Analysis of risks and costs in intruder detection with Markov Decision Processes

Jorma Jormakka

Department of Communications and Networking, Aalto University, Espoo, Finland

Sourangshu Ghosh

Department of Civil Engineering, Indian Institute of Technology Kharagpur, Kharagpur, West Bengal, India

Abstract

Let us assume that defence mechanisms are so strong that the average outcome of a hacking attack is unsuccessful. How to calculate the costs arising from false positives and false negatives in intruder detection? Is it better for the hacker to make fewer but more effective attacks rather than several but less effective attacks? How to calculate the difference between these alternative strategies?

Keywords: combinatorics, risk analysis, decision analysis.

1. Background

Markov Decision Process (MDPs) is stochastic control processes that are discrete in nature. These processes are extensively discussed first Bellman [1] and Howard [2]. They are very much used in modeling various optimization problems as they give a nice general framework to model the decision process particularly where there might be several random outcomes that can be controlled partly by the decision maker. One of those problems is security intrusion processes that are based on hacker decisions. Intrusion is growing concern today because of the apparent weakness of various information databases and systems due to attack by hackers which poses a major security threat. There has been much research in developing and designing fault-tolerant architectures which can prevent such intrusions [3]. The first major work on using statistical techniques to model this dates back to 1980 by Anderson who proposed for such a statistical intrusion detection system [4] and the statistical intrusion detection model proposed by Dening using n-gram and Markov chain data models [5]. Researchers are also using various other statistical machine learning processes such as by Markov chains [6,7,8], hidden Markov models [9]. In Recent days researchers are also starting to use models based on artificial immune systems(Machine Learning instance or Rule Based systems that are based and inspired by biological immune systems of vertebrates) [10,11,12,13].
As the other machine learning models MDPs are also widely used to make stochastic models to understand the intrusion processes [14,15,16,17]. These models assume that the state transition probabilities & costs and other such model parameters that are taken during each decision stage shall be controlled by the decision maker explicitly. The performances of such intrusion systems based upon MDPs are dependent on the rule which describes how the appropriate control actions are taken and implemented. The MDPs are able to apprehend the security reinstatement after doing a reset action like server rotation initiating [18] or recovery sequence [19] etc or by apprehending the possible temporarily interrupting of a task being carried out of a intrusion from a defend action like to kill a process that is vital and critical for the intrusion to continue[20]. In the next section we shall discuss the Markov Decision Process.

2. Introduction

Let us assume, that there are two kinds of connections: user connections arriving with the rate λ_u and finishing with the rate μ_u; and hacker connections arriving and finishing with the rates λ_h and μ_h, respectively. Let us make a discrete time stochastic process and let n denote the discrete time parameter. Accepting a hacker results to expenses: let the cost of accepting one hacker be ω_H. Detecting hackers also leads to expenses, as the security breach must be analysed. Let ω_A be the cost of analysing one hacker connection. Finally, rejecting a user connection also results to expenses as a loss of income or value of the connection. Let this cost be ω_B.

The goal is obtaining a formula for the variance of the cost, a scalar variable for cost describing the sum of all expenses, as is customary in the Markov Decision Theory, is not sufficient. Instead, in this modelling method the cost variable r appears as a state variable and the state of the system is a triplet (n,q,r). The probability of (n,q,r) is denoted by $s_{n,q,r}$ and the probabilities of a false positive and a false negative are denoted by p_{FP} and p_{FN} respectively.

2. Markov Decision Process (MDP) model

Let the total time in the model be finite, and let the finishing time T be divided into time slots of the size T/N, thus, the model has discrete time and let n be the time parameter. The possible transitions from

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 April 2021 doi:10.20944/preprints202104.0713.v1

(n,q,r) with their probabilities in a time unit are described as follows: (a check for free capacity is done before a check for a hacker)

- a hacker is accepted:
  $(n,q,r) \to (n+1, q+e_h, r+\omega_H)$ with probability
  $$\frac{T}{N} 1_{u \in R_q} \lambda_h p_{FN} , \qquad (1)$$
- a user is accepted: $(n,q,r) \to (n+1, q+e_u, r)$ with probability $\frac{T}{N} 1_{u \in R_q} \lambda_u (1-p_{FP})$,
- a hacker is noticed and rejected:
  $(n,q,r) \to (n+1, q, r+\omega_A)$ with probability
  $\frac{T}{N} 1_{u \in R_q} \lambda_h (1-p_{FN})$,
- a user is taken for a hacker and rejected:
  $(n,q,r) \to (n+1, q, r+\omega_B+\omega_A)$ with probability
  $\frac{T}{N} 1_{u \in R_q} \lambda_u p_{FP}$,
- the state does not change: $(n,q,r) \to (n+1, q, r)$ with probability
  $$1-\frac{T}{N}\left(\lambda_u + 1_{u \in R_q} \lambda_h + \sum_{j \in \{u,h\}} \mu_j q_j\right),$$
- congestion, a user is rejected:
  $(n,q,r) \to (n+1, q, r+\omega_B)$ with probability
  $\frac{T}{N}(1-1_{u \in R_q})\lambda_u$,
- a user finishes: $(n,q,r) \to (n+1, q-e_u, r)$ with probability $\frac{T}{N} \mu_u q_u$,
- a hacker finishes: $(n,q,r) \to (n+1, q-e_h, r)$ with probability $\frac{T}{N} \mu_h q_h$.

The backward transition probabilities
$$(n,q,r) \xrightarrow{p'_{n+1,q_j,r_j}} (n+1, q_j, r_j) \qquad (2)$$
sum to one: $1 = \sum p'_{n+1,q_j r_j}$. Notice, that there is no backward equation, that is
$$s_{n,q,r} \neq \sum p'_{n+1,q_j r_j} s_{n+1,q_j r_j} . \qquad (3)$$
An equation can be expressed only with forward transition probabilities from $(n-1, q', r')$ to (n,q,r) as a forward equation $s_{n+1,q,r} = \sum p_{n,q_j r_j} s_{n,q_j r_j}$. Then $1 \neq \sum p_{n,q_j r_j}$. The forward transition equation is obtained by inverting the backward transitions:

$$\begin{aligned} s_{n+1,q,r} &= s_{n,q,r} - \frac{T}{N}\left(\lambda_u + 1_{u \in R_q} \lambda_u + \sum_{j \in \{u,h\}} \mu_j q_j\right) s_{n,q,r} \\ &+ \frac{T}{N} 1_{u \notin R_q} \lambda_u s_{n,q,r-\omega_B} \\ &+ \frac{T}{N} 1_{u \in R_{q-e_u}} \lambda_u (1-p_{FP}) s_{n,q-e_u,r} \\ &+ \frac{T}{N} 1_{u \in R_q} \lambda_u p_{FP} s_{n,q,r-\omega_B-\omega_A} + \frac{T}{N} 1_{u \in R_q} \lambda_h (1-p_{FN}) s_{n,q,r-\omega_A} \\ &+ \frac{T}{N} 1_{u \in R_{q-e_h}} \lambda_h p_{FN} s_{n,q-e_h,r-\omega_H} + \frac{T}{N} \sum_{j \in \{u,h\}} \mu_j (q_j+1) s_{n,q+e_j,r} . \end{aligned} \qquad (4)$$

Let us define:
$\lambda'_u = \lambda_u (1-p_{FP})$, $\lambda'_h = \lambda_h p_{FN}$, $\omega_u = 0$, $\omega_h = \omega_H$.
Then $\lambda_u p_{FP} = \lambda_u - \lambda'_u$ and $\lambda_h (1-p_{FN}) = \lambda_h - \lambda'_h$.
Inserting to (4) gives

$$\begin{aligned} s_{n+1,q,r} &= s_{n,q,r} - \frac{T}{N} \sum_{j \in \{u,h\}} \mu_j q_j s_{n,q,r} - \frac{T}{N}(\lambda_u + \lambda_u) s_{n,q,r} \\ &+ \frac{T}{N}(\lambda_u - \lambda'_u) s_{n,q,r-\omega_B-\omega_A} \\ &+ \frac{T}{N}(\lambda_h - \lambda'_h) s_{n,q,r-\omega_A} + \frac{T}{N} \lambda'_u s_{n,q-e_u,r-\omega_u} \\ &+ \frac{T}{N} \lambda'_h s_{n,q-e_h,r-\omega_h} + \frac{T}{N} \sum_{j \in \{u,h\}} \mu_j (q_j+1) s_{n,q+e_j,r} . \end{aligned} \qquad (5)$$

We can derive the following result for $n \to t$, where t is a continuous time parameter. These results assume that in the initial state at $t=0$ the state probabilities q are in a stationary state and the total cost is zero.

Theorem 1. *Let us assume the attacker is using one effective attack causing cost ω_H if the attack goes unnoticed. The probability of the state q with cost r at the time t is*

$$s_{t,q,r} = A e^{-t(\lambda_u+\lambda_h)+t\lambda_u(1-p_{FP})} \prod_{j \in \{u,h\}} \frac{1}{q_j!}\left(\frac{\lambda'_j}{\mu_j}\right)^{q_j} \cdot \sum_{\substack{j_1=j_2=j_3=0 \\ r=\omega_H q_h + \sum_{k=1}^{3} \beta_k j_k}}^{\infty} \prod_{k=1}^{3}\left(\frac{1}{j_k!}(t\alpha_k)^{j_k}\right) \qquad (6)$$

where
$\alpha_1 = \lambda_h p_{FN}$, $\alpha_2 = \lambda_u p_{FP}$, $\alpha_3 = \lambda_h (1-p_{FN})$,
$\beta_1 = \omega_H$, $\beta_2 = \omega_A + \omega_B$, $\beta_3 = \omega_A$,
$\lambda'_u = \lambda_u (1-p_{FP})$, *and* $\lambda'_h = \lambda_h p_{FN}$.

Let us assume the attacker is using K less effective attacks, each causing cost $\omega_H K^{-1}$ if the attack goes unnoticed and each having the arrival rate λ_h. The corresponding probability is

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 April 2021 doi:10.20944/preprints202104.0713.v1

$$s_{t,q,r} = Ae^{-t\sum_i((\lambda_{u,i}+\lambda_{h,i})+t\lambda_{u,i}(1-p_{FP}))} \prod_{j\in\{u,h\}} \prod_{i\in I} \frac{1}{q_{j,i}!}\left(\frac{\lambda'_{j,i}}{\mu_{j,i}}\right)^{q_{j,i}}$$

$$\cdot \sum_{\substack{j_{1,i}=j_{2,i}=j_{3,i}=0 \\ r_i=\sum_i \omega_{H,i}q_{h,i}+\sum_{k=1}^{3}\beta_{k,i}j_{k,i}}}^{\infty} \prod_{k=1}^{3}\prod_{i\in I}\left(\frac{1}{j_{k,i}!}t^{j_{k,i}}\alpha_{k,i}^{j_{k,i}}\right) \quad (7)$$

where

$$\alpha_{1,i} = \lambda_{h,i}p_{FN},\ \alpha_{2,i} = \lambda_{u,i}p_{FP}$$

$$\alpha_{3,i} = \lambda_{h,i}(1-p_{FN}),$$

$$\beta_{1,i} = \omega_{H,i} = \frac{1}{K}\omega_{H1},\ \beta_{2,i} = \omega_A+\omega_B,\ \beta_{3,i} = \omega_A,$$

$$\lambda'_{u,i} = \lambda_{u,i}(1-p_{FP}),\ and\ \lambda'_{h,i} = \lambda_{h,i}p_{FN}.$$

Proof: If a solution satisfying the recursion equation and the initial values is found it is the solution because recursion equations have a unique solution from given initial values. We select trial values and then check that the state equation obtained by summing over r is in a stationary state and that the cost is zero in the initial state. Let us look for a solution of the form

$$s_{n,q,r} = \prod_{j\in\{u,h\}}\frac{1}{q_j!}\left(\frac{\lambda'_j}{\mu_j}\right)^{q_j} s_{n,r-\sum_{j\in\{u,h\}}\omega_j q_j} = s_q s_{n,r-c},$$

where $c = \sum_{j\in\{u,h\}}\omega_j q_j$. (8)

This solution form satisfies

$$\mu_j q_j s_{n,q,r} = \lambda'_j s_{n,q-e_j,r-\omega_j} \text{ and} \quad (9)$$

$$\mu_j(q_j+1)s_{n,q+e_j,r} = \lambda'_j s_{n,q,r-\omega_j} \text{ for } j\in\{u,h\}.$$

Let us notice, that (9) means that the state equation is in steady state, i.e. summing over r we have the detailed balance equations in this case. Inserting this attempt yields an equation where q appears as a parameter and we can divide both sides by s_q. The remaining equation is (10)

$$s_{n+1,r-c} = s_{n,r-c} + \frac{T}{N}\sum_{j\in\{u,h\}}\lambda'_j s_{n,r-c-\omega_j} - \frac{T}{N}\sum_{j\in\{u,h\}}\lambda_j s_{n,r-c}$$

$$+\frac{T}{N}(\lambda_u-\lambda'_u)s_{n,r-c-\omega_B-\omega_A} + \frac{T}{N}(\lambda_h-\lambda'_h)s_{n,r-c-\omega_A}.$$

This is easily solved with the generating function

$$G_n(v) = \sum_{r=0}^{\infty}s_{n,q,r}v^r = s_q\sum_{r=0}^{\infty}s_{n,r-c}v^r, \quad (11)$$

where $s_{n,q,r} = 0$ if $r<0$. Thus

$$G_{n+1}(v) = G_n(v)(1-\frac{T}{N}\sum_j\lambda_j + \frac{T}{N}\sum_j\lambda'_j v^{\omega_j}$$

$$+\frac{T}{N}(\lambda_u-\lambda'_u)v^{\omega_A+\omega_B} + \frac{T}{N}(\lambda_h-\lambda'_h)v^{\omega_A}). \quad (12)$$

Let us write the equation as

$$G_{n+1}(v) = G_n(v)\left(1+\frac{T}{N}\sum_{k\in I}g_k(v)\right). \quad (13)$$

Then by assigning $t/n = T/N$ and letting $N\to\infty$

$$G_t(v) = G_0(v)\lim_{n\to\infty}\left(1+\frac{t}{n}\sum_{k\in I}g_k(v)\right)^n \quad (14)$$

$$= G_0(v)\lim_{n\to\infty}\prod_{k\in I}\left(1+\frac{t}{n}g_k(v)\right)^n = G_0(v)e^{t\sum_{k\in I}g_k(v)}$$

The term $G_0(v)$ can be taken as a constant. There are only three $g_k(v)$, which depend on v:

$$g_0(v) = -(\lambda_u+\lambda_h) \quad (15)$$

$$g_1(v) = \lambda'_u v^{\omega_u} = \lambda_u(1-p_{FP})v^0 = \lambda_u(1-p_{FP})$$

$$g_2(v) = \alpha_1 v^{\beta_1} = \lambda'_h v^{\omega_h} = \lambda_h p_{FN}v^{\omega_H}$$

$$g_3(v) = \alpha_2 v^{\beta_2} = (\lambda_u-\lambda'_u)v^{\omega_A+\omega_B} = \lambda_u p_{FP}v^{\omega_A+\omega_B}$$

$$g_4(v) = \alpha_3 v^{\beta_3} = (\lambda_h-\lambda'_h)v^{\omega_A} = \lambda_h(1-p_{FN})v^{\omega_A}$$

Thus

$$G_t(v) = G_0 e^{-t(\lambda_u+\lambda_h)+t\lambda_u(1-p_{FP})}e^{t\sum_{k=1}^{3}\alpha_k v^{\beta_k}} \quad (16)$$

$$= G_0 e^{-t(\lambda_u+\lambda_h)+t\lambda_u(1-p_{FP})}\prod_{k=1}^{3}\sum_{j_k=0}^{\infty}\frac{1}{j_k!}\left(t\alpha_k v^{\beta_k}\right)^{j_k}$$

Let us pick up the coefficient of v^r:

$$s_{t,r} = \quad (17)$$

$$G_0 e^{-t(\lambda_u+\lambda_h)+t\lambda_u(1-p_{FP})}\sum_{\substack{j_1=j_2=j_3=0 \\ r=\sum_{k=1}^{3}\beta_k j_k}}^{\infty}\prod_{k=1}^{3}\left(\frac{1}{j_k!}t^{j_k}\alpha_k^{j_k}\right)$$

and thus

$$s_{t,q,r} = Ae^{-t(\lambda_u+\lambda_h)+t\lambda_u(1-p_{FP})}\prod_{j\in\{u,h\}}\frac{1}{q_j!}\left(\frac{\lambda'_j}{\mu_j}\right)^{q_j}$$

$$\cdot\sum_{\substack{j_1=j_2=j_3=0 \\ r=\omega_u q_u+\omega_h q_h+\sum_{k=1}^{3}\beta_k j_k}}^{\infty}\prod_{k=1}^{3}\left(\frac{1}{j_k!}(t\alpha_k)^{j_k}\right). \quad (18)$$

The solution starts from an initial value $t=0$ where the Markov chain for state probabilities (obtained by summing (4) over r) is in a stationary state and the total cost in the process is zero. Formula (18) has summation over a set of partitions, but a good approximation is not very difficult to evaluate: the term $j_k!$ makes all but small values of j_k insignificantly small. The cost grows as

$$p_q(t) = \sum_{r=0}^{\infty}rs_{t,q,r}. \quad (19)$$

We have derived (6). Let us now consider the effect of using one strong attack or many smaller attacks. The average cost is not affected but the cost distribution is changed. The numbers

$$s_{t,q,r}\,,\ r\geq 0 \qquad (s_{n,q}=\sum_{r=0}^{\infty}s_{n,q,r}\,) \tag{20}$$

give the cost distribution. If we use several small attacks, the analysis proceeds in the same way as above, with the exception that there will be for each attack $i\in I$ terms $g_{k,i}(v)$ as above. Then (21)

$$s_{t,q,r}=Ae^{-t\sum_i((\lambda_{u,i}+\lambda_{h,i})+t\lambda_{u,i}(1-p_{FP}))}\prod_{j\in\{u,h\}}\prod_{i\in I}\frac{1}{q_{j,i}!}\left(\frac{\lambda'_{j,i}}{\mu_{j,i}}\right)^{q_{j,i}}$$

$$\cdot\sum_{\substack{j_{1,i}=j_{2,i}=j_{3,i}=0\\ r_i=\sum_i(\omega_{u,i}q_{u,i}+\omega_{h,i}q_{h,i})+\sum_{k=1}^{3}\beta_{k,i}j_{k,i}}}^{\infty}\prod_{k=1}^{3}\prod_{i\in I}\left(\frac{1}{j_{k,i}!}t^{j_{k,i}}\alpha_{k,i}^{j_{k,i}}\right).$$

We obtained the expression (7).

Formulas (6) and (7) are rather complicated. The following theorem allows easier comparison.

Theorem 2. *Let us assume the attacker is using one effective attack causing cost ω_H if the attack goes unnoticed and the hacker connections have the arrival rate λ_h. The probability of the state q with cost r at the time t*

$$s_{t,q,r}=\sum_{\substack{j_1=j_2=j_3=0\\ r=\omega_H q_h+\sum_{k=1}^{3}\beta_k j_k}}^{\infty}B_{j_1,j_2,j_3}(t)AC(t,q)\ . \tag{22}$$

Let us assume the attacker is using K less effective attacks, each causing cost $\omega_H K^{-1}$ if the attack goes unnoticed and each having the arrival rate λ_h. The state probability of a combined state is

$$s_{t,q,r,K}=\sum_{\substack{j_{k,i}=0\\ i=1,\dots,K\\ q_k=\sum_{i=1}^{K}q_{k,i},\,k\in\{u,h\}}}^{\infty}s_{t,q,r} \tag{23}$$

$$=\sum_{\substack{j_1=j_2=j_3=0\\ r=\omega_H q_h+\sum_{k=1}^{3}\beta_k j_k-\frac{K-1}{K}(\omega_H q_h+j_1)}}^{\infty}K^{j_1+j_3}B_{j_1,j_2,j_3}(t)A'C(t,q)K^{q_h}e^{-(K-1)t\lambda_h}$$

Here

$$C(t,q)=e^{-t(\lambda_u+\lambda_h)+t\lambda_u(1-p_{FP})}\prod_{j\in\{u,h\}}\frac{1}{q_j!}\left(\frac{\lambda'_j}{\mu_j}\right)^{q_j}$$

and $B_{j_1,j_2,j_3}(t)=\prod_{k=1}^{3}\frac{1}{j_k!}t^{j_k}\alpha_k^{j_k}$.

The numbers A and A' are chosen so that the total probability is one.

Proof: Let us first establish a small result. We can consider a single service system with arrival rate λ_j as a multiservice system with K classes, each with arrival rate $\lambda_{j,i}/K$. The steady state probabilities must be the same if we sum over all ways $q_j=\sum_i q_{j,i}$.

Thus

$$\sum_{\substack{i=1\\ q_j=\sum_{i=1}^{K}q_{j,i}}}^{K}\prod_{i=1}^{K}\frac{1}{q_{j,i}!}\left(\frac{\lambda_{j,i}}{\mu_{j,i}}\right)^{q_{j,i}}=\frac{1}{q_j!}\left(\frac{\lambda_j}{\mu_j}\right)^{q_j}\text{, i.e.}$$

$$\sum_{\substack{i=1\\ q_j=\sum_{i=1}^{K}q_{j,i}}}^{K}\prod_{i=1}^{K}\frac{1}{q_{j,i}!}=\frac{1}{q_j!}K^{q_j}\ . \tag{24}$$

Let us mention that there is a purely combinatorial proof of (22), i.e. without knowledge of the product form solution [22] for a multiservice network. Let us first notice that

$$K^q\binom{n}{q}=\sum_{k=0}^{n}\binom{n}{k}\binom{n-k}{q-k}(K-1)^{q-k} \tag{25}$$

holds for $K>1$. (23) resembles a bit Wandermolde convolution but is quite simple. It follows easily by expanding $\left(1-\frac{1}{K-1}\right)^q$ as a binomial series

$$\left(1-\frac{1}{K-1}\right)^q=\sum_{k=0}^{q}\binom{q}{k}\left(\frac{1}{K-1}\right)^k \tag{26}$$

and by changing the summation from q to $n\geq q$. (24) follows from (25) by writing

$$\sum_{q_{j,K}=0}^{n}\binom{n}{q_{j,K}}\binom{n-q_{j,K}}{q_j-q_{j,K}}K^{q_j-q_{j,K}}=\binom{n}{q_j}K^{q_j}$$

$$\sum_{q_{j,K}=0}^{n}\binom{n}{q_{j,K}}\sum_{\substack{i=1\\ q_j-q_{j,K}=\sum_{i=1}^{K-1}q_{j,i}}}^{K-1}\prod_{i=1}^{K-1}\frac{(n-q_{j,K})!}{q_{j,i}!(n-q_{j,K}-\sum_{i=1}^{K-1}q_{j,i})}=\binom{n}{q_j}K^{q_j}$$

$$\sum_{\substack{i=1\\ q_j=\sum_{i=1}^{K}q_{j,i}}}^{K}\frac{n!}{(n-q_{j,K})!q_{j,K}!}\prod_{i=1}^{K-1}\frac{(n-q_{j,K})!}{q_{j,i}!(n-q_{j,K}-\sum_{i=1}^{K-1}q_{j,i})}=\frac{n!}{q_j!(n-q_j)!}K^{q_j}$$

$$\sum_{\substack{i=1\\ q_j=\sum_{i=1}^{K}q_{j,i}}}^{K}\prod_{i=1}^{K}\binom{n}{q_{j,1}\ \ .\ \ .\ \ .\ \ q_{j,K}}$$

$$=\sum_{\substack{i=1\\ q_j=\sum_{i=1}^{K}q_{j,i}}}^{K}\prod_{i=1}^{K}\frac{n!}{q_{j,i}!(n-\sum_{i=1}^{K}q_{j,i})}=\frac{n!}{q_j!(n-q_j)!}K^{q_j}$$

$$=K^{q_j}\binom{n}{q_j} \tag{27}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 April 2021 doi:10.20944/preprints202104.0713.v1

and multiplying both sides by $(n-q_j)!/n!$.

Let us now compare the case when there is one strong attack with cost ω_H, or K smaller (identical) attacks with $\omega_{H,i}=\omega_H/K$. Let the combined arrival rate of the smaller attacks be K times large. This is obtained by setting $\lambda_{h,i}=\lambda_h$. The user traffic is not affected, but it is also divided to K types in (21). In order to keep the total arrival rate constant, let us set $\lambda_{u,i}=\lambda_u/K$. Service times and detection probabilities are not changed: $\mu_{j,i}=\mu_j$, $p_{FN,i}=p_{FN}$, $j\in\{u,h\}$, $i=1,\ldots,K$. Let us sum over all combinations of $q_{j,i}$ giving

$$q_j=\sum_{i=1}^{K}q_{j,i}\ ,\ j\in\{u,h\} \qquad (28)$$

in order to combine the results. The summation is complicated and we will do it in small parts. From (24) follows

$$\sum_{j\in\{u,h\}}\ \sum_{\substack{i=1\\ q_{j,i}=\sum_{i=1}^{K}q_{j,i}}}^{K}\ \prod_{j\in\{u,h\}}\prod_{i=1}^{K}\frac{1}{q_{j,i}!}\left(\frac{\lambda'_{j,i}}{\mu_{j,i}}\right)^{q_{j,i}} \qquad (30)$$

$$=\left(\sum_{\substack{i=1\\ q_{u,i}=\sum_{i=1}^{K}q_{u,i}}}^{K}\ \prod_{i=1}^{K}\frac{1}{q_{u,i}!}\left(\frac{\lambda'_{u,i}}{\mu_{u,i}}\right)^{q_{u,i}}\right)\left(\sum_{\substack{i=1\\ q_{h,i}=\sum_{i=1}^{K}q_{h,i}}}^{K}\ \prod_{i=1}^{K}\frac{1}{q_{j,i}!}\left(\frac{\lambda'_{h,i}}{\mu_{h,i}}\right)^{q_{h,i}}\right)$$

$$=K^{q_u}\frac{1}{q_u!}\left(\frac{\lambda'_u}{K\mu_u}\right)^{q_u}K^{q_h}\frac{1}{q_h!}\left(\frac{\lambda'_h}{\mu_h}\right)^{q_h}=K^{q_h}\prod_{j\in\{u,h\}}\frac{1}{q_j!}\left(\frac{\lambda'_j}{\mu_j}\right)^{q_j}.$$

Let us simplify the term

$$e^{-t(\sum\lambda_{u,i}+\sum\lambda_{h,i})+t\sum_i\lambda_{u,i}(1-p_{FP,i})}=e^{-(K-1)t\lambda_h}e^{-t(\lambda_u+\lambda_h)+t\lambda_u(1-p_{FP})}$$

The coefficients in the case of many small attacks are

$$\alpha_{1,i}=\lambda_{h,i}p_{FN,i}=\lambda_h p_{FN}=\alpha_1, \qquad (32)$$

$$\alpha_{2,i}=\lambda_{u,i}p_{FP,i}=\frac{1}{K}\lambda_u p_{FP}=\frac{1}{K}\alpha_2,$$

$$\alpha_{3,i}=\lambda_{h,i}(1-p_{FN,i})=\alpha_3,$$

$$\beta_{1,i}=\omega_{H,i}=\frac{1}{K}\omega_H=\frac{1}{K}\beta_1,$$

$\beta_{2,i}=\omega_A+\omega_B=\beta_2$, and $\beta_{3,i}=\omega_A=\beta_3$.

Next let us calculate

$$\prod_{k=1}^{3}\prod_{i=1}^{K}\frac{1}{j_{k,i}!}t^{j_{k,i}}\alpha_k^{j_{k,i}}=\left(\prod_{i=1}^{K}\frac{1}{j_{1,i}!}t^{j_{1,i}}\alpha_1^{j_{1,i}}\right)\cdot \qquad (33).$$

$$\left(\left(\frac{1}{K}\right)^{\sum_{i=1}^{K}j_{2,i}}\prod_{i=1}^{K}\frac{1}{j_{2,i}!}t^{j_{2,i}}\alpha_2^{j_{2,i}}\right)\left(\prod_{i=1}^{K}\frac{1}{j_{3,i}!}t^{j_{3,i}}\alpha_3^{j_{3,i}}\right).$$

Let us sum

$$\sum_{k=1}^{3}\ \sum_{\substack{j_{k,1}=\ldots=j_{k,K}=0\\ j_k=\sum_{i=1}^{K}j_{k,i}}}^{\infty}\ \prod_{k=1}^{3}\prod_{i=1}^{K}\frac{1}{j_{k,i}!}t^{j_{k,i}}\alpha_k^{j_{k,i}} \qquad (34)$$

$$=\sum_{k=1}^{3}\left(\frac{1}{K}\right)^{j_2}\sum_{\substack{j_{k,1}=\ldots=j_{k,K}=0\\ j_k=\sum_{i=1}^{K}j_{k,i}}}^{\infty}\left(\prod_{i=1}^{K}\frac{1}{j_{k,i}!}t^{j_{k,i}}\alpha_k^{j_{k,i}}\right)$$

$$=K^{-j_2}\prod_{k=1}^{3}K^{j_k}\frac{1}{j_k!}t^{j_k}\alpha^{j_k}=K^{j_1+j_3}\prod_{k=1}^{3}\frac{1}{j_k!}t^{j_k}\alpha^{j_k}.$$

We have already summed the terms over i and in the summation index for r in the case of small attacks we can take any index i, for instance $i=1$, since all small attacks are identical. We get

$$r=\omega_{u,1}q_u+\omega_{h,1}q_h+\sum_{k=1}^{3}\beta_{k,1}j_k \qquad (35)$$

$$=\omega_u q_u+\frac{1}{K}\omega_h q_q+\left(\frac{1-K}{K}\right)j_i+\sum_{i=1}^{K}\beta_k j_k\ .$$

Combining all parts we get the final result: For one strong attack with the cost ω_H for one attack if an attacker gets in and the arrival rate λ_h, the state probability is

$$s_{t,q,r}=\sum_{\substack{j_1=j_2=j_3=0\\ r=\omega_u q_u+\omega_h q_h+\sum_{k=1}^{3}\beta_k j_k}}^{\infty}B_{j_1,j_2,j_3}(t)AC(t,q)\ . \qquad (36)$$

For K small identical small attacks with the cost ω_H/K for one attack if an attacker gets in, and with the combined arrival rate $K\lambda_h$, the state probability of a combined state is

$$s_{t,q,r,K}=\sum_{\substack{j_{k,i}=0\\ i=1,\ldots,K\\ q_k=\sum_{i=1}^{K}q_{k,i},k\in\{u,h\}}}^{\infty}s_{t,q,r}= \qquad (37)$$

$$\sum_{\substack{j_1=j_2=j_3=0\\ r=\omega_u q_u+\omega_h q_h+\sum_{k=1}^{3}\beta_k j_k-\frac{K-1}{K}(\omega_H q_h+j_1)}}^{\infty}K^{j_1+j_3}B_{j_1,j_2,j_3}(t)A'C(t,q)K^{q_h}e^{-(K-1)t\lambda_h}$$

Here

$$C(t,q)=e^{-t(\lambda_u+\lambda_h)+t\lambda_u(1-p_{FP})}\prod_{j\in\{u,h\}}\frac{1}{q_j!}\left(\frac{\lambda'_j}{\mu_j}\right)^{q_j}$$

and $B_{j_1,j_2,j_3}(t)=\prod_{k=1}^{3}\frac{1}{j_k!}t^{j_k}\alpha_k^{j_k}$. (38)

The numbers A and A' are chosen so that the total probability is one. Let us mention that the solution is not unique, by selecting different initial values the solution takes different forms, but the selected initial values lead into relatively easy closed form formulas. This finishes the proof of Theorem 2.

3. Conclusion

We derived expressions (6) and (7) from which the cost distribution can be calculated and simplified the result into (22), (23). Formulas (22) and (23) are still complicated, but let us look at the range of the index r in (22). It takes higher values in (22) than in (23). This shows that using many small attacks decreases variance even though the average effect is the same. The morale is the same as in [1], you should gamble with high bets if chances of winning are small, but the example in this paper is more difficult than those in [21]. Expressions for risks in this kind of a gamble remain complicated, but can be derived. For other applications of MDP models in telecommunications, see [23]. MDP models have also been used in intruder detection previously, e.g. in [24].

References

[1] R.Bellman, "*A Markovian Decision Process*", Journal of Mathematics and Mechanics. 6 (5): 679-684 JSTOR 24900506, 1957

[2] R.A.Howards, "*Dynamic Programming and Markov Process*", TheM.I.TPress,1960

[3] P. Ver´ıssimo, N. Neves and M. Correia. "*Intrusion-tolerant architectures: concepts and design," in Architecting Dependable Systems"*, LNCS 2677:3-36, Springer, 2003.

[4] Anderson, J.P.: *Computer security threat monitoring and surveillance*. Technical report, James P. Anderson Co., Fort Washington, PA (1980)

[5] Denning, D.E.: *An intrusion-detection model*. IEEE Transactions on Software Engineering 13 (1987) 222–232.

[6] Davison, B.D., Hirsh, H.: *Predicting sequences of user actions*. In: Proceedings of the AAAI-98/ICML-98 Joint Workshop on AI Approaches to Time-series Analysis. (1998) 5–12

[7] DuMouchel, W.: *Computer intrusion detection based on bayes factors for comparing command transition probabilities*. Technical Report 91, National Institute of Statistical Sciences, Research Triangle Park, NC (1999)

[8] Ju, W.H., Vardi, Y.: A hybrid high-order markov chain model for computer intrusion detection. Technical Report 92, National Institute of Statistical Sciences, Research Triangle Park, NC (1999)

[9] Lane, T., Brodley, C.E.*": An empirical study of two approaches to sequence learning for anomaly detection"*. Machine Learning 51 (2003)73–107

[10] Forrest, S., Perelson, A.S., Allen, L., Cherukuri, R.*:" Self-nonself discrimination in a computer*." In: Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy, Los Alamitos, CA, IEEE Computer Society Press (1994)

[11] Balthrop, J., Esponda, F., Forrest, S., Glickman, M.*: Coverage and generalization in an artificial immune system.* In Langdon, W.B., Cantu-Paz, E., Mathias, K., Roy, R., Davis, D., Poli, R., Balakrishnan, K., Hanovar, V., Rudolph, G., Wegener, J., Bull, L., Potter, M.A., Schultz, A.C., Miller, J.F., Burke, E., Jonaska, N., eds.:Proceedings of the Genetic and Evolutionary Computation Conference (GECCO 2002), Morgan Kaufmann (2002) 3–10

[12] Dasgupta, D., Gonz´alez, F.: *An immunity-based technique to characterize intrusions in computer networks*. IEEE Transactions on Evolutionary Computation 6 (2002) 1081–1088

[13] Kim, J., Bentley, P.J.: *Towards an artificial immune system for network intrusion detection: An investigation of clonal selection with a negative selection operator.* In: Proceedings of the 2002 Congress on Evolutionary Computation. (2001)

[14] E. Jonsson and T. Olovsson. "*A quantitative model of the security intrusion process based on attacker behavior*," IEEE Trans. on Software Engineering, 23(4):1-11, Apr 1997.

[15] D. Nicol, W. Sanders and K. Trivedi. "*Model-based evaluation: from dependability to security*," IEEE Trans. on Dependable and Secure Computing, 1(1):48-65, Jan 2004.

[16] B. Madan, et al. "*A method for modeling and quantifying the security attributes of intrusion tolerant systems*," Performance Evaluation,56:167-186,(2004).

[17] A. Arnes, et al. "*Real-time risk assessment with network sensors and intrusion detection systems*," in Computational Intelligence and Security, 388-397, Springer, 2005.

[18] Y. Huang, D. Arsenault and A. Sood. "*Incorruptible selfcleansing intrusion tolerance and its application to DNS security*," J. of Networks, 1(5):21-30, Sep 2006.

[19] K. Joshi, et al. "*Automated recovery using bounded partially observable Markov decision processes*," in Proc. of Dependable Systems and Networks (DSN), 445:456, Jun 2006.

[20] O. Kreidl and T. Frazier. "*Feedback control applied to survivability: a host-based autonomic defense system*," IEEE Trans. on Reliability, 53(1):148-166, Mar 2004.

[21] L. Dubins, L. Savage, *How to gamble if you must, inequalities for stochastic processes,* McGraw-Hill, 1965.

[22] F. P. Kelly, *Reversibility and Stochastic Networks*, New York: Wiley, 1979.

[23] E. Altman, "Applications of Markov Decision Processes in telecommunications: a survey," *Research Report RR-3984*, MISTRAL-project, INRIA, 2000, p.51.

[24] T. Darling, and M.A. Shayman, "Network Intruder Location Using Markov Decision Processes," in *Third International Workshop on Recent Advances in Intrusion Detection (RAID 2000)*, 2000.