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 $\lambda_u$ and finishing with the rate $\mu_u$; and hacker connections arriving and finishing with the rates $\lambda_h$ and $\mu_h$, 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 $\omega_H$. Detecting hackers also leads to expenses, as the security breach must be analysed. Let $\omega_A$ 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 $\omega_B$.

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
Let us define:
\[ \lambda' = \lambda_u(1 - p_{FP}), \quad \lambda_h = \lambda_h P_{FN}, \quad \omega_u = 0, \quad \omega_h = \omega_H. \]
Then \( \lambda_u P_{FP} = \lambda_u - \lambda' \) and \( \lambda_h (1 - P_{FN}) = \lambda_h - \lambda'_h. \)

Inserting to (4) gives
\[ s_{n+1,q,r} = s_{n,q,r} - \frac{T}{N} \sum_{j \in [u,h]} \mu_j (q_j + 1) s_{n,q,r} + \frac{T}{N} (\lambda_u + \lambda'_u) s_{n,q,r} \]
\[ + \frac{T}{N} \lambda'_u s_{n,q,r} - \frac{T}{N} \sum_{j \in [u,h]} \mu_j (q_j + 1) s_{n,q,r} + \frac{T}{N} (\lambda_h - \lambda'_h) s_{n,q,r} - \frac{T}{N} \lambda'_h s_{n,q,r} + \frac{T}{N} \sum_{j \in [u,h]} \mu_j (q_j + 1) s_{n,q,r} + e_j, r. \]

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 \( \lambda_h \). The corresponding probability is
\[ s_{n,q,r} = A e^{-\sum_{j} (a_{ij} + b_{ij}) t + \sum_{i,j} (\lambda_{ij} + \lambda_{ji}) (1 - p_{FP})} \prod_{j=0}^{\infty} \prod_{j=0}^{\infty} \left( \frac{1}{q_j \lambda_j} \right)^{q_j} \]

where

\[ \alpha_{i,j} = \lambda_{i,j}PFN, \alpha_{2,j} = \lambda_{2,j}PFP \]

\[ \beta_{i,j} = \omega_{i,j}PFN, \beta_{2,j} = \omega_{2,j}PFP \]

\[ \lambda_{1,i} = \lambda_{1,i}PFP \]

\[ \lambda_{2,i} = \lambda_{2,i}PFP \]

\[ \lambda_{3,i} = \lambda_{3,i}PFP \]

The 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

\[ s_{n,q,r} = \prod_{j=0}^{\infty} \prod_{j=0}^{\infty} \left( \frac{1}{q_j \lambda_j} \right)^{q_j} s_{n,r} \sum_{j=0}^{\infty} \alpha_j q_j = s_q s_{n,r,c} \]

where \( c = \sum_{j=0}^{\infty} \alpha_j q_j \).

This solution form satisfies

\[ \mu_j q_j s_{n,q,r} = \lambda_j s_{n,q-r,j} + \alpha_j q_j s_{n,q-j,\infty} \]

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

\[ s_{n+1,r-c} = s_{n,r-c} + \frac{T}{N} \sum_{j=0}^{\infty} s_{n,r-c,j} + \frac{T}{N} \sum_{j=0}^{\infty} s_{n,r-c,j} \]

This is easily solved with the generating function

\[ G_n(v) = \sum_{r=0}^{\infty} s_{q,r} v^r = s_q \sum_{r=0}^{\infty} s_{q,r} v^r \]

where \( s_{q,r} = 0 \) if \( r < 0 \). Thus

\[ G_{n+1}(v) = G_n(v)(1 + \frac{T}{N} \sum_{j=0}^{\infty} s_{j} v^{\lambda_j}) \]

\[ + \frac{T}{N} (\lambda_{1}\lambda_{1}v^{\lambda_1} + \lambda_{2}\lambda_{2}v^{\lambda_2}) \]

Let us write the equation as

\[ G_{n+1}(v) = G_n(v) \left( 1 + \frac{T}{N} \sum_{k=1}^{\infty} g_k(v) \right) \]

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

\[ G_v(v) = G_0(v) \lim_{n \to \infty} \left( 1 + \frac{T}{n} \sum_{k=1}^{\infty} g_k(v) \right)^n \]

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

\[ g_0(v) = \frac{- (\lambda_{1} + \lambda_{2})}{v^{\lambda_{1} + \lambda_{2}}} \]

\[ g_1(v) = \frac{(\lambda_{1} + \lambda_{2} + v^{\lambda_{1} + \lambda_{2}})}{v^{\lambda_{1} + \lambda_{2}}} \]

\[ g_2(v) = \frac{(\lambda_{1} + \lambda_{2} + v^{\lambda_{1} + \lambda_{2}})}{v^{\lambda_{1} + \lambda_{2}}} \]

Thus

\[ G_v(v) = G_0(v) \sum_{k=1}^{\infty} \left( 1 + \frac{T}{n} \sum_{k=1}^{\infty} g_k(v) \right)^n \]

Let us pick up the coefficient of \( v^r \):

\[ s_{r,r} = \sum_{j=1}^{\infty} \sum_{j=1}^{\infty} \left( \frac{1}{j!} \right)^{k} \]

\[ G_0 e^{-t(\lambda_{1} + \lambda_{2}) + t(\lambda_{1} + \lambda_{2})} \sum_{k=1}^{\infty} \left( \frac{1}{j!} \right)^{k} \]

\[ \sum_{k=1}^{\infty} \left( \frac{1}{j!} \right)^{k} \]

\[ \sum_{r=0}^{\infty} s_{r,r} v^r \]

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 \( j! \) makes all but small values of \( j \) insignificantly small. The cost grows as

\[ p_q(t) = \sum_{r=0}^{\infty} r s_{r,q,r} \]

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
\[ s_{t,q,r} \cdot \mathcal{A}(t,q) \]  
\[ s_{t,q,r} = \sum_{r=0}^{\infty} s_{n,q,r} \]  
(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
\[ s_{t,q,r} = A e^{-r(\lambda_{t,q} + \tilde{\lambda}_h)} \prod_{j=0}^{\infty} \frac{1}{q_j} \left( \frac{\lambda_{t,j}}{\mu_{t,j}} \right)^q_{j,i} \]
\[ s_{t,q,r} = A e^{-r(\lambda_{t,q} + \tilde{\lambda}_h)} \prod_{j=0}^{\infty} \frac{1}{q_j} \left( \frac{\lambda_{t,j}}{\mu_{t,j}} \right)^q_{j,i} \]
(21)

\[ s_{t,q,r} = A e^{-r(\lambda_{t,q} + \tilde{\lambda}_h)} \prod_{j=0}^{\infty} \frac{1}{q_j} \left( \frac{\lambda_{t,j}}{\mu_{t,j}} \right)^q_{j,i} \]
\[ s_{t,q,r} = A e^{-r(\lambda_{t,q} + \tilde{\lambda}_h)} \prod_{j=0}^{\infty} \frac{1}{q_j} \left( \frac{\lambda_{t,j}}{\mu_{t,j}} \right)^q_{j,i} \]
(22)

The steady state probabilities must
\[ \sum_{q_j=0}^{\infty} q_j = 1 \]
(24)

Proof: Let us first establish a small result. We can consider a single service system with arrival rate \( \lambda_j \) as a multiservice system with \( K \) classes, each with arrival rate \( \lambda_{j,i} / K \). The effective attack causing cost \( q_j \) at the time \( t \)
\[ q_j = \sum_{q_j,i} q_j \]
(25)

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
\[ K^q q_j = \sum_{k=0}^{n} \binom{n}{k} (n-k)(K-1)^{q-k} \]
(26)

and by changing the summation from \( q \) to \( n \geq q \). (24) follows from (25) by writing
\[ \sum_{q_j=0}^{n} \binom{n}{q_j} q_j \]
(27)

Here
\[ C(t,q) = e^{-r(\lambda_{t,q} + \tilde{\lambda}_h)(1-p_{rr})} \prod_{j=0}^{\infty} \frac{1}{q_j} \left( \frac{\lambda_{t,j}}{\mu_{t,j}} \right)^q_{j,i} \]
and
\[ B_{h_j,i}(t) = \prod_{k=1}^{\infty} \frac{1}{q_k} \left( \frac{\lambda_{h,j}}{\mu_{h,j}} \right)^q_{j,i} \]
The numbers \( A \) and \( A' \) are chosen so that the total probability is one.

\[ q_j = \sum_{q_j,i} q_j \]
(28)
and multiplying both sides by \((n - q_j)/n!\).

Let us now compare the case when there is one strong attack with cost \(\omega_H\), or \(K\) smaller (identical) attacks with \(\omega_{H,j} = \omega_H/ K\). Let the combined arrival rate of the smaller attacks be \(\lambda_h, i = \lambda_h\). The user traffic is not changed: \(\mu_{ij} = \mu_j\), \(P_{FN,i} = P_{FN,j} = \mu(\lambda_h)\), \(i = 1, ..., K\). Let us sum over all combinations of \(q_{ij}\) giving

\[
q_j = \sum_{i=1}^{K} q_{ij}, \quad j \in \{u, h\}
\]

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

\[
\begin{align*}
\sum_{j=\{u, h\}}^{K} \sum_{i=1}^{K} \prod_{j=1}^{K} \prod_{i=1}^{K} \frac{1}{q_{ij}!} \left( \frac{\lambda_{ij}^j}{\mu_{ij}} \right)^{q_{ij}j} \\
= \sum_{q_u} \sum_{q_h} \prod_{q_u} \prod_{q_h} \frac{1}{q_u!} \left( \frac{\lambda_{u}^u}{\mu_{u}} \right)^{q_u} \frac{1}{q_h!} \left( \frac{\lambda_{h}^h}{\mu_{h}} \right)^{q_h} \\
= K^{q_u} \frac{1}{q_u!} \left( \frac{\lambda_{u}^u}{\mu_{u}} \right)^{q_u} \frac{1}{q_h!} \left( \frac{\lambda_{h}^h}{\mu_{h}} \right)^{q_h} = K^{q_h} \prod_{j=\{u, h\}}^{K} \frac{1}{q_j!} \left( \frac{\lambda_{ij}^j}{\mu_{ij}} \right)^{q_{ij}j} 
\end{align*}
\]

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

\[
r = \omega_{u} q_{u} + \omega_{h} q_{h} + \sum_{k=1}^{K} \beta_{k} j_{k}
\]

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

\[
s_{t,q,r} = \sum_{j_{1} \leq j_{2} \leq j_{3}} B_{j_{1}, j_{2}, j_{3}}(t) A^C(t, q) \cdot (36)
\]

For \(K\) small identical small attacks with the cost \(\omega_{H}/K\) 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

\[
s_{t,q,r,K} = \sum_{j_{1} \leq j_{2} \leq j_{3}} s_{t,q,r} \cdot (37)
\]

Here

\[
C(t, q) = e^{-l(\lambda_{u} + \lambda_{h}) + l(1 - p_{FP})} \prod_{j \in \{u, h\}} q_j \cdot (38)
\]

and

\[
B_{j_{1}, j_{2}, j_{3}}(t) = \prod_{k=1}^{K} \frac{1}{j_{k}!} \left( \frac{\lambda_{k}^j}{\mu_{j}} \right)^{q_{j}k} \cdot (39)
\]

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 game 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