Security Analysis of Enterprise Network Based on Stochastic Game Nets Model

Yuanzhuo Wang, Chuang Lin, Senior Member, IEEE, Yang Wang, Kun Meng
Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China
Email: {yzwang, clin, ywang, mengkun08}@csnet1.cs.tsinghua.edu.cn

Abstract—In this paper, we propose a novel modeling method, Stochastic Game Nets (SGN), and use it to model and analyze the security issues in enterprise networks. Firstly, the definition and modeling algorithm of Stochastic Game Nets are given. And then we apply the Stochastic Game Nets method to describe the attack and defense course in the enterprise networks successfully, and find a Nash equilibrium. Finally we analyze the confidentiality and integrity of the enterprise network quantificationally based on the model. The method can also be applied to other areas with respect to a game.

Keywords— Stochastic Game Net, Enterprise Network, Security Analysis, Integrity, Confidentiality.

I. INTRODUCTION

Enterprise networks interconnect islands of departmental, local and remote computing and communication resources. They provide many benefits to organizations using them, such as the enhancement of efficiency, allowing employees greater flexibility in their work habits etc. As the role of enterprise networks, they are keeping expanding in theirs support of both internal and external connectivity in the form of emerging internet, intranet and extranet applications. Unfortunately, owing to all kinds of reasons, the networks always are under the hazard of illegal intrusion. This has given rise to the dichotomy faced by those partaking in the information economy paradigm. Security has become an ever increasingly critical element for enterprise network design and implementation.

More recently, the notion of intrusion tolerance has been advocated to allow the system to continue performing its intended function despite partially successful attacks, e.g., see Nicol, Sanders and Trivedi [1]. Wang [2] describes DoS attack and DDoS attacks as a queue model. Most attempts to validate security mechanisms and strategies have been qualitative analysis by showing the process employed to construct a security system. In face of various attack behaviors, security specialists are interested in knowing how an intruder enters enterprise networks, and how to prevent or to counteract attacks more efficiently. The quantificationial security analysis for enterprise network can make the security mechanisms and strategies more effective.

Game theory now has been introduced to the field of network security and computer security. In Lye and Wing [3], a game theoretic method for analyzing the security of computer networks was presented. The interactions between an attacker and the administrator were modeled as a two-player stochastic game for which best-response strategies (Nash Equilibrium) were computed. Mahimkar and Shmatikov [4] proposed a new protocol for preventing malicious bandwidth consumption, and demonstrated how game-based formal methods could be successfully used to verify availability-related security properties of network protocols. Liu, Zang and Yu [5] presented a general incentive-based method to model attacker intent, objectives, and strategies (AIOS) and a game-theoretic approach to infer AIOS. Wang and Reiter [6] and Bencsath, Buttyn and Vajda [6] proposed the puzzle auction mechanism to defend the DoS and DDoS attacks based on game theory. Xu and Lee [7] used game-theoretical framework to analyze the performance of their proposed DDoS defense system and to guide its design and performance tuning accordingly. Browne [8] described how static games can be used to analyze attacks involving complicated and heterogeneous military networks.

In most previous work, the interactions between the attacker and administrator are described as some game relations. A purely competitive (zero-sum) stochastic game would always make us find a Nash equilibrium. However, for the complex network structure, the game theory has not enough modeling abilities to describe interaction relations. It is hard to upbuild comprehensive and exact models of network security. Secondly, complicated state transitions make us hard to model the dynamic behaviors of participators in computer networks by the existing modeling methods. Thirdly, in the general game model, the full state space can be extremely large. However, we are interested in only a small subset of states which are related to attack scenarios. In addition, for reality, it may be difficult to quantify the rewards for some actions and the associated transition probabilities.

Therefore, in this paper, we propose a novel modeling method, Stochastic Game Nets, which can well model and analyze the game issues by taking advantages of Stochastic Petri Nets. Stochastic Game Nets are suitable to investigate the complex and dynamic game related issues in network security. We use Stochastic Game Nets to model and analyze the network attacks, compute the Nash equilibrium and best-response strategies to defend attacks. We believe that the Stochastic Game Nets (SGN) could open a new avenue to deal with the game related issues in the field of network security.

The rest of the paper is organized as follows. Section 2 introduces the definitions and useful properties of Stochastic Game Nets. In Section 3, enterprise network and its security problems will be analyzed. In Section 4 the Stochastic Game Nets are applied to model attack and defense behaviors in enterprise network. Section 5 analyzes the confidentiality and integrity based on the model. Section 6 concludes the paper.

This work was supported by the National Natural Science Foundation of China (No.60803123, No.60673187, No.60673160 and No.60673054) and China Postdoctoral Science Foundation funded project (No. 20080430040).
II. STOCHASTIC GAME NETS

We first provide the definition of Stochastic Game Nets. Note that this definition extends definition of Stochastic Petri Nets (SGN) by means of the Stochastic Game mechanism, whose understanding may refer to [9] for more details.

Definition 1. A Stochastic Game Net is represented as the nine-tuple vector $\text{SGN}= (N, P, T, F, \pi, \lambda, R, U, M_0)$, where

1. $N= \{1, 2, \ldots, n\} \text{ denotes the set of players,}$
2. $P$ is a finite set of places,
3. $T = T^1 \cup T^2 \cup \cdots \cup T^n$ is a finite set of transitions, where $T_k$ is the set of transitions with respect to player $k$ for $k \in N$,
4. $\pi : T \rightarrow [0, 1]$ is a routing policy representing the probability of choosing a particular transition,
5. $F \subseteq I \cup O$ is a set of arcs, where $I \subseteq P \times T$ and $O \subseteq (T \times P)$ such that $P \cap T = \emptyset$ and $P \cup T \neq \emptyset$, where $\phi$ is a empty set, for a convenience, we denote $x = \{y | (x, y) \in F\}$ the pre-set of $x$, similarly, $x = \{y | (y, x) \in F\}$ the post-set of $x$,
6. $R : T \rightarrow (R_1, R_2, \ldots, R_n)$ is a reward function for the players taking each transition, where $R_i \in (-\infty, +\infty)$ for $i \in N$,
7. $\lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_n\}$ is a set of transition firing rates in the transition set, where $\lambda$ is the number of transitions,
8. $U$ is the utility function of players, and
9. $M_0$ is the initial marking.

In this definition, we need to further explain the firing rule of the SGN=$ (N, P, T, F, \pi, \lambda, R, U, M_0)$. A marking $m$ represents a distribution of the tokens in Stochastic Game Nets. Each token $s$ is related with a reward vector $h(s)=h_0(s), h_1(s), \ldots, h_n(s)$ as its property, where $h_0(s)$ is the reward of player $k$ for token $s$. Each element of $T$ represents a class of possible changes of markings. Such a change of $t \in T$, also called transition firing, consists of removing tokens from a subset of places and adding them to another according to the expressions labeling the arcs. A transition $t$ is enabled under a marking $M$ whenever, $M(t) \neq \emptyset$, where $(p,t) \in F$, $p \in P$.

Players get the reward $R(t)$ after the firing of the transition $t$ and the reward is recorded in the reward vector $h$ of the token.

Definition 2 (Strategy): In a SGN model, a strategy for player $k$ is described as a vector $\pi^k=(\pi^k_1, \pi^k_2, \ldots, \pi^k_n)$, where $\pi^k_i$ is the probability that Player $k$ takes action $t_j$ and $w=[T]$. Given a $n$ players game, let $\pi = (\pi^1, \pi^2, \ldots, \pi^n)$, player $k$'s utility is defined as $U^k(\pi, p)$ (always simplified to $U^k(\pi)$), where $p$ denotes the initial state of player $k$.

Definition 3. In a game, Let $P$ be the whole state space, $T^k$ be the action set of player $k$. We call $P^k$ the state set of player $k$, and $P^k = \bigcup_{t=1}^{T_k} P^i_t$, where for $t \in T_k$, $P^i_t = \{p \in T^k | p \in t, p \in P\}$. In other words, at the state $p \in P_t$, player $k$ can take action $t$.

Definition 4. It is a unilaterally competitive game if for each $i \in N$, $U^i(\pi^i) > U^j(\pi^i)$ if and only if $U^j(\pi^i) > U^i(\pi^j)$ for all $j \in N, j \neq i$.

For analyzing complicated game problems, it is an effective method to set up the player models respectively and then combine into a whole model. In one unilaterally competitive game, SGN player models have the useful proposition as the follows.

Proposition 1. In a unilaterally competitive game, for player $i, j$, the state sets are $P^i$ and $P^j$ respectively, then $P^i \cap P^j = \emptyset$.

Proof: Let $\pi = (\pi^1, \pi^2, \ldots, \pi^n)$ and denote $\pi = (\pi^i, \pi^j)$. Suppose $P^i \cap P^j = \emptyset$. Because the utility value of the player $i$ is determined by initial state and the corresponding strategy, also by the assumption and $T^i \cap T^j = \emptyset$, we obtain that the utility value of the player $i$ is only related to $\pi^i$. For $i \neq j$, there exist $\pi = (\pi^i, \pi^j)$ and $\pi^i = (\pi^i^i, \pi^i^j)$ such that $U^i(\pi^i) > U^j(\pi^i)$ and $U^j(\pi^i) > U^i(\pi^j)$. Let $\pi^i^i = (\pi^i^i^i, \pi^i^j)$ and $\pi^i^j = (\pi^i^i, \pi^i^j)$, so $U^i(\pi^i^i) > U^j(\pi^i^j)$ and $U^j(\pi^i^j) > U^i(\pi^i^i)$.

This is a contradiction to the condition the game is unilaterally competitive. Therefore the initial assumption must be false, in other words, $P^i \cap P^j = \emptyset$.

Definition 5 (Nash Equilibrium): Given an $n$ players game, a mixed strategy Nash Equilibrium (NE) is a vector $\pi^*=(\pi^*^1, \pi^*^2, \ldots, \pi^*^n)$ such that $U^i(\pi^*^1, \pi^*^2, \ldots, \pi^*^i, \ldots, \pi^*^n) \geq U^j(\pi^*^1, \pi^*^2, \ldots, \pi^*^i, \ldots, \pi^*^n)$ for $i=1, 2, \ldots, n$, where $\pi^i$ is any alternative mixed strategy of player $k$ except for $\pi^i$.

For a NE $\pi^*$, no player does not have has an incentive to deviate from its mixed strategy given that the others do not deviate. Moreover, there is no mutual incentive for anyone of the players to deviate their equilibrium strategies $\pi^e^1, \ldots, \pi^e^n$. A deviation will mean that some of them will have lowered their optimal expected utility. So, the NE is also known as best responses.

Theorem 1. For a Stochastic Game Net $SGN= (N, P, T, F, \pi, \lambda, R, U, M_0)$. If the integer $n<\infty$, and the two sets $P$ and $T$ contain finite elements, then there exists a Nash Equilibrium under the setting of mixed strategies.

Proof: For a game with finite states, there exists at least one mixed strategy Nash Equilibrium (see [10]). So it remains to prove that a stochastic game net is associated with a game. In fact, for the case of $P^i \cap P^j = \emptyset$, the corresponding game is a programming problem. For the case of $P^i \cap P^j \neq \emptyset$, the states $P^i \cap P^j$ is the states space of the corresponding game, the rule of transitions fire in SGN is the rule of the game and $U$ is the utility function of the game. Therefore, there exists a mixed strategy Nash Equilibrium under the setting of mixed strategies.

In the rest of this section, we present an algorithm for solving the Stochastic Game Nets to find the NE.

Step one: Construct SGN models for each player

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2009 proceedings.
First we need identify the game elements and make certain the actions of different players. And then assign reward values.

(1) Construct the set of transitions $T$. It consists of all possible actions. For all transitions out of the game element states, identify the corresponding game actions. Note that there will always be an inaction $\varphi$, which represents that a player takes no action at all. The action set is the complete set of all these actions, $\varphi$ included. All actions will not necessarily be available in all states. We use transition $T_t$ to refer to the set of actions available in some state.

(2) Assign reward values $R$. In SGN model, we assign values $R: T \to (\mathcal{R}_1, \mathcal{R}_2, ..., \mathcal{R}_n)$, $\mathcal{R}_j \in (-\infty, +\infty)$ to each transitions $T$ to represent the reward gained by the player when an action finished. If the reward is negative, it expresses the player suffered loss. Reward can be used to social status and satisfaction versus disrespect and disappointment, as well as real values, e.g. financial gain and loss.

(3) Construct the set of places $P$. We use the places to describe the states of the system or player according to the results or infections of the actions. And use the arc $F$ denotes the consequence between the $P$ and $T$.

Step two: Describe the condition of the Nash Equilibrium

The objective of each player is to maximize its expected utility. Let $P \in \mathbb{R}^n$ be a discount factor, the expected utility as the distribution probability vectors of length $n$ for a discounted stochastic game can be found by solving a nonlinear programming problem (NLP). For a two-player stochastic game, we get the NLP like that

\[
\min_{u, \pi} \sum_{i=1}^{M} \sum_{p \in \mathcal{P}} \mathbb{E}[u(p, \pi)]
\]

s.t. $R(p, \pi) \pi^2(p) + \delta \pi R(p) \pi^2(p) \leq u(p, \pi), \quad i = 1, ..., |P|$

\[
\pi^*(p, \pi) = \frac{R(p, \pi) \pi^2(p)}{u(p, \pi)}
\]

where $T(p, u) = (p(p_1 | p_{11}, i_1), ..., p(p_1 | p_{11}, i_1))^{M} \in \mathcal{R}$.

Step Four: Construct the combination model and analysis

This step is to construct the whole model based on the above steps. The material method is as follows

(1) Combine the places $P$ that denote the same meanings in SGN models of different players. According to Proposition 1, there must be some places different players can take their actions in the game.

(2) Take computational results multi-strategy $\pi$ as the choice probabilities to transitions $T$ in the whole model.

(3) Assume the preferences $\lambda$ for each transition $t \in T$ in the SGN, which express the different action abilities.

III. SECURITY IN ENTERPRISE NETWORK

A. Enterprise Network

Consider the enterprise network shown in Fig. 1(left). It consists of Internet and intranet. The intranet includes administration server, information center, and some workstations at least. The perimeter router connects to the ISP router with a serial line.

![Enterprise network](image)

Figure 1. Enterprise network and its security role model

For analyzing the security of the network, we simply the network as Fig.1(right). In the simplified one, a node in the graph is a physical entity such as a server or workstation. We model the security threat by node attacker, and the defense as the administrator part by nodes InforCenter, AdminServer and
Workstation, respectively. An edge in the graph represents a direct communication path.

B. Action

An action pair (one from the attacker and one from the administrator) causes the system to move from one state to another in a probabilistic manner. A single action of the attacker can be any part of his attack strategies, such as flooding a server with SYN packets or downloading the password file.

When a player does nothing, we denote this inaction as $\theta$. Attacker consists of all the actions he can take in all the states, They can be described as \{Attack_httpd, Attack_ftpd, Continue_attacking, Deface_webportal_leave, Install_sniffer, Run_DOS_virus, Crack_Infor_center_root_password, Crack_workstation_root_password, Capture_data, Shutdown_Network\}. His action candidates in each state are whole or a part of above attack actions. For example, in the state Normal operation, the attacker has actions Attack_httpd, Attack_ftpd and $\theta$.

Actions for the administrator are mainly taking preventive or restorative measures. The actions of the administrator can be described in the following \{Remove_compromised_account, Restart_httpd, Remove_comromised_account_sniffer, Restore_Webportal_remove_compromised\}. His action candidates in each state are whole or a part of above attack actions. For example, in the state Normal operation, the administrator has actions $\lambda$, Restart_httpd, $\theta$.

We assume that the administrator does not know whether there is an attacker or not. Also, the attacker may have several objectives and strategies that the administrator does not know. Furthermore, not all of the attacker's actions can be observed.

IV. SGN MODEL OF ENTERPRISE NETWORK

In this section, we describe some main security problems of enterprise network by SGN model. We show attacker model as Fig.2. Fig.3 shows the administrator's viewpoint. In these figures, places represent network states containing the symbolic name. Each transition is labeled with an action $(p, r)$, where $p$ is the probability of the transition and $r$ is the reward. Due to the room constraints, values of parameters for each action are shown in Fig. 2 and Fig. 3.

We assume whenever the administrator find the attack launched, he must adopt the corresponding defense steps. As show in Fig. 3, there are a group of models.


In the model of Fig.4, the gray transitions denote the attacker’s actions, and the white transitions denote the administrator’s actions. We give the $\lambda$ and $\pi$ of transitions as Tab.1, where $\lambda$ denotes the action ability and $\pi$ denotes the...
choice probability. The values of $\pi$ are computational results of the Nash equilibrium strategies in step three.

<table>
<thead>
<tr>
<th>$t$</th>
<th>tat1</th>
<th>tat2</th>
<th>tat3</th>
<th>tat4</th>
<th>tat5</th>
<th>tat6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1.5</td>
<td>1.5</td>
<td>1.5</td>
<td>1.5</td>
</tr>
<tr>
<td>$\lambda$</td>
<td>0.33</td>
<td>0.1</td>
<td>0.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\tau$</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>tat7</td>
<td>tat8</td>
<td>tat9</td>
<td>tat10</td>
<td>tat11</td>
<td>tat12</td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>1.5</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>$\tau$</td>
<td>0.5</td>
<td>0.5</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>tad1</td>
<td>tad2</td>
<td>tad3</td>
<td>tad4</td>
<td>tad5</td>
<td>tad6</td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>1.5</td>
<td>1.5</td>
<td>2</td>
<td>2</td>
<td>1.5</td>
<td></td>
</tr>
<tr>
<td>$\tau$</td>
<td>0.33</td>
<td>0.9</td>
<td>0.33</td>
<td>0.9</td>
<td>0.9</td>
<td></td>
</tr>
</tbody>
</table>

V. SECURITY ANALYSIS

Here, we concern the confidentiality and integrity of the enterprise network. Confidentiality is the absence of unauthorized disclosure of Information and is denoted as the probability that the normal network services are affected or destroyed. So the confidentiality can be shown as the following formula.

$$I = P_{\text{Webportal defaced}} \times P_{\text{Adminserver Dos}} \times P_{\text{Network shut down}}$$

where $P_{\text{Webportal defaced}}$, $P_{\text{Adminserver Dos}}$, and $P_{\text{Network shut down}}$ denote the probability that the number of the token is zero in the places $\text{Webportal defaced}$, $\text{Adminserver Dos}$, and $\text{Network shut down}$. Integrity is the absence of improper system alterations, preventing improper or unauthorized change. Here it is described as the probability that the normal network services are affected or destroyed. So the integrity can be shown as the following formula.

$$I = P_{\text{Webportal defaced}} \times P_{\text{Adminserver Dos}} \times P_{\text{Network shut down}}$$

VI. CONCLUSION

In this paper, we propose a security model for enterprise network by a novel modeling method SGN which is a good model to model and deal with the complicated and dynamic game issues. The model inherits the efficient and flexible modeling approach of Stochastic Petri Nets, and also make well use of the game-theoretical framework from Stochastic Game theory. Based on it, we computed the strategy $\pi$ as the choice probabilities under Nash equilibrium and analyzed the confidentiality and integrity of enterprise network.

REFERENCES