 Arizona Avenue, Santa Monica, CA 90401, USA. His e-mail contact is sibu@google.com, siburay@gmail.com.

Q. Zheng (✉) · S. Ray · X. Hong
Department of Computer Science, University of Alabama, Box 870290, Tuscaloosa, AL 35487-0290
e-mail: qzheng@cs.ua.edu

S. Ray
e-mail: sibu@cs.ua.edu

X. Hong
e-mail: hxy@cs.ua.edu

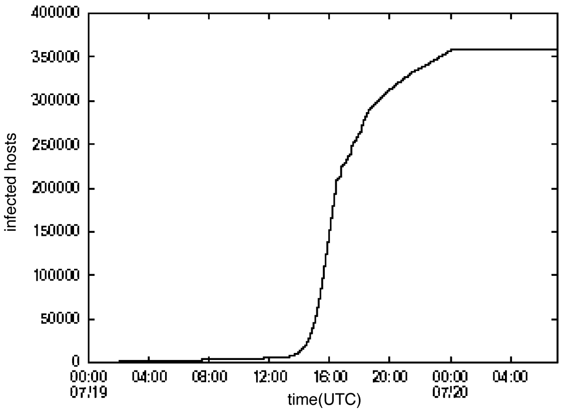


Fig. 1 Cumulative total machines infected by Code Red worm (from www.caida.org)

and access controls. However, despite the advancements of research on these mechanisms and the large amount of network security methods deployed over the world, intrusions still occur. Intrusion detection systems are then designed to detect intrusions and invoke corresponding actions. Yet even a highly sophisticated intrusion detection system could fail. Thus, it is highly desired that today's computer systems, be it Internet, ad hoc networks, or sensor networks, are intrusion tolerant (Lala, 2003; Verissimo et al., 2003), i.e., the system are able to continue its operation even under attacks. When this happens, the performance of the system might degrade due to intrusion but the service it provides must never stop. In the meantime, the system's owners will typically use large amount of resources to restore the system. Let us take an Internet worm attack for example. Fig. 1 shows the spread of Internet worm named Code Red in 2001. It infected hundreds of thousands of machines and caused a huge damage (Berghel, 2001; Moore et al., 2002). The figure shows that the infection rate was low at the beginning. Then during a certain period the rate became very high. The number of infected machines increased quickly. Eventually, the infection stopped when either all the machines are infected or people learned how to defend the worm, and more and more machines were restored. The worm finally died out and all machines became normal again. Clearly, restoration of the system (here the system is all the machines that could be infected) started at a certain time and the effort leaded to final recovery of the whole system.

One of the key problems in the restoration procedure regards to the resource allocation strategies and the cost associated with, specifically, a minimal cost is desired. In this paper we model the cost as a total of service loss and resource expense that incurred during the restoration procedure. We present analyses on resource allocation towards achieving the minimal total cost. In the area of network security, cost has been used as a factor in analyzing how well protocols defend against denial of service attacks (Meadows, 2001), in suggesting investment strategies of security solutions (Gordon and Loeb, 2002), and in server replication strategies (Ray et al., 2006). Researchers also examined the components of cost and its calculation (Dubendorfer et al., 2004; Patterson, 2002). Worm spread has also been widely analyzed (Zou et al., 2002; Zou et al., 2005; Ma et al., 2005; Liljenstam et al., 2003). However, work in these directions have not presented research on the problem of resource allocation for restoration procedure in order to minimize the cost.

In this paper, we present cost analysis on resource allocation for the restoration procedure in the dynamic context of intrusion tolerant services during both the attacking and recovering (may last after a system was totally compromised) activities. We focus ourselves on abstract systems instead of studying a particular attacking event like Code Red worm. A mapping from the model presented in Zou et al., (2002) for Code Red worm to our model will be presented as an example. Generally, our problems are formulated for heterogeneous systems. We then present detailed analysis based on its special case: homogeneous systems. In our study, a system is comprised of a large number of machines (nodes) which are classified based on their restoration properties, e.g., recovery speed and restoration cost. In a heterogeneous system, machines have different restoration properties and different restoration costs; while in a homogeneous system, all machines have the same restoration property, so each incurs the same restoration cost. The owner of the system has limited resource. When a system is attacked, machines in the system are compromised one after another. In the worst case, all machines are compromised and provide no service. During the time, the owner also recovers compromised machines.

We investigate the achievable minimal total cost and corresponding resource allocation strategy for different situations. The key parameters that influence the cost are the speeds of compromising and recovering, namely, compromise rate v and restoration rate u. These two rates demonstrate various properties and interplay differently. In this research, we include both constant rates and time-variant rates in terms of the speed of compromising and recovering. Further, we consider the fact that the restoration rate is constrained by the resource allocated. The relationship can be either linear or obeying *the law of diminishing marginal utility* (Baumol and Blinder, 2004). We analyze all these cases. We model the total cost as a sum of service loss and resource expense. In lacking of closed form solutions, we present numerical results showing impact of various system parameters, e.g, the compromise rate, the initial system damage percentage, etc., on the critical conditions for a successful system restoration, and on the achievable minimal cost. The analysis and the results presented in the paper sheds a light on optimal usage of resources in combating network security breaches.

The rest of the paper is organized as follows. Section 2 briefly reviews related work. Section 3 describes the system model and the cost model. Section 4 presents analysis based on time-invariable properties of both compromise rate and restoration rate. Section 5 gives analysis based on time-variant properties of both rates. We map our analysis to the spread of the Internet worm Code Red. Numerical results are given in Section 6. Section 7 concludes the paper.

2. Related work

This work relates to many research fields including Internet worm research, system/service reliability and fault tolerance, system recovery and cost analysis. In the Internet worm research area, a lot of work has been presented. They mainly focus on one or several of the following topics: modeling the spread of Internet worms (Chen et al., 2003; Zou et al., 2002); worm detection (Rohloff and Basar, 2005; Zou et al., 2005); exploring new types of worms (Chen and Ji, 2005; Ma et al., 2005); developing worm defense techniques (Antonatos et al., 2005; Castaneda et al., 2004); and simulating worm spread and defense techniques (Liljenstam et al., 2003; Wagner et al., 2003). These work have presented in depth insights for understanding worm propagation and defense strategies as well as simulation tools. But system restoration procedure is not a major issue in these studies.

When system failures are concerned, research goes in two directions, one investigates the causes of the failures, the other builds resilience in the presences of failures. The causes for computer system failures was studied in Gray (1986), with a discovery that the main source for the failures is the operators, accounting for 42% errors; and software fault comes next, with 25% in total. The paper also introduces techniques to achieve software fault-tolerant, including process-pairs, defensive programming, etc. Similarly, Internet service is studied in Oppenheimer et al. (2003). The largest cause for Internet services failure is operation errors, with network failure comes second. The paper introduces a concept called *Time To Repair*—the time from when the problem is detected to when the service is restored to its previous service level. The *Time To Repair* has been used to study many services. In one case, the average time to repair the back-end server failures is 14 hours. The paper also provides techniques to mitigate failures, for examples, component isolation and proactive restart. In relating to our study, the *Time To Repair* shows similar importance as the total time of recovery in characterizing a system status. However, in both existing work, failures caused by security attacks, such as intrusion and denial of service, are not considered.

Along the other direction, researchers have proposed the concept of *Recovery Oriented Computing* (Patterson et al., 2002). This is based on the philosophy of living with failures instead of avoiding them, given the fact that even the most robust system could encounter failures. The work concentrates on *Mean Time to Repair (MTTR)* rather than *Mean Time to Failure (MTTF)*. The goal is to reduce recovery time and hence, the total cost of ownership. To achieve this goal, various research tasks are conducted, for example, system-wide support for un-do (Brown, 2003), integrated diagnostic support (Chen et al., 2002), and dependability benchmarking (Brown et al., 2004). Different from these work, our paper focuses on optimal resource allocation strategies in the recovery stage.

Currently, the work of recovery from a compromised system is performed mostly manually and is time-consuming. In this regard, the cost of human resources dominates the cost of computing resources. Researchers are working on designing automated intrusion recovery system (Goel et al., 2005). The system Taser introduced in Goel et al. (2005) is able to selectively recover file system after an intrusion is detected. It reverts the effects of operations performed by processes affected by the intrusion and preserves operations of legitimate processes. The success of this work will greatly reduce the expense in the restoration procedure we study. But our cost analysis considers both the service loss and resource expense and looks for the critical point that achieves the minimum cost. Given the reduced expense, the owner of the system could allocate more resource for restoration. We expect the system can be restored quicker and at a lower minimum cost.

In relating to cost analysis, many researchers have used cost as a valuable metric. In Meadows (2001), a cost based framework is used to evaluate a protocol's ability of defending against denial of service attack. In Gordon and Loeb (2002), the authors studies the optimal amount of investment on security solutions in order to protect a system. The system consists of components with different vulnerabilities. The results suggest that the system owner should not focus her investment on high vulnerable components since they might be extremely expensive to protect, rather she should invest on moderate vulnerable components. To defend against junk emails, the authors of Dwork and Naor (1993) propose to impose cost to email senders by forcing them to compute some middle-hard functions. Spamers who send huge amount of junk mails will be deterred. The authors of Ray et al. (2006) use cost-benefit analysis to define the robustness of a fault tolerant system. This robustness is defined as the minimum of possible values of the sum of the cost for compromising the system's components and the benefit of the remaining components.

Models for computing the cost of Internet service interruption were proposed in Dubendorfer et al. (2004); Patterson (2002). In Dubendorfer et al. (2004), the authors point out that the cost of Internet interruption consists of the following four parts: downtime loss which includes productivity loss (employees cannot get their job done) and revenue loss (lost transactions of customers); disaster recovery (the cost of recovery); liability (customers ask for compensation payments); customer loss (customers leave because of dissatisfaction). In Patterson (2002), the author gave a formula to calculate the cost of downtime. The calculation takes into consideration of *employee costs per hour*, *fraction employees affected by outage*,

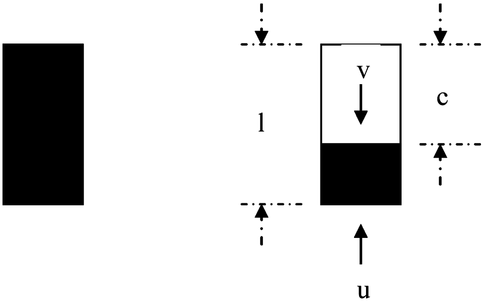


Fig. 2 Normal (left) and partially compromised system (right)

average income per hour and*fraction income affected by outage*. These results directly relate to our work. In our paper, we consider the costs incurred during the period of recovery, which map to the downtime loss and disaster recovery in Dubendorfer et al. (2004). We also use a general *cost index* as a base in all the analysis. The calculation method in Patterson (2002) provides a way to supply the cost index with real monetary value. On the other hand, all these work do not study the resource allocation problem for minimizing the cost.

3. The system model

When a system is in a restoration procedure, the state of a system is decided by the rates of two opposite parties: the compromise rate v of the attacker and the restoration rate u of the owner. If the compromise rate v of the attacker is larger than the restoration rate u of the owner, more and more nodes in the system will be compromised. On the contrary, if restoration rate u is larger, increasing number of nodes will turn back to normal. The system is illustrated in Fig. 2 as a rectangle, where the shaded area represents the uncompromised part of the system, i.e., the service is still available. Particularly, the left rectangle in the figure is a normal system and the right one is a partially compromised system. In Fig. 2, l is the full service ability of the system, for example, the total number of nodes in the system; c is the portion of the system that has been compromised, e.g., the number of infected nodes. The attacker and the owner compete with each other in order to gain full control over the system. The rate of compromise v is decided by the attacker. But the owner can adjust her restoration rate u which in turn is constrained by the amount of resource that she allocates, for example, budget, or manpower. In this system model, the compromise rate v could be constant or time-variant; the restoration rate u could also be constant or time-variant.

We identify two types of cost in the restoration procedure. The first type is a service *loss* cost C_1. It comes from the fact that the compromised system can only provide a degraded service to its clients. The second type is a restoration *expense* cost C_2. It comes from the fact that the system owner must utilize all possible resources she possesses to put the system back to work. These include manpower, investment on new security software and hardware, the cost of recourse to security companies, etc. The total cost C is the sum of the loss and the expense: $C = C_1 + C_2$. To avoid ambiguous in the units of the costs, we use a notion of *cost index* in our analysis. The *service loss* and *restoration expense* should have different ways to convert to the unified *cost index*. But it is not our intension to find detailed calculation in this study.

The total cost is affected by the two closely related components. If the system owner consumes more resources, that is, increases the expense C_2, the system will be restored faster and the loss C_1 will be smaller. If, on the contrary, the system owner consumes less resources, that is, the expense C_2 is small, the system will be restored slower and the loss C_1 will be large. Both C_1 and C_2 are impacted by u, v and other system parameters. Complexities come from many aspects: compromise rate v could be constant or time-varying, the usage of resources is not necessarily contributing to the restoration linearly, or the rate of restoration u could also be constant or time-varying.

In our analysis, we will use a continuous model to approximate the discrete number of computers compromised, given that the accuracy is achievable when the system contains a large number of computers. Such assumption is common in worm spread research, for example, in the modelling of Code Red worm (Zou et al., 2002). We also assume that resource can be spent at arbitrary granularity and thus is regarded as a continuous variable. A good approximation is achievable if the amount of resource is large. Otherwise, once the optimal allocation is found in continuous case, a brute force search in the neighborhood will give optimal or near optimal integer solution.

4. Models for constant rates

In this section we study the case when both compromise rate v and restoration rate u are constant over time. However, the restoration rate is constrained by the resources allocated, either linearly or obeying *the law of diminishing marginal utility*. In the following, we present the basic models for constant rates first (Subsection 4.1). We then analyze the cases of linear relation and the law of diminishing marginal utility subsequently in Subsections 4.2 and 4.3.

4.1. General models

The basic models derived here are for constant rates of both compromise and restoration. Consider a heterogeneous system that consists of n homogeneous subsystems. To simplify our analysis, we assume the resource allocation is static. That is, if the restoration task on one subsystem finishes first, the resources allocated to this subsystem for restoration will not be reallocated to another not yet fully restored system. Because different subsystems have different cost and restoration properties, compromise rate and restoration rate are different from subsystem to subsystem. For example, the compromise rate v will be different for different subsystems due to the different security levels. Given the n homogeneous subsystems, let v_i and u_i, $i = 1, ..., n$ be the compromise rates and restoration rates for each subsystem respectively. We assume that the owner has enough resources for each sub-system, so that $u_i > v_i, i = 1, ..., n$ holds. This is necessary for successful restorations.

Consider a homogeneous subsystem i. We assume the system state illustrated in the right side of Fig. 2 is the time that the system is detected compromised. We define this time as time 0. Corresponding c and l in Fig. 2 for the subsystem is c_i and l_i. The restoration rate is decided by the amount of resources the owner deploys. Let x_i be the resource allocation rate. Restoration rate u_i is thus a function of x_i. We denote it as $u_i(x_i)$. Also let the maximum loss to be m_i per time unit which occurs when the system is totally compromised and no longer be able to provide any service. We define the per time unit loss as *loss rate*. When the system is only partially compromised, the loss rate will not reach the maximum rate m_i since it continues to provide service in a degraded level. Suppose the loss rate at any time is proportional to the percentage of system compromised. Thus at time 0, the loss rate is $\frac{c_i}{l_i}m_i$.

It is easy to see that the loss rate at time t is:

$$\frac{c_i - (u_i(x_i) - v_i)t}{l_i} m_i$$

The restoration procedure needs following time to finish:

$$\frac{c_i}{u_i(x_i) - v_i} \tag{1}$$

So the loss in this period is

$$\begin{aligned} C_{1i} &= \int_0^{\frac{c_i}{u_i(x_i)-v_i}} \frac{c_i - (u_i(x_i) - v_i)t}{l_i} m_i \, dt \\ &= \frac{m_i c_i^2}{2l_i(u_i(x_i) - v_i)} \end{aligned} \tag{2}$$

Next we calculate the expense for restoring the subsystem i. Given the total time required for restoration (1), the expense during this period is

$$C_{2i} = \frac{c_i}{u_i(x_i) - v_i} x_i \tag{3}$$

Thus the total cost incurred during the period of restoration for subsystem i is

$$\begin{aligned} C_i &= C_{1i} + C_{2i} \\ &= \frac{m_i c_i^2}{2l_i(u_i(x_i) - v_i)} + \frac{c_i}{u_i(x_i) - v_i} x_i \end{aligned} \tag{4}$$

Now we define the problem of allocating resources in a heterogeneous system that achieves the minimum total cost as:

minimize

$$f(x_1, ..., x_n) = \sum_{i=1}^{n} \left(\frac{m_i c_i^2}{2l_i(u_i(x_i) - v_i)} + \frac{c_i}{u_i(x_i) - v_i} x_i \right) \tag{5}$$

subject to

$$\sum_{i=1}^{n} \frac{c_i}{u_i(x_i) - v_i} x_i \le Q, \quad u_i(x_i) > v_i, \quad i = 1, ..., n$$

Where Q is the upper bound of owner's resource.

With (5) as the basic total cost model, we calculate the minimum cost in the next two subsections for different relations between the restoration rate and the resource in need, namely, linear or non-linear (*the law of diminishing marginal utility*).

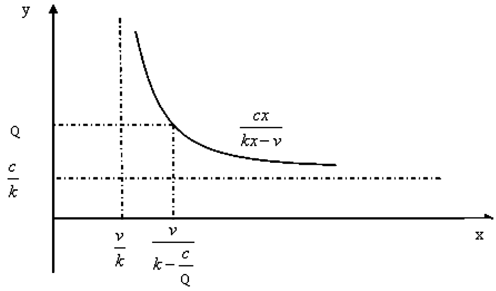


Fig. 3 constraints $\frac{c}{kx-v}x \leq Q$ and $kx > v$.

4.2. Linear relation

In this section, we study the case where the restoration rate increases linearly as the amount of resources allocated increases. For each subsystem i, we define the following relation where k is a constant.

$$u_i(x_i) = kx_i$$

Thus the minimum cost problem for restoring the heterogeneous system can be formulated as

$$\text{minimize}$$

$$f(x_1, ..., x_n) = \sum_{i=1}^{n} \left(\frac{m_i c_i^2}{2l_i(kx_i - v_i)} + \frac{c_i}{kx_i - v_i} x_i \right) \tag{6}$$

$$\text{subject to}$$

$$\sum_{i=1}^{n} \frac{c_i}{kx_i - v_i} x_i \leq Q, \tag{7}$$

$$kx_i > v_i, \quad i = 1, ..., n$$

4.2.1. Homogeneous system

To demonstrate how to minimize the cost, we take a homogeneous system as an example. In a homogeneous system, the problem becomes:

$$\text{minimize}$$

$$f(x) = \frac{mc^2}{2l(kx - v)} + \frac{c}{kx - v} x \tag{8}$$

$$\text{subject to}$$

$$\frac{c}{kx - v} x \leq Q, \tag{9}$$

$$kx > v \tag{10}$$

Constraints are shown in Fig. 3. If $Q \leq \frac{c}{k}$, the first constraint (9) can not be satisfied. This means that either there is not enough resource (Q is too small) or too many machines have been compromised before the owner starts to restore (c is too large). In both cases, the owner will not be able to restore her system. If $Q > \frac{c}{k}$, the solution for the constraints is $x \geq \frac{v}{k-c/Q}$. This means that to make the total expense ($\frac{c}{kx-v}x$) not exceed the resource limit Q, the per time unit allocated resource must be greater or equal to $\frac{v}{k-c/Q}$. Note this constraint overwrites (10). It states that the restoration rate needs to be fast enough to ensure overall recovery. The derivative of $f(x)$ is

$$f'(x) = \frac{-cv - k^2}{(kx - v)^2} < 0$$

Thus $f(x)$ monotonically decreases as x increases. This verifies that to make the total cost minimum, the larger the x when $x \geq \frac{v}{k-c/Q}$, the better.

The same conclusion can be reached alternatively. Considering the loss part $\frac{mc^2}{2l(kx-v)}$, apparently when x is greater, the loss is less because the time needed for restoration is less. For the expense part $h(x) = \frac{c}{kx-v}x$, since its derivative $h'(x) = \frac{-cv}{(kx-v)^2} < 0$, we have the observation that the greater the x, the smaller the expense. In summary, when x increases, both loss and expense decreases, leading to the same conclusion, i.e., the larger the x, the smaller the total cost. The results can be generalized to the heterogeneous system: for each subsystem i, as x_i increases, both loss and expense decreases. Also, the larger the x_i, the easier the constraints (7) are satisfied.

4.2.2. Off-line restoration

The above analysis is given for the systems that keep online during the period of restoration. Here we discuss an alternative situation where the system could be disconnected entirely and then be restored. Obviously, this scheme violates our intrusion tolerant assumption. However, it could happen in real life and thus worth discussion. We compute the costs for the situation.

Consider a homogeneous subsystem i. The time to restore this system is $c_i/u_i(x_i)$. Since the system is disconnected, the loss rate remains as m_i. So the total loss is $m_i c_i/u_i(x_i) = m_i c_i/(kx_i)$. The total expense is $(c_i/u_i(x_i))x_i = c_i/k$. Notice that no matter how restoration rate changes, the total expense is a constant. So the total cost for restoring a homogeneous system is $m_i c_i/(kx_i) + c_i/k$.

Thus in a heterogeneous system, to find the minimum cost, we need to solve

minimize

$$f(x_1, ..., x_n) = \sum_{i=1}^{n} \left(\frac{m_i c_i}{kx_i} + c_i/k \right)$$

subject to

$$\sum_{i=1}^{n} \frac{c_i}{k} \leq Q$$

The constraint poses a hard limit on resource for the owner to complete the restoration with a success. When the owner has enough resource, increasing x_i leads to reduced restoration time and hence the deduced loss. On the other hand, no matter how x_i changes, the expense part $\sum_{i=1}^{n} c_i/k$ is a fixed value. So, to minimize the total cost, the owner should let resource allocation rate for each subsystem x_i as large as possible.

4.3. The law of diminishing marginal utility

In this section we define the nonlinear relationship between the resource usage and the restoration rate. The relationship between the restoration rate and the amount of resources allocated should satisfy *the law of diminishing marginal utility* (Baumol and Blinder, 2004). That is, the restoration rate increases as the allocated resources increases but at an increasing reduced pace. We first define and discuss the minimum cost problem for the heterogeneous system scenario, then we extend our discussion to the homogeneous system to obtain more direct results.

The law of diminishing marginal utility is well used in economics. It states that as the individual's consumption increases, the marginal utility of each additional unit declines. This Law applies to our restoration and allocation problem nicely. In our cases, the Law says that as the amount of allocated resources increases, the restoration rate increases but the amount of this increase declines. According to the definition, the law of diminishing marginal utility requires that

$$\frac{du(x)}{dx} > 0, \frac{d^2u(x)}{dx^2} < 0 \tag{11}$$

This leads to the following restoration function:

$$u(x) = kx^{\mu}, \; 0 < \mu < 1 \tag{12}$$

4.3.1. Heterogeneous system

In a heterogeneous system, we have the restoration functions for each subsystems:

$$u_i(x_i) = kx_i^{\mu}, \;\; 0 < \mu < 1, \;\; i = 1, ..., n$$

The problem of how to allocate resources so that the total cost is minimum can be formulated as:

minimize

$$f(x_1, ..., x_n) = \sum_{i=1}^{n} \left(\frac{m_i c_i^2}{2l_i(kx_i^{\mu} - v_i)} + \frac{c_i}{kx_i^{\mu} - v_i} x_i \right) \tag{13}$$

subject to

$$\sum_{i=1}^{n} \frac{c_i}{kx_i^{\mu} - v_i} x_i \le Q, \;\; kx_i^{\mu} > v_i, \;\; i = 1, ..., n$$

This problem can be solved using Kuhn-Tucker conditions (Kuhn and Tucker, 1951). For this purpose, we transform it to a maximum problem:

maximize

$$g(x_1, ..., x_n) = \sum_{i=1}^{n} \left(-\frac{m_i c_i^2}{2l_i(kx_i^{\mu} - v_i)} - \frac{c_i}{kx_i^{\mu} - v_i} x_i \right) \tag{14}$$

subject to

$$\sum_{i=1}^{n} \frac{c_i}{kx_i^{\mu} - v_i} x_i \le Q, \quad kx_i^{\mu} > v_i, \quad i = 1, ..., n$$

Let

$$\ell = g(x_1, ..., x_n) + \lambda \left(Q - \sum_{i=1}^{n} \frac{c_i}{kx_i^{\mu} - v_i} x_i \right)$$

where λ is Lagrange multiplier. Then the Kuhn-Tucker conditions, which are necessary for finding a maximum, are:

$$\frac{\partial \ell}{\partial x_i} \le 0, \quad i = 1, ..., n$$

$$x_i \ge 0, \quad i = 1, ..., n$$

$$x_i \frac{\partial \ell}{\partial x_i} = 0, \quad i = 1, ..., n \tag{15}$$

$$\sum_{i=1}^{n} \frac{c_i}{kx_i^{\mu} - v_i} x_i \le Q, \tag{16}$$

$$\lambda \ge 0,$$

$$\lambda \left(Q - \sum_{i=1}^{n} \frac{c_i}{kx_i^{\mu} - v_i} x_i \right) = 0. \tag{17}$$

In our scenario, all $x_i > 0, i = 1, ..., n$. Thus (15) leads to $\frac{\partial \ell}{\partial x_i} = 0$. So

$$x_i^{\mu} + \frac{m_i c_i \mu}{2l_i(1 + \lambda)(\mu - 1)} x_i^{\mu - 1} + \frac{v_i}{k(\mu - 1)} = 0, \; i = 1, ..., n \tag{18}$$

In addition, in order to satisfy (17) we must have either $\lambda = 0$ or $\sum_{i=1}^{n} \frac{c_i}{kx_i^{\mu} - v_i} x_i = Q$.
Case i - $\lambda = 0$. When $\lambda = 0$, we have

$$x_i^{\mu} + \frac{m_i c_i \mu}{2l_i(\mu - 1)} x_i^{\mu - 1} + \frac{v_i}{k(\mu - 1)} = 0, \; i = 1, ..., n$$

Let the solution for each equation be $x_i^0, i = 1, ..., n$. If x_i^0 satisfies (16) and $kx_i^{\mu} > v_i$, the set $\{x_i^0, i = 1, ..., n\}$ is a candidate for the global maximum.

Case ii - $\sum_{i=1}^{n} \frac{c_i}{kx_i^{\mu}-v_i} x_i = Q$. Suppose the solution for (18) is $\{x_i^1(\lambda), i = 1, ..., n\}$ (Notice that λ is a variable). Put each $\{x_i^1(\lambda)\}$ into $\sum_{i=1}^{n} \frac{c_i}{kx_i^{\mu}-v_i} x_i = Q$, we can solve for λ (may have several solutions). If the constraint $\lambda \geq 0$ is satisfied, we can use the λ in $\{x_i^1(\lambda)\}$ to calculate $\{x_i^1\}$, $i = 1, ..., n$. If $\{x_i^1\}$ satisfies constraint $kx_i^{\mu} > v_i$, the set $\{x_i^1, i = 1, ..., n\}$ is a candidate for the global maximum.

So the global maximum is the maximum of $f(x_1^0, ..., x_n^0)$ and $f(x_1^1, ..., x_n^1)$. As we know, this maximum is the minimum for our original minimum problem (13).

4.3.2. Homogeneous system

The homogeneous system, as a special case of the heterogeneous system, allows us to simplify the problem definition and to extend the above general discussions to concrete formulas as results. First of all, the problem of allocating resources to minimize the total cost is expressed as below:

minimize

$$f(x) = \frac{mc^2}{2l(kx^{\mu} - v)} + \frac{c}{kx^{\mu} - v} x \tag{19}$$

subject to

$$\frac{c}{kx^{\mu} - v} x \leq Q, \tag{20}$$

$$kx^{\mu} > v. \tag{21}$$

We then transform the problem description to the equivalent maximum problem:

maximize

$$g(x) = -\frac{mc^2}{2l(kx^{\mu} - v)} - \frac{c}{kx^{\mu} - v} x \tag{22}$$

subject to

$$\tfrac{c}{kx^{\mu}-v} x \leq Q, \quad kx^{\mu} > v.$$

Let

$$\begin{aligned} \ell &= g(x) + \lambda \left(Q - \frac{c}{kx^{\mu} - v} x \right) \\ &= -\frac{mc^2}{2l(kx^{\mu} - v)} - \frac{c}{kx^{\mu} - v} x + \lambda \left(Q - \frac{c}{kx^{\mu} - v} x \right) \\ &= -\frac{mc^2/2l}{kx^{\mu} - v} - \frac{c(1+\lambda)x}{kx^{\mu} - v} + \lambda Q \end{aligned}$$

where λ is Lagrange multiplier. Then the Kuhn-Tucker conditions are:

$$\frac{\partial \ell}{\partial x} \leq 0, \quad x \geq 0, \quad x \frac{\partial \ell}{\partial x} = 0 \tag{23}$$

$$\frac{c}{kx^{\mu}-v}x \leq Q, \ \ \lambda \geq 0, \ \ \lambda\left(Q-\frac{c}{kx^{\mu}-v}x\right)=0 \tag{24}$$

Since $x > 0$ in our problem, constraints in (23) lead to $\frac{\partial \ell}{\partial x} = 0$. That is:

$$\frac{ck(1+\lambda)(\mu-1)x^{\mu}+\frac{mc^2}{2l}k\mu x^{\mu-1}+cv(1+\lambda)}{(kx^{\mu}-v)^2}=0$$

So

$$x^{\mu}+\frac{mc\mu}{2l(1+\lambda)(\mu-1)}x^{\mu-1}+\frac{v}{k(\mu-1)}=0 \tag{25}$$

From constraints in (24) we must have either $\lambda = 0$ (constrained by $\frac{c}{kx^{\mu}-v}x \leq Q$), or $\frac{c}{kx^{\mu}-v}x = Q$ (constrained by $\lambda \leq 0$). These two conditions lead to our following analysis.

Case i $-\lambda = 0$. When $\lambda = 0$, (25) becomes

$$x^{\mu}+\frac{mc\mu}{2l(\mu-1)}x^{\mu-1}+\frac{v}{k(\mu-1)}=0$$

To ease the discussion, we rewrite the above equation to:

$$x^{\mu}=\frac{mc\mu}{2l(1-\mu)}x^{\mu-1}+\frac{v}{k(1-\mu)} \tag{26}$$

Fig. 4 shows the corresponding curves for the left and the right side of the equation (26). The intersection of these two curves is the solution. Given $0 < \mu < 1$, x^{μ} monotonically increases and $\frac{mc\mu}{2l(1-\mu)}x^{\mu-1}+\frac{v}{k(1-\mu)}$ decreases. So there is one and only one cross point which we denote as x_0. If x_0 satisfies $\frac{c}{kx_0^{\mu}-v}x_0 \leq Q$ and $kx_0^{\mu} > v$, x_0 is a candidate for the global maximum.

Case ii - $\frac{c}{kx^{\mu}-v}x = Q$. This condition can be rewritten as:

$$\frac{c}{Q}x = kx^{\mu}-v \tag{27}$$

The solution for this condition is shown in Fig. 5. Depending on the values of coefficients, line $\frac{c}{Q}x$ may have two, one or zero intersections with curve $kx^{\mu}-v$. We discuss each case below.

If the two curves intersect, we claim that there must be two cross points, unless these two points converge to one (the case when the two curves are tangent, we will discuss this next). The reason is that $\lim_{x\to\infty}\frac{kx^{\mu}-v}{\frac{c}{Q}x}=0$, when $0 < \mu < 1$. Thus, as long as there is the left intersection of the two curves, straight line $\frac{c}{Q}x$ will eventually be larger than curve $kx^{\mu}-v$, leading to the right intersection. With some k and μ, the right point may come very slow. We denote these two intersections as x_1 and x_2 ($x_1 = x_2$ when they merge to one). We then put x_1, x_2 to (25). From (25) and x_1, we find λ_1. If $\lambda_1 \leq 0$, x_1 is a candidate for the global maximum. Similarly, from (25) and x_2, we find λ_2. If $\lambda_2 \leq 0$, x_2 is also a candidate for the global maximum.

Combined with the previous discussions, the global maximum will be the maximum of $g(x_0)$, $g(x_1)$, and $g(x_2)$. As we know, the maximum for our transformed problem (22) is the

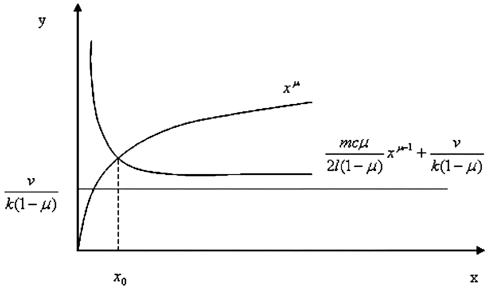


Fig. 4 Solution for $x^{\mu} = \frac{mc\mu}{2l(1-\mu)}x^{\mu-1} + \frac{v}{k(1-\mu)}$

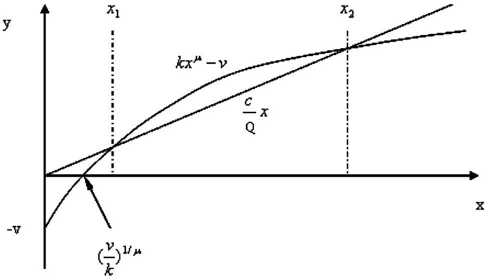


Fig. 5 Solution for $\frac{c}{Q}x = kx^{\mu} - v$

minimum for our original minimum problem (19). We will use numerical methods to obtain solutions for the minimum cost problem.

The case when the two curves are tangent allows us to obtain critical observations with regards to the boundary conditions. When this happens, we have

$$\frac{c}{Q} = k\mu x^{\mu-1}$$

Together with (27), we obtain the boundary condition for satisfying the constraint (20):

$$\left(\frac{c}{Qk\mu}\right)^{\frac{\mu}{\mu-1}} = \frac{v}{d-k\mu} \tag{28}$$

Condition (28) leads to important results, such as the minimum resource required for a success restoration given v and c, or the maximum number of machines c allowed to be compromised before the owner has to start restoration given v and Q. More results will be given in Section 6.

The last case is that the two curves have no intersections, either due to the fact that $\frac{c}{Q}$ is too large or v is too large (Fig. 5). $\frac{c}{Q}$ being too large implies either there is not enough resource or too many computers have been compromised before the owner begin to restore. In both cases, the system can not be restored. v being too large means the compromise rate is too high, system cannot be restored either.

5. Model for time-variant rates

In this section we study the case when both compromise rate v and restoration rate u are functions varying with time. The spread of Internet worm is an example of such case. In

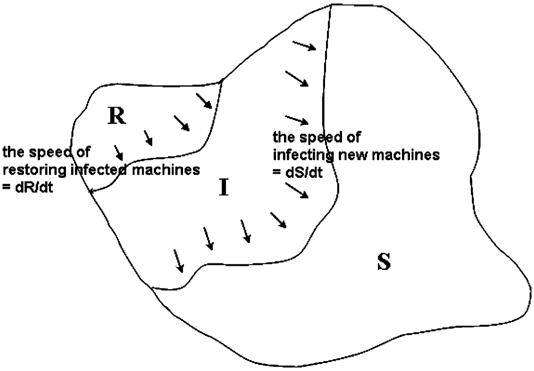

R
I
S
the speed of restoring infected machines = dR/dt
the speed of infecting new machines = dS/dt

Fig. 6 $-\frac{dI}{dt}$, which equals to $\frac{dS}{dt} + \frac{dR}{dt}$, is the net rate that corresponds to the previous $u - v$.

this section, we base our cost analysis on the worm spread model. Since worms are usually developed with a specific system and its particular vulnerability in mind, we treat the system as homogeneous. In the analysis, we define the relation between the restoration rate and the resource allocation rate to obey *the law of diminishing marginal utility.*

5.1. Worm spread model

Internet worm spread has been considered as a phenomenon very similar to epidemic in biology area. It is thus modelled using SIR epidemic model in Chen et al. (2003); Zou et al. (2002). The SIR epidemic model (Brauer and Castiloo-Chavez, 2001) is described below:

$$\frac{dS}{dt} = -\beta S(t)I(t) \tag{29}$$

$$\frac{dI}{dt} = \beta S(t)I(t) - \alpha I(t) \tag{30}$$

$$\frac{dR}{dt} = \alpha I(t) \tag{31}$$

Where, for the warm spread, $S(t)$ is the number of machines that are not yet infected by worm; $I(t)$ is the number of machines that has been infected and infectious; $R(t)$ is the number of machines that has been restored and will not be infected again. The parameters β and α characterize the propagation of the worm, i.e., β is the infection rate, and α is the removal rate of infectives. The model is based on the following assumptions (Brauer and Castiloo-Chavez, 2001):

1. An average infective makes contact sufficient to transmit infection with βN others per unit time, where N represents total population size: $N = S(t) + I(t) + R(t)$.
2. A fraction α of infectives leave the infective class per unit time.

Mapping to our study, where u is the restoration rate and v is the attack rate, then $u - v$ is the net rate of the system transforming between the state of totally normal and fully compromised. Thus, $-\frac{dI}{dt}$ in epidemic model has its counterpart $u - v$ in our model. This is illustrated in Fig. 6. $\frac{dS}{dt}$ has physical meaning in SIR as the increment or decrement of the number of susceptible machines in one unit time; these machines are infected and join the I group. So the rate of worm compromise, or the rate of infecting new machines, is $\frac{dS}{dt}$. The meaning of $\frac{dR}{dt}$ is the increment or decrement of the number of restored machines in one unit time;

these machines comes from the I group. So the rate of restoration, or the rate of converting those infected machines back to normal, is $\frac{dR}{dt}$. The net rate is thus $u - v = |\frac{dR}{dt}| - |\frac{dS}{dt}|$. Notice that $\frac{dR}{dt} = \alpha I(t)$ is always positive and $\frac{dS}{dt} = -\beta S(t)I(t)$ is always negative, we have $u - v = |\frac{dR}{dt}| - |\frac{dS}{dt}| = \frac{dR}{dt} + \frac{dS}{dt}$, which, according to the SIR model, is exactly $-\frac{dI}{dt}$.

5.2. Cost analysis

With the mappings to SIR, the loss rate at time t is (recall from Fig. 2):

$$\frac{c - \int_0^t (u - v)\,dt}{l} m$$

Suppose the epidemic starts at time 0, lasts for τ time until the network is fully normal again, the loss due to service degradation is

$$\begin{aligned} C_1 &= \int_0^\tau \frac{c - \int_0^t (u - v)\,dt}{l} m\,dt \\ &= \int_0^\tau \frac{c - \int_0^t (-\frac{dI}{dt})\,dt}{l} m\,dt \\ &= \int_0^\tau \frac{c + I(t) - I(0)}{l} m\,dt \end{aligned}$$

In the formula, $c = 0$ and $I(0) = 0$, because almost no machine is compromised or infective at the very beginning of the warm spread. Also l equals to N by definition, because N is the total population. Thus, we have the simplified loss equation as following:

$$C_1 = \int_0^\tau \frac{I(t)}{N} m\,dt \tag{32}$$

Now let us calculate the expense. The recovery rate $u = \frac{dR}{dt}$ is time variant, i.e.,

$$u(t) = \frac{dR}{dt} = kx^\mu(t)$$

thus,

$$x(t) = \left(\frac{1}{k}\frac{dR}{dt}\right)^{1/\mu}$$

The total expense is

$$C_2 = \int_0^\tau x(t)\,dt$$

Plug in $\frac{dR}{dt} = \alpha I(t)$ (from SIR model equation (31)), the expense becomes:

$$C_2 = \int_0^{\tau} \left(\frac{\alpha}{k} I(t)\right)^{1/\mu} dt \tag{33}$$

The total cost then, incurred from the time epidemic outbreaks to the time the network finally goes back to normal, is

$$\begin{aligned} C &= C_1 + C_2 \\ &= \int_0^{\tau} \left[\frac{I(t)}{N} m + \left(\frac{\alpha}{k} I(t)\right)^{1/\mu}\right] dt \end{aligned} \tag{34}$$

The cost is affected by many parameters. We will present numerical results in the next section.

6. Numerical solutions

In previous sections we have introduced our cost models based on theoretical analysis. The analyses show that the optimal solutions are impacted by many parameters and no closed forms can be immediately obtained for many cases. In this section we provide numerical analyses for the homogenous system to study the boundary conditions for various system statuses and the interplay of various system parameters towards the minimum cost. All the numerical solutions are obtained through Maple (MapleSoft, 2004).

6.1. Constant rates

The analysis presented in Section 4.3 considers the situation where compromise rate v and restoration rate u are constant over time, but the restoration rate is constrained by the resources usage under *the law of diminishing marginal utility*. The minimum cost is affected by various parameters, including c, the portion of the system compromised at time $t = 0$, and the system's total resource Q. For the purpose of easy illustration, we use and present integer numbers as cost indexes in the results. These numbers allow us to show the relations among the variables in question and the scale of changing trends. The specific system parameters are: the network is composed of $l = 1,000$ nodes; at the time that the owner is alerted of the attack, the system has $c = 50$ nodes compromised; the maximum loss rate is $m = 10,000$ when the system is totally compromised; the maximum resource the owner has is $Q = 100,000$; and the compromise rate is $v = 100$. Many of parameters are varied for the different results we show. But when not varied, they take the above default values. Parameters used by *the law of diminishing marginal utility* are picked at $k = 3$ and $\mu = 1/2$.

6.1.1. Boundary condition

For a system under an attack, i.e., v and c are known, the minimum resource needed for a successful recovery is given by equation (28). On the other hand, if a system is constrained by its total resource, the latest time the restoration must start can also be calculated through equation (28). We show numerically how the constraints affect the objectives, using some of the parameters listed above. The obtained relation among the parameters is $c = \frac{9Q}{4v}$.

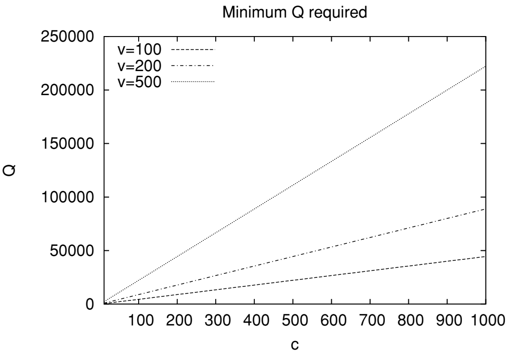


Fig. 7 Minimum resource required for a successful restoration

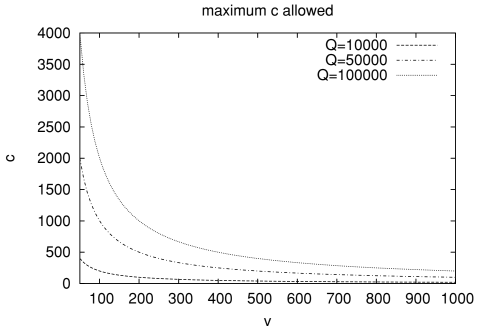


Fig. 8 Maximum number of machines allowed to be compromised before a successful restoration

Fig. 7 shows the minimum resources required for a successful restoration with different values of c and v. It is clear that the overall resource required increases linearly with the time that the restoration starts. And also, the faster (larger v) the compromising speed, the larger the overall resource needed, and a faster pace of increasing. On the other hand, when a system has a limited total resource, Fig. 8 gives the maximum number of machines (c) allowed to be compromised before restoration as a function of the compromised rate. It shows c decreases quickly (more than linear) when the compromise rate increases. This suggests that with resource constraints, the stronger the attack, the earlier the restoration must start.

6.1.2. Minimum cost

Fig. 9 and Fig. 10 give results relating to the minimum cost. Fig. 9 shows how the minimum costs are influenced by the attacking status c and v. It reports that larger c(x axis), i.e., later start of restoration, results in higher minimum cost (y axis). Also when the attack is strong, i.e., the compromise rate v is large, the owner has to spend much more resources. The increasing in the minimum cost is faster when v is larger. Fig. 10 demonstrates how the resource allocation rates that achieve the minimum costs (denoted as x^*) are affected by c and v. Again, late start in recovery (large c) increases the optimal resource allocation rate, i.e., the larger portion of the system being compromised at the time that the owner starts restoration, the higher resource spending rate. The figure shows that the influence from attacking rate v is greater than c. The figure also shows that a double in attacking rate (from $v = 100$ to $v = 200$) results in more than double in the resource allocation rate. A further examination

Fig. 9 influence of restoration start time on the minimum cost

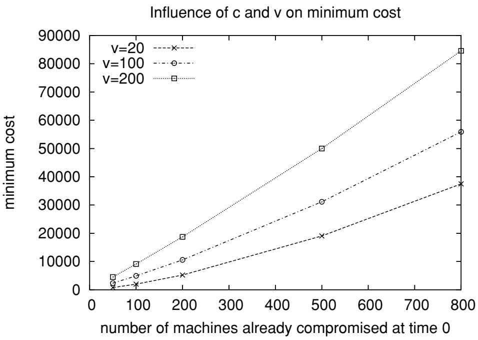
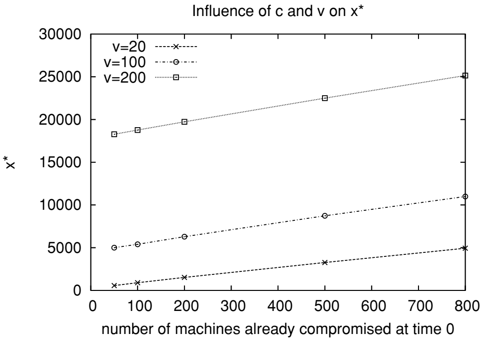


Fig. 10 x* for different start time



on equation (19) results in the following form,

$$f(x) = \left(m\frac{c}{2l} + x\right)\frac{c}{kx^{\mu} - v}$$

which suggests that when x^* is large, loss is insignificant compared to expense, since $\frac{c}{2l}$ is usually small. The two figures also indicate that x^* is large compared to the minimum cost. This indicates that the owner should allocate as much resource per unit time as possible to shorten the recovery time so to achieve minimum cost in total.

6.2. Time-variant rates

The cost for systems with worm-spread-based rates is given in (34). It is impacted by parameters α and β (implicitly, through $I(t)$). Recall that, in the model, α represents restoration effort and β represents compromise rate. We set other parameters according to the statistics from the research on Code Red worm (Moore et al., 2002). The parameters are:

$$N = 300,000, \alpha = \frac{1}{3}, \beta = 6 \times 10^{-6}$$

Thus, this is a system consisting of 300, 000 machines, with an average period of 3 time units of staying in the infective state for those infected machines, and a rate of $6 \times 10^{-6} * 300000 = 1.8$ machines per time unit for a single infected machine to infect others. Note α or β may change in our figures. We also change the loss rate m (in a scale of billion per time unit, denoted as b/u in the figures) to demonstrate its influence on the cost.

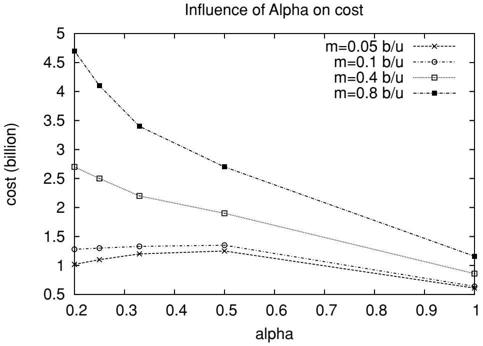


Fig. 11 The influence of alpha on cost

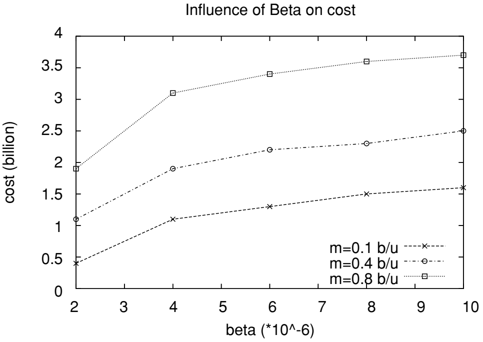


Fig. 12 The influence of beta on cost

Fig. 11 shows the decreasing trends of the cost when α increases. Increasing α means that the average time a machine stayed in the infective state decreases. This comes from the facts that more resources are allocated to restore the system, and the restoration time is shortened. The net effect is the reduction in the total cost. The figure also shows that when m is low (0.1 or 0.05 billion per time unit), the cost is less influenced by the time period that a machine remains as infective.

Fig. 12 reports the influence from β. A larger β means the worm spread faster. To keep the average time a machine staying in infective the same ($\alpha = 1/3$), a larger amount of resources must be allocated. So when β increases, the cost monotonically increases. The figure also shows that the larger the m, the higher the cost.

7. Conclusions

In this paper, we provide analysis on the cost incurred in resource allocation when restoring compromised systems. The cost includes the loss due to the degraded service and the expense due to the resources spent in restoration. Our problems are formulated for heterogeneous systems. We then present detailed analysis based on its specially case: homogeneous systems. We show how to achieve minimal cost by reasonably allocating limited available resources. We study constant and time-variant rates for compromising and restoration procedures. We also consider linear and non-linear relation between restoration rate and resource usage. We have used our model to analyze the cost of worm spread, making our contribution to the area of Internet worm study. The numerical results show impact from various system parameters, e.g, the compromise rate, the initial system damage percentage, etc.. They also show the critical conditions for a successful system restoration, and the achievable minimum cost. The analysis and the results presented in the paper sheds a light on optimal usage of resources in combating network security breaches.

Acknowledgment The authors would like to thank the anonymous reviewers for their invaluable comments.

References

Antonatos S, Akritidis P, Markatos EP, Anagnostakis KG (2005) Defending against hitlist worms using network address space randomization. In WORM '05: Proceedings of the 2005 ACM workshop on Rapid malcode, New York, NY, USA, ACM Press, 30–40

Baumol WJ, Blinder AS (2004) Economics: Principles and Policy. South-Western College Pub

Berghel H (2001) The code red worm. Commun. ACM 44(12):15–19

Brauer F, Castiloo-Chavez C (2001) Mathematical Models in Population Biology and Epidemiology. Springer-Verlag, New York

Brown A (2003) A recovery-oriented approach to dependable services: Repairing past errors with system-wide undo. Technical Report UCB//CSD-04-1304, UC Berkeley Computer Science, December

Brown A, Chung L, Kakes W, Ling C, and Patterson D (2004) Experience with evaluating human-assisted recovery processes. In Proceedings of the 2004 International Conference on Dependable Systems and Networks

Castaneda F, Sezer EC, Xu J (2004) Worm vs. worm: preliminary study of an active counter-attack mechanism. In WORM '04: Proceedings of the 2004 ACM workshop on Rapid malcode, New York, NY, USA, ACM Press, 83–93

Chen M, Kiciman E, Fratkin E, Brewer E, Fox A (2002) Pinpoint: Problem determination in large, dynamic, internet services. In Proceedings of the International Conference on Dependable Systems and Networks (IPDS Track)

Chen Z, Gao L, Kwiat K (2003) Modeling the spread of active worms. In Proceedings of INFOCOM 2003, IEEE, 1890–1900.

Chen Z, Ji C (2005) A self-learning worm using importance scanning. In WORM '05: Proceedings of the 2005 ACM workshop on Rapid malcode, New York, NY, USA, ACM Press, 22–29

Dubendorfer T, Wagner A, Plattner B (2004) An economic damage model for large-scale internet attacks. In Proceedings of the 13th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises (WET ICE 2004)

Dwork C, Naor M (1993) Pricing via processing or combatting junk mail. In CRYPTO '92: Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology, London, UK, Springer-Verlag, 139–147

Goel A, Po K, Farhadi K, Li Z, de Lara E (2005) The taser intrusion recovery system. In SOSP '05: Proceedings of the twentieth ACM symposium on Operating systems principles, New York, NY, USA, ACM, Press, 163–176.

Gordon LA, Loeb MP (2002) The economics of information security investment. ACM Transactions on Information and System Security, 5(4):438–457

Gray J (1986) Why do computers stop and what can be done about it? In Proceedings of the 5th Symposium on Reliablity in Distributed Software and Database Systems

Kuhn HW, Tucker AW (1951) Nonlinear programming. In Proceedings of the Second Berkeley Symposium on Mathematical Statistics and Probability, University of California, Press, 481–492

Lala JH (2003) Introduction. In Proceedings of the Foundations of Intrusion Tolerant Systems (OASIS'03), IEEE, x–xix.

Liljenstam M, Nicol DM, Berk VH, Gray RS (2003) Simulating realistic network worm traffic for worm warning system design and testing. In WORM '03: Proceedings of the 2003 ACM workshop on Rapid malcode, New York, NY, USA, ACM Press, 24–33.

Ma J, Voelker GM, Savage S (2005) Self-stopping worms. In WORM '05: Proceedings of the 2005 ACM workshop on Rapid malcode, New York, NY, USA ACM Press, 12–21.

MapleSoft. (2004) Maple. In http://www.maplesoft.com

Meadows C (2001) A cost-based framework for analysis of denial of service in networks. Journal of Computer Security, 9(1–2):143–164

Moore D, Shannon C, Brown J (2002) Code-red: a case study on the spread and victims of an internet worm. In Proceedings of the ACM SIGCOMM/USENIX Internet Measurement Workshop, ACM, 273–284.

Oppenheimer D, Ganapathi A, Patterson D (2003) Why do internet services fail, and what can be done about it? In Proceedings of the 4th USENIX Symposium on Internet Technologies and Systems (USITS '03)

Patterson D (2002) A simple way to estimate the cost of downtime. In Proceedings of LISA '02: Sixteenth Systems Administration Conference, 185–188

Patterson D, Brown A, Broadwell P, Candea G, Chen M, Cutler J, Enriquez P, Fox A, Kiciman E, Merzbacher M, Oppenheimer D, Sastry N, Tetzlaff W, Traupman J, Treuhaft N (2002) Recovery-oriented computing (roc): Motivation, definition, techniques, and case studies. Technical Report UCB//CSD-02-1175, UC Berkeley Computer Science

Ray S, Zheng Q, Hong X, Kwiat K (2006) Integrity function—a framework for server replication and placement in adversarial environment. In submitted to IEEE Transactions on Parallel and Distributed Systems

Rohloff K, Basar T (2005) The detection of rcs worm epidemics. In WORM '05: Proceedings of the 2005 ACM workshop on Rapid malcode, New York, NY, USA, ACM Press, 81–86

Verissimo PE, Neves NF, Correia MP (2003) Intrusion tolerant architectures: Concepts and design. Architecting Dependable System, Lecture Notes in Computer Science, 2677(44):3–36

Wagner A, Dubendorfer T, Plattner B, Hiestand R (2003) Experiences with worm propagation simulations. In WORM '03: Proceedings of the 2003 ACM workshop on Rapid malcode, New York, NY, USA, ACM Press, 34–41

Zou C, Gong W, Towsley D (2002) Code red worm propagation modeling and analysis. In Proceedings of the 9th ACM conference on Computer and communications security, ACM, 138–147

Zou CC, Gong W, Towsley D, Gao L (2005) The monitoring and early detection of internet worms. IEEE/ACM Trans. Netw. 13(5):961–974