Computers and Mathematics with Applications 65 (2013) 1234–1253

Contents lists available at SciVerse ScienceDirect

Computers and Mathematics with Applications

journal homepage: www.elsevier.com/locate/camwa

# The configuration and detection strategies for information security systems

Hulisi Öğüt

*Department of Business Administration, TOBB University of Economics and Technology, Söğütözü Cad, No:43 Ankara, Turkey*

ARTICLE INFO

*Keywords:*
Intrusion detection system
Base rate fallacy
Configuration policy

ABSTRACT

Intrusion Detection Systems (IDSs) have become an important element of the Information Technology (IT) security architecture by identifying intrusions from both insiders and outsiders. However, security experts questioned the effectiveness of IDSs recently. The criticism known as Base Rate fallacy states that when IDS raises an alarm, the event is more likely to be benign rather than intrusive since the proportion of benign activity is significantly larger than that of intrusive activity in the user population. In response to too many false alarms, system security officers (SSO) either ignore alarm signals or turn off the IDS as the information provided by IDS is very skeptical. To alleviate this problem of IDSs, Ogut et al. (2008) [6] suggest that the firm may choose to wait to get additional signal and to make better decision about user type. One of the limitations of their model is that configuration point at which IDSs operate (the false negative and false positive rates) is exogenously given. However, the firm trying to minimize expected cost should also make a decision regarding the configuration level of IDSs since these probabilities are one of the determinants of future cost. Therefore, we extend Ogut et al. (2008) [6] by considering configuration and waiting time decisions jointly in this paper. We formulate the problem as dynamic programming model and illustrate the solution procedure for waiting time and configuration decision under optimal policy when cost of undetected hacker activity follows step wise function. As it is difficult to obtain waiting time and configuration decision under optimal policy, we illustrate the solution procedures for under myopic policy and focus on the characteristics of configuration decision under myopic policy. Our numerical analysis suggested that configuration decision is as important as waiting time decision to decrease the cost of operating IDS.

## 1. Introduction

Increasing use of the Internet for conducting business has made firms vulnerable to cyber attacks. Security breaches may compromise confidentiality, integrity and availability of critical information assets. Firms employ a variety of mechanisms to deal with information technology (IT) security breaches. Preventive technologies such as firewalls and anti-virus software are example of such IT security controls and they aim to stop intrusion from outsiders. Detection based systems complement the preventive technologies by detecting intrusions from both outsiders managing to break preventive technologies and malicious insiders who often create serious threat to organization (Secprodonline 2007). One of the most widely employed detective control mechanisms is the Intrusion Detection Systems (IDSs). IDSs try to detect intrusions when they occur by analyzing network packets and system log files. An IDS runs continually in the background and generates an alarm when it detects something that it considers as suspicious, anomalous, or illegal [1,2].

*E-mail address:* hogut@etu.edu.tr.

0898-1221/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.camwa.2012.05.015

The effectiveness of IDSs is measured using two parameters: the likelihood of (i) giving a signal upon an intrusion and (ii) being silent when there is no intrusion. Recently, some security experts evaluate the performance of the IDS in terms of these two measures and report that one of the biggest problems of the IDSs is to raise too many false alarms [3]. The criticism known as the base-rate fallacy states that when IDS raises an alarm, event is more likely to be benign rather than intrusive since the proportion of benign activity is significantly larger than that of intrusive activity in the user population [4]. Thus, the firm incurs high cost if it ignores the base rate (prior) and takes immediate action after every alarm. Base-rate fallacy stems from the well-known Bayes' theorem that shows the relationship among a posterior probability $P(A_i \mid B)$, a prior probability $P(A_i)$, and a conditional probability $P(B \mid A_i)$. Bayes' theorem is stated as the following well-known formula:

$$P(A_i \mid B) = \frac{P(A_i) \cdot P(B \mid A_i)}{\sum_{i=1}^{n} P(A_i) \cdot P(B \mid A_i)}.$$

The base-rate fallacy arises from the fact that when the probability distribution of $A$ is highly skewed, $P(A_i \mid B)$ may become very low. For example, consider an intrusion detection scenario in which there are two types of users: benign and hackers. We assume that the probability that a user is a hacker, $P$ (hacker), is equal to 1/1000. Let the following probabilities define the quality of the IDS: $P$ (alarm signal|hacker) $=P$ (no-alarm signal|benign user) $=0.7$. Using the Bayes' theorem, we can compute $P$ (hacker|alarm-signal) $\cong 0.002$. In other words, when the IDS raises an alarm, the probability that the user is benign is 99.8%. These probabilities imply that IDS raises too many alarms for benign events. In response to too many false alarms, system security officers (SSO) either ignore alarm signals or turn off the IDS as the information provided by IDS is very skeptical. However, some researchers state that IDSs are the only available mechanism to deal with intrusions that have bypassed preventive technologies and should be used even with their current problems [5].

To alleviate base rate fallacy problem of IDSs, Ogut et al. [6] suggest that the firm may choose to wait to get additional signal and to make better decision about user type rather than terminating user session immediately after an alarm or ignoring all alarms from IDS. However, waiting is costly as hacker may cause more damage to the firm. Consequently, they address the problem of when to take an action following a signal from the IDS by considering the tradeoff between possibilities of more damage and making more informed decision. However, one of the limitations of their model is that the false negative and false positive rates of the IDS are exogenously given. Since configuration decision which is defined as the choice of false alarm probability affects the probability of future alarm and no-alarm signals, these probabilities are one of the determinants of future cost. Thus, the firm trying to minimize expected cost should take into account configuration decision. For this reason, we extend Ogut et al. [6] by considering configuration and waiting time decisions together. The polices developed in this paper can be implemented as a decision support system (DSS) that uses the IDS signals as input to make a recommendation about the optimal level of configuration which is the level of the false alarm probability and when to take action against a user.

We formulate the problem as dynamic programming model and illustrate the solution procedure for waiting time and configuration decisions under optimal policy when cost of undetected hacker activity follows step-wise function. As it is difficult to obtain waiting time and configuration decision under optimal policy, we illustrate the solution procedures for waiting time and configuration decision under myopic policy. We analyzed three cases using linear cost function. When the arrival rate of signal from hacker is greater than arrival rate of signal from benign user, we have found that myopic configuration level increases (decreases) when (i) cost of false alarm becomes lower (higher), (ii) prior probability that user being a hacker increases (decreases), (iii) cost of damage per time unit becomes higher (lower) and (iv) arrival rate of signal from hacker decreases (increases). Changes in the arrival rate of signal from a benign user do not affect the configuration level. When the arrival rate of a signal from a hacker is less than the arrival rate of a signal from a benign user and waiting times under myopic policy are greater than zero, we have found that the myopic configuration policy is not affected by the changes in the prior probability that user is hacker, the cost of false alarm and the damage cost per unit time. However, a more frequent signal from a hacker (benign user) decreases (increases) the configuration level under myopic policy. When the arrival rate of a signal from a hacker is less than the arrival rate of a signal from a benign user and one of the waiting times under myopic policy is equal to zero, configuration level under myopic policy increases (decreases) when (i) cost of false alarm decreases (increases), (ii) the prior probability that a user being a hacker increases (decreases) (iii) damage cost per unit time increases (decreases) and (iv & v) the arrival rate of a signal from a benign user and a hacker decreases (increases). In the simulation, we compare the cost performances of four policies: myopic policy with fixed configuration, optimal policy with fixed configuration, policy with myopic configuration (myopic configuration policy) and policy with optimal configuration (optimal configuration policy). As we expected, the cost incurred under the policy with optimal configuration is the lowest, while the cost incurred under myopic policy with fixed configuration is the highest. In addition, the myopic configuration policy performs better than optimal policy with fixed configuration. Our results from simulation analysis suggested that the behavior of optimal configuration policy is similar to the behavior of myopic configuration policy. For that reason, we believe that theoretical results obtained for myopic policy is likely to hold for optimal policy as well. Furthermore, we observe that the optimal configuration level is higher than the myopic configuration level in our analysis. Moreover, our simulation results show that the myopic configuration policy is nearly identical to the optimal configuration policy.

The organization of the rest of our paper is as follows. In the next section, we review the relevant literature. We describe our model of the intrusion detection problem in Section 3. In Section 4, we derive the optimal policy. In Section 5, we study the myopic policy and analyze its characteristics analytically. We have performed the simulation analysis in Sections 6 and 7 concludes the paper.

## 2. Literature review

The majority of research on IDS has focused on designing or improving algorithms to detect malicious events. When a user takes an action, these events are recorded in the user log files and these are the primary inputs for the detection technologies in order to classify the user type as benign or hacker. IDS uses either signature based or anomaly based detection technology to protect an organization's information asset. In the signature based detection technology, user log files are searched for known attack signatures and an alarm is raised if any familiar pattern is found. Signature based detection technology is similar to Anti-Virus software and the signature database should be updated frequently for the proper functioning of IDS. This technology suffers mainly from false negative error as it detects only known attacks. Studies focusing on the signature based IDS system can be found on [7–11]. In the anomaly detection algorithm, the user's action is compared with the normal user profile and IDS raises an alarm if the user's profile differs significantly from the normal user profile. Contrary to signature based technology, anomaly based detection technology is able detect a novel attack. Researches related to an anomaly based system are discussed in [9,12–16]. Although these two research streams aim to increase the accuracy of IDS by decreasing either false positive error or false negative error, costs of false positive and false negative errors are ignored. As these errors have different effects on the cost of operating IDS, Lee et al. [17] proposed an IDS model that incorporates various cost elements in the intrusion detection setting.

Recently, researchers have started to investigate the economic aspects of IDS. Earlier studies in this line of research focus on optimal configuration policies by taking into account various cost parameters. Configuration refers to choosing an optimal operating point of IDS to minimize the total cost of intrusion detection. Ulvila and Gaffney [18] proposed a decision analysis approach to configure IDS by taking into account false positive and false negative errors. They showed that both configuration and cost analysis methods should be considered to improve the value of IDS. Cavusoglu and Raghunathan [19] compared Gaffney and Ulvia's decision theoretic approach with the game theoretic approach. Unlike the decision theoretic approach, the game theoretic approach takes into account the hacker's strategic action in response to the firm's decision and they have found that it achieved better results than the decision theoretic approach for IDS configuration as it considers more information. However, it is more difficult to estimate parameters used in the game theoretic approaches such as hacker's utility for hacking and penalty parameters when she is caught. Ryu and Rhee [20] analyzed three types of IT security models: the simple intrusion prevention model, dual threshold model and dual filtering model. The simple intrusion prevention model is similar to Ulvila and Gaffney's [18] model. The dual threshold model operates at two points: high threshold value and low threshold value. If the abnormality score of an event is less (higher) than low (high) threshold value, (no action) action is taken to block the event. If the numerical score of event is between these two points, the event is manually investigated. In the dual filtering model, an event passes the inferior intrusion prevention systems (IPS) at first and it is filtered through the superior IPS if the first IPS raises alarm signal. However, the delay cost of holding benign event is incurred in this case. In their analysis, they found that both latter models reduce the operating cost of IDS and cost reduction is higher when IDS quality is higher. In a related paper, Yue and Çakanyildirim [21] investigated the optimal configuration decision and the responses given to the alarm signal. These responses are the reactive approach (manual investigation of alarm signal) which is relatively slow and accurate, the proactive approach (terminating user session immediately) which is relatively rapid and inaccurate and mixture of these strategies for the batches of alarm signals. Their analysis showed that value of cost parameters and investigation rate parameters determine the type of response given to alarm signals. The speed of alarms' arrival and clearance also affect the decision variables. Bensoussan et al. [22] study the balance between making better decision via improved detection system and the cost of maintaining the detection system. In a related paper, Mookerjee et al. [23] discussed also hacker behavior that occur in response to improvements in the detection system as a result of maintenance effort. Cavusoglu et al. [24] show that the interaction between IDS and firewall technologies should be considered in order to benefit from these technologies.

One of the primary implications of these papers is that both the configuration and the cost of operating IDS should be taken into account to increase the value of the IDS. However, these researches ignore the behavior of user within the IDS and they assume that the cost of hacking is fixed. For this reason, we extended Ogut et al. [6] by jointly considering configuration and cost optimization in this paper. Unlike the above papers, we model user behaviors within the IDS over time by taking into account multiple signals and the arrival rate of these signals from the hacker and the benign user. The definitions of notations used in the paper are given in Table 1.

## 3. Model description

We consider individual user interacting with IDS. There are two user types: *hacker and benign* and the proportion of hacker in the user population is $p_0$%. There can be many user actions such as invoking system commands arriving at different times before a user leaves the system or user's session is terminated and $i$th user action arrives at time $t_i$. We assumed that the arrival time of user action is exponentially distributed with parameter $\lambda_H$ for a hacker and $\lambda_B$ for a benign user, respectively. The exponential distribution of arrival time of user action is consistent with empirical observation of hacker action recorded

**Table 1**
The definition of notation used in the paper.

| | |
|---|---|
| $\phi$ | The probability of false alarm |
| $f^H(s)$ | The probability density function of hacker's abnormality score |
| $f^B(s)$ | The probability density function of benign user's abnormality score |
| $F^H(t)$ | The cumulative density function of hacker's abnormality score |
| $F^B(t)$ | The cumulative density function of benign user's abnormality score |
| $\Omega(\phi)$ | The probability of true alarm |
| $c_{Bi}$ | The cost of false positive after $i$th signal. |
| $c_H(t)$ | Damage cost caused by undetected hacking activity at time $t$ |
| $p_i$ | Posterior probability that the user is a hacker after $i$th signal. |
| $f_i$ | The firm's waiting time after the $i$th user action |
| $t_i$ | Arrival time of $i$th user action |
| $\lambda_H$ | Arrival rate of hacker user action |
| $\lambda_B$ | Arrival rate of benign user action |
| $C_H(S_{i+1}, t_{i+1})$ | Expected cost during $[t_{i+1}, \infty)$ if the user is hacker |
| $C_B(S_{i+1}, t_{i+1})$ | Expected cost during $[t_{i+1}, \infty)$ if the user is benign |
| $C(S_{i+1}, t_{i+1})$ | Total expected cost during $[t_{i+1}, \infty)$ |
| $S_i$ | Vector of signal until $i$th user action |

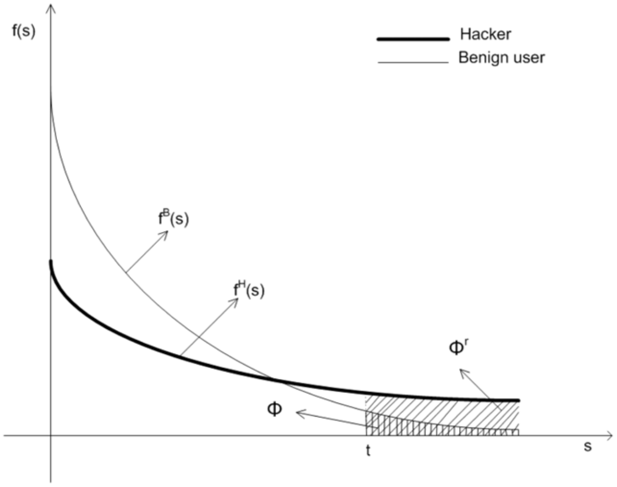

**Fig. 1.** Evaluation of abnormality score.

by Jonsson and Olusson [25]. After analyzing every user action, IDS raises either no-alarm signal or alarm signal if it suspects there is an intrusion. Let $S_i = 0$ and $S_i = 1$ denote no-alarm or an alarm signal generated after the $i$th user action respectively. Once an alarm is given by IDS, it can be a either true alarm or false alarm as IDS is imperfect in terms of classifying a benign user and a hacker. We define the false alarm probability as

$$\phi := P\text{ (IDS raises an alarm | User is benign).}$$

In this paper, we refer to configuration decision as the making choice of $\phi$. Similarly, we define the true alarm probability as

$$\Omega(\phi) := P\text{(IDS raises an alarm | User is hacker).}$$

The function $\Omega(\phi)$ is known as the *Receiver Operating Characteristic* (ROC) curve. The *ROC* curve is commonly used to display the relationship between the true alarm and false alarm rate in classification applications such as medical diagnosis systems, signal detection etc. (e.g. [26,27]; see Figures 1 and 2) *ROC* curve satisfies $\frac{\partial\Omega(\phi)}{\partial\phi} > 0$ and $\frac{\partial^2\Omega(\phi)}{\partial\phi^2} < 0$ meaning that true alarm probability increases at a decreasing rate when false alarm probability increases. We also assume that the probability of getting alarm signal from the hacker is higher than the probability of getting alarm signal from the benign user (i.e. $\Omega(\phi) > \phi$). We choose a power function for the relationship between false alarm and true alarm probability as it is the most commonly used functional form for *ROC* curve [19–21]. Mathematically, the power function can be represented as

$$\Omega(\phi) = \phi^r$$

where $r$ is between zero and one and the high value of $r$ implies that IDS quality is poor. This functional form is derived based on the assumption that the probability density function of the hacker and benign user's abnormality score is exponentially distributed [19]. The relationship between abnormality score ($s$) and the probability density function of hacker ($f^H(s)$) and benign user ($f^B(s)$) is illustrated in Fig. 1. As the abnormality score increases, the probability density function of the benign user decreases faster than the probability density function of the hacker. Abnormality score is calculated with a

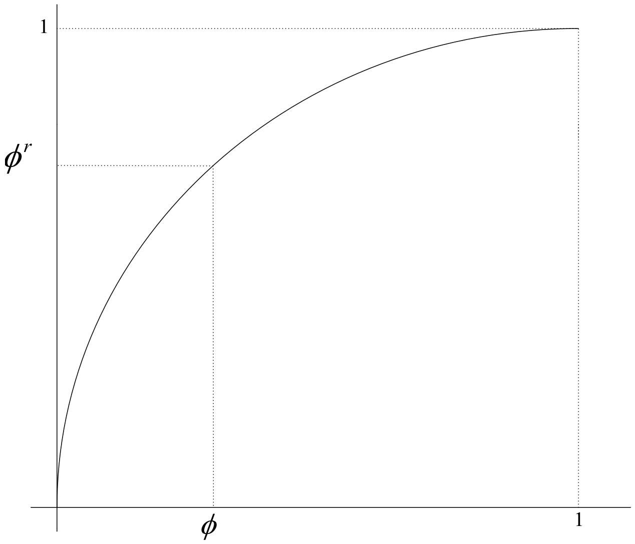

**Fig. 2.** The *ROC* curve.

variety of inputs such as information in network packets (source, destination, packet size, and time) or/and information in audit trials by using the classifier technique trained with the historical data [28–30]. Given these probability distributions, the threshold value ($t$) is set and an alarm is raised if the user's abnormality score ($s$) is higher than threshold value ($t$). As it is shown in Fig. 1, the threshold value determines the probability of false positives ($\phi = \int_{s=t}^{\infty} f^B(s)ds = 1 - F^B(t)$) and true positives ($\phi^r = \int_{s=t}^{\infty} f^H(s)ds = 1 - F^H(t)$) in Fig. 2 [19,20]. Since $F^H(t)$ and $F^B(t)$ are the cumulative distribution of exponential distribution, ($r = \frac{\ln(1-F^H(t))}{\ln(1-F^B(t))}$) is constant and between 0 and 1.

The quality of IDS is determined by the shape of the *ROC* curve. If true alarm probability increases for a given false alarm probability the quality of IDS improves. Specifically, the higher the area under the *ROC* curve, the better the quality of IDS. Given a *ROC* curve, the security officer decides the point at which IDS operates and the configuration decision determines true and false alarm probabilities. Based on these probabilities and signal history, a firm calculates posterior probability. We use $p_i$ to denote the posterior probability that the user is a hacker after the $i$th signal.

In our model, the firm incurs two types of cost as in [18]: The cost of taking action against a benign user (cost of false alarm) and the damage cost caused by undetected hacker activity. The firm incurs the former cost when it incorrectly takes an action against a benign user. We assumed that the duration of a user's action is relatively short and the cost due to undetected hacker activity is much higher than the cost of false positive error. For this reason, we assumed that the cost of a false positive to be constant for $i$th user action and this cost is denoted as $c_{Bi}$. Note that the cost of a false positive may change during the user's session but it stays constant for a specific user action. The damage cost caused by undetected hacking activity is denoted as $c_H$ and it is a non-decreasing function of time as it represents the cumulative cost (i.e., $\frac{\partial c_H}{\partial t} \geq 0$).

The sequences of activities are as follows. Before each user action, a configuration decision is given by the system security officer (SSO). When a user's action is observed, the user's abnormality score is computed and an alarm (no-alarm) signal is raised if the computed score is greater (less) than the threshold level. Thus, if the threshold level is set low, configuration level and the probability that IDS raises an alarm for an event will be high as it is illustrated in Fig. 1. After each signal from the IDS, the firm updates its posterior probability that the user is a hacker (or benign) and computes its optimal waiting time. We use $f_i$ to denote the firm's waiting time after the $i$th user action and $f_i \in [0, \infty)$. Thus, the firm will take immediate action if $f_i = 0$ and the firm will wait for next signal to come if $f_i = \infty$. Next, we present the following proposition in order to offer rationale for waiting time.

**Proposition 1.** *The expected $p_i$ is monotonically increasing (decreasing) in i if user happens to be a hacker (benign user).*

{The proofs for all propositions are in the Appendix.}

Proposition 1 suggested that the classification accuracy of the user type improves upon observing additional signals. However, the firm cannot wait indefinitely for the arrival of signal if the user happens to be a hacker. Consequently, the waiting time allows the firm to restrict the damage cost if the user is a hacker and to a grant grace period if the user is a benign user. Therefore, we adopted the following waiting time strategy. If no new user action arrives therefore IDS raises no new signal at the end of the waiting time, the firm concludes that the user is a hacker and blocks her session. If new user action arrives before waiting time ends, the firm updates the posterior probability based on this new signal and computes a new waiting time $f_{i+1}$, for the next user action. For example, in Fig. 3, the firm computes the posterior probability based on new signal and sets a new waiting time $f_{i+1}$ instead of terminating the user's session at $t_{i+1}$ since $(i+1)$th user action arrives

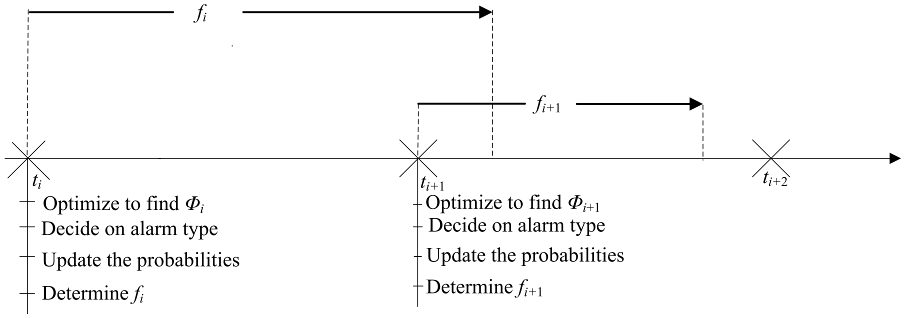

**Fig. 3.** Illustration of waiting time policy.

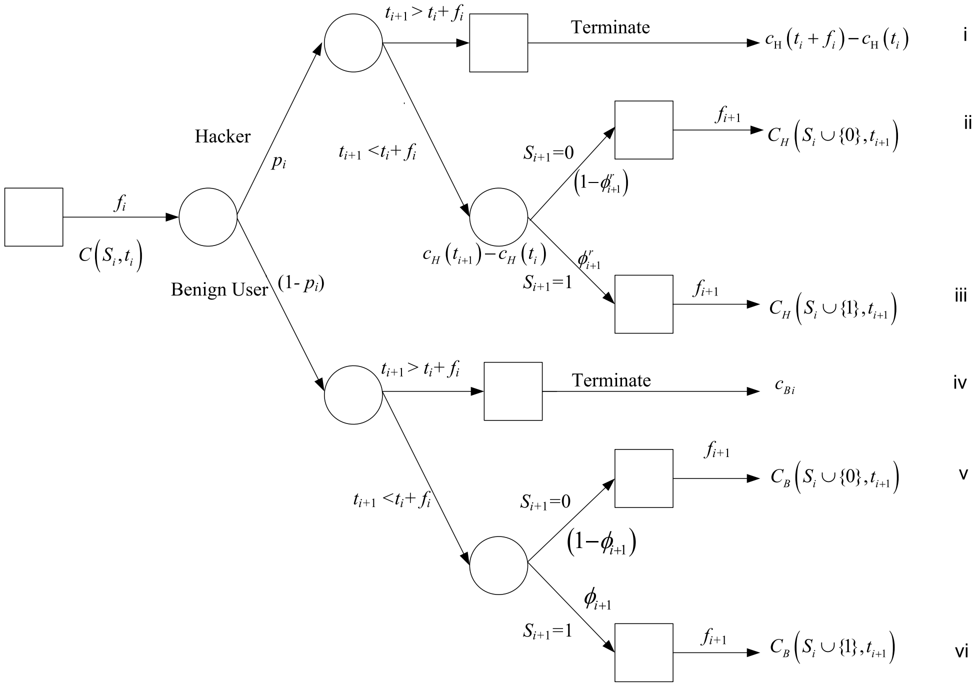

**Fig. 4.** Decision tree representation of intrusion detection at time $t_i$.

before the end of the waiting time (i.e. $t_{i+1} < t_i + f_i$). However, the firm concluded that the user is a hacker and takes action at $(t_{i+1} + f_{i+1})$ because no new user action arrives before $(t_{i+1} + f_{i+1})$. Note that in our example the $(i+2)$th signal will never arrive because the user session would have been terminated before. We show it in the figure for illustration purposes.

## 4. Optimal policy

In this section, we derive the optimal waiting policy, $f_i^*$, when the $i$th signal about a user is received at time $t_i$. We derive $f_i^*$ by minimizing the expected cost during the period $[t_i, \infty)$. The decision tree for computing the expected cost during $[t_i, \infty)$ is given in Fig. 4. There are two possibilities for a given type of user when the firm decides to wait for $f_i$ units of time at time $t_i$: A new signal arrives before $t_i + f_i$ and a new signal does not arrive before $t_i + f_i$.

If a new signal does not arrive before $t_i + f_i$, the firm concludes that the user is a hacker and takes action at time $t_i + f_i$. In this situation, the firm computes expected cost based on two cases. In the first case (case (i)), the user is a hacker and the cost incurred due to detected hacker activity at $t_i + f_i$ is $c_H(t_i + f_i) - c_H(t_i)$. The firm's estimated probability of the case is $p_i e^{-\lambda_H f_i}$. In the second case (case (iv)), the user is benign and the cost of incorrectly concluding that a benign user is a hacker is $c_{Bi}$. The firm's estimated probability of this case is $(1 - p_i)e^{-\lambda_B f_i}$.

If a new signal arrives before $t_i + f_i$, the firm computes a new optimal waiting time based on four possible cases. In the first case (case (ii)), the user is a hacker and a new no-alarm signal is generated by the IDS before the firm takes action. The expected cost during $[t_i, \infty)$ is $(c_H(t_{i+1}) - c_H(t_i) + C_H(S_i \cup \{0\}, t_{i+1}))$ where $c_H(t_{i+1}) - c_H(t_i)$ is the cost incurred during $[t_i, t_{i+1})$ and $C_H(S_i \cup \{0\}, t_{i+1})$ is the cost incurred after $t_{i+1}$. In the second case (case (iii)), the user is a hacker

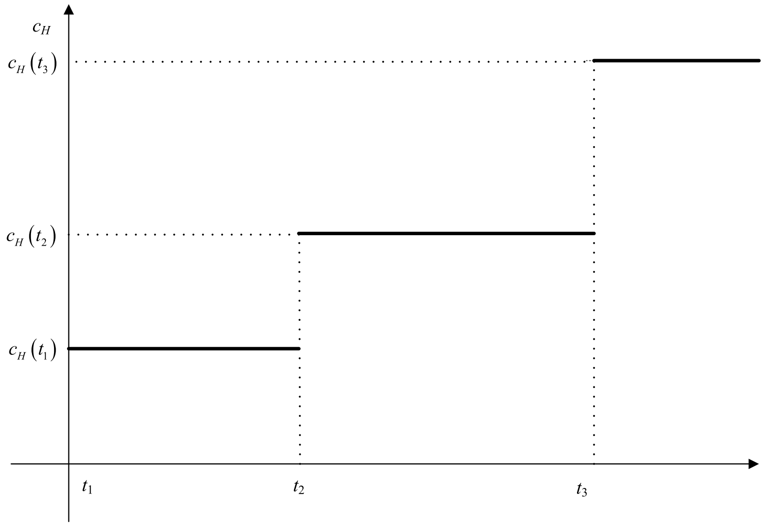

**Fig. 5.** Step-wise function for $c_H$.

and a new alarm signal is generated by the IDS before the firm takes action. Similar to case (ii), the cost during $[t_i, \infty)$ is $(c_H(t_{i+1}) - c_H(t_i) + C_H(S_i \cup \{1\}, t_{i+1}))$. In the third case (case (v)), the user is benign and new no-alarm signal is generated by the IDS before the firm takes action. The cost incurred during $[t_i, t_{i+1})$ is zero and the expected cost of a false positive for future user actions is $C_B(S_i \cup \{0\}, t_{i+1})$. In the fourth case (case (vi)), the user is benign and a new alarm signal is generated by the IDS before the firm takes action. The cost incurred during $[t_i, t_{i+1})$ is again zero, but the expected cost of false positive during future user actions is given by $C_B(S_i \cup \{1\}, t_{i+1})$.

Using the decision tree, the firm will minimize following expected cost at $t_i$ by choosing optimal waiting time:

$$\begin{aligned} C(S_i, t_i) = \min_{f_i} p_i & \left\{ e^{-\lambda_H f_i}[c_H(t_i + f_i) - c_H(t_i)] + \int_{t_i}^{t_i+f_i} \lambda_H e^{-\lambda_H(t_{i+1}-t_i)}([c_H(t_{i+1}) - c_H(t_i)] \right. \\ & \left. + \ (1 - \phi^r_{i+1}) C_H(S_i \cup \{0\}, t_{i+1}) + \phi^r_{i+1} C_H(S_i \cup \{1\}, t_{i+1}))dt_{i+1} \right\} \\ & + (1 - p_i) \left\{ e^{-\lambda_B f_i}(c_{Bi}) + \int_{t_i}^{t_i+f_i} \lambda_B e^{-\lambda_B(t_{i+1}-t_i)}[(1 - \phi_{i+1}) C_B(S_i \cup \{0\}, t_{i+1}) + \phi_{i+1} C_B(S_i \cup \{1\}, t_{i+1})]dt_{i+1} \right\}. \end{aligned} \tag{1}$$

The solution procedure of the model given in Eq. (1) is backward induction. However, obtaining an analytical solution for optimal waiting time may be impossible except for simple functional forms for $c_H$. To illustrate the backward induction procedure, we use a step-wise cost function for undetected hacker activity in the next section.

### 4.1. Derivation of the optimal waiting time policy for a step-wise cost function

The step-wise function used for the cost of undetected hacker activity ($c_H$) is shown in Fig. 5. The step-wise function is chosen to illustrate the solution procedure for three reasons. First, the step-wise function is a reasonable approximation for damage cost caused by hacker actions. This approximation states the entire damage from hacker action occurs instantaneously when hacker takes action and hacker will not cause further damage until she takes next action. Second, it is possible to determine optimal waiting time by using the step-wise function. Third, any continuous cost function for undetected hacking activity can be approximated using a step-wise function.

For our illustration, we assumed that user takes three actions and leaves the system at the third action if the user's session is not terminated before. We made this assumption for simplification purposes only and relaxing this assumption is possible at the expense of more calculations. We assumed that the first signal arrives when the user enters the system (i.e. $t_1 = 0$). After these assumptions, our original objective function will change to the following form:

$$\begin{aligned} C(S_1, t_1) = \min_{f_1} p_1 & \left\{ \int_{t_1}^{t_1+f_1} \lambda_H e^{-\lambda_H(t_2-t_1)}([c_H(t_2) - c_H(t_1)] + (1 - \phi^r_2) C_H(S_1 \cup \{0\}, t_2) + \phi^r_2 C_H(S_1 \cup \{1\}, t_2))dt_2 \right\} \\ & + (1 - p_1) \left\{ e^{-\lambda_B f_1} c_{B1} + \int_{t_1}^{t_1+f_1} \lambda_B e^{-\lambda_B(t_2-t_1)}[(1 - \phi_2) C_B(S_1 \cup \{0\}, t_2) + \phi_2 C_B(S_1 \cup \{1\}, t_2)]dt_2 \right\}. \end{aligned} \tag{2}$$

The above model uses the fact that damage cost due to hacking increases only when hacker takes an action (i.e. $c_H(t_i+f_i) = c_H(t_i)$ when $(t_i + f_i) < t_{i+1}$). If we assume that $s$ takes a value of 0 or 1 when IDS raises no-alarm or an alarm signal respectively, the following equalities hold given that the user leaves the system at $t_3$:

$$C_B(S_1 \cup \{s\}, t_2) = e^{-\lambda_B (f_2|S_2=s)} c_{B2}; \qquad C_H(S_1 \cup \{s\}, t_2) = (1 - e^{-\lambda_H (f_2|S_2=s)})(c_H(t_3) - c_H(t_2)).$$

As the solution procedure is backward induction, we determine the optimal waiting policy starting at the second user action at $t_2$. The firm will minimize the following cost expression at $t_2$ by choosing the waiting time $f_2$ as:

$$\min_{(f_2|S_2=s)} (p_2 \mid S_2 = s) C_H(S_1 \cup \{s\}, t_2) + (1 - (p_2 \mid S_2 = s)) C_B(S_1 \cup \{s\}, t_2). \tag{3}$$

We obtained the following optimal waiting policy at time $t_2$ from the solution of the above model.

If $\lambda_B > \lambda_H$,

$$(f_2^* \mid S_2 = s) = \frac{\ln(\lambda_B[1 - (p_2 \mid S_2 = s)]c_{B2}) - \ln(\lambda_H (p_2 \mid S_2 = s)[c_H(t_3) - c_H(t_2)])}{\lambda_B - \lambda_H}.$$

If $\lambda_B \le \lambda_H$,

$$\begin{Bmatrix} (f_2^* \mid S_2 = s) = 0 & \text{if } (p_2 \mid S_2 = s)[c_H(t_3) - c_H(t_2)] < [1 - (p_2 \mid S_2 = s)]c_{B2} \\ (f_2^* \mid S_2 = s) = \infty & \text{if } (p_2 \mid S_2 = s)[c_H(t_3) - c_H(t_2)] \ge [1 - (p_2 \mid S_2 = s)]c_{B2} \end{Bmatrix}.$$

We should point out that waiting time of infinity ($\infty$) means that the firm waits until next user actions arrives or the user leaves the system. After deciding the optimal waiting time at $t_2$, the firm will determine the configuration level at $t_2$. This is required for computing optimal waiting time at $t_1$ as the probability that the user is a hacker depends on the configuration level in Eq. (3). For that purpose, SSO needs to consider alarm and no-alarm cases as the configuration level determines the probabilities of these cases. Thus, the firm will minimize the following cost function by choosing the configuration level.

$$\begin{aligned} C(S_2, t_2) = \min_{\phi_2} P(S_2 = 0) &\left( (p_2 \mid S_2 = 0) \int_{t_2}^{t_2 + (f_2^*|S_2=0)} \lambda_H e^{-\lambda_H (t_3 - t_2)} (c_H(t_3) - c_H(t_2)) dt_3 \right. \\ &\left. + \ (1 - (p_2 \mid S_2 = 0)) e^{-\lambda_B (f_2^*|S_2=0)} c_{B2} \right) \\ &+ P(S_2 = 1) \left( (p_2 \mid S_2 = 1) \int_{t_2}^{t_2 + (f_2^*|S_2=1)} \lambda_H e^{-\lambda_H (t_3 - t_2)} (c_H(t_3) - c_H(t_2)) dt_3 \right. \\ &\left. + \ (1 - (p_2 \mid S_2 = 1)) e^{-\lambda_B (f_2^*|S_2=1)} c_{B2} \right) \end{aligned} \tag{4}$$

where

$$p_i = \begin{Bmatrix} \dfrac{\phi_i^r p_{i-1}}{\phi_i (1 - p_{i-1}) + \phi_i^r p_{i-1}} & \text{if } (S_i = 1) \\ \dfrac{[1 - \phi_i^r] p_{i-1}}{[1 - \phi_i](1 - p_{i-1}) + [1 - \phi_i^r] p_{i-1}} & \text{if } (S_i = 0) \end{Bmatrix}. \tag{5}$$

Using Eqs. (4) and (5) together, the objective function can be written as

$$\begin{aligned} C(S_2, t_2) = \min_{\phi_2} &\left( (1 - \phi_2^r) p_1 \int_{t_2}^{t_2 + (f_2^*|S_2=0)} \lambda_H e^{-\lambda_H (t_3 - t_2)} (c_H(t_3) - c_H(t_2)) dt_3 + (1 - p_1)(1 - \phi_2) e^{-\lambda_B (f_2^*|S_2=0)} c_{B2} \right. \\ &\left. + \ \phi_2^r p_1 \int_{t_2}^{t_2 + (f_2^*|S_2=1)} \lambda_H e^{-\lambda_H (t_3 - t_2)} (c_H(t_3) - c_H(t_2)) dt_3 + (1 - p_1) \phi_2 e^{-\lambda_B (f_2^*|S_2=0)} c_{B2} \right). \end{aligned} \tag{6}$$

It is not possible to get a closed solution form of the configuration level from Eq. (6). However, it is possible to get the optimal level of $\phi_2$ for a given $\phi_1$ via simulation in which optimal configuration level is searched at the interval [0, 1]. Note that the waiting time and the optimal confirmation level at $t_1(\phi_2^*)$ depends on $\phi_1$. Thus, the firm needs to choose confirmation level at $t_1$ by minimizing the following expression:

$$\begin{aligned} C(S_1, t_1) = \min_{\phi_1} &\left( \phi_1^r p_0 \int_{t_1}^{t_1 + (f_1^*|S_1=0)} \lambda_H e^{-\lambda_H (t_2 - t_1)} [(c_H(t_2) - c_H(t_1)) + (1 - (\phi_2^*)^r) C_H(S_1 \cup \{0\}, t_2) \right. \\ &+ (\phi_2^*)^r C_H(S_1 \cup \{1\}, t_2)] dt_2 + (1 - \phi_1^r)(1 - p_0) \\ &\times \left( e^{-\lambda_B (f_1^*|S_1=0)} c_{B1} + \int_{t_1}^{t_1 + (f_1^*|S_1=0)} \lambda_B e^{-\lambda_B (t_2 - t_1)} [(1 - \phi_2^*)(C_B(S_1 \cup \{0\}, t_2)) \right. \end{aligned}$$

$$
\begin{aligned}
&+\ \phi_2^*(C_B(S_1\cup\{1\},t_2))]dt_2\Bigg)\Bigg)+\Bigg(\phi_1 p_0\int_{t_1}^{t_1+(f_1^*|S_1=1)}\lambda_H e^{-\lambda_H(t_2-t_1)}[(c_H(t_2)-c_H(t_1))\\
&+(1-(\phi_2^*)^r)C_H(S_1\cup\{0\},t_2)+(\phi_2^*)^r C_H(S_1\cup\{1\},t_2)]dt_2\\
&+(1-\phi_1)(1-p_0)\Bigg(e^{-\lambda_B(f_1^*|S_1=1)}c_{B1}+\int_{t_1}^{t_1+(f_1^*|S_1=1)}\lambda_B e^{-\lambda_B(t_2-t_1)}[(1-\phi_2^*)(C_B(S_1\cup\{0\},t_2))\\
&+\ \phi_2^*(C_B(S_1\cup\{1\},t_2))]dt_2\Bigg)\Bigg)
\end{aligned}
$$

where

$$
(f_1^*|S_1=s)=\frac{\ln\left(\frac{(1-(p_1|S_1=s))\lambda_B[c_{B1}-((1-\phi_2^*)C_B(S_1\cup\{0\})+\phi_2^*(C_B(S_1\cup\{1\})))]}{(p_1|S_1=s)[(c_H(t_2)-c_H(t_1))+\lambda_H((1-(\phi_2^*)^r)C_H(S_1\cup\{0\})+(\phi_2^*)^r C_H(S_1\cup\{1\}))]}\right)}{\lambda_B-\lambda_H}
$$

and $C_B(S_1\cup\{s\},t_2)=e^{-\lambda_B(f_2|S_2=s)}c_{B2};\ C_H(S_1\cup\{s\},t_1)=(1-e^{-\lambda_H(f_2|S_2=s)})(c_H(t_3)-c_H(t_2))$.

The analysis demonstrates the standard backward induction algorithm used for dynamic programming models to derive the optimal waiting time policy when the damage cost follows a stepwise function. Although it is not possible to find analytical solution for the optimal configuration level, it can be obtained via simulation. For the other cost functions, two strategies can be followed. The first strategy is to approximate the damage cost using step-wise function and apply the backward induction algorithm described in this section. The second strategy is to solve a myopic model that minimizes the cost associated with the user's current action. We analyze this model in the next section.

## 5. Myopic configuration policy

In this section, we analyze the configuration and waiting time decision under myopic policy. We call the policy myopic since we consider only the current action of the user and we minimize the expected cost during the period between $t_i$ and the next decision point which is the minimum of the arrival of the next signal and the end of the waiting time. As we ignore future user action, we set the values of $C_H(S_i\cup\{s\},t_{i+1})$ and $C_B(S_i\cup\{s\},t_{i+1})$ to zero in Eq. (1). Thus, the firm will minimize the following expected cost function:

$$
\begin{aligned}
C(\hat{S}_i,t_i)&=\min_{f_i} p_i\int_{t_i}^{t_i+f_i}\lambda_H e^{-\lambda_H(t_{i+1}-t_i)}[c_H(t_{i+1})-c_H(t_i)]dt_{i+1}\\
&\quad+e^{-\lambda_H f_i}p_i[c_H(t_i+f_i)-c_H(t_i)]+e^{-\lambda_B f_i}(1-p_i)c_{Bi}.
\end{aligned}
\tag{7}
$$

The waiting time under myopic policy $(f_i^*)$ will satisfy the following first order condition of the above function:

$$
e^{-\lambda_H f_i^*}p_i\left[\frac{\partial c_H(t_i+f_i^*)}{\partial f_i^*}\right]=\lambda_B e^{-\lambda_B f_i^*}(1-p_i)c_{Bi}.
\tag{8}
$$

After deciding on the waiting time under myopic policy, the firm will decide on the configuration level under myopic policy. For that purpose, it will minimize following expected cost:

$$
\begin{aligned}
\min_{\phi_i}&\Bigg\{P(S_i=0)\Bigg((p_i\mid S_i=0)\int_{t_i}^{(t_i+f_i^*|S_i=0)}\lambda_H e^{-\lambda_H(t_{i+1}-t_i)}[c_H(t_{i+1})-c_H(t_i)]dt_{i+1}\\
&+e^{-\lambda_H(f_i^*|S_i=0)}(p_i\mid S_i=0)[c_H(t_i+(f_i^*\mid S_i=0))-c_H(t_i)]+e^{-\lambda_B(f_i^*|S_i=0)}(1-(p_i\mid S_i=0))c_{Bi}\Bigg)\\
&+P(S_i=1)\Bigg((p_i\mid S_i=1)\int_{t_i}^{t_i+(f_i^*|S_i=1)}\lambda_H e^{-\lambda_H(t_{i+1}-t_i)}[c_H(t_{i+1})-c_H(t_i)]dt_{i+1}\\
&+e^{-\lambda_H(f_i^*|S_i=1)}(p_i\mid S_i=1)[c_H(t_i+(f_i^*\mid S_i=1))-c_H(t_i)]+\ e^{-\lambda_B(f_i^*|S_i=1)}(1-(p_i\mid S_i=1))c_{Bi}\Bigg)\Bigg\}
\end{aligned}
\tag{9}
$$

where $P(S_i=1)=\phi_i(1-p_{i-1})+\phi_i^r p_{i-1}$ and $P(S_i=0)=(1-\phi_i)(1-p_{i-1})+(1-\phi_i^r)p_{i-1}1$.

We illustrate the solution procedure by using a linear cost function as it is difficult to obtain solutions for the other types of cost functions. The linear cost function helps us identify characteristics of configuration level as well. We get the following objective function when we replace Eq. (5) in Eq. (9) and we assume that cost due to undetected hacker activity increases linearly with time:

$$\min_{\phi_i} L = \left\{ \frac{(1-\phi_i^r)p_{i-1}A(1-e^{-\lambda_H(f_i^*|S_i=0)})}{\lambda_H} + (1-\phi_i)(1-p_{i-1})e^{-\lambda_B(f_i^*|S_i=0)}c_{Bi} \right.$$
$$\left. + \frac{\phi_i^r p_{i-1}A(1-e^{-\lambda_H(f_i^*|S_i=1)})}{\lambda_H} + \phi_i(1-p_{i-1})e^{-\lambda_B(f_i^*|S_i=1)}c_{Bi} \right\} \qquad (10)$$

where myopic waiting time policy is given as follows for $s \in \{0, 1\}$.

If $\lambda_B > \lambda_H$,

$$(f_i^* \mid S_i = s) = \frac{\ln\left(\frac{\lambda_B(1-(p_i|S_i=s))c_{Bi}}{(p_i|S_i=s)A}\right)}{(\lambda_B - \lambda_H)}.$$

If $\lambda_B \le \lambda_H$,

$$\left\{ \begin{array}{ll} (f_i^* \mid S_i = s) = 0 & \text{if } \dfrac{A(p_i \mid S_i = s)}{\lambda_H} \ge (1-(p_i \mid S_i = s))c_{B\,i} \\ (f_i^* \mid S_i = s) = \infty & \text{if } \dfrac{A(p_i \mid S_i = s)}{\lambda_H} < (1-(p_i \mid S_i = s))c_{B\,i} \end{array} \right\}$$

where $\frac{A(p_i|S_i=s)}{\lambda_H}$ represents the cost of waiting next signal and $(1-(p_i \mid S_i = s))c_{B\,i}$ represents the cost of taking immediate action. Thus, if the cost of waiting next signal is greater than the cost of taking immediate action, the firm takes immediate action (i.e. $(f_i^* \mid S_i = s) = 0$). Otherwise, the firm will wait next signal to come (i.e. $(f_i^* \mid S_i = s) = \infty$). Note that waiting time policy depends on the ratio of $A/c_{B\,i}$ in both cases.

We will analyze two cases separately as we get a different optimal configuration level. When $\lambda_B > \lambda_H$, the myopic configuration level satisfies the following equation:

$$r\phi_i^{r-1}p_{i-1}\left[\frac{A(1-e^{-\lambda_H(f_i^*|S_i=1)})}{\lambda_H} - \frac{A(1-e^{-\lambda_H(f_i^*|S_i=0)})}{\lambda_H}\right] = (1-p_{i-1})[e^{-\lambda_B(f_i^*|S_i=0)}c_{B\,i} - e^{-\lambda_B(f_i^*|S_i=1)}c_{B\,i}] \qquad (11a)$$

where left hand side represents the marginal cost of increasing configuration due to hacking and right hand side represents marginal cost of increasing configuration due to taking action against benign user. After modifying Eq. (11a), we got the following equation:

$$\lambda_B r(e^{\lambda_H((f_i^*|S_i=1)-(f_i^*|S_i=0))} - 1) = \lambda_H(e^{\lambda_B((f_i^*|S_i=1)-(f_i^*|S_i=0))} - 1). \qquad (11b)$$

Derivation of Eqs. (11a) and (11b) can be found in the Appendix. Note that the difference between waiting times after no-alarm and alarm signal $((f_i^* \mid S_i = 0) - (f_i^* \mid S_i = 1))$ depends on myopic configuration level and arrival rate of signal from benign user and hacker. Although solution for myopic configuration can be obtained only via numerical analysis, the Eq. (11b) allows us to analyze the behavior of myopic configuration policy to the changes in parameters. These are summarized in Proposition 2.

**Proposition 2.** *When $\lambda_B > \lambda_H$ and $(f_i^* \mid S_i = 0) > 0$, $(f_i^* \mid S_i = 1) > 0$,*

$$\text{(i)}\ \frac{\partial\phi_i^*}{\partial p_{i-1}} = 0, \qquad \text{(ii)}\ \frac{\partial\phi_i^*}{\partial c_{B\,i}} = 0, \qquad \text{(iii)}\ \frac{\partial\phi_i^*}{\partial A} = 0 \qquad \text{(iv)}\ \frac{\partial\phi_i^*}{\partial\lambda_H} < 0 \quad \textit{and} \quad \text{(v)}\ \frac{\partial\phi_i^*}{\partial\lambda_B} > 0.$$

Proof of Proposition 2 is in the Appendix. Proposition 2(i)–(iii) show that optimal myopic configuration level is independent of prior probability $(p_{i-1})$, the cost of false alarm and damage cost per unit time $(A)$ as a change in these parameters changes the expected cost in Eq. (10) with the same proportion and the Eq. (11b) does not depend on these parameters. The fourth result states that a more frequent signal from a hacker decreases the optimal myopic configuration level as the cost of hacking decreases. However, a more frequent signal from a benign user increases myopic configuration level as it becomes easier to differentiate a benign user from the hacker.

These results depend on the assumption that waiting times should be positive and if it does not hold, (i.e. $(f_i^* \mid S_i = 0) > (f_i^* \mid S_i = 1) = 0$), the results in Proposition 2 will no longer be valid. In this case, myopic configuration policy will satisfy the following equation when we replace $(f_i^* \mid S_i = 1) = 0$ in Eq. (10):

$$\frac{r(\phi^*)^{r-1}p_{i-1}A(1-e^{-\lambda_H(f_i^*|S_i=0)})}{\lambda_H} = (1-p_{i-1})c_{B\,i}(1-e^{-\lambda_B(f_i^*|S_i=0)}). \qquad (12)$$

Similar to Eq. (11), the right hand side of the Eq. (12) represents the marginal cost of taking action against a hacker and the left side of the equation represents the marginal cost of taking action against a benign user. Note that the configuration policy depends on the ratio of $A/c_{B\,i}$ as both the waiting time policy and Eq. (12) depend on the ratio of $A/c_{B\,i}$ for the determination of configuration policy. The characteristics of myopic configuration policy in Eq. (12) are summarized in the following proposition.

**Proposition 3.** *When* $\lambda_B > \lambda_H$ *and* $(f_i^* \mid S_i = 0) > (f_i^* \mid S_i = 1) = 0$,

$$\text{(i)}\ \frac{\partial \phi_i^*}{\partial c_{B\,i}} < 0, \qquad \text{(ii)}\ \frac{\partial \phi_i^*}{\partial p_{i-1}} > 0, \qquad \text{(iii)}\ \frac{\partial \phi_i^*}{\partial A} > 0, \qquad \text{(iv)}\ \frac{\partial \phi_i^*}{\partial \lambda_H} < 0 \qquad \text{(v)}\ \frac{\partial \phi_i^*}{\partial \lambda_B} < 0.$$

Proof of Proposition 3 is in the Appendix. Proposition 3(i) states that high cost of incorrectly concluding that a benign user is a hacker lowers the myopic configuration level since raising the alarm signal becomes more costly. Proposition 3(ii) and (iii) show that the higher prior probability that a user is a hacker and higher damage cost per unit time result in a higher myopic configuration level as the cost of raising no-alarm signal increases. Proposition 3(iv) states that a more frequent signal from a hacker decreases the myopic configuration level as the expected cost due to hacking decreases. In Proposition 3(v), the configuration level decreases with a more frequent signal from a benign user as the IDS differentiates a benign user from a hacker better.

When $\lambda_B \le \lambda_H$, the firm will either take immediate action ($f_i = 0$) or wait for the next signal to arrive ($f_i = \infty$). Since waiting times after an alarm are not greater than waiting times after no-alarm (i.e. $(f_i \mid S_i = 0) \ge (f_i \mid S_i = 1)$), three possible cases arise. These are (i) $(f_i \mid S_i = 1) = (f_i \mid S_i = 0) = 0$, (ii) $(f_i \mid S_i = 1) = (f_i \mid S_i = 0) = \infty$ or (iii) $(f_i \mid S_i = 1) = 0$, $(f_i \mid S_i = 0) = \infty$. For the first two cases, configuration decision is independent of expected cost. For this reason, we examine only the third case and we get the following objective function when values of $(f_i \mid S_i = 1) = 0$ and $(f_i \mid S_i = 0) = \infty$ are replaced in Eq. (10).

$$\min_{\phi_i} \left\{ (1-\phi_i)(1-p_{i-1})c_{B\,i} + \frac{\phi_i^r p_{i-1} A}{\lambda_H} \right\}. \tag{13}$$

From the first order condition of the above equation, it is possible to get configuration level as

$$\phi_i^* = \left[ \frac{r p_{i-1} A}{(1-p_{i-1}) c_{B\,i} \lambda_H} \right]^{\frac{1}{1-r}}. \tag{14}$$

Further analysis of myopic configuration policy, characterized by Eq. (14), shows the following results.

**Proposition 4.** *When* $\lambda_B \le \lambda_H$, *and* $(f_i \mid S_i = 1) = 0$, $(f_i \mid S_i = 0) = \infty$,

$$\text{(I)}\ \frac{\partial \phi_i^*}{\partial c_{B\,i}} < 0, \qquad \text{(ii)}\ \frac{\partial \phi_i^*}{\partial p_{i-1}} > 0, \qquad \text{(iii)}\ \frac{\partial \phi_i^*}{\partial A} > 0, \qquad \text{(iv)}\ \frac{\partial \phi_i^*}{\partial \lambda_H} < 0 \qquad \text{(v)}\ \frac{\partial \phi_i^*}{\partial \lambda_B} = 0.$$

The first two results are similar to Proposition 3(i) and (ii). As $\frac{A}{\lambda_H}$ represents the damage cost if the next signal is awaited, we get $\frac{\partial \phi_i^*}{\partial A} > 0$ and $\frac{\partial \phi_i^*}{\partial \lambda_H} < 0$ in Proposition 4(iii) & (iv). The arrival rate of a signal from a benign user ($\lambda_B$) does not affect the configuration level as the firm takes immediate action when the alarm signal is received.

We also would like to note that under the assumption of Propositions 3 and 4, raising a no-alarm (alarm) signal will be more likely for further user actions and the waiting time is expected to increase (decrease) over time if the user happens to be benign (hacker). This is because Proposition 1 states that if the user is benign (hacker), the probability that a user is believed to be benign (hacker) will increase over time. Consequently, the configuration level decreases (increases) due to Propositions 3(i) and 4(i) and waiting time decreases (increases) due to Proposition 3(ii) of [6] if the user is benign (hacker).

While we expected that the cost incurred under waiting times polices with fixed configurations is greater than the cost incurred under waiting times with dynamic configurations, we should determine how much cost reduction is achieved through adopting dynamic configuration policies rather than fixed configuration policies since the implementation of myopic (optimal) configuration policy requires more computation than myopic (optimal) policy with fixed configuration. For that purpose, we compare the performance of these policies through numerical analysis in the next section.

## 6. Comparison of optimal and myopic policies

In our simulations, the user type was generated form Bernoulli probability distribution with parameter $p_0$. The time that the user enters the system is zero. The user leaves the system after two actions if her session is not terminated earlier. We limited the number of user actions to two as this is the minimum number of user actions to compare with the myopic policy's configuration policies. The cost due to the hacking increases linearly with time. (i.e., $C_H(t) = At$) where $A$ is the intensity of damage due to hacking. We assumed that the user is risk neutral and the arrival rate of the hacker's action is greater than the

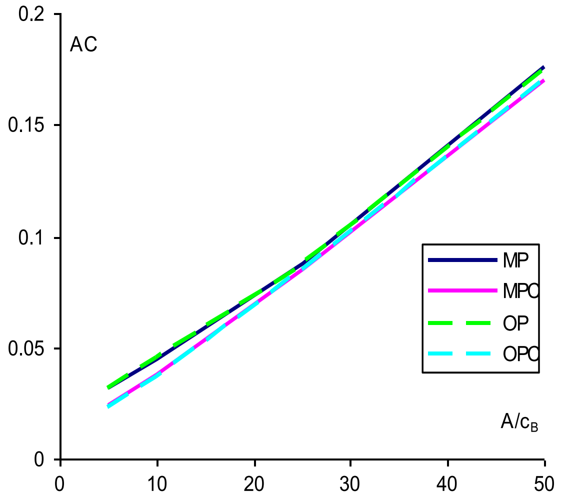

**Fig. 6.** Impact of $A/c_B$ on average cost.

arrival rate of the benign user's action. This assumption is required in order to get positive waiting times. We also assume that cost of a false positive for each user action is the same for simplicity (i.e. $c_{B1} = c_{B2} = c_B$). We used power function for *ROC* curve in our simulation.

We simulated 100 batches of 1000 users for each set of parameter values. The following ranges of parameter values are used in our analysis: $p_0 \in \{0.001, 0.01, 0.05, 0.1\}$; $\lambda_B \in \{2, 4, 8, 16\}$; $\lambda_H \in \{0.25, 0.5, 1, 1.5\}$ $C_H(t) = At$, $A/c_B \in \{1, 10, 25, 50\}$. We assumed that the proportion of hackers is much smaller than the proportion of benign users in the user population. For this reason, we determine the proportion of benign users as a small value. We choose the relative ratio of $A/c_B$ rather than the level of $A$ and $c_B$ as optimal configuration and myopic configuration level can be dependent on the level of $A/c_B$. We also assume that the cost due to the undetected hacker activity is much larger than the cost of false positive and determine the parameters of $A/c_B$ and $\lambda_H$ accordingly. Thus, the defaults parameter values of simulations are chosen as: $p_0 = 0.01$, $\lambda_H = 1$, $\lambda_B = 2$, and $A/c_B = 25$.

We compare the cost performance of four polices in our analysis: optimal waiting time policy with fixed configuration (*OC*), myopic waiting time policy with fixed configuration (*MC*), optimal waiting time policy with optimal configuration (optimal configuration policy (*OPC*)) and myopic waiting time policy with myopic configuration (myopic configuration policy (*MPC*)). Waiting time polices with fixed configurations (*MC* and *OC*) are used for benchmarking purposes and they are analyzed by Ogut et al. [6] earlier. We set false alarm and true alarm probabilities as $\phi = 0.01$ and $\phi^r = 0.75$ respectively for these policies. The quality parameter of IDS is derived as $r = \frac{\ln 0.75}{\ln 0.01} = 0.06247$.

The behaviors of myopic and optimal configuration policy to the changes in parameter values are also analyzed. We would like to note that these are the configuration levels set at time 0. We are interested in determining whether theoretical results of Propositions 2 or 3 hold for myopic policy. We consider optimal configuration policy (*OPC*) and myopic configuration policy (*MPC*) only for configuration comparison as other polices have a fixed configuration level. We would like to compare the cost performance of these four policies as well.

We presented our results in two separate categories: (i) effects of firm's internal cost parameter, the ratio of damage cost per time unit ($A$) to cost of taking action against benign user ($c_B$) and (ii) effects of parameters related to the hacking environment, prior probability that the user is a hacker ($p_0$) and arrival rate of a signal from a hacker and benign user ($\lambda_H$ and $\lambda_B$).

Fig. 6 summarizes the results of the change in the ratio of damage cost to cost of false positive ($A/c_B$) on all policies. As $A/c_B$ increases, hacker causes higher damage due to undetected activity compared to cost of taking action against benign users. Furthermore, waiting time decreases and a shorter waiting time results in an increase in the number of incorrect decisions where the benign user is a hacker. Thus, average costs ($AC$) are higher for all polices for a higher level of $A/c_B$. IDS also raises more alarms in order to detect intrusion earlier since the cost of taking action becomes smaller. Thus, configuration level ($\phi$) increases with the increase in $A/c_B$ in Fig. 7.

The hacking environment is characterized by the proportion of hackers in the user population ($p_0$) and the rates at which hackers and benign users interact with the system ($\lambda_B$ *and* $\lambda_H$). Fig. 8 summarizes the effect of the proportion of hackers in the user population ($p_0$). A higher proportion of hackers in the user population and resulting decrease in waiting time increases average cost ($AC$) as a result of the increase in the number of hackers and the increase in the number of incorrect decisions where the benign user is a hacker. We would like to note that when the proportion of hackers reaches a threshold level, the firm takes immediate action against all users and average cost ($AC$) under all policies starts to decrease as the proportion of hackers increases. We have also found that IDS raises more alarms in response to the higher proportion of hackers in the user population. Thus, configuration level ($\phi$) increases with the increase in $p_0$ in Fig. 9.

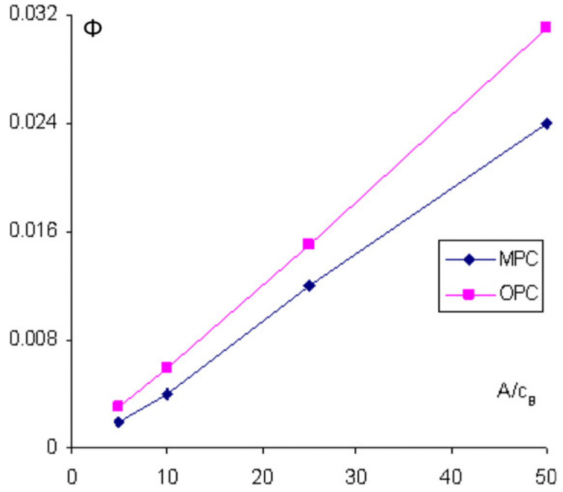

**Fig. 7.** Impact of $A/c_B$ on configuration level.

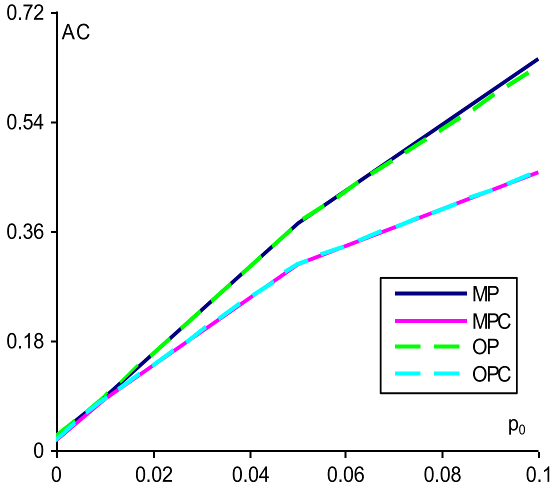

**Fig. 8.** Impact of prior probability on average cost.

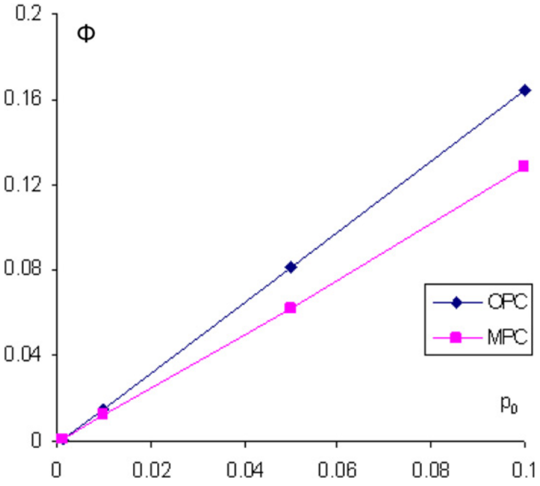

**Fig. 9.** Impact of prior probability on configuration level.

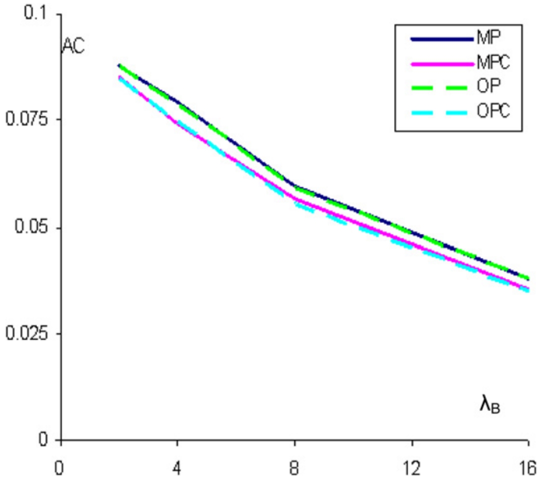

**Fig. 10.** Impact of $\lambda_B$ on average cost.

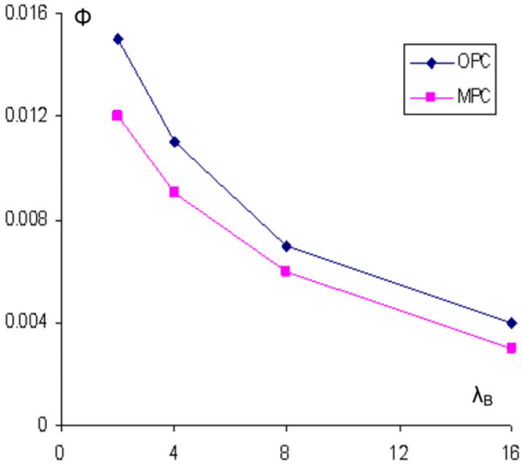

**Fig. 11.** Impact of $\lambda_B$ on configuration level.

**Table 2**
Statistics about performance of policies relative to myopic policy.

| | Mean | Minimum | Maximum |
|---|---|---|---|
| Myopic configuration | 11.80 | 1.39 | 28.79 |
| Optimal policy | 0.37 | 0.00 | 1.81 |
| Optimal configuration | 12.51 | 3.19 | 29.15 |

When the arrival rate of a signal from the benign user ($\lambda_B$) increases, the average cost ($AC$) decreases since the firm's expected cost of taking action against benign user ($e^{-\lambda_B f_i} c_{Bi}$) decreases. The alarm rate and configuration level ($\phi$) decreases as well as the marginal cost of taking action against the benign user. When the signals from a hacker become more frequent (i.e. $\lambda_H$ increases), the firm's average cost ($AC$) decreases as the expected cost due to hacking decreases. For the same reasoning, the configuration level ($\phi$) decreases as a result of the increase in the rate of signal from hacker (see Figs. 10–13).

In summary, the myopic policy with fixed configuration ($MC$) has the highest and the optimal configuration policy ($OCP$) has the lowest cost among all polices. We have also found that average cost under myopic configuration policy ($MCP$) is lower than average cost under optimal policy with fixed configuration ($OC$). This result shows that configuration policies are as important as waiting time policies. To get a more meaningful result, statistics that show how worse the performance of the myopic policy is compared to other policies are presented as well. We found that the average difference between the costs under the specific policy and the myopic policy expressed as the percentage of the cost under the specific policy, i.e., $(\frac{\text{cost under myopic policy}-\text{cost under specific policy}}{\text{cost under specific policy}})*100$, ranged from 0% to 29.15%. These results are summarized in Table 2.

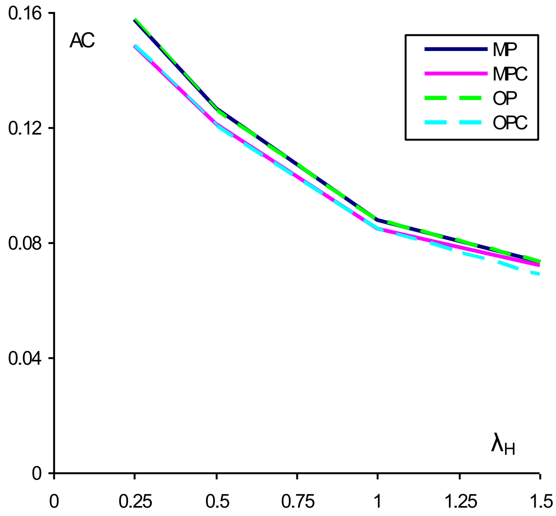

**Fig. 12.** Impact of $\lambda_H$ on average cost.

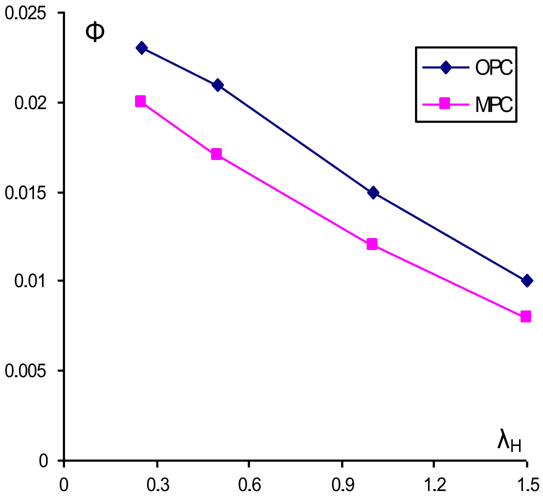

**Fig. 13.** Impact of $\lambda_H$ on configuration level.

**Table 3**
Statistics about standard deviation of policies.

| | Mean | Minimum | Maximum |
|---|---|---|---|
| Myopic policy | 0.07 | 0.01 | 0.14 |
| Myopic configuration policy | 0.06 | 0.01 | 0.11 |
| Optimal policy | 0.06 | 0.01 | 0.12 |
| Optimal configuration policy | 0.06 | 0.01 | 0.11 |

Because arrival time of user actions and user type are generated form probability distribution, we also reported the standard errors of the cost. Based on Tables 2 and 3, we can say that the cost difference between myopic and optimal configuration polices and the standard errors of each policy are small enough to make the differences between these policies insignificant. This comparison enables us to conclude that the myopic configuration policy ($MCP$) is a good substitute for the optimal configuration policy ($OCP$). Thus, we suggested to use the myopic configuration policy instead of the optimal configuration policy as it is easier to implement. Furthermore, the myopic configuration policy does not need to take into account the number of user actions since it considers the current user action only.

To sum up, we found that the optimal configuration level is higher than the myopic configuration level in our simulation. That is because the optimal configuration policy considers current and future user action. Our simulation results support the theoretical results of Proposition 3 rather than the theoretical results of Proposition 2. This shows that the zero waiting time after the alarm signal is a valid assumption. Our analysis also shows that the behavior of the optimal configuration policy is similar to the behavior of the myopic configuration policy to the change in parameters. Thus, the theoretical result of Proposition 3 is likely to hold for optimal configuration policy. We have also observed that the cost performance of myopic configuration policy is nearly identical to the optimal configuration policy.

## 7. Conclusion

In this paper, we extend waiting time policies proposed by Ogut et al. [6] by making configuration a decision variable. We formulated the firm's problem as a stochastic dynamic programming model and derived the optimal waiting time policy about a firm's action when it receives a signal. However, an optimal configuration policy can be obtained only via numerical analysis. Because the optimal configuration and waiting time policies may be difficult to implement in many situations, we also analyzed myopic configuration and waiting time policies. Then we conducted a numerical analysis to compare optimal and myopic policies with fixed and dynamic configuration. Our simulations suggested that the configuration decision significantly affects the performance of policies. We also compare the behavior of the optimal configuration policy and myopic configuration policy to the change in parameters and we have found that theoretical result of myopic policy applies to optimal polices, and the configuration level for the optimal policy is higher than the configuration level for the myopic policy. We also identified that the cost performance of myopic and optimal configuration policies are similar to each other.

Policies derived in these papers provide better decision support to firms employing IDS. However successful implementation of these policies depends on the realistic estimates of the parameters used in our model. For that purpose, the history of user log files can be sourced for user related parameters such as arrival rate of signals from benign users and hackers and proportion of hackers in the user population. Recently, many firms began to collect data about hacker behavior through the honey pots as well [31,32]. Although the damage cost due to security breaches is relatively more difficult to estimate, researches aims to quantify such costs in recent years [17,33–37].

The paper contributes to the literature in many ways. Our paper extends the paper by Ogut et al. [6] and show that the configuration decision is as important as the waiting time decision. We also extend the configuration paper of Ulvila and Gaffney [18] by adding a time dimension and showing how the dynamic decision of configuration and detection is made in intrusion detection systems.

The research described in this paper can be extended in several ways. We used a decision theoretic model, however a game theoretic model incorporating strategic interaction between the hacker and firm might be insightful as well. Another way of extending our paper is considering multiple signals rather than binary signals as researchers begin to analyze the performance of IDS by incorporating additional information such as attack severity and attack frequencies.

## Appendix

**Proof for Proposition 1.** We will show the following inequality for the proof of Proposition 1.

$$(p_{i+1}|\text{hacker}) = (p_{i+1}|S_{i+1}=1)^{*}P(S_{i+1}=1|\text{hacker}) + (p_{i+1}|S_{i+1}=0)^{*}P(S_{i+1}=0|\text{hacker}) > p_i \tag{A.1}$$

(A.1) can be written explicitly as

$$\begin{aligned}&\frac{\phi^r_{i+1}p_i}{\phi_{i+1}(1-p_i)+\phi^r_{i+1}p_i}\phi^r_{i+1} + \frac{(1-\phi^r_{i+1})p_i}{(1-\phi_{i+1})(1-p_i)+(1-\phi^r_{i+1})p_i}(1-\phi^r_{i+1}) > p_i\\ &\quad = \frac{\phi^r_{i+1}p_i}{\phi_{i+1}(1-p_i)+\phi^r_{i+1}p_i}[\phi_{i+1}(1-p_i)+\phi^r_{i+1}p_i]\\ &\quad\quad + \frac{(1-\phi^r_{i+1})p_i}{(1-\phi_{i+1})(1-p_i)+(1-\phi^r_{i+1})p_i}[(1-\phi_{i+1})(1-p_i)+(1-\phi^r_{i+1})p_i]\end{aligned} \tag{A.2}$$

or

$$\frac{\phi^r_{i+1}p_i}{\phi_{i+1}(1-p_i)+\phi^r_{i+1}p_i}(\phi^r_{i+1}-\phi_{i+1})(1-p_i) + \frac{(1-\phi^r_{i+1})p_i}{(1-\phi_{i+1})(1-p_i)+(1-\phi^r_{i+1})p_i}(\phi_{i+1}-\phi^r_{i+1})(1-p_i) > 0. \tag{A.3}$$

Since $\frac{\phi^r_{i+1}p_i}{\phi_{i+1}(1-p_i)+\phi^r_{i+1}p_i} > \frac{(1-\phi^r_{i+1})p_i}{(1-\phi_{i+1})(1-p_i)+(1-\phi^r_{i+1})p_i}$ and $(\phi^r_{i+1} > \phi_{i+1})$,

$$\frac{\phi^r_{i+1}p_i}{\phi_{i+1}(1-p_i)+\phi^r_{i+1}p_i}(\phi^r_{i+1}-\phi_{i+1})(1-p_i) + \frac{(1-\phi^r_{i+1})p_i}{(1-\phi_{i+1})(1-p_i)+(1-\phi^r_{i+1})p_i}(\phi_{i+1}-\phi^r_{i+1})(1-p_i) > 0. \tag{A.4}$$

That is, $(p_{i+1}|\text{hacker}) > p_i$.

The proof for the benign user is similar to the above.

**Derivation of** Eqs. (11a) and (11b)

The firm minimizes the following

$$\min_{\phi_i} L = \left\{ \frac{(1-\phi_i^r)p_{i-1}A(1-e^{-\lambda_H(f_i^*|S_i=0)})}{\lambda_H} + (1-\phi_i)(1-p_{i-1})c_{B\ i}e^{-\lambda_B(f_i^*|S_i=0)} \right.$$
$$\left. + \frac{\phi_i^r p_{i-1}A(1-e^{-\lambda_H(f_i^*|S_i=1)})}{\lambda_H} + \phi_i(1-p_{i-1})c_{B\ i}e^{-\lambda_B(f_i^*|S_i=1)} \right\}.$$

First order condition of the above equation is

$$\frac{\partial L}{\partial \phi_i} = \left[ \begin{array}{l} (-\lambda_B(1-p_{i-1})c_{B\ i}(1-\phi_i)e^{-\lambda_B(f_i^*|S_i=0)} + p_{i-1}A(1-\phi_i^r)e^{-\lambda_H(f_i^*|S_i=0)})\dfrac{\partial(f_i^* \mid S_i=0)}{\partial \phi_i} \\ (-\lambda_B(1-p_{i-1})c_{B\ i}\phi_i e^{-\lambda_B(f_i^*|S_i=1)} + p_{i-1}A\phi_i^r e^{-\lambda_H(f_i^*|S_i=1)})\dfrac{\partial(f_i^* \mid S_i=1)}{\partial \phi_i} \end{array} \right]$$
$$+ r\phi_i^{r-1}p_{i-1}\left[ \frac{A(1-e^{-\lambda_H(f_i^*|S_i=1)})}{\lambda_H} - \frac{A(1-e^{-\lambda_H(f_i^*|S_i=0)})}{\lambda_H} \right]$$
$$- (1-p_{i-1})[e^{-\lambda_B(f_i^*|S_i=0)}c_{B\ i} - e^{-\lambda_B(f_i^*|S_i=1)}c_{B\ i}] = 0.$$

The first two terms are equal to 0 since

$$(f_i^* \mid S_i = 1) = \frac{\ln\left(\frac{\lambda_B\phi_i(1-p_{i-1})c_{B\ i}}{\phi_i^r p_{i-1}A}\right)}{(\lambda_B-\lambda_H)}; \qquad (f_i^* \mid S_i = 0) = \frac{\ln\left(\frac{\lambda_B[1-\phi_i](1-p_{i-1})c_{B\ i}}{[1-\phi_i^r]p_{i-1}A}\right)}{(\lambda_B-\lambda_H)}.$$

Thus, we get Eq. (11a) as

$$\frac{\partial L}{\partial \phi_i} = \frac{r\phi_i^{r-1}p_{i-1}A}{\lambda_H}(e^{-\lambda_H(f_i^*|S_i=0)} - e^{-\lambda_H(f_i^*|S_i=1)}) - (1-p_{i-1})c_{B\ i}(e^{-\lambda_B(f_i^*|S_i=0)} - e^{-\lambda_B(f_i^*|S_i=1)}) = 0.$$

Since $(f_i^* \mid S_i = 1) = \frac{\ln(\frac{\lambda_B\phi_i(1-p_{i-1})c_{B\ i}}{\phi_i^r p_{i-1}A})}{(\lambda_B-\lambda_H)}$, we can get Eq. (11b) as

$$\lambda_B r(e^{\lambda_H((f_i^*|S_i=1)-(f_i^*|S_i=0))} - 1) = \lambda_H(e^{\lambda_B((f_i^*|S_i=1)-(f_i^*|S_i=0))} - 1). \quad \square$$

**Proof for Proposition 2.**

$$\lambda_B r(e^{\lambda_H(f_i^1-f_i^0)} - 1) - \lambda_H[e^{\lambda_B(f_i^1-f_i^0)} - 1] = 0 \tag{A.5}$$

where

$$f_i^1 - f_i^0 = \frac{\ln\left(\frac{\lambda_B\phi(1-p_{i-1})c_{B\ i}}{\phi^r p_{i-1}A}\right)}{(\lambda_B-\lambda_H)} - \frac{\ln\left(\frac{\lambda_B[1-\phi](1-p_{i-1})c_{B\ i}}{[1-\phi^r]p_{i-1}A}\right)}{(\lambda_B-\lambda_H)}$$
$$= \frac{\ln\left(\frac{\phi[1-\phi^r]}{\phi^r[1-\phi]}\right)}{(\lambda_B-\lambda_H)}.$$

Denote $Z = \ln(\frac{\phi[1-\phi^r]}{\phi^r[1-\phi]})$. Then Eq. (A.5) an be written as

$$\lambda_B r\left(e^{\frac{\lambda_H Z}{(\lambda_B-\lambda_H)}} - 1\right) = \lambda_H\left[e^{\frac{\lambda_B Z}{(\lambda_B-\lambda_H)}} - 1\right]. \tag{A.6}$$

Proofs of Propositions 2(i), 1(ii) and (iii) are due to Eq. (A.6).

Using (A.6), we can write that

$$\left(e^{\frac{\lambda_H Z}{(\lambda_B-\lambda_H)}}\right) = \lambda_H M + 1 \tag{A.7}$$

$$\left[e^{\frac{\lambda_B Z}{(\lambda_B-\lambda_H)}}\right] = \lambda_B r M + 1 \tag{A.8}$$

where $M > 0$. Dividing (A.8)–(A.7), we get,

$$\frac{\lambda_B rM + 1}{\lambda_H M + 1} = \left(\frac{\phi[1-\phi^r]}{\phi^r[1-\phi]}\right) = \frac{[\phi - \phi^{r+1}]}{[\phi^r - \phi^{r+1}]}. \tag{A.9}$$

If we increase (decreases), $\lambda_B(\lambda_H)$, left hand side of Eq. (A.9) increases. Then we need to determine the sign of $\frac{\partial(\frac{\phi[1-\phi^r]}{\phi^r[1-\phi]})}{\partial\phi} = \frac{\phi^r[(1-r)-\phi^r+r\phi]}{[\phi^r-\phi^{r+1}]^2}$. Since $\frac{\partial(r+\phi^r-r\phi)}{\partial\phi} = r\phi^{r-1} - r = 0 \Rightarrow \phi = 1$, the maximum value of $(r + \phi^r - r\phi)$ is achieved when $\phi = 1$. This shows that $\frac{\partial(\frac{\phi[1-\phi^r]}{\phi^r[1-\phi]})}{\partial\phi} > 0$. Thus, $\frac{\partial\phi}{\partial\lambda_H} < 0$ and $\frac{\partial\phi}{\partial\lambda_B} > 0$. □

**Proof for Proposition 3. When** $(f_i^* \mid S_i = 0) > (f_i^*|S_i = 1) = 0$, Eq. (10) reduces the following equation

$$C = \left\{\frac{[1-\phi_i^r]p_{i-1}A(1-e^{-\lambda_H(f_i^*|S_i=0)})}{\lambda_H} + [1-\phi_i](1-p_{i-1})e^{-\lambda_B(f_i^*|S_i=0)}c_{B\ i} + \phi_i(1-p_{i-1})c_{B\ i}\right\} \tag{A.10}$$

where $(f_i^* \mid S_i = 0) = \frac{\ln(\frac{\lambda_B(1-\phi)(1-p_{i-1})c_{B\ i}}{(1-\phi^r)p_{i-1}A})}{(\lambda_B-\lambda_H)}$.

From the first order condition of Eq. (A.10), we get the following

$$\begin{aligned}\frac{\partial C}{\partial \phi_i} &= \frac{-r\phi_i^{r-1}p_{i-1}A(1-e^{-\lambda_H(f_i^*|S_i=0)})}{\lambda_H} - (1-p_{i-1})e^{-\lambda_B(f_i^*|S_i=0)}c_{B\ i} + (1-p_{i-1})c_{B\ i} \\ &\quad + (1-\phi_i^r)p_{i-1}Ae^{-\lambda_H(f_i^*|S_i=0)}\frac{\partial(f_i^* \mid S_i = 0)}{\partial\phi_i} - \lambda_B(1-\phi_i)(1-p_{i-1})e^{-\lambda_B(f_i^*|S_i=0)}\frac{\partial(f_i^* \mid S_i = 0)}{\partial\phi_i} = 0.\end{aligned} \tag{A.11}$$

Since last two terms are equal to zero in Eq. (A.11), we get

$$\frac{\partial C}{\partial \phi_i} = \frac{-r\phi_i^{r-1}p_{i-1}A(1-e^{-\lambda_H(f_i^*|S_i=0)})}{\lambda_H} + (1-p_{i-1})c_{B\ i}(1-e^{-\lambda_B(f_i^*|S_i=0)}) = 0. \tag{A.12}$$

Second order condition of Eq. (A.10) is given below. The sign of SOC should be positive as we have a minimization problem.

$$\begin{aligned}\frac{\partial^2 C}{\partial \phi^2} &= \frac{-r(r-1)\phi_i^{r-2}p_{i-1}A(1-e^{-\lambda_H(f_i^*|S_i=0)})}{\lambda_H} - r\phi_i^{r-1}p_{i-1}A(e^{-\lambda_H(f_i^*|S_i=0)})\frac{\partial(f_i^* \mid S_i = 0)}{\partial\phi} \\ &\quad + \lambda_B(1-p_{i-1})e^{-\lambda_B(f_i^*|S_i=0)}c_{B\ i}\frac{\partial(f_i^*|S_i = 0)}{\partial\phi} > 0.\end{aligned}$$

After rearranging terms in Eq. (A.12), we get the following equation.

$$\frac{(1-e^{-\lambda_B(f_i^*|S_i=0)})}{(1-e^{-\lambda_H(f_i^*|S_i=0)})} = \frac{r\phi_i^{r-1}p_{i-1}A}{(1-p_{i-1})c_{B\ i}\lambda_H}. \tag{A.13}$$

Using (A.13), we can write that

$$(1-e^{-\lambda_B(f_i^*|S_i=0)}) = r\phi_i^{r-1}p_{i-1}AK \Rightarrow e^{-\lambda_B(f_i^*|S_i=0)} = (1-r\phi_i^{r-1}p_{i-1}AK) > 0; \tag{A.14}$$

$$(1-e^{-\lambda_H(f_i^*|S_i=0)}) = (1-p_{i-1})c_{B\ i}\lambda_H K \Rightarrow e^{-\lambda_H(f_i^*|S_i=0)} = (1-(1-p_{i-1})c_{B\ i}\lambda_H K) > 0 \tag{A.15}$$

where $K > 0$.

We divide Eqs. (A.14)–(A.15) and we get

$$\frac{e^{-\lambda_H(f_i^*|S_i=0)}}{e^{-\lambda_B(f_i^*|S_i=0)}} = e^{(\lambda_B-\lambda_H)(f_i^*|S_i=0)} = \frac{\lambda_B[1-\phi](1-p_{i-1})c_{B\ i}}{[1-\phi^r]p_{i-1}A} = \frac{(1-(1-p_{i-1})c_{B\ i}\lambda_H K)}{(1-r\phi_i^{r-1}p_{i-1}AK)}. \tag{A.16}$$

Rearranging (A.16),

$$\Delta = \lambda_B(1-\phi)(1-p_{i-1})c_{B\ i}(1-r\phi_i^{r-1}p_{i-1}AK) - (1-(1-p_{i-1})c_{B\ i}\lambda_H K)(1-\phi^r)p_{i-1}A = 0 \tag{A.17}$$

$$\frac{\partial C}{\partial \phi_i} = \frac{-r\phi_i^{r-1}p_{i-1}A(1-e^{-\lambda_H(f_i^*|S_i=0)})}{\lambda_H} + (1-p_{i-1})c_{B\ i}(1-e^{-\lambda_B(f_i^*|S_i=0)}) = 0.$$

From (A.17), we get the following comparative statistics,

$$\begin{aligned}
\frac{\partial \Delta}{\partial A} &= -(1-(1-p_{i-1})c_{B\,i}\lambda_H K)[1-\phi^r]p_{i-1} - \lambda_B[1-\phi](1-p_{i-1})c_{B\,i} r\phi_i^{r-1}p_{i-1}K < 0 \Rightarrow \frac{\partial \phi}{\partial A} > 0\\
\frac{\partial \Delta}{\partial c_{B\,i}} &= (1-p_{i-1})\lambda_H K[1-\phi^r]p_{i-1}A + \lambda_B[1-\phi](1-p_{i-1})(1-r\phi_i^{r-1}p_{i-1}AK) > 0 \Rightarrow \frac{\partial \phi}{\partial c_{B\,i}} < 0\\
\frac{\partial \Delta}{\partial p_{i-1}} &= \big\{-(c_{B\,i}\lambda_H K)[1-\phi^r]A - (c_{B\,i}\lambda_H K)[1-\phi^r]p_{i-1}A - \lambda_B[1-\phi]c_{B\,i}(1-r\phi_i^{r-1}p_{i-1}AK)\\
&\quad - \lambda_B[1-\phi](1-p_{i-1})c_{B\,i}(r\phi_i^{r-1}AK)\big\}\\
&< 0 \Rightarrow \frac{\partial \phi}{\partial p_{i-1}} > 0\\
\frac{\partial \Delta}{\partial \lambda_H} &= (1-p_{i-1})c_{B\,i}K[1-\phi^r]p_{i-1}A > 0 \Rightarrow \frac{\partial \phi}{\partial \lambda_H} < 0\\
\frac{\partial \Delta}{\partial \lambda_B} &= [1-\phi](1-p_{i-1})c_{B\,i}(1-r\phi_i^{r-1}p_{i-1}AK) > 0 \Rightarrow \frac{\partial \phi}{\partial \lambda_B} < 0. \quad \square
\end{aligned}$$

## References

[1] T. Escamilla, Intrusion Detection: Network Security Beyond the Firewall, John Wiley & Sons, 1998.
[2] D. Russell, G.T. Gangemi, Computer Security Basics, O'Reilly & Associates, Inc., 1992.
[3] D. Newman, N. Snyder, R. Thayer, Crying wolf: false alarms hide attacks. http://www.networkworld.com/techinsider/2002/0624security1.html (accessed at 21/03/2012).
[4] S. Axellson, The base-rate fallacy and the difficulty of intrusion detection, ACM Transaction on Information and System Security 3 (3) (2000) 186–205.
[5] G. Shipley, ISS real secure pushes past newer IDS players, Network Computing (1999).
[6] H. Ogut, H. Cavusoglu, S. Raghunathan, Intrusion detection polices for IT security breaches, INFORMS Journal on Computing (2008) 112–123.
[7] P. Porras, R. Kemmerer, Penetration state transition analysis — a rule based intrusion detection approach, IEEE Eight Annual Computer Security Applications Conference (1992) 220–229.
[8] K. Ilgun, Ustat: a real-time intrusion detection system for unix, Master's Thesis, Computer Science Department, UCSB, 1992.
[9] T. Lunt, A survey of intrusion detection systems, Computers and Security 12 (1993) 405–418.
[10] S. Kumar, E. Spafford, A pattern matching model for misuse intrusion detection, The COAST Project, Purdue University, 1996.
[11] F. Monrose, A. Rubin, Authentication via keystroke dynamics, in: 4th ACM Conference on Computer and Communications Security, 1997.
[12] P. D'haeseleer, S. Forrest, P. Helman, An immunological approach to change detection: algorithms, analysis, and implications, in: IEEE Symposium on Security and Privacy, 1996.
[13] P. Porras, P. Neumann, Emerald: event monitoring enabling responses to anomalous live disturbances, Proceedings of the 20th National Information Systems Security Conference (1997) 353–365.
[14] D. Frincke, J. Evans, D. Aucutt, Hierarchical management of misuse reports, ICCI'96.
[15] P. Neumann, P. Porras, Experience with emerald to date, in: Proceedings of First USENIX Workshop on Intrusion Detection and Network Monitoring, 1999, pp. 73–80.
[16] D. Zamboni, E. Spafford, New directions for the AAPHID architecture, in: Recent Advances in Intrusion Detection, 1999.
[17] W. Lee, W. Fan, M. Miller, S. Stolfo, E. Zadok, Toward cost-sensitive modeling for intrusion detection and response, Journal of Computer Security (2001).
[18] J. Ulvila, J. Gaffney, A decision analysis method for evaluating computer intrusion detection systems, Decision Analysis 1 (2004) 35–50.
[19] H. Cavusoglu, S. Raghunathan, Configuration of detection software: a comparison of decision and game theory approaches, INFORMS Journal on Decision Analysis 1 (3) (2004) 131–148.
[20] Y. Ryu, H. Rhee, Improving intrusion prevention models: dual-threshold and dual-filter approaches, INFORMS Journal on Computing 20 (3) (2008) 356–367. www.secprodonline.com/articles/63386/ (accessed at 21/03/2012).
[21] W. Yue, M. Çakanyildirim, Intrusion prevention in information systems: reactive and proactive responses, Journal of Management Information Systems 24 (1) (2007) 329–353.
[22] A. Bensoussan, R. Mookerjee, V. Mookerjee, W.T. Yue, Maintaining a diagnostic knowledge-based systems: a control theoretic approach, Management Science 55 (2) (2009) 294–360.
[23] V. Mookerjee, R. Mookerjee, A. Bensoussan, W.T. Yue, When Hackers talk: managing information security under variable attack rates and information dissemination, Information Systems Research 22 (3) (2011) 606–623.
[24] H. Cavusoglu, S. Raghunathan, H. Cavusoglu, Configuration of and interaction between information security technologies: the case of firewalls and intrusion detection systems, Information Systems Research 20 (2) (2009) 198–217.
[25] E. Jonsson, T. Olusson, A quantitative model of the security intrusion process based on attacker behavior, IEEE Transaction on Software Engineering 23 (4) (1997) 235–245.
[26] H.L. Van Trees, Detection, Estimation, and Modulation Theory, Part 1, John Wiley, 2001.
[27] M.H. Zweig, G. Campbell, Receiver operating characteristic (ROC) plots: a fundamental evaluation tool, Clinical Chemistry 39 (1993) 561–577.
[28] R. Durst, T. Champion, B. Witten, E. Miller, L. Spagnuolo, Testing and evaluating computer intrusion detection systems, Communication of ACM 42 (7) (1999) 53–61.
[29] R. Lippmann, J.W. Haines, D.J. Fried, J. Korba, K. Das, The 1999 DARPA off-line intrusion detection evaluation, Computer Networks 34 (4) (2000) 579–595.
[30] J. McHugh, Testing intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln laboratory, ACM Transactions on Information and System Security 3 (4) (2000) 262–294.
[31] Honeynet project, Know Your Enemy: Learning about Security Threats, Addison Wesley, 2004.
[32] L. Spitzner, Honeypots: Tracking Hackers, Addison-Wesley, 2002.
[33] C. Irvine, T. Levin, Toward a taxonomy and costing method for security services, in: 15th Annual Computer Security Applications Conference, 1999, p. 183.
[34] H. Wei, D. Frinke, O. Carter, C. Ritter, Cost-benefit analysis for network intrusion_detection systems, in: CSI 28th Annual Computer Security Conference, 2001.

[35] T. Toth, C. Kruegel, Evaluating the impact of automated intrusion response mechanisms, in: 18th Annual Computer Security Applications Conference, 2002, p. 301.

[36] S. Stolfo, W. Fan, W. Lee, A. Prodromidis, Cost-based modeling for fraud and intrusion detection: results from the JAM project, in: DARPA Information Survivability Conference & Exposition — Volume 2, 2000, p. 1130.

[37] H. Cavusoglu, B. Mishra, S. Raghunathan, The effect of internet security breach announcements on market value: capital market reaction for breached firms and internet security developers, International Journal of Electronic Commerce 9 (1) (2004) 69–105.