Modeling Abstraction Hierarchy Levels of the Cyber Attacks Using Random Process

Gilles Durrieu, Emmanuel Frénod, Thierry Morineau, Thong Nguyen

Scientific Research Publishing

Open Journal of Statistics, 2017, 7, 500-520
http://www.scirp.org/journal/ojs
ISSN Online: 2161-7198
ISSN Print: 2161-718X

Modeling Abstraction Hierarchy Levels of the Cyber Attacks Using Random Process

Gilles Durrieu[1], Emmanuel Frenod[1], Thierry Morineau[2], Thong Quoc Nguyen[1]

[1]Université de Bretagne Sud, Laboratoire de Mathématiques de Bretagne Atlantique, UMR CNRS 6205, Campus de Tohannic, Vannes, France
[2]Université de Bretagne Sud, Centre de Recherches en Psychologie, Cognition, Communication-CRPCC EA 1285, Campus de Tohannic, Vannes, France
Email: quoc-thong.nguyen@univ-ubs.fr

How to cite this paper: Durrieu, G., Frenod, E., Morineau, T. and Nguyen, T.Q. (2017) Modeling Abstraction Hierarchy Levels of the Cyber Attacks Using Random Process. *Open Journal of Statistics*, **7**, 500-520.
https://doi.org/10.4236/ojs.2017.73035

Received: April 18, 2017
Accepted: June 25, 2017
Published: June 28, 2017

Abstract

Aspects of human behavior in cyber security allow more natural security to the user. This research focuses the appearance of anticipating cyber threats and their abstraction hierarchy levels on the mental picture levels of human. The study concerns the modeling of the behaviors of mental states of an individual under cyber attacks. The mental state of agents being not observable, we propose a non-stationary hidden Markov chain approach to model the agent mental behaviors. A renewal process based on a nonparametric estimation is also considered to investigate the spending time in a given mental state. In these approaches, the effects of the complexity of the cyber attacks are taken into account in the models.

Keywords

Cyber Attacks, Abstraction Hierarchy, Hidden Markov Chain, Nonparametric Estimation, Renewal Process

1. Introduction

Cyber security provides protection and prevention for a network system. However, security technology is sometime perceived as an obstacle [1]. For some users, the difficulties in security implementation may overwhelm them. The relation between cyber defense and cyber attack is fundamentally a cognitive issue. The cyber attacker wants to manipulate the reflection of the defender. The purpose is to establish a cognitive support system for agents, the persons who involve directly the cyber security processes, are expected to be always aware of cyber threats. Based on the human factors/ergonomics concept of abstraction hierarchy, the agents being in a high abstraction hierarchy level of the mental

picture are able to improve their self-defense against the cyber threats. The role of hierarchical knowledge is important in decision-making process, since the decision-makers have to adapt to the requirements of the situation under the specific condition in order to develop the proper actions [2] [3].

In a degraded situation of work, the agents have finally to implement a concrete solution after analyzing the problem. In cognitive terms, they go down in the abstraction hierarchy level of the environment [3] [4] [5]. The decision support system must facilitate the possibility to navigate through the different abstraction hierarchy levels and intervene in the problem solving process to permit the agents to visit the best abstraction level for controlling the situation. At the high level of abstraction hierarchy, the agents can manage the defense against a cyber attack on the system more efficiency [4]. This means that they have a more global and abstract mental representation of the cyber attack and its consequences. The remainder of this paper is organized as follows. In Section 2.1, we give a description on the attacks simulation system. The cyber security center of the University of Southern Brittany simulates the cyber attacks and practices the defense procedure. In Section 2.2, the relationship between the psychological aspects of the agents and the security levels is explained. The ergonomic reactions to the cyber threats are mentioned as well. In Section 3, we develop a statistical model using hidden Markov chain with the requisite properties from the psychological aspects to infer the mental picture of an agent from a set of observations. In Section 4, we propose a parametric model based on the hidden Markov chain, and validate the behavior of the simulated data from the psychological viewpoint. Section 5 is devoted for the learning procedure of the model from the data, and the estimation method for the parameters as well as the abstraction hierarchy level of the mental picture is also detailed in the section. The survival functions given state are investigated in Section 6. The nonparametric estimation for the survival functions is described in Section 7. The concluding remarks are given in Section 8.

2. Problem Description

We describe the cyber attacks simulation and the psychological aspects associated to the abstraction hierarchy of the cyber threats.

2.1. Attacks Simulation System

A cyber security center at University of Southern Brittany, France has been invested to do research on cyber attack and cyber defense (http://www.cyber-security-center.com). There are two main teams in the simulation system:

1) The attack team (aka red team) plays a role as an attacker, this team creates the cyber pseudo-attacks derived from around the world. A sequence of cyber attacks is simulated to attack the security system of the defense team.

2) The defense team (aka blue team) includes IT group, SOC (security operation center) group, the forensic group and the management department. In gen-

eral, these groups will have to detect the attack(s) through abnormal accesses such as multiple suspected connections to the server. The groups also report the damages, describe the procedure of the attacks. The description of the attack(s) is sent to the management department. Based on the collected data, the agents' job is to analyze the severity of the damage, the sophisticated level of the invasion. After analyzing the situation, they need to find the strategy to defend the system, and resolve the damage.

The scheme of the attack simulation system is illustrated in Figure 1. The focus of our concern, from the psychological viewpoint, is the human aspect of these agents. Specifically, mental state of the agent that affects the behavior is studied. The mental state of the agents in the blue team is important since they are the ones who have to comprehend the situation and make the appropriate decisions. Under stressful situation, their mental state may not help the agents have a complete evaluation of the situation. For example, if the agent loses consciousness of the functional purpose of a potential threat on the system (*i.e.* invading the system), and focuses only on the form of the attack processes (*i.e.* attack's dynamics), the agent may fail in judgment on the danger of a given attack process, and then commit errors.

2.2. Psychological Aspects

2.2.1. Work Domain Analysis of a Cyber Threat

Different hierarchy levels of the mental states are studied in ergonomics science [5] [6]. Construction of the abstraction hierarchy levels could use the Work Domain Analysis approach (WDA) [7]. This is the initial phase of cognitive work analysis. The aim of WDA in our scenario is to model the constraints that

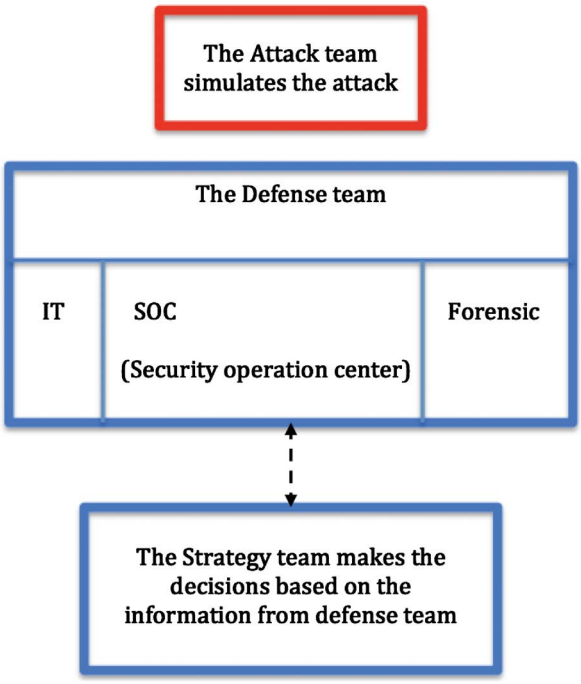

Figure 1. Cyber attack simulation system.

relate to the purposive and physical context of the cyber threats. One characteristic of WDA is that it is event-independent. In other words, WDA generally represents categories of knowledge on work domain [8]. Therefore, when confronted with an unanticipated event, the agents can rely on their knowledge of the threat constraints to explore variety ways of dealing with the situation. The Abstraction Hierarchy is made of five abstraction levels [3] [8]:

S5 General purposes: comprehended at the highest level of abstraction hierarchy. When the agent perceives the event at this level, the fundamental purposes of the attack and its origin are recognized thoroughly.

S4 Abstract functions: at this hierarchy level, the agent is capable of understanding the laws, the principles, the attack sophistication and smartness.

S3 Processes: the process relates to the goal such as a set of dynamic flows of the event, information or sequence of states. In other words, the agent can perceive the requisite elements to achieve the goal.

S2 Physical functions: represents the functional values directly associated with the concrete forms, such as Trojans, viruses.

S1 Physical forms: apparent forms such as broken files, attack occurrence, or code lines of a virus, that can be perceived by an agent.

Here we have one-to-one relation between the abstraction hierarchy levels of the cyber attacks and the mental picture levels of the agent. When the agent is at a certain mental level, that agent perceives the respective abstraction hierarchy level of the cyber attack. It is essential for the agent to perceive the abstraction hierarchy level of the attack at the best level in order to have the best performance. When the diagnosis is executed at the highest level, then when the agent goes down in the abstraction hierarchy to specify the best solution and envisage several alternatives, the solution will be exhausted.

A scam email sent through the system (ex: service@paypal.com service.paypal@pay-paypal.com). We illustrate the levels of abstraction depicted by the abstraction hierarchy, and the mental model:

In high-level behaviors, the diagnosis stage focuses on the fundamental meaning of the suspected content. The agent seems to visit often the high levels of abstraction (abstraction functions, general purposes) to improve the understanding of the content of the email, which can lead to better performance, the solution can be exhausted. In the low-level behaviors, the low levels of abstraction are more often visited. The subject's attention is on the physical form (or physical functions) of the email. The real address mail (service.paypal@pay-paypal.com) hidden under the exposed address (service@paypal.com) is perceived. The interface in the content of the email replicated from the legitimate email from PayPal (icons, images, color, symbol...) gains trust. Even if the agent recognizes that the email is illegitimate, the poor performance may cause a risk (e.g. a Trojan installed).

From the example, we have learned a relation between the mental behaviors of human and the abstraction hierarchy levels of a cyber attack that is observed. Once again, the human-centered security, or self-defense from the agent is an

effective layer in the cyber security system, beside innovative technologies. However, these levels of abstraction hierarchy as well as the mental picture levels can be only deduced from the observable data. The observable outcomes that imply the mental state of the agent is discussed in the sequel.

2.2.2. The Reaction Time to an Arrival Cyber Attack

The interaction of a person to a computer is more likely different according to the current mental state of that one. Usually, the attackers never want their attacks detected. Therefore, if the agents lack awareness, intrusion can be perceived as a normal access, or the detection could be too late. From this argument, we propose the following assumption:

- When a person is in high awareness, which means the actions will be based on the fundamental knowledge of the cyber threats. Then the situation will be perceived at its high abstraction hierarchy level. Roughly speaking, the brain is always on high alert, which helps it detect the abnormal access soon. Even if the detection is a false alarm, the system is still secure.
- In contrast, if one is in a low level of mental state, that person lacks awareness of the potential dangers from an access. The attack will be perceived at its low abstraction hierarchy level (e.g. physical form), since the brain is 'tired' to process the information to detect the abnormal activities. In the cognitive terms, the reaction is low level behaviors. The agent focuses only on the technical issues rather, the concrete form than the main purpose of the attack. Therefore, the attack can pass and continue until it reaches the goal(s) or being detected.

With this observation, we propose R is a random variable representing the time since the cyber threat arrives until the agent is aware of its activity. Very likely, the high hierarchy levels agents spend less time to detect abnormal access than the ones are in lower hierarchy levels. Let μ_R denote the mean value of R, this value μ_R is constructed by three components

$$\mu_R = b_R + V_R(z) + D_R(z),$$

where b_R represents the basic reaction time of the agent with respect to the current mental state, or the time needed for the agent to perceive the appearance of an event's arrival [9], z denotes the complexity of the attack, $V_R(.)$ is the average time needed in order to comprehend the content of the event; the value depends on the complexity of the message and $D_R(.)$ represents the average time required to reach the decision after comprehending the content.

3. Hidden Markov Based Model

Since the mental state at a certain time of the agent is unable to observe, and could be only inferred from the observable data, this unobserved information can be considered as a hidden sequence. In this section, we construct a model using the hidden Markov chain to adjust the data. Particularly, the hidden Markov chain can be applied for modeling the abstraction hierarchy level of the attack that the agent perceived as well as the corresponding mental picture level of

that agent. Let us assume that the mental picture state is classified into K levels/states (hidden). The set of states is denoted by

$$S = \{s_1, s_2, \cdots, s_K\}.$$

The elements are arranged in the increased order, *i.e.* the state level k is represented by s_k. Without misunderstanding, it can be written $s_i > s_j$ if $i > j$.

The mental states of the agent are illustrated by a random process $X = (X_n)$, X_n represents the mental state of the agent at the time n, $X_n \in S$, where n is a positive integer in $\{1, 2, \cdots, N\}$. We assume that the process satisfies the Markov property given by

$$P(X_n \mid X_{n-1}, X_{n-2}, \cdots, X_1) = P(X_n \mid X_{n-1}).$$

The meaning of this property is that, given the information in the recent past, the state at the present is independent of the further pasts. The state transition probability distribution $A_n = \{a_{ij}^{(n)}\}$ is the transition matrix for $1 \le i, j \le K$ where the coefficients

$$a_{ij}^{(n)} = P(X_n = s_j \mid X_{n-1} = s_i)$$

are the probability that the state moves from s_i to s_j at time n. The transition probabilities satisfy the stochastic constraints, $a_{ij}^{(n)} \ge 0$, and $\sum_{j=1}^{K} a_{ij}^{(n)} = 1$. It is intuitively observed that one of the factors which can directly affect the mental state is the attack that the agent suffered. Particularly, the more complex attack that the subject suffered, the more likely the agent is at the lower level of mental state at the current observation n. Therefore, the value at the current state depends not only on the state of the subject previously but also on the attacks that occurred in the recent past. With this argument, we describe the transition probabilities including the effect of the cyber attack given by

$$\tilde{a}_{ij}(z_{n-1}) := a_{ij}^{(n)} = P(X_n = s_j \mid X_{n-1} = s_i, z_{n-1}),$$

where z_n is the level (or complexity) of the attack at time n. We propose the requisite properties for the transition probabilities: if $z_{n-1} \le z_n$, the attack z_n is not less complex than the attack z_{n-1}. In other words, the subject suffers no less complicated attack than previous time, then

1) if $i > j$, $\tilde{a}_{ij}(z_{n-1}) \le \tilde{a}_{ij}(z_n)$, the agent is more likely to go down in mental state level,

2) if $i < j$, $\tilde{a}_{ij}(z_{n-1}) \ge \tilde{a}_{ij}(z_n)$, the agent is less likely to go up in mental state level,

3) $\tilde{a}_{ii}(z_{n-1}) \le \tilde{a}_{ii}(z_n)$ if s_i is a low mental level,

4) $\tilde{a}_{ii}(z_{n-1}) \ge \tilde{a}_{ii}(z_n)$ if s_i is a high mental level.

With these properties, it is necessary to categorize S into high levels and low levels subsets under the cognitive viewpoint. In the totally ordered index set I, $S = \{s_i\}_{i \in I}$, there exists $\omega > \inf I$ such that

$$S_l = \{s_i \in S \mid i < \omega\} \text{ is a set of low hierarchy states,}$$

$S_h = \{s_i \in S \mid i \geq \omega\}$ is a set of high hierarchy states.

The sequence $O = (O_1, O_2, \cdots, O_N)$ represents the observations and $V = \{v_m\}$ is a set of observable outcomes corresponding to the possible informations collected from the agent. The distribution of the observation in each state is given by $B = \{b_k(.)\}$, where $b_k(.)$ is the distribution of the observation in state s_k.

Finally, the last component of the Hidden Markov chain is the initial state distribution $\pi = \{\pi_1, \pi_2, \cdots, \pi_K\}$ of X_1, where π_i is the probability that the model is in state s_i at the time $n = 1$, $\pi_i = P(X_1 = s_i), 1 \leq i \leq K$. Figure 2 shows the general sheme of a Markov chain.

4. Two-State Model

4.1. Model Description

We construct a parametric model that satisfies the aforementioned properties in Section 3 for the hidden process (X_n). Assuming that the set of states S has two states, $S = \{0,1\}$. Under this assumption, the values represent the low and high levels of mental state respectively. A sequence of attacks z is considered, $z = (z_1, z_2, \cdots, z_n, \cdots, z_{N-1})$, where z_n, as mentioned, is the level of the attack detected at the time n. The variable z_n takes the non-negative integer values. At the cyber security center, the attacks are simulated in four levels: (1) Low, (2) Normal, (3) High and (4) Emergency. Assuming that only the most recent attack affects the current mental state, *i.e.*

$$P(X_n = x_n \mid X_{n-1} = x_{n-1}, z_{n-1}, \cdots, z_1) = P(X_n = x_n \mid X_{n-1} = x_{n-1}, z_{n-1}).$$

In order to satisfy the properties of the transition probabilities in the model, it is required that the probability

$$P(X_n = 1 \mid X_{n-1} = x, z_{n-1}) \tag{1}$$

decreases with respect to z_{n-1}. We consider the following expression of the transition probability

$$P(X_n = 1 \mid X_{n-1} = x, z_{n-1}) = \exp\left(\left(1 + \log(1 + z_{n-1})\right) \log a_x\right), \tag{2}$$

where a_x is the probability that the high level status is recorded at the present time n, $X_n = 1$, given the previous recorded status is x, $X_{n-1} = x$, and there is no effective attack,

$$P(X_n = 1 \mid X_{n-1} = x, z_{n-1} = 0) = a_x.$$

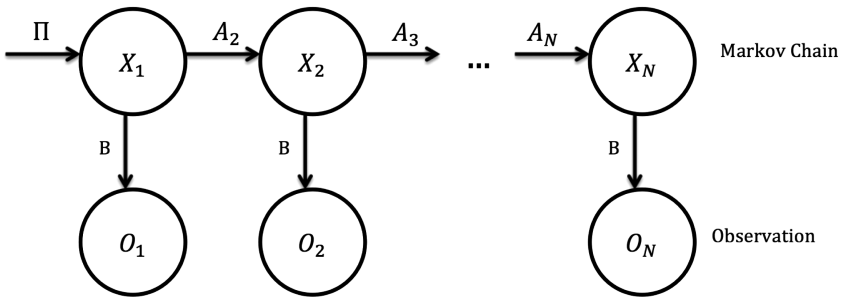

Figure 2. Hidden Markov chain scheme.

The term "no effective attack" has to be understood that the attack is very easy to manipulate or it is a false alarm of the agent. With this observation, without any effective attack, a_1 is considered as a parameter presenting the "self-maintain" ability of the agent, and a_0 presents the ability of "self-recover" of the agent. These two parameters a_0 and a_1 are the personal characteristics of an agent and can be measured using the simulated cyber attacks.

From (2), we observe that if the agent is at the high level of mental state, the probability that the agent remains in that level, $P(X_n = 1 | X_{n-1} = 1, z_{n-1})$, decreases with respect to the level of the attack, which leads to the probability of decreasing in the mental state becomes greater,

$$P(X_n = 0 | X_{n-1} = 1, z_{n-1}) = 1 - P(X_n = 1 | X_{n-1} = 1, z_{n-1}). \quad (3)$$

Similarly, (2) shows that the one being at the lower level will harder goes up in the mental level after suffering an effective attack, *i.e.* $P(X_n = 1 | X_{n-1} = 0, z_{n-1})$ decreases with respect to the level of the recent attack. These are the properties proposed in Section 3.

4.2. Simulation Study

From (2), we generate a sequence of length 30 with self-recover and self-maintain parameters equal to $a_0 = 0.7$, $a_1 = 0.9$, and $P(X_1 = 1) = 0.9$. The simulated sequence is given in Table 1. The first row represents the complexity of attack in the past that affects the state of X_n. As described in Subsection 4.1, the attack with complexity $z_n = 0$ is ineffective. The second row is the realization $x = (x_n)$ of (X_n).

With the high self-maintain values, the mental level of the agent is capable of remaining high even after high level attacks. The high values of self-recover parameter can help the agent in the low state easier regain the high level. Table 2 corresponds to the simulation associated to a smaller value of the self-recover parameter ($a_0 = 0.4$).

The sequence of observation $O = (O_1, O_2, \cdots, O_N)$ is simulated from the distribution b_i's. Let us assume that b_i's follow the Gaussian distribution,

$$O_n |_{X_n = i} \sim \mathcal{N}(\mu_i, \sigma_i^2),$$

where μ_i is the mean value of the observation when the state of the subject is in level *i*, and σ_i^2 is the variance. Figure 3 displays the simulated observations and we observe the difference between the two sets of data.

Table 1. Simulated sequence of length 30 with $P(X_1 = 1) = 0.9$, $a_0 = 0.7$, $a_1 = 0.9$.

z	2	1	1	2	1	3	2	3	0	0	2	1	1	0	4	2	0	4	3	1	4	0	3	4	3	3	3	2	0	0
x	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	0	1	0

Table 2. Simulated sequence of length 30 with $P(X_1 = 1) = 0.9$, $a_0 = 0.4$, $a_1 = 0.9$.

z	1	0	4	2	3	0	3	4	2	0	1	2	4	4	2	4	3	3	3	4	0	2	2	1	1	4	1	2	2	3
x	1	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0

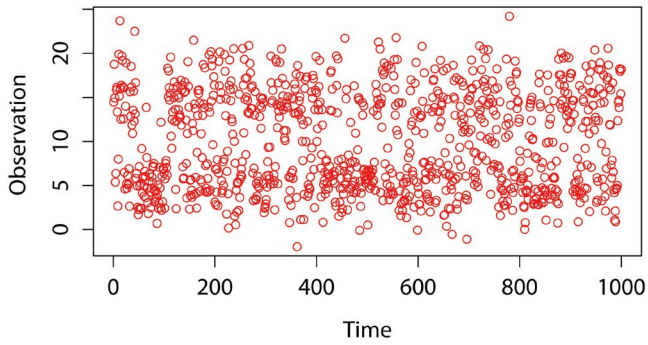

Figure 3. One thousand values of the observation are simulated with $P(X_1 = 1) = 0.9$, $a_0 = 0.4$, $a_1 = 0.9$, the parameters of $\left(\mu_0, \sigma_0^2\right)$ and $\left(\mu_1, \sigma_1^2\right)$ are respectively (15, 3) and (5, 2).

5. Estimating the Parameters and Reconstructing the Hidden States

We describe a procedure based on the Maximum Posterior Marginal (MPM) [10] [11] maximizing the marginal posterior distribution $P\left(X_n \mid O\right)$. We recall the forward-backward procedures [12] [13]. The forward-backward probabilities are defined by:

$$\alpha_n(i) = P\left(O_1 = o_1, \cdots, O_n = o_n, X_n = s_i\right), \tag{4}$$

and

$$\beta_n(i) = P\left(O_{n+1} = o_{n+1}, \cdots, O_N = o_N \mid X_n = s_i\right). \tag{5}$$

However, the original recursion derived from (4) and (5) has numerical problems [10] [14]. The replaced joint probabilities have been proposed by Devijver *et al.* [14]

$$\alpha_n(i) \approx P\left(X_n = s_i \mid O_1 = o_1, \cdots, O_n = o_n\right) \tag{6}$$

$$\beta_n(i) \approx \frac{P\left(O_{n+1} = o_{n+1}, \cdots, O_N = o_N \mid X_n = s_i\right)}{P\left(O_{n+1} = o_{n+1}, \cdots, O_N = o_N \mid O_1 = o_1, \cdots, O_n = o_n\right)}. \tag{7}$$

Using the numerically stable recursions, the forward-backward probabilities are approximated as follow:

- Forward initialization:

$$\alpha_1(i) = \frac{\pi_i b_i\left(o_1\right)}{\sum_{j=1}^{K} \pi_i b_i\left(o_1\right)}, \text{ for } 1 \le i \le K.$$

- Forward induction:

$$\alpha_n(j) = \frac{b_j\left(o_n\right) \sum_{i=1}^{K} \alpha_{n-1}(i) a_{ij}^{(n)}}{\sum_{l=1}^{K} b_l\left(o_n\right) \sum_{i=1}^{K} \alpha_{n-1}(i) a_{il}^{(n)}}, \text{ for } 1 \le j \le K, 2 \le n \le N.$$

The backward $\beta_n(i)$ is also calculated inductively as follows:

- Backward initialization:

$$\beta_N(i) = 1, \text{ for } 1 \le i \le K$$

- Backward induction:

$$\beta_n(i)=\frac{\sum_{j=1}^{K} a_{ij}^{(n+1)} b_j(o_{n+1})\beta_{n+1}(j)}{\sum_{l=1}^{K} b_l(o_{n+1})\sum_{j=1}^{K}\alpha_n(i)a_{jl}^{(n+1)}},\quad \text{for } 1\le i\le K, n=N-1,N-2,\cdots,1.$$

In case of two-state model in Section 4, the transition probabilities $a_{ij}^{(n)}$ are computed by (2) and (3). We define the probability

$$\xi_n(i,j)=P\left(X_n=s_i, X_{n+1}=s_j \mid O,\lambda\right)$$

of being in the states s_i and s_j at respectively times n and $n+1$ given the model λ, where λ denotes the complete parameters set of the model and O the sequence of observations.

The probability $\xi_n(i,j)$ can be written using forward backward variables

$$\begin{aligned}\xi_n(i,j)&=\frac{\alpha_n(i)a_{ij}^{(n+1)}b_j(o_{n+1})\beta_{n+1}(j)}{P(O\mid\lambda)}\\&=\frac{\alpha_n(i)a_{ij}^{(n+1)}b_j(o_{n+1})\beta_{n+1}(j)}{\sum_{l=1}^{K}\sum_{m=1}^{K}\alpha_n(l)a_{lm}^{(n+1)}b_l(o_{n+1})\beta_{n+1}(m)}.\end{aligned}$$

Moreover, the marginal a posterior probability, *i.e.* the probability of being in state s_i at time n given the observation and the model, can be obtained as follow

$$\gamma_n(i)=P\left(X_n=s_i\mid O,\lambda\right)=\sum_{j=1}^{K}\xi_n(i,j)=\frac{\alpha_n(i)\beta_n(i)}{\sum_{l=1}^{K}\alpha_n(l)\beta_n(l)}.$$

In order to obtain the MPM solution, each element $\hat{X}_n$ is attributed to the state s_{i_n} that maximizes $\gamma_n(i)$.

The estimation of parameters of the model λ is updated by EM algorithm [15] [16]. With $O=(O_1,\cdots,O_N)$ to be the observed data and the state sequence $X=(X_1,\cdots,X_N)$ to be hidden, the complete-data likelihood function is $P(O,X\mid\lambda,z)$. Where z is the observed sequence of attacks introduced in Section 4. The EM algorithm first finds the expectation of the log-likelihood of the complete data (E-step) with respect to the hidden data X given the observation and the initial or previous λ'

$$\begin{aligned}Q(\lambda,\lambda')&=E\left(\log P(O,X\mid\lambda,z)\mid O,\lambda',z\right)\\&=\sum_{x\in\mathcal{X}}\log P(O,x\mid\lambda,z)P(x\mid O,\lambda',z).\end{aligned}$$

In fact, for the easier calculation, the used density is $P(O,x\mid\lambda',z)=P(x\mid O,\lambda',z)P(O\mid\lambda',z)$. Since the factor $P(O\mid\lambda',z)$ is not depending on λ, the sub-sequence steps are not effected. Then, the following form of function Q is used

$$Q(\lambda,\lambda')=\sum_{x\in\mathcal{X}}\log P(O,x\mid\lambda,z)P(O,x\mid\lambda',z).\tag{8}$$

The second step is to determine the maximum with respect to λ of Q

(M-step). Given a state sequence x, $P(O, x \mid \lambda, z)$ is represented as

$$P(O, x \mid \lambda, z) = \pi_{x_1} \prod_{n=2}^{N} a^{(n)}_{x_{n-1}x_n} \prod_{n=1}^{N} b_{x_n}(o_n).$$

Then the Q function is

$$\begin{aligned} Q(\lambda, \lambda') = &\sum_{x \in \mathcal{X}} \log \pi_{x_1} P(O, x \mid \lambda', z) + \sum_{x \in \mathcal{X}} \left(\sum_{n=1}^{N} \log b_{x_n}(o_n) \right) P(O, x \mid \lambda', z) \\ &+ \sum_{x \in \mathcal{X}} \left(\sum_{n=2}^{N} \log a^{(n)}_{x_{n-1}x_n} \right) P(O, x \mid \lambda', z). \end{aligned} \tag{9}$$

The parameters are now separated into three independent terms, and each term can be optimized individually. The first term is

$$\begin{aligned} \sum_{x \in \mathcal{X}} \log \pi_{x_1} P(O, x \mid \lambda', z) &= \sum_{x_1=1}^{K} \log \pi_{x_1} \sum_{x_2=1}^{K} \cdots \sum_{x_N=1}^{K} P(O, x_1, \cdots, x_N \mid \lambda', z) \\ &= \sum_{i=1}^{K} \log \pi_i P(O, x_1 = i \mid \lambda', z). \end{aligned}$$

The optimization with the constraint $\sum_{i=1}^{K} \pi_i = 1$ is solved by using the Lagrange multiplier and we obtain

$$\pi_i = \frac{P(O, x_1 = i \mid \lambda', z)}{P(O \mid \lambda', z)} = P(x_1 = i \mid O, \lambda', z).$$

The second term in (9) becomes

$$\sum_{x \in \mathcal{X}} \left(\sum_{n=1}^{N} \log b_{x_n}(o_n) \right) P(O, x \mid \lambda', z) = \sum_{n=1}^{N} \sum_{i=1}^{K} \log b_i(o_n) P(O, x_n = i \mid \lambda', z).$$

When the distribution of $\{b_i\}$ is Gaussian, the solution for the optimization of this term is

$$\mu_i = \frac{\sum_{n=1}^{N} o_i \times P(O, x_n = i \mid \lambda', z)}{\sum_{n=1}^{N} P(O, x_n = i \mid \lambda', z)},$$

and

$$\sigma_i^2 = \frac{\sum_{n=1}^{N} (o_n - \mu_i)^2 \times P(O, x_n = i \mid \lambda', z)}{\sum_{n=1}^{N} P(O, x_n = i \mid \lambda', z)}.$$

The third term in (9) can be written as

$$\begin{aligned} &\sum_{x \in \mathcal{X}} \left(\sum_{n=2}^{N} \log a^{(n)}_{x_{n-1}x_n} \right) P(O, x \mid \lambda', z) \\ &= \sum_{n=2}^{N} \sum_{x_{n-1}=1}^{K} \sum_{x_n=1}^{K} \log a^{(n)}_{x_{n-1}x_n} \sum_{x_1=1}^{K} \cdots \sum_{x_N=1}^{K} P(O, x_1, \cdots, x_{n-1}, x_n \cdots, x_N \mid \lambda', z) \\ &= \sum_{n=2}^{N} \sum_{i=1}^{K} \sum_{j=1}^{K} \log a^{(n)}_{ij} P(O, x_{n-1} = i, x_n = j \mid \lambda', z). \end{aligned}$$

With the two-state model in Section 4, the transition probabilities are expressed as

$$P(X_n = 1 \mid X_{n-1} = x, z_{n-1}) = \exp\left(\left(1 + \log(1 + z_{n-1})\right)\log a_x\right),$$

$$P(X_n = 1 \mid X_{n-1} = x, z_{n-1}) = \exp\left(\left(1 + \log(1 + z_{n-1})\right)\log a_x\right),$$

For the notational convenience, we denote $g_n(z) = 1 + \log(1 + z_{n-1})$. Then the third term of Q can be rewritten as

$$\begin{aligned}
&\sum_{n=2}^{N}\sum_{i=1}^{K}\sum_{j=1}^{K} \log a_{ij}^{(n)} P(O, x_{n-1} = i, x_n = j \mid \lambda', z) \\
&= \sum_{n=2}^{N}\Big(g_n(z)\log a_0 P(O, x_{n-1} = 0, x_n = 1 \mid \lambda', z) \\
&\quad + \log\left(1 - a_0^{g_n(z)}\right) P(O, x_{n-1} = 0, x_n = 0 \mid \lambda', z) \\
&\quad + g_n(z)\log a_1 P(O, x_{n-1} = 1, x_n = 1 \mid \lambda', z) \\
&\quad + \log\left(1 - a_1^{g_n(z)}\right) P(O, x_{n-1} = 1, x_n = 0 \mid \lambda', z)\Big).
\end{aligned}$$

This term has to be maximized under the constraints $0 < a_0, a_1 < 1$. This optimization problem is solved numerically by BFGS algorithm [17]. We generate 100 sequences of states (X_n) of length 3000 with the two-state model in Section 4. The observations are simulated according to the Gaussian distribution. Table 3 shows the means and standard deviations of the estimators of a_0 and a_1 from 100 replicates, the parameters of (μ_0, σ_0^2) and (μ_1, σ_1^2) are respectively (13, 16) and (5, 4). The rate of correctly reconstructing the hidden states is in average 93.32%, which means approximately 2800/3000 hidden states are correctly detected. Figure 4 displays the goodness-of-fit between the true and the estimated distributions.

At the Cyber Security Center, we conducted the simulated attacks and the students were playing a role as the agents in the defense team. There are 67 valid sets of data collected. The values of the collected outcomes, time of reaction, are shown in Figure 5. As mentioned, four complexity levels of the attacks are observed. The mental states deduced from the observations are represented by the circles and the stars. The stars represent the low mental level, and the circles represent the high mental level. Figure 6 shows the Gaussian distributions with the estimated parameters. The short reaction time, corresponding to the high mental level, is more concentrated than the reaction time at low level of abstraction hierarchy. In this experiment, roughly speaking, the reaction time of a person at high mental state is usually within three hours. The average reaction time at high mental state of the person is 1.7 hour.

Table 3. Descriptive statistics for the estimators of a_0 and a_1 from 100 samples. The sample length is 3000.

	True	Estimators Mean	Std.
a_0	0.4	0.397	0.016
a_1	0.8	0.801	0.013

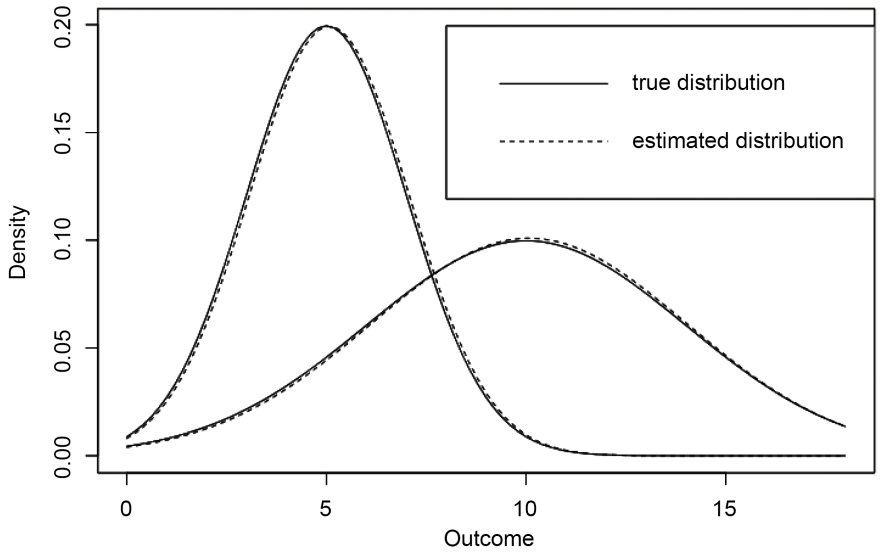

Figure 4. Fit of the estimation for the simulated observations.

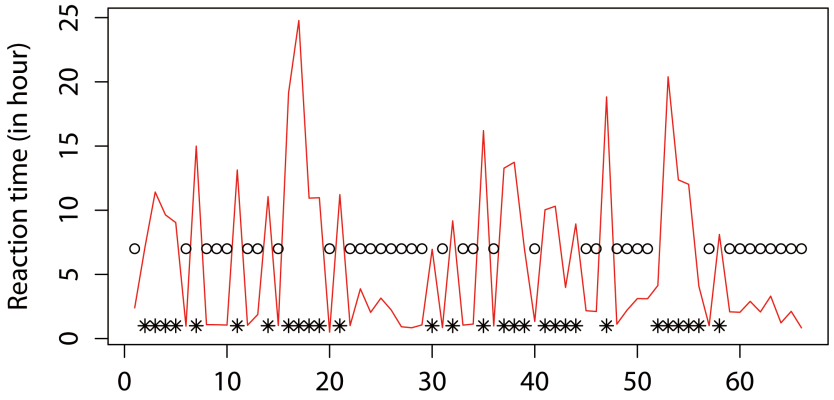

Figure 5. An example of the reaction time from 67 observations, and the implied hierarchy states from these observations (circles and stars). Higher states are presented by the circles and lower states are presented by the stars.

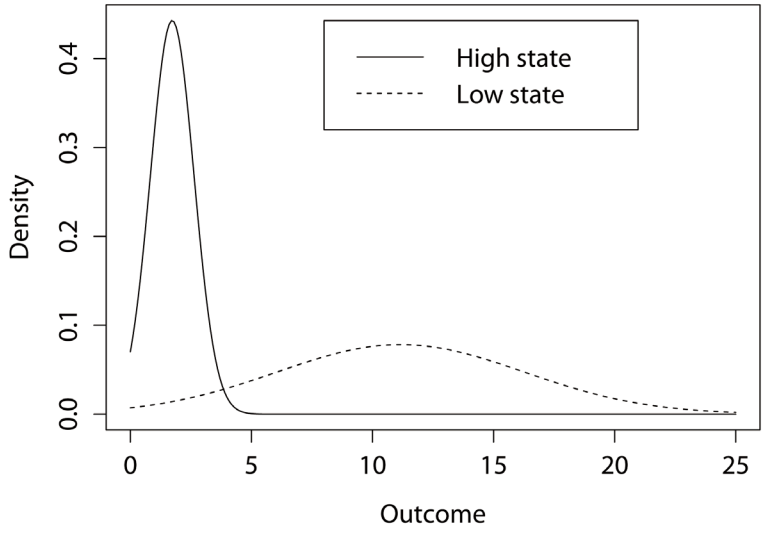

Figure 6. The distributions of two states estimated from the observation.

6. Two-State Renewal Model

The spending time in a given state is investigated. We propose to model the variation of mental levels of the agent over time by a piecewise-constant continuous-time process $(X_t)_{t\geq 0}$ with two states. Similarly to the Hidden Markov chain based model, we consider the mental level of an agent to be either high or low at a time. We thus have the state given by $E=\{-1,1\}$, where -1 stands for the low mental level, while the high level is denoted by 1. For any $t\geq 0$, X_t taking its value on E models the mental level of the agent. Indeed, as shown in Figure 7, at each time one may consider that an agent is either in low mental leval or high mental level.

The process (X_t) changes its location at random times, called jump times. Let (T_k) denote the sequence of the jump times of (X_t). For a renewal process, one also considers the inter-jumping times (S_k), for any $k\geq 1$, $S_k=T_k-T_{k-1}$. The first inter-jumping times S_1 is usually unknown since the limit of the observable time. The sequence (Y_k) of location of (X_t) is also taken into account

$$Y_k=X_t,\quad \text{for } T_k\leq t<T_{k+1}.$$

The sequence (Y_k) is assumed to be a Markov chain on $(E,\mathcal{B}(E))$. As the above construction, the discrete-time process (Y_k,S_k) contains all the information of (X_t). In our particular case, the behavior of the process (X_t) also depends on the complexity of the arrived attacks z_t. The step function z_t presents the priority of the attack detected at time t, z_t is non-negative. The values of z_t is deterministic for all t. For $k\geq 1$ and for $t\geq 0$, the conditional distribution of the S_k's satisfies

$$\begin{aligned}&P(S_{k+1}>t\,|\,Y_k,\cdots,Y_0,S_k,\cdots,S_1,z_t)\\&=P(S_{k+1}>t\,|\,Y_k,z_t)=\exp\left(-\int_0^t\bar{\lambda}(Y_k,s,z_t)\mathrm{d}s\right).\end{aligned}$$

The function $\bar{\lambda}$ is called the conditional jump rate of the process (X_t). The integral of $\bar{\lambda}$ which is the cumulative jump rate is also considered,

$$\forall(y,t,z_t)\in E\times\mathbb{R}_+\times\mathbb{Z}_+,\Lambda(y,t,z_t)=\int_0^t\bar{\lambda}(y,s,z_t)\mathrm{d}s.$$

The value of z_t plays a role in the moment of jump of (X_t). Intuitively, if

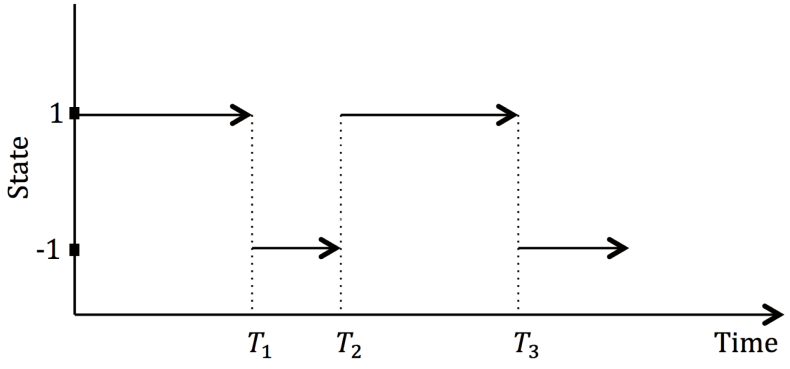

Figure 7. Example of trajectory of the two-state renewal process for modeling mental state level.

Y_k is at low level, the complex cyber attack will probably prolong the inter-jumping time. In contrast, if Y_k is at high level, the inter-jumping time will be more likely shortened. With this argument, we propose the following form of the cumulative jump rate

$$\Lambda(y,t,z_t)=(1+z_t)^y\int_0^t\lambda(y,s)\mathrm{d}s.$$

Since the prior information about the behavior of the agent at a given state is unknown and it depends on the particular individual, a parametric model could not be chosen. Therefore, the nonparametric estimation of the cumulative jump rate is studied instead. In the sequence, the number of observed jumps is denoted by *m*. The estimator of the cumulative jump rate is proposed by the Nelson-Aalen estimator [18] [19]

$$\hat{\Lambda}_m(y,t,z_t)=\sum_{k=1}^m R_m(y,S_{k+1})\mathbf{1}_{\{Y_k=y\}}\mathbf{1}_{\{S_{k+1}\le t\}},$$

where $\mathbf{1}_A$ is indicator function, and $R_m(y,t)$ is defined as follow

$$R_m(y,t)=\begin{cases}\dfrac{1}{L_m(y,t)} & \text{if } L_m(y,t)>0\\ 0 & \text{otherwise,}\end{cases}$$

where $L_m(y,t)$ counts how many times S_{k+1}'s are not less than t under state $Y_k=y$,

$$L_m(y,t)=\sum_{k=1}^m\mathbf{1}_{\{Y_k=y\}}\mathbf{1}_{\{S_{k+1}\ge t\}}.$$

The first inter-jumping time S_1 is usually omitted since it is unknown. Moreover, when the process (X_t) is hidden, only the approximation $(\hat{S}_k)$ of (S_k) is able to obtained. We do not compute the Nelson-Aalen estimator $\hat{\Lambda}_m(y,t,z_t)$ but an approximation of this estimator $\tilde{\Lambda}_m(y,t,z_t)$ from $(\hat{S}_k)$, see for details [20].

Moreover, the conditional survival functions H associated with Λ can also be estimated from this approximate cumulative jump rate. These functions take values between 0 and 1, whereas the range of values taken by $\tilde{\Lambda}_m$ depends on m, this is called the Fleming-Harrington estimator ([21]) of H. For any $y\in E$, $t\ge 0$, it is given by

$$\tilde{H}_m(y,t,z_t)=\exp\left(-\tilde{\Lambda}_m(y,t,z_t)\right).$$

7. Estimation Procedure

In practice, the process (X_t) cannot be observed directly. Assuming that the observable process is (G_t), and the behavior of these signals depends on the process (X_t). Indeed, the values of G_t should be small when X_t is high, and large when X_t is low. The values of process (G_t) are collected in a fixed time interval $[0,T]$. For a particular agent, the values of (G_t) are in an interval $[a,d]\in\mathbb{R}_+$. For a finite set of $\{t_i\,|\,i\in\overline{1:N}\}$ in $[0,T]$, let $V_i=G_{t_i}$ be a random

variable with the corresponding continuous probability density function *f*. The number of modes, called $N(f)$, of *f* is unknown. However, this $N(f)$ can be 'guessed' by using the Silverman test [22]. Intuitive speaking, the frequency of the signal G_t around the value *x* can be represented by $f(x)$. In order to have a clear relation between *f* and G_t, the following assumptions are proposed

Assumptions 7.1

1. There exists a pair (b,c), with $a<b<c<d$, such that, $\forall t\in[0,T]$, $X_t=1$ then $G_t<b$, and $X_t=-1$ then $G_t>c$.

2. $N(f)\le 2$, f has no flat part and has at most one anti-mode (at θ if $N(f)=2$).

The first assumption expresses natural behavior that the smaller values according the threshold *b* of G_t always reflect the high mental level of the agent, and vice versa the signals G_t greater than *c* reflect the low mental level of the agent. This assumption separates out the values of G_t that we know almost surely the mental level. When the signals are between *b* and *c*, the mental state of the agent can be either high or low. Note that *b* and *c* can arbitrarily close to each other. The second one particularly means that the density function *f* has either one mode or two modes. Function *f* has one mode means that the state of the agent is most likely unchanged, except the signals outside $[b,c]$. Two modes occur, statistically, when the agent has been in both states during the observation.

In the case that $N(f)=1$, for instance $mode(f)>\dfrac{b+c}{2}$, we set *b* as a threshold to determine the hidden states and approximate inter-jumping times S_k's. The instants G_t crosses this threshold will lead to the approximation of S_k's. The same argument is applied as $mode(f)\le\dfrac{b+c}{2}$.

For $x\in\mathbb{R}$, the kernel density estimator $f_N(x)$ of $f(x)$ is

$$f_N(x)=\frac{1}{Nh_N}\sum_{i=1}^{N}K\left(\frac{x-G(t_i)}{h_N}\right),$$

where *K* is the Gaussian kernel, $K(t)=\dfrac{1}{\sqrt{2\pi}}\exp\left(-\dfrac{1}{2}t^2\right)$ for $t\in\mathbb{R}$, and h_N is the positive real bandwidth. Using the method in [22], we choose $h_N=h_{crit}$ which is defined as

$$h_{crit}=\min\left\{h: f_N \text{ has at most } N(f) \text{ modes}\right\}. \tag{10}$$

Assuming that, in case $N(f)=2$, f_N has a unique anti-mode located at θ_N. In order to properly estimate the density *f* with $N(f)$ modes, we also need the following assumptions (for details see [23]).

Assumptions 7.2

1) *f* is uniformly continuous on $\mathbb{R}$.

2) $f\in\mathcal{C}^2(]a,d[)$.

3) $\lim_{t\downarrow a}f^{(1)}(t)>0$ and $\lim_{t\uparrow d}f^{(1)}(t)<0$.

Under the assumptions and the chosen h_N as (10), the convergence of θ_N

toward θ is ensured. When N is large enough, it is able to construct θ_N from the signal (G_t). The estimator θ_N of θ will be taken as a threshold, and the moment G_t crosses it or b or c will be used to construct an approximation of S_k's. We define the sets $I^-(x)$ and $I^+(x)$, in which $I^-(x)$ is the subset of $\{t_i \mid i \in \overline{1:N}\}$ such that $G_{t_i} \le x$ for all $t_i \in I^-(x)$, $I^-(x) = \{t_i \mid G_{t_i} \le x\}$ and $I^+(x) = \{t_i\} \setminus I^-(x)$. It is noted that

$$I^-(b) \subset I^-(\theta_N) \subset I^-(c)$$

$$I^+(b) \supset I^+(\theta_N) \supset I^+(c).$$

For later use, we also define set $D(t) = \{t_i \mid t_i \le t\}$. The procedure for the approximation of S_k's is described in two cases, single mode density and two modes density. For the presenting purpose, we define three temporary sequences $(Y'_k), (S'_k)$ and (T'_k) with k is an integer.

Single Mode Density Algorithm

Without the loss of generality, assuming that $mode(f) > \dfrac{b+c}{2}$, then the chosen threshold is b. Depending on the first observed signal G_{t_1}, we label the state of Y'_0. If $G_{t_1} < b$, Y'_0 is set to equal to 1. Otherwise, Y'_0 equals to -1. Then the observation time set $\{t_i\}$ is updated. The new times set $\{t_i\}_{\text{new}} = \{t_i\}_{\text{old}} \setminus D(t_1)$, this procedure of updating $\{t_i\}$ is in order to update the sets $I^{\pm}(x)$. Let us assume $G_{t_1} < b$, and Y'_0 is set to equal to 1. The procedure to construct (Y'_k), (S'_k) and (T'_k) is described as follow.

Set $T'_0 = t_1$ and $T'_1 = \min I^+(b)$, the temporary inter-jump is approximated by $S'_1 = T'_1 - T'_0$, then we update the set $\{t_i\}$ with $D(T'_1)$ and label the state of $Y'_1 = -1$. At the second loop, $T'_2 = \min I^-(b)$, the second temporary inter-jump $S'_2 = T'_2 - T'_1$, we update again the set $\{t_i\}$ with $D(T'_2)$ and label the state of $Y'_2 = 1$. The procedure repeats until the update of set $\{t_i\}$ is empty. In case $G_{t_1} \ge b$, and Y'_0 equals to -1, the procedure is similar. The approximation of the inter-jumping times $(\hat{S}_k)$ is then (S'_k), and the deduced hidden states $(\hat{Y}_k)$ is (Y'_k).

Two Modes Density Algorithm

When the kernel density has two modes, three interesting thresholds are b, θ_N and c. The procedure to construct the sequences (Y'_k), (S'_k) and (T'_k) are described, with $T'_0 = t_1$, as follow

Step 1. Compare $\min I^-(b)$ and $\min I^+(c)$

if $\min I^-(b) \le \min I^+(c)$

set $Y'_0 = 1$, the high state

update the set $\{t_i\}$ with $D\left(t = \min I^-(b)\right)$

set $T'_1 = \min I^+(\theta_N)$

else $\left(\min I^-(b) > \min I^+(c)\right)$

set $Y'_0 = -1$, the low state

update the set $\{t_i\}$ with $D\left(t = \min I^+(c)\right)$

set $T'_1 = \min I^-(\theta_N)$

Step 2. set $S'_1 = T'_1 - T'_0$,

Step 3. update the set $\{t_i\}$ with $D(T_1')$; repeat again from Step 1.

The loop stops when either $I^+(c)$ or $I^-(b)$ is empty. The loop stops at iteration K', if $I^-(b)$ is not empty, then the state of $Y_{K'}' = 1$. Otherwise, if $I^+(c)$ is not empty, the state is then $Y_{K'}' = -1$. In case $I^+(c)$ and $I^-(b)$ are empty but the set $\{t_i\}$ is not empty, the last state is set as the previous state $Y_{K'}' = Y_{K'-1}'$. And $S_{K'+1}' = \max\{t_i\} - T_{K'}'$. Finally, to obtain the approximation $(\hat{Y}_k)$ and $(\hat{S}_k)$, we merge the values under the same state of (Y_k') and (S_k'). For example, we obtain the sequences $(Y_k') = (y_0 = 1, 1, -1, -1, -1, 1, y_6 = 1)$, $(S_k') = (s_1, s_2, s_3, s_4, s_5, s_6, s_7)$, then $(\hat{Y}_k) = (\hat{Y}_0 = 1, \hat{Y}_1 = -1, \hat{Y}_2 = 1)$ and $(\hat{S}_k) = (\hat{S}_1 = s_1 + s_2, \hat{S}_2 = s_3 + s_4 + s_5, \hat{S}_3 = s_6 + s_7)$.

With the parametric model described in Section 4, we generated $N = 800$ observations of the signal G, the observed times are t_i on the interval $[0, T]$, $t_i = \frac{iT}{N}$. The threshold is computed from our procedure (**Figure 8**). From these simulated data, we give $\tilde{H}_m(y, t, z_t)$ for $y \in \{\text{High}, \text{Low}\}$ in **Figure 9** with $T = 24$ hours. In this simulation, there are 615/800 moments that the values are at high state. Psychological speaking, the agent is in the high mental state most of the pseudo-observed time. Statistically, the solid red line presents the 'survival' time in high mental state, and the dash line presents the 'survival' time in low mental state. Due to the technical issues, we have not collected the observed times during the simulation of the cyber attacks. However, these promising results from the simulated observations show the potential application in determining the mental state of an agent. This helps us understand the mental characteristic of each agent based on the behavior of his or her survival functions estimated for a long period of time.

The simulations, estimations, and figures presented in the paper are implemented using R language [24].

8. Concluding Remarks

The cyber security relating to the human behavior and specifically the cognitive

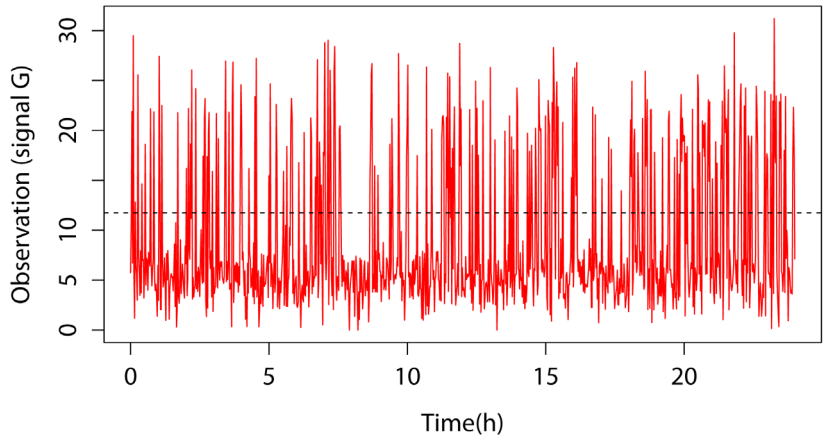

Figure 8. An example of signal G_t with the corresponding threshold computed from our procedure.

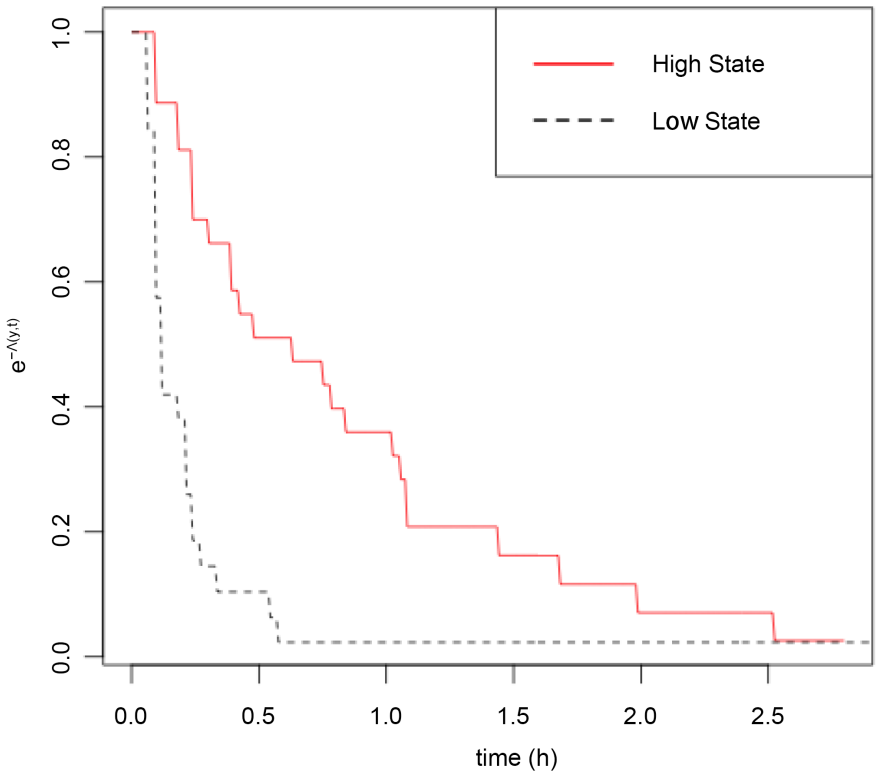

Figure 9. Fleming-Harrington estimates of the survival functions with respect to t for the abstraction hierarchy states.

aspects were explored. The perception of the cyber threats perceived by the agents was described by the Work Domain Analysis. The relationship between the abstraction hierarchy levels of a cyber threat and mental picture states of a human user is equivalent. We also explained the important role of the mental picture level of an agent to the security of system during the cyber attacks.

A non-stationary hidden Markov model was applied to the detection of the mental states of the agent. A parametric two-state model was proposed to simulate the variation of the mental states under the stress of the cyber attacks. The estimation algorithm for the parameters was developed based on the EM algorithm. The reconstruction of the hidden mental states is developed from the maximum posterior marginal method. We also studied the model and the estimation method on simulations as well as the observations from real-world data sets. The spending time in a given state was also investigated. The estimation based on a nonparametric framework was developed. We anticipate that this approach could have a significant contribution to understand mental characteristics of the agents dealing with the cyber threats.

References

[1] Pfleeger, S.L. and Caputo, D.D. (2012) Leveraging Behavioral Science to Mitigate Cyber Security Risk. *Computers & Security*, **31**, 597-611.

[2] Klein, G.A. and Calderwood, R. (1991) Decision Models: Some Lessons from the Field. *IEEE Transactions on Systems, Man and Cybernetics*, **21**, 1018-1026.

[3] Rasmussen, J. (1985) The Role of Hierarchical Knowledge Representation in Decision Making and System Management. *IEEE Transactions on Systems, Man and Cybernetics*, **SMC-15**, 234-243.

[4] Meineri, S. and Morineau, T. (2014) How the Psychological Theory of Action Identification Can Offer New Advances for Research in Cognitive Engineering. *Theoretical Issues in Ergonomics Science*, **15**, 451-463. https://doi.org/10.1080/1463922X.2013.815286

[5] Morineau, T. (2011) Turing Machine Task Analysis: A Method for Modelling Affordances in the Design Process. *International Journal of Design Engineering*, **4**, 58-70. https://doi.org/10.1504/IJDE.2011.041409

[6] Morineau, T., Frenod, E., Blanche, C. and Tobin, L. (2009) Turing Machine as an Ecological Model for Task Analysis. *Theoretical Issues in Ergonomics Science*, **10**, 511-529. https://doi.org/10.1080/14639220802368849

[7] Vicente, K.J. (1999) Cognitive Work Analysis: Toward Safe, Productive, and Healthy Computer-Based Work. CRC Press, Boca Raton.

[8] Naikar, N., Hopcroft, R. and Moylan, A. (2005) Work Domain Analysis: Theoretical Concepts and Methodology. Tech. Rep., DTIC Document.

[9] Posner, M.I. (1980) Orienting of Attention. *Quarterly Journal of Experimental Psychology*, **32**, 3-25. https://doi.org/10.1080/00335558008248231

[10] Fjortoft, R., Delignon, Y., Pieczynski, W., Sigelle, M. and Tupin, F. (2003) Unsupervised Classification of Radar Images Using Hidden Markov Chains and Hidden Markov Random Fields. *IEEE Transactions on Geoscience and Remote Sensing*, **41**, 675-686.

[11] Geman, S. and Geman, D. (1984) Stochastic Relaxation, Gibbs Distributions, and the Bayesian Restoration of Images. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **PAMI-6**, 721-741.

[12] Rabiner, L.R. (1989) A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition. *Proceedings of the IEEE*, **77**, 257-286. https://doi.org/10.1109/5.18626

[13] Rabiner, L.R. and Juang, B.H. (1986) An Introduction to Hidden Markov Models. *IEEE ASSP Magazine*, **3**, 4-16. https://doi.org/10.1109/MASSP.1986.1165342

[14] Devijver, P.A. (1988) Champs aléatoires de pickard et modélisation d'images digitales. *Traitement du Signal*, **5**, 131-150.

[15] Bilmes, J.A., *et al.* (1998) A Gentle Tutorial of the em Algorithm and Its Application to Parameter Estimation for Gaussian Mixture and Hidden Markov Models.

[16] Dempster, A.P., Laird, N.M. and Rubin, D.B. (1977) Maximum Likelihood from Incomplete Data via the em Algorithm. *Journal of the Royal Statistical Society. Series B* (*Methodological*), **39**, 1-38.

[17] Nocedal, J. and Wright, S. (2006) Numerical Optimization. Springer Science & Business Media, Berlin, Heidelberg.

[18] Andersen, P.K., Borgan, O., Gill, R.D. and Keiding, N. (2012) Statistical Models Based on Counting Processes. Springer Science & Business Media, Berlin, Heidelberg.

[19] Azas, R., Dufour, F., Gégout-Petit, A., *et al.* (2013) Nonparametric Estimation of the Jump Rate for Non-Homogeneous Marked Renewal Processes. In: *Annales de l Institut Henri Poincaré, Probabilités et Statistiques*, **49**, 1204-1231. https://doi.org/10.1214/12-AIHP503

[20] Azais, R., Coudret, R. and Durrieu, G. (2014) A Hidden Renewal Model for Moni-

toring Aquatic Systems Biosensors. *Environmetrics*, **25**, 189-199. https://doi.org/10.1002/env.2272

[21] Fleming, T.R. and Harrington, D.P. (1984) Nonparametric Estimation of the Survival Distribution in Censored Data. *Communications in Statistics—Theory and Methods*, **13**, 2469-2486. https://doi.org/10.1080/03610928408828837

[22] Silverman, B.W. (1981) Using Kernel Density Estimates to Investigate Multimodality. *Journal of the Royal Statistical Society. Series B* (*Methodological*), **43**, 97-99.

[23] Coudret, R., Durrieu, G. and Saracco, J. (2015) Comparison of Kernel Density Estimators with Assumption on Number of Modes. *Communications in Statistics—Simulation and Computation*, **44**, 196-216. https://doi.org/10.1080/03610918.2013.770530

[24] R Core Team (2015) R: A Language and Environment for Statistical Computing. R Foundation for Statistical Computing, Vienna, Austria. https://www.R-project.org