SANDIA REPORT

SAND2010-7046
Unlimited Release
Printed September 2010

Modeling Attacker-Defender Interactions in Information Networks

Michael J. Collins

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online ordering: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2010-7046
Unlimited Release
Printed September 2010

Modeling Attacker-Defender Interactions in Information Networks

Michael J. Collins
Dept. 5635 Analytics and Cryptography
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185
mjcolli@sandia.gov

Abstract

The simplest conceptual model of cybersecurity implicitly views attackers and defenders as acting in isolation from one another: an attacker seeks to penetrate or disrupt a system that has been protected to a given level, while a defender attempts to thwart particular attacks. Such a model also views all non-malicious parties as having the same goal of preventing all attacks. But in fact, attackers and defenders are interacting parts of the same system, and different defenders have their own individual interests: defenders may be willing to accept some risk of successful attack if the cost of defense is too high. We have used game theory to develop models of how non-cooperative but non-malicious players in a network interact when there is a substantial cost associated with effective defensive measures. Although game theory has been applied in this area before, we have introduced some novel aspects of player behavior in our work, including

- A model of how players attempt to avoid the costs of defense and force others to assume these costs
- A model of how players interact when the cost of defending one node can be shared by other nodes
- A model of the incentives for a defender to choose less expensive, but less effective, defensive actions.

Acknowledgment

Thanks to Lyndon Pierson for suggesting this line of research, to Randall Laviolette and David Dumas for implementing a simulation of the iterated Aspnes Model, to Jared Saia for helpful discussions about game theory, and to Rolf Riesen for developing and maintaining the Latex sand report class.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Our general framework for analyzing the behavior of non-cooperative nodes in a network under attack is a game-theoretic model of inoculation against viral infection introduced by Aspnes et al. [1], which we brief y describe (for terminology and concepts of game theory, see [4]). Each "player" in this game is a node in an undirected connected graph $\mathcal{G}$ with n nodes. Nodes represent network hosts that might become infected, while edges represent direct communication links through which a virus might spread. Each node has two possible pure strategies: either do nothing, or inoculate itself (i.e. install anti-viral protection). After the nodes have made their choices, an attacker selects one node uniformly at random to infect. Infection then propagates through the graph; a non-inoculated node becomes infected if any of its neighbors are infected.

Let I be the set of inoculated nodes. These inoculated nodes are in effect removed from the graph, leaving a (possibly disconnected) graph $\mathcal{G}_I$. Let v be the initial node selected by the attacker. If v is inoculated, then v is not infected and thus no nodes become infected. Otherwise, the infected nodes are precisely the nodes in the connected component containing v. Henceforth "component" will always mean a connected component of $\mathcal{G}_I$.

Let C be the cost of inoculation, and L be the loss suffered by an infected node. Thus if a node u inoculates, its cost is simply C; otherwise its cost is $L\frac{k_u}{n}$, where k_u is the size of u's component, since $\frac{k_u}{n}$ is the probability of this component recieving the initial infection. Given these costs, the *threshold* size for a component is $t = n\frac{C}{L}$: the set I gives a Nash equilibrium if and only if both of these conditins hold:

- each component has size at most t
- de-inoculating any node $j \in I$ (i.e. putting it and all its adjacent edges back in the graph) creates a component of size at least t

In other words, if a component is larger than t, then each node in that component would be better off paying the cost C to inoculate; if an inouculated node could rejoin the graph and be in a component smaller than t, it would be better off not paying the cost of inoculation. Since the properties of the game are determined by the ratio C/L, we will sometimes normailze and assume $L = 1$.

We def ne the *social cost* of I to be the sum of individual costs. In general there can be many equilibria with widely varying social costs, and it might be impossible to attain the minimum

social cost at equilibrium. The *price of Anarchy*, def ned as the ratio of the maximum social cost of a Nash equilibrium to the minimum social cost attainable by any set of strategies, can be as large as $n/2$. Our overall goal will be to f nd ways to improve social cost, subject to the restriction that the behavior of self-interested parties will always lead to an equilibrium. In the next two chapters we consider ways to achieve this goal by modifying the original game.

Chapter 2

Iterated Aspnes Model

2.1 Dynamic Inoculation

We can reach a pure-strategy equilibrium in the inouclation game via the following process. Begin with no inoculated nodes. At each time step, if there exists a node which could reduce its cost by changing its strategy (i.e. if we are not at equilibrium), choose one such node at random and change its strategy. This process will f nd an equilibrium in no more than $2n$ steps [1].

We now consider what happens if we allow nodes to keep switching their strategies after an equilibrim has been reached. As before, we begin at time 0 with no inoculated nodes. Now at each time step, exactly one *dissatisfied* node (chosen at random) can change its status. We def ne dissatisfaction as follows: If the current conf guration I is not an equilibrium, then a node is dissatisf ed if it can increase its utility by changing its status; otherwise (i.e. at equilibrium) a node v is dissatisf ed if there exists some other equilibrium in which v's status is different and v's cost is lower. In our case this means that at equilibrium, all inoculated nodes (and no others) are dissatisf ed. An inoculated node v might choose to de-inoculate and join a large component; this temporarily increases v's cost, but now all members of v's connected component are dissatisf ed, and v hopes that some other members of the component will bear the cost of inoculation to create a small component.

2.1.1 Analysis of the Star

Consider the "star graph" $G = K_{1,n-1}$, and call the central node z. As before let t be the threshold component size. It is easily seen that the social optimum is to inoculate just z. The simplicity and symmetry of this graph makes it possible to fully analyze its behavior, which is summarized in f gure 2.1. We begin in a state with no inoculated nodes. With probability $1 - t/n$, z is inoculated before reaching equilibrium. Now we are in a state with z inoculated and at least t leaves uninoculated. At this point all inoculated leaves will de-inoculate, eventually reaching the (socially optimal) equilibrium point at which only z is inoculated. Then z will de-inoculate, returning the graph to the initial state of no inoculations.

On the other hand, from the no-inoculation state, with probability t/n we reach a (sub-optimal) equilibrium in which z is part of a component of size t (i.e. $n - t$ leaves inoculate consecutively

in the first $n-t$ steps). Now one leaf node will de-inoculate, taking the graph out of equilibrium. Then, with probability $t/(t+1)$, a leaf inoculates, looping back to the prior state. Otherwise z inoculates; now just as before the graph must go to the socially optimal state and back to the starting state.

Thus we really have a Markov process with two states corresponding to the two equilibria. Initially we enter the preferable state with probability $1-t/n$, and once in it remain there with probability $1-t/n$. Once we have entered the less desirable state, we remain there with probability $t/(t+1)$.

For fixed costs C and L, the expected duration of the sub-optimal equilibrium tends to infinity as $n \to \infty$. However, for fixed n, as $\frac{C}{L} \to 0$ the fraction of time spent in the socially optimal equilibria approaches 1.

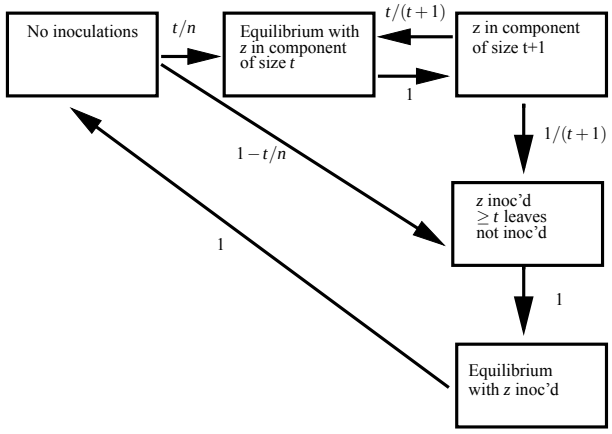

Figure 2.1. Markov process on a Star Graph

2.1.2 Taking Turns

Suppose we have two nodes a, b such that we are in equilibrium if exactly one of them inoculates. Each node would prefer to have the other one inoculated, but each node would rather inoculate than have neither inoculated. An obvious way to share this cost would be to "take turns", alternating between the two equilibrium states. Such *iterated* games have been well-studied. Given an original two-player game, we can assume that the game will be played infinitely many times, with future payoffs exponentially discounted by a factor of δ: i.e. if p_i is a players (original) payoff in the ith iteration, then his total payoff for the entire game is $\sum_i p_i \delta^i$. Now a player's strategy must specify what to do at each iteration, and his choice of action at the ith iteration can be an arbitrary function of all previous actions by both players.

The simplest strategy in this case is "oblivious alteration"; player a inoculates at even-numbered

time steps regardless of b's actions, and b inouculates at odd-numbered steps regardless of a's actions. This is easily seen to be an equilibrium; either player would inccrease its cost by playing any other strategy. Another natural strategy is the so-called "grim" strategy; alternate until the other player fails to inoculate when he should, then never inoculate. It is well-known that in the famous "prisoners dilemma", such a strategy creates an equilibrium in which both players always cooperate for mutual benef t. The idea is that the "threat" of responding to a non-cooperative action gives each player incentive to cooperate. However, in the inoculation game, both players playing the grim strategy is is *not* an equilibrium; even after player a deviates from taking turns, player b is still better off incoulating when a does not. So in this game there is no need for a threat of sub-optimal behavior to maintain equilibrium.

2.2 Adding Propagation Delay

We modify the Aspnes model by considering that once a virus infects an uninoculated node u, it takes time for the virus to spread to other nodes in its connected component. The cost of future infections is exponentially discounted by a factor of ϕ. Let λ be the exponential rate at which infection spreads; i.e. in the r^{th} time step after initial infection, λ^r new nodes get infected. The cost of being infected is normalized to 1. Let the size of u's component be $s = 1+\lambda+\lambda^2+\cdots\lambda^k$; then a virus will need k time steps to propagate through the entire component. We call k the *diameter* of the component. Now u's expected cost is

$$\frac{s}{n}\sum_{d=0}^{k}\phi^d\frac{\lambda^d}{s} = \frac{1}{n}\sum_{d=0}^{k}(\phi\lambda)^d$$

since the infection starts in u's component with probability $\frac{s}{n}$, in which case u is infected at time d with probability $\frac{\lambda^d}{s}$. We can interpret ϕ^d as the probability that the virus is still alive at time d; in other words at each time step, the virus is globally destroyed with probability $1-\phi$ (because a patch is deployed, the network conf guration changes, et cetera). The sum is

$$\frac{(\phi\lambda)^{k+1}-1}{n(\phi\lambda-1)} \approx \frac{(\phi\lambda)^{k+1}}{n(\phi\lambda-1)}$$

assuming $\phi\lambda > 1$ and k large. Now we consider the threshold value of s, i.e. the component size at which the expected cost of infection equals the cost C of inoculation. This will happen when

$$k = \frac{\log_\lambda(Cn(\phi\lambda-1))}{1+\log_\lambda\phi} - 1$$

which gives a component size of

$$\frac{(Cn(\phi\lambda-1))^{1/(1+\log_\lambda\phi)}}{\lambda-1} \tag{2.2.1}$$

(since $s \approx \lambda^{k+1}/(\lambda-1)$). Note that with $\phi = 1$ the break-even point is $s = Cn$, just as in the original Aspnes inoculation model: this is exactly as it should be, since with $\phi = 1$ it does not

matter when u gets infected. On the other hand, consider what happens as $\phi \to \lambda^{-1}$. Then the expected cost approaches k/n, and the break-even point is $k = Cn$, giving a component size of

$$\frac{\lambda^{Cn+1} - 1}{\lambda - 1}$$

assuming of course that this is less than n, which will happen if $C < d^{-1}$ where d is the diameter of the entire graph.

Is there any logical connection between ϕ and λ? If $\phi = \lambda^{-r}$ then (2.2.1) becomes

$$\frac{(Cn(\lambda^{1-r} - 1))^{1/(1-r)}}{\lambda - 1}$$

with

$$k = \frac{\log_\lambda (Cn(\lambda^{1-r} - 1))}{1 - r} - 1$$

although we do not know if we can assign some simple intuitive meaning to the parameter r.

Finally, consider what happens with $\phi < \lambda^{-1}$. Still assuming that k is large, the expected cost is

$$\frac{(\phi\lambda)^{k+1} - 1}{n(\phi\lambda - 1)} \approx \frac{1}{n(1 - \phi\lambda)}$$

and the break-even point is

$$\frac{1}{n(1 - \phi\lambda)} = C\,.$$

If C is larger than this, then no node has any incentive to inoculate.

Chapter 3

Aspnes Model with Cost Sharing

A crucial feature of the Aspnes model is that one node can benef t from another node's decision to inoculate. We have considered what happens when some nodes seek to avoid the cost of inoculation and force others to inoculate, and how nodes can agree to share costs by taking turns. We now consider a model in which one node can pay part of the cost of another node's inoculation. Such *cost-sharing* models of network games have been studied by several authors ([2, 3]), but this idea has not, so far as we are aware, been applied to the Aspnes model previously. Formally, we have the same situation as before, but now the strategy of player i is a vector $a^i = (a^i_1 \ldots a^i_n)$, where a^i_j is the contribution made by node i to the inoculation of node j. Node j will be inoculated if and only if

$$\sum_{1 \le i \le n} a^i_j \ge C \, .$$

The individual cost for node i is

$$\sum_{1 \le j \le n} a^i_j + L\frac{k_i}{n}$$

where as before k_i is the size of the component κ_i containing node i (or zero if i is inoculated). We have the following

Theorem 3.0.1. *Let $\sigma = (a^1, a^2, \ldots a^n)$ be an equilibrium in the cost-sharing Aspnes game. Then*

1. *$\sum_j a^i_j \le C$ for all nodes i*
2. *$\sum_i a^i_j$ is either 0 or C for all nodes j*
3. *Each $k_i \le n\frac{C}{L}$*
4. *If j is inoculated but de-inoculating j would not increase the size of κ_i, then $a^i_j = 0$*

Also, the cost-sharing game and the original game have the same minimum social cost.

Proof. Any node i violating (1) could reduce its cost by inoculating itself (i.e. setting $a^i_i = C$) and paying nothing for any other node. If (2) does not hold for some j, then all nodes i with $a^i_j \ne 0$ could reduce their cost by reducing their contributions to j without changing j's inoculation status. If (3) does not hold then any node in κ_i could reduce its cost by inoculating itself. Any node i

violating (4) could reduce its cost by setting $a^i_j = 0$, since this would not increase i's probability of infection; we call this condition *locality*. Note in particular this implies that, if i is inoculated, then i does not contribute to the cost of inoculating any node other than (perhaps) itself.

Since the cost-sharing game has a strictly larger set of strategies, its minimum social cost can be no greater. On the other hand, let $\sigma = (a^1, a^2, \ldots a^n)$ be a strategy vector minimizing social cost in the cost-sharing game (note σ need not be an equilibrium), and let I be the resulting set of inoculated nodes. Since cost is minimized, the total amount spent on inoculations is exactly $C|I|$. Thus we can obtain the same social cost in the original game by inoculating all the nodes in I and no others. □

Although cost-sharing cannot improve the social optimum, it can create better equilibria. Given an inoculation set I which is not an original equilibrium, but which is in some sense "socially desireable" (i.e. has lower social cost), we wish to know if there exists a cost-sharing equilibrium which incoulates I.

Given a graph $\mathscr{G}$, let $u \in I$ where there exists a cost-sharing equilibrium that innoculates I. Suppose there are k components $\tau_i, \ldots \tau_k$ of $\mathscr{G}_I$ connected to to u, with sizes $t_i, \ldots t_k$. Let $t = \sum_i t_i$ and let $\hat{t}_j = t - t_j$. Since we are at equilibrium, u's contribution to its own inoculation must be no greater than $\frac{L}{n}(t+1)$. Therefore there must be some node v in some τ_i whose contribution to u is at least

$$\frac{C - L(t+1)/n}{t} = \frac{C}{t} - \frac{L}{n}\frac{t+1}{t}$$

since, because of locality, no other nodes can contribute to u. However, since we are at equilibrium, this contribution must also be no greater than $\frac{L}{n}(\hat{t}_i + 1)$. Combining these inequalities yields

$$\frac{nC}{L} \leq t(\hat{t}_i + 2 + 1/t)$$

thus we have the necessary condition

$$t \geq \sqrt{\frac{nC}{L}} - 1 \,. \tag{3.0.1}$$

Any component created by de-inoculating a node in I must be at least this large. Note that if this bound could be attained it would give an order-of-magnitude reduction in component sizes: without cost sharing, any component created by de-inoculation must have size linear in n. In fact an improvement of this magnitude can be attained, which we can see by letting $\mathscr{G}$ be a cycle on n vertices. We normalize to $C = 1$ and consider what happens as n becomes large with L f xed. Without cost-sharing, an equilibrim will have L inoculated nodes breaking the path into components of size n/L, for a social cost of

$$L + \frac{L}{n} L(n/L)^2 = L + n \,. \tag{3.0.2}$$

However, with $\sqrt{nL}$ innoculated nodes and components of size $\sqrt{n/L}$ we would have a social cost of

$$\sqrt{nL} + \frac{L}{n}\sqrt{n/L}(n/\sqrt{nL})^2 = 2\sqrt{nL} \,. \tag{3.0.3}$$

This social cost can be attained at equilibrium by cost sharing. If each non-inoculated node shares equally in the cost of protecting the nearest inoculated node, its cost is $\sqrt{L/n}$; by not making this contribution, a node would create a component of size $2\sqrt{n/L}$, incurring a larger cost of $\frac{2L}{n}\sqrt{n/L} = 2\sqrt{L/n}$.

Chapter 4

An Attacker-Defender Game

One of the classic two-player games studied in economic applications of Game Theory is the "inspection game" [4]. In this game the f rst player is an employee, the second player the employer. The employer must decide wether to incur some cost in order to inspect and verify that the worker has done his job and produced some value; the worker must decide whether to work (earning his wage minus the 'cost' of working) or to shirk (and risk earning nothing if the employer has decided to inspect). In that game we can compute the 'optimal' wage which maximizes the employer's expected payoff at equilibrium.

In the network-security version of this game we have an attacker who must decide whether to risk stealing an asset of value v, where the cost of getting caught is p; and a defender who must decide whether to scan the network (at a cost of s) to detect attack and protect the asset. Normalizing to $v = 1$, we have the payoff matrix

$$\begin{pmatrix} -1,1 & 0,0 \\ -s,-p & -s,0 \end{pmatrix} \tag{4.0.1}$$

Let α be the probability of scanning, and let β be the probability of attacking. Clearly if $s > 1$ the equilibrium solution is "never scan, always attack"; otherwise we have equilibrium at

$$\alpha = \frac{1}{1+p} \tag{4.0.2}$$

$$\beta = s \tag{4.0.3}$$

At equilibrium the attacker's (expected) payoff is zero and the defender's expected cost is s. Note that in this model there is no incentive for the defender to "invest" in a more intensive scan (i.e. higher s) which will impose a stronger deterrent (i.e. higher p) on the attacker; if s and p increase, the attacker's strategy will respond so as to keep the defender's expected loss constant. Thus this model is biased toward using a cheaper, less effective scan but employing it more often.

Now we consider a more general problem in which a scan will succeed with probability ϕ. The payoff matrix becomes

$$\begin{pmatrix} -1,1 & 0,0 \\ -s-(1-\phi),1-\phi-\phi p & -s,0 \end{pmatrix} \tag{4.0.4}$$

which gives an equilibrium of

$$\alpha = \frac{1}{\phi(1+p)} \tag{4.0.5}$$

$$\beta = \frac{s}{\phi} \tag{4.0.6}$$

The attacker's payoff is still zero and the defender's expected cost is $-\beta = -s/\phi$. Now we assume that there is some functional relationship between s and ϕ such that we can buy a better scan (larger ϕ) by increasing s. Now the optimal choice of s depends on the exact function which connects these two parameters; the defender will choose the scanning technique to minimize s/ϕ. Note that again, the defender's expectation does not depend on the attacker's risk p, and there is no incentive for the defender to invest in increasing p.

In a network with many nodes, we can interpret these probabilities as the fraction of nodes that are scanned and the fraction of nodes that are attacked at a given time.

References

[1] James Aspnes, Kevin L. Chang, and Aleksandr Yampolskiy. Inoculation strategies for victims of viruses and the sum-of-squares partition problem. *J. Comput. Syst. Sci*, 72(6):1077–1093, 2006.

[2] Maria-Florina Balcan, Avrim Blum, and Yishay Mansour. Circumventing the price of anarchy: Leading dynamics to good behavior, January 2010.

[3] Moses Charikar, Howard J. Karloff, Claire Mathieu, Joseph Naor, and Michael E. Saks. Online multicast with egalitarian cost sharing. In Friedhelm Meyer auf der Heide and Nir Shavit, editors, *SPAA*, pages 70–76. ACM, 2008.

[4] Drew Fudenberg and Jean Tirole. *Game Theory*. MIT press, 1991.

[5] Tamara K. Locke. Guide to preparing SAND reports. Technical report SAND98-0730, Sandia National Laboratories, Albuquerque, New Mexico 87185 and Livermore, California 94550, May 1998.

Sandia National Laboratories