Analysis of Attack Actions for E-Commerce Based on Stochastic Game Nets Model

Yuanzhuo Wang, Chuang Lin, Kun Meng
Department of Computer Science and Technology, Tsinghua University Beijing 100084, China
Email: {wangyuangzhuo, chlin}@ tsinghua.edu.cn

Junjie Lv
Business School,Beijing Technology and Business University, Beijing 100037, China
Email: lvjj@th.btbu.edu.cn

Abstract—**In this paper, we propose a novel modeling method, Stochastic Game Nets (SGN) and use it to model and analyze the attack actions in electronic commerce (e-commerce). 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 e-commerce. Finally we analyze the attack time and attack probability in the e-commerce quantificationally based on the model successfully. The method can also be applied to other areas with respect to a game.**

Index Terms—**Stochastic Game Nets; e-commerce; analysis of attack actions; security**

I. INTRODUCTION

Electronic commerce (e-commerce) refers to the exchange of goods and services over the Internet. All major retail brands have an online presence, and many brands have no associated bricks and mortar presence. E-commerce systems are relevant for the services industry. For example, online banking and brokerage services allow customers to retrieve bank statements online, transfer funds, pay credit card bills, apply for and receive approval for a new mortgage, buy and sell securities, and get financial guidance and information.

Nowadays, e-commerce has become an important technology for the dissemination of information and transferring business critical data from customers to businesses. A secure system accomplishes its task with no unintended side effects. Security is not a number of features, but a system process. The weakest link in the chain determines the security of the system. This has given rise to the dichotomy faced by those partaking in the information economy paradigm. Security has become an ever increasingly critical element of e-commerce designs and implementations.

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]. Most attempts to validate security mechanisms and strategies have been qualitative by showing the process employed to construct a security system. In face of various attack Actions, security specialists are interested in knowing how an intruder enters e-commerce systems, and how to prevent or to counteract attacks more efficiently. The quantificational security analysis for e-commerce can make the security mechanisms and strategies more effective.

Game theory has been recently proposed by several studies for a theoretical analysis of network security [2][3]. In [4] a model for attacker and intrusion detection system (IDS) is designed as action within a two-person, nonzero-sum, non cooperative game framework. The possible use of game theory for development of decision and control algorithms is investigated. In [5], authors regard the interactions between an attacker and the defender as a two-player, non-cooperative, zero-sum, finite stochastic game and formulate an attack defense stochastic game model for the game. Liu, Zang and Yu [6] 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 [7] and Bencsth, Buttyn and Vajda [7] proposed the puzzle auction mechanism to defend the DoS and DDoS attacks based on game theory. Xu and Lee [8] used game-theoretical framework to analyze the performance of their proposed DDoS defense system and to guide its design and performance tuning accordingly.

On the other hand, the quantitative evaluation of the e-commerce security is more and more important. [10] presents a quantitative model to measure known Unix security vulnerabilities using a privilege graph, which is transformed into a Markov chain. The model allows for the characterization of operational security expressed as the mean effort to security failure, as proposed by [9]. Based on the game theoretic, some methods to model and compute the probabilities of malicious user actions for use in stochastic models is suggested, the optimal strategy of the attack is calculated and, following the approach of [11]. In [12][13], Karin Sallhammar etc. researched the quantitative measure methods unite the game theory and stochastic models.

In most previous work, the interactions between the attacker and defender are described as some game

relations. A purely competitive (zero-sum) stochastic game would always make us find a Nash equilibrium. A general-sum stochastic game would allow us to find potentially multiple Nash equilibrium. A Nash equilibrium gives an idea of the administrator for the attacker's strategy and a plan for how to do in each state in the event of an attack. According to the Nash equilibrium, we could know about the attacker's best attack strategies. By using a stochastic game model, we are also able to capture the probabilistic nature of the state transitions, which is more realistic.

However, some essential limitations of solutions affect applications of the game theory in network security. Firstly, for the complex network structure, the game theory has not enough modeling abilities to describe interaction relations. The comprehensive and exact models of network security are hard to upbuild. Secondly, the complicated state transitions make us hard to model the dynamic Actions of participators in computer networks by using the existing modeling methods. At the same time, it is difficult to update when conditions change. 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 in attack scenarios. In addition, for reality, it may be difficult to quantify the rewards for some actions and the associated transition probabilities.

In the predecessor of this paper [14][15] stochastic game nets (SGN) is proposed to compute and analyze the expected game actions and Nash equilibrium as a part of the transition probabilities in SGN is introduced. In this paper, we apply SGN to model and analyze the e-commerce attacks and defendence and compute the Nash equilibrium. By analyzing the attack time and probability in the e-commerce quantificationally, we explain the strategies are reasonable and instruct the administrator apply these results to enhance the security of their system We believe that it could open a new avenue to deal with the problems of e-commerce 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, the modeling and analysis method are researched based on the SGN model. Section 4 analyzes attack actions of e-commerce and its security problems. In Section 5 the Stochastic Game Nets are applied to model attack and defense Actions in e-commerce. Section 6 analyzes the attack time and probability in the e-commerce quantificationally using the SGN model. Section 7 concludes the paper.

II. STOCHASTIC GAME NETS

A. In this section, we define Stochastic Game Nets (SGN), and then give some useful properties for the Stochastic Game Nets. We first provide the definition for 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 SGN= (N, P, T, F, π, λ, R, U, M0), where

(1) $N = \{1,2,\ldots n\}$ 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 Tk is the set of transitions with respect to player k for $k \in N$,

(4) π : T→[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 $P \cap T = \phi$ and $P \cup T \neq \phi$, where ϕ is a empty set, for a convenience, we denote $\cdot x = \{y \mid (y, x) \in F\}$ the pre-set of x, similarly, $x \cdot = \{y \mid (x, y) \in F\}$ the post-set of x,

(6) $R : T \to (\Re_1, \Re_2,\ldots,\Re_N)$ is a reward function for the players taking each transition, where $\Re_i \in (-\infty,+\infty)$ for $i \in N$,

(7) $\lambda = \{\lambda_1, \lambda_2,\ldots, \lambda_w\}$ is a set of transition firing rates in the transition set, where w 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 $h(s)=(h_1(s), h_2(s),\ldots, h_n(s))$ as its property, where $h_k(s)$ 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, $M(p) \neq \phi$, 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 $\pi^k = (\pi(t_1^k), \pi(t_2^k),\ldots,\pi(t_{w_j}^k))$, where $\pi(t_j^k)$ is the probability that Player k takes action t_j and $w_j=|T^k|$.

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 simplied 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 $P^k = \bigcup_{t \in T_k} p_t^k$, where for $t \in T^k$, $p_t^k = \{p \mid t \in T^k, p \in t, p \in P\}$. In other words, at the state $p \in p_t^k$, player k can take action t.

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

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

Definition 5 (Nash Equilibrium): Given a N players game, a Nash Equilibrium (NE) is a vector $\pi^* = (\pi^{1*}, \pi^{2*}, \dots, \pi^{N*})$ such that
$$U^k(\pi^{1*}, \dots \pi^{(k-1)*}, \pi^{k*}, \pi^{(k+1)*}, \dots \pi^{N*}) \geq U^k(\pi^{1*}, \dots \pi^{(k-1)*}, \pi^k, \pi^{(k+1)*}, \dots \pi^{N*})$$
where $k=1,2,\dots,N$, π^k is any alternative mixed strategy of player k except for π^{k*}.

For a NE π^*, 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 $\pi^{1*}, \pi^{2*}, \dots, \pi^{N*}$. A deviation will mean that some of them will have lowered their optimal expected utility. So, the NE is also known as best responses. Note that if the two sets P and T contain finite elements, then the two sets λ and F both have finite elements. In this case, a Stochastic Game Net (N, P, T, F, π, λ, R, U, M_0) can be mapped to an N-person game, where the transition set T in the Stochastic Game Nets composes the finite of strategies, and U corresponds to the reward functions in the N-person game. Based on this, according to Nash's theorem in Nash[10]. There is at least one NE under the setting of mixed strategies. Therefore, we can clearly obtain the following theorem.

Theorem 1. For an 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 exits a 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 optimal strategy of each player, i.e., to find the NE. In what follows, we give the details of the four steps in our algorithm.

A. Construct SGN models for each player

First we need identify the game elements and make certain the actions of different players and then assign reward values.

(1) Constructing the transitions set T. It consists of all possible actions. Note that there will always be an action ϕ for players, which represents that the player takes no action at all. T is a complete set of all actions. But, all actions will not necessarily be available in any special state. We use transition T_i to refer to the set of actions available in the state i.

(2) Assigning reward values R. In SGN model, we assign values $R:T \to (\Re_1, \Re_2)$, $\Re_i \in (-\infty, +\infty)$ 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) Constructing 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.

B. Describe the the utility of players

The objective of each player is to maximize its expected return. For the constructed SGN, the utility of the player is equal to the sum of utility of places he passed until leave the SGN. We denote
$$U^k(\pi, p_I) = E\{\sum_{i=1}^{\#P} \delta_i u^k(p_i)\}, \qquad k=1,2.$$
where p_I is the initial place of strategy π, $\delta_i \in [0,1]$ is the discount index of place p_i where if p_i is not the place the strategy π passed then $\delta_i = 0$, otherwise, δ_i is identified a proper value, the expectation operator E is used to mean that player k plays π^k, i.e., player k chooses an action using the probability distribution $\pi^k(p_i)$ at place p_i and receives a reward $u^k(p_i)$, where

$$u^k(p) = \sum_{t^1 \in T^1, t^2 \in T^2} \{\pi^1(p, t^1) R^k(p, t^1, t^2) \pi^2(p, t^2)\}, \qquad (1)$$

$R^k(p, t^1, t^2)$ is the reward gained by player k at p under two players choose the action t^1 and t^2 respectively. In order to determine the optimal Defense strategy, we must find the Nash Equilibrium $\pi^* = (\pi_1^*, \pi_2^*)$.

C. Solve the Nash Equilibrium

Our model relies on the basic assumption of game theory, which states that a rational player will always try to maximize his own reward. For each place p_i, which is modeled as a matrix game G_i, where the action sets of attacker and defender are $A_i = \{a_1, a_2, \dots, a_K\}$ and $D_i = \{d_1, d_2, \dots, d_L\}$ respectively. For the attacker, if an attack action is chosen in place p_i, and that the intrusion is successful and remains undetected, the system may transfer to another place p_j where the game can continue. The possible outcomes can be denoted as a $K \times L$ matrix, moreover, γ_{kl} is the total outcome associated with the action pair (a_k, d_l).

$$\gamma_{kl} = \begin{cases} r_{kl} + \sum_j \delta_j U(p_j) & \text{successful attacks} \\ c_{kl} & \text{otherwise} \end{cases} \qquad (2)$$

where r_{kl} denotes the attacker's reward at place p_i when attacker choose action a_k and the defender response d_l, considering the effection of the following other places, we use $U(p_i)$ to denote the expected utility at place p_i and $\delta_i \in [0,1]$ is the discount parameter. By the same method, we can construct a $|A_i| \times |D_i|$ matrix at place p_i for attacker, which has the form

$$U(p_i)= \begin{array}{|c||c|c|c|} \hline & d_1 & \cdots & d_m \\ \hline\hline a_1 & \gamma_{11} & \cdots & \gamma_{1m} \\ \hline \cdots & \cdots & \gamma_{kl} & \cdots \\ \hline a_n & \gamma_{n1} & \cdots & \gamma_{nm} \\ \hline \end{array} \qquad (3)$$

We can expect an attacker and defender to behave in accordance with the probability distribution $\pi_i^1 = (\pi_i^1(a_1), \pi_i^1(a_2), \ldots, \pi_i^1(a_K))$ and $\pi_i^2 = (\pi_i^2(d_1), \pi_i^2(d_2), \ldots, \pi_i^2(d_L))$. So the utility of attacker in game is $E(\pi_i^1, \pi_i^2) = \sum_{\forall a_k \in A_i} \sum_{\forall d_l \in D_i} \pi_i^1(a_k) \pi_i^2(d_l) r_{kl}$. For Simply, we use zero-sum game elements to model the interactions between an attacker and the defender. An attacker who does not know the defense strategy, therefore thinking of the defender as a counter-player in the game who tries to minimize the attacker's reward. Hence, the optimal attack strategy of P_i, and its corresponding defense strategy, is obtained by solving

$$\max_{\pi_i^1} \min_{\pi_i^2} E(\pi_i^1, \pi_i^2) \qquad (4)$$

These strategies will be denoted π_i^1 and π_i^2 respectively. The value of game, denoted $U(p_i)$, is defined as the expected outcome when π_i^1 and π_i^2 are used, i.e.

$$U(p_i) = \max_{\pi_i^1} \min_{\pi_i^2} E(\pi_i^1, \pi_i^2) \qquad (5)$$

The purpose of the stochastic game model is to predict the complete set of attack probability vectors $\pi^{1*} = \{\pi_i^{1*}\}$ to be used in the defender rate matrix Q. To find the π_i^{1*} strategies for all game elements in the stochastic game, refer to [12], one can use Alg. 1, which is based on the Shapley algorithm [16].

TABLE I.   ALGORITHM TO COMPUTE EXPECTED STRATEGY

Algorithm 1 Compute player(m)'s expected strategy in SGN
01: **Function** Strategy_for_ player(m)
02:   **Initialize** $U = \{U(p_i)\}$
03:   **repeat**
04:     **for** each place $p_i \in P^m$ do
05:         compute the matrix $U(p_i) = [r_{kl}]$
06:     **end for**
07:     **for** each game element $p_i \in P^m$ **do**
08:         update the value vector $N(i) \leftarrow Value[U(p_i)]$
09:     **end for**
10:     **until** $N(i) = Value[U(p_i)], \forall p_i \in P$
11:     **for** each game element $p_i \in P^m$ **do**
12:         $\pi_i^m \leftarrow Solve[U(p_i)]$
13:     **end for**
14:   **return** $\pi^{m*} = \{\pi_i^{m*}\}$; /* the set of equilibrium vectors, it is the optimal strategy for player m */

We believe that the optimal attack strategy set $\pi^* = \{\pi_i^*\}$ will be a good indication of the expected attack probabilities.

D. Construct the SGN

This step is to construct the whole model for every player based on the above step computational results. The material method is as follows

(1) Assume the preferences λ for each transition T in the whole model, which express the different action abilities.

(2) If, in place k, the action a_i^k of player A will impede the player B's, then we describe this case by the success probability. Namely, in SGN combine models, the action success probability of the play B should multiply by the following coefficient α.

$$\alpha = \frac{\lambda_B}{\lambda_B + \lambda_A} \times p_{success}^A(a_i^k) \qquad (6)$$

Where $p_{success}^A(a_i^k)$ is the success probability of the player A's action a_i^k. λ_B and λ_A are the rates of the transitions, and λ_B denotes the action ability of player B, and λ_A is the action ability of player A.

(3) The actions of the player A make the player enter another state. So the correlative the actions of the player B have the different beginning places in SGN model. The beginning places should change to the places expressed the results of player A's actions.

(4) Take the above step computational results multi-strategy π as the choice probabilities to transitions T in the combine model.

II. ANALYSIS OF ATTACK ACTIONS

In the network, an attacker often has many atomic attack actions to choose between. He may also choose to interrupt an ongoing attack at a certain stage, or not to start the attack at all. It is necessary to analyze all the options an attacker has in every place in SGN model. Assuming that for each place k ($k = 1, \ldots, n$), an attacker can take m_k actions

Attack by choosing one of the possible atomic attack actions a_i^k, where $i = 1, \ldots, m_k - 1$. We can analyze these actions as following rules

(1) If the action succeeds the attacker will receive the reward associated with the particular attack.

(2) If the action fails no reward will be achieved.

(3) If the action is detected, the attacker will receive the cost associated with the attack.

Resign and interrupt the ongoing attack. This is denoted action a_{mk}^k. The attacker will most likely experience this option as a defeat, hence, by resigning he will receive a cost, which magnitude depends on both how far the attack has proceeded as well as the probability that the attack would have remained undetected if he had chosen to continue.

The probability that the attacker will choose action i in state k will be denoted $p_{attack}(a_i^k)$. Hence, for each place k in the SGN model, the attacker's expected choice of action can be represented by a probability vector

$$p_{attack}(a^k) = (p_{attack}(a_1^k), \ldots, p_{attack}(a_{mk}^k))$$

where $\sum_{i=1}^{m_k} p_{attack}(a_i^k) = 1$, Hence, $p_{attack} = \{p_{attack}(a_k)|i = 1, \ldots$

$\ldots, n\}$, will be the complete set of decision probability vectors for the SGN model. To continue an attack from place k, the attacker not only has to decide upon an atomic attack action but he also must succeed with the action. Assuming that the reward and cost result from the transitions, the probability that an attacker may cause a transition of the system from place k to the places that denote attack results can therefore be computed as

$$p_{attack}(a_i^k) = P[M(p_r) \neq 0] = 1 - P[M(p_r) = 0] \qquad (7)$$

Where $M[p_r]$ denotes the token number in the place p_r, p_r denote the result places of attack actions. Namely the $P_{attack}(a_i^k)$ is the probability that the attack result place is not empty. We can compute the attack time based on the throughput of the transition in the SGN model as (8).

$$TH_{atttack} = \sum_{M \in H} P[M]\lambda_{attack} \qquad (8)$$

Where H is marking set of the attack transition, λ_{attack} is firing rate of the attack transition. So the attack time can be computed as following.

$$T_{attack} = \frac{1}{TH_{attack}} \qquad (9)$$

If the attacker chooses action a_{mk}^k, or fails, no state change occurs. Hence, to incorporate attacker action in the transition probabilities when parameterizing a SGN model, one should identify all atomic attack actions, i.e., those transitions that can be caused by attackers, assign success probabilities to the atomic attack actions, and compute and assign decision probabilities to the atomic attack actions.

III. SECURITY IN E-COMMERCE

A. Game in E-Commerce

In a typical e-commerce experience, a shopper proceeds to a Web site to browse a catalog and make a purchase. This simple activity illustrates the four major players in e-commerce security. One player is the shopper who uses his browser to locate the site. The site is usually operated by a merchant, also a player, whose business is to sell merchandise to make a profit. As the merchant business is selling goods and services, not building software, he usually purchases most of the software to run his site from third-party software vendors. The software vendor is the last of the three legitimate players. The attacker is the player whose goal is to exploit the other three players for illegitimate gains. The Fig. 1 illustrates the players in a shopping experience. Here, we think the web site and software provider as the illegitimate defender.
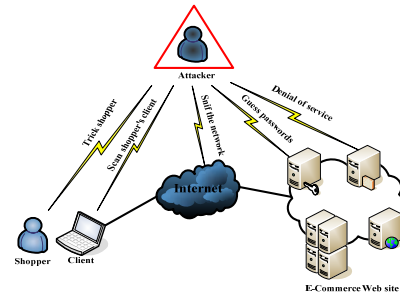

Figure 1.   Points the attacker can target

The attacker can besiege the players and their resources with various damaging or benign schemes that result in system exploitation. Threats and vulnerabilities are classified under confidentiality, integrity, and availability. A threat is a possible attack against a system. It does not necessarily mean that the system is vulnerable to the attack. Vulnerability is a weakness in the system, but it is not necessarily known by the attacker. Vulnerabilities exist at entry and exit points in the system. Attacks against e-commerce Web sites are so alarming, they follow right after violent crimes in the news. Practically every month, there is an announcement of an attack on a major Web site where sensitive information is obtained. The developers producing e-commerce software are pulled from the same pool of developers as those who work on other software. In fact, this relatively new field is an attraction for top talent. The criminal population did not undergo a sudden explosion, but the incentives of an e-commerce exploit are a bargain compared to other illegal opportunities. Actions

According to the above security analysis, the attack and defense actions are described as follows:

1) Attack Actions

● Tricking the shopper

Some of the easiest and most profitable attacks are based on tricking the shopper. These attacks involve surveillance of the shopper's Action, gathering information to use against the shopper.

● Scanning the shopper's client

Based on the opened ports found, the attacker can use various techniques to gain entry into the user's system. Upon entry, they scan your file system for personal information, such as passwords.

● Sniffing the network

The attacker monitors the data between the shopper's computer and the server. He collects data about the shopper or steals personal information, such as credit card numbers.

● Guessing passwords

This style of attack is manual or automated. Manual attacks are laborious, and only successful if the attacker knows something about the shopper. The attacker can automate to go against multiple sites at one time.

● Using denial of service attacks

The denial of service attack involves getting the server to perform a large number of mundane tasks, exceeding the capacity of the server to cope with any other task. This attack not only causes the target site to experience problems, but also the entire Internet as the number of packets is routed via many different paths to the target.

2) Defense Actions

Despite the existence of hackers and crackers, e-commerce remains a safe and secure activity. The resources available to large companies involved in e-Commerce are enormous. These companies will pursue every legal route to protect their customers. Fig. 2 shows a high-level illustration of defenses available against attacks.
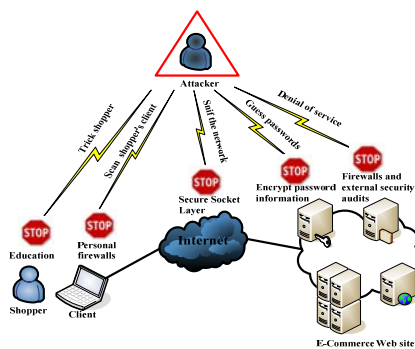
Figure 2.   Attacks and their defenses

At the end of the day, your system is only as secure as the people who use it. Education is the best way to ensure that the shoppers take appropriate precautions:

● Education

Before the beginning of e-commerce, let shoppers know about the security mechanisms and possible attack action adequately.

● Install personal firewalls

Install personal firewalls for the client machines.

● Secure Socket Layer

Encrypt the stream using the Secure Socket Layer (SSL) protocol to protect information flowing between the client and the e-Commerce Web site.

● Encrypt password information

Store password information in encrypted form.

● External security audits and firewalls

Use appropriate policies, firewalls, and routine external security audits.

In addition, use threat model analysis, strict development policies, and external security audits to protect software running the Web site. Based on the game course between the attacker and defender, we can two action sets. Specially, when a player does nothing, we denote this inaction as ϕ.

Action_Attacker={*Trick_shopper, Scan_client，Sniff_ network, Guess_passwords, Use_DoS,* ϕ}={a_1, a_2, a_3, a_4, a_5, a_6,}.

Action_Defender={*Education, Install_personal_firewalls,   Secure_Socket_Layer, Encrypt_password, External_security_ audits,* ϕ}={d_1, d_2, d_3, d_4, d_5, d_6}.

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

IV.   SGN MODEL OF E-COMMERCE

In this section, we describe the above actions in the e-commerce by SGN. The Fig. 3 shows how the attacker sees the situation change as a result of his actions. The Fig. 4 shows the defender's viewpoint. In these Figures, places represent network states containing the symbolic name. Each transition is labeled with an action $t(p, r)$, p is the success probability of the transition, and r denotes the reward, in which the attacker need make choice to attack actions.
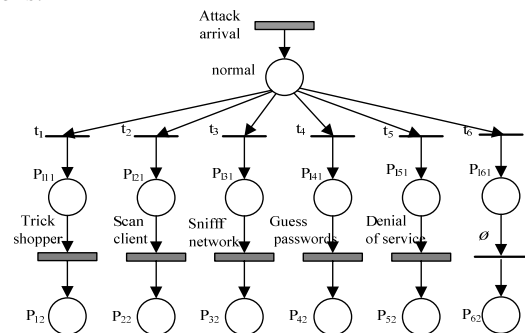

Figure 3.   Attacker's view model

We assume the defender will take the defenses as Fig. 2. When the attack happening, attack actions must be effected by the corresponding defenses. So In the Fig. 4, there are a group of models.
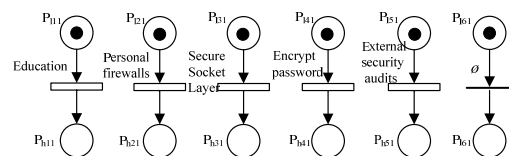

Figure 4.   Defender's view model

In the Fig. 4, there are 10 places, where {p_{l11}, p_{l21}, p_{l31}, p_{l41}, p_{l51}} denote the low security level the normal state. And {p_{h11}, p_{h21}, p_{h31}, p_{h41}, p_{h51}} denote the high security level the normal state, which are the results of the defense actions. In addition, in these model, the actions have the success probabilities and as follows.

TABLE II.   PARAMETERS OF THE COMBINATION MODEL

	Transitions	Success probability	Reward
Attack actions	*Trick_shopper*	0.6	$r_{a1}=4$
	Scan_client	0.7	$r_{a2}=5$
	Sniff_network	0.4	$r_{a3}=10$
	Guess_passwords	0.3	$r_{a4}=7$
	Use_DoS	0.5	$r_{a5}=2$
	∅	1	$r_{a6}=0$
Defense actions	*Education*	0.9	$r_{d1}=10$
	Install_personal_firewalls	1	$r_{d1}=10$
	Secure_Socket_Layer	0.8	$r_{d1}=10$
	Encrypt_password	0.8	$r_{d1}=10$
	External_security_audits	0.7	$r_{d1}=10$
	∅	1	$r_{d1}=0$

According to (3), the game matrix at place p_{normal}, and the utility under the equilibrium for attacker, which have the form

	d_1	d_2	d_3	d_4	d_5	d_6
a_1	c_{11}	r_{a1}	r_{a1}	r_{a1}	r_{a1}	r_{a1}
a_2	r_{a2}	c_{22}	r_{a2}	r_{a2}	r_{a2}	r_{a2}
a_3	r_{a3}	r_{a3}	c_{33}	r_{a3}	r_{a3}	r_{a3}
a_4	r_{a4}	r_{a4}	r_{a4}	c_{44}	r_{a4}	r_{a4}
a_5	r_{a5}	r_{a5}	r_{a5}	r_{a5}	c_{55}	r_{a5}
a_6	r_{a6}	r_{a6}	r_{a6}	r_{a6}	r_{a6}	c_{66}

$U(p_{normal})=$

Where we assume the other parameters $c_{11}=2$, $c_{22}=1$, $c_{33}=2$, $c_{44}=1$, $c_{55}=3$. By using Alg. 1, the strategies and utilities of the SGN model be solved. The optimal attack strategy vectors $\pi^*=\{\pi_1=0.0001, \pi_2=0.4614, \pi_3=0.2307, \pi_4=0.3076, \pi_5=0.0001, \pi_6=0.0001\}$ and the utility $U(p_{normal})=4.9231$. They will then be used in the transition probability of the combined model for the security evaluation and analysis.

By the above method we mentioned, we construct the co-mbination model based on the player models, Fig. 3 and Fig. 4. The SGN combination model can be shown as Fig. 5.
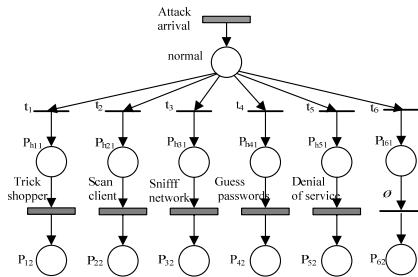

Figure 5. SGN combination model

In the model of Fig.5, the gray transitions denote the attacker's actions, and the success probability of the transitions can be computed by (6) . We give the action ability λ and choice probability π of transitions as Table III. The values of π are computational results using the algorithm we proposed.

TABLE III. PARAMETERS OF THE COMBINATION MODEL

	Transitions	Action ability	Choice probability	Success probability
Attack actions	*Trick_shopper*	8	0.0001	0.1846
	Scan_client	12	0.4614	0.2333
	Sniff_network	8	0.2307	0.1818
	Guess_passwords	5	0.3076	0.1235
	Use_DoS	8	0.0001	0.1111
	∅	0	0.0001	1
	Education	9	1	0.9
Defense actions	*Install_personal_firewalls*	10	1	1
	Secure_Socket_Layer	12	1	0.8
	Encrypt_password	10	1	0.8
	External_security_audits	7	1	0.7
	∅	0	1	1

V. SECURITY ANALYSIS

Now we use the software package SPNP (Stochastic Petri Net Package) [17] to compute the model and analyze the attack actions. We mainly concern the attack action time and probability for the e-commerce. According to the SGN model, we can find the attack time and attack probability can be computed by formulae (7) and (9). For different attack arrival rate, the attack probability with the network system time can be shown as the Fig. 6. From the Figures, we can find the attack probability increases as the system time increases. Some attack actions, such as *Scan_client, Sniff_ network, Guess_passwords,* should be defended inevitably. The other attack action can be controlled effectively.
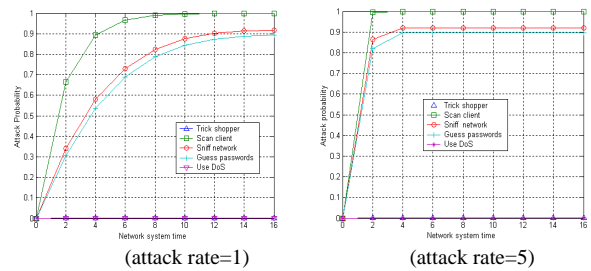

(attack rate=1)   (attack rate=5)

Figure 6. Attack probability with network system time(attack rate=1)
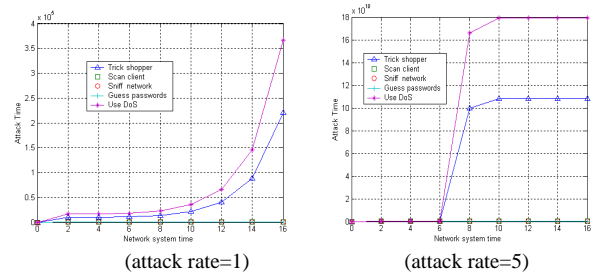

(attack rate=1)   (attack rate=5)

Figure 7. Attack time with network system time(attack rate=1)

Fig. 7 shows the time different attack actions intrude into system successfully. Obviously, *Use_DoS* and *Trick_shopper* need more time for attackers. From the four figures, we can find that as the system tends to the steady state, the successful attack probability has nothing to do with the attack rate. This is an important conclusion, according to which, the administrators can consider the fixed attack probability and time for a given network when design the defendence stratgies and which are only relate to the ability and anticipant reward of the attacker, and are independent of the attack rate. Based on the above SGN model, some other security attributes can also be evaluated and analyzed. And then the corresponding effective defending mechanism can be designed.

VI. Conclusion

In this paper, we propose a security model for e-commerce by a novel modeling method, Stochastic Game Nets. The model could inherit 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 the model, we computed the strategy π as the choice probabilities under Nash equilibrium and analyzed time and probabilities of different attack actions for e-commerce. And some useful results have been obtained. According to these results, some effective defending mechanism can be designed.

References

[1] D.M. Nicol, W.H. Sanders, and K.S. Trivedi. Model-based evaluation: From depend-ability to security. IEEE Transactions on Dependability and Secure Computing,1(1), 2004.

[2] K. Sallhammar, S. J. Knapskog, and B. E. Helvik, "Using stochastic game theory to compute the expected Action of attackers", in Proceedings of the 2005 International Symposium on Applications and the Internet (Saint2005) Workshops, 2005.

[3] Karin Sallhammar, B. E. Helvik and S. J. Knapskog, "Towards a Stochastic Model for Integrated Security and Dependability Evaluation", In Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), 2006.

[4] T. Alpcan and T. Basar. A game theoretic approach to decision and analysis in network intrusion detection. In Proceedings of the 42nd IEEE Conference on Decision and Control, 2003.

[5] Wei Jiang, Zhi-hong Tian, Hong-li Zhang, and Xin-fang Song. A Stochastic Game Theoretic Approach to Attack Prediction and Optimal Active Defense Strategy Decision. 2008 IEEE International Conference onNetworking, Sensing and Controlpp, 2008.648-653

[6] P. Liu, W. Zang, and M. Yu. Incentive-based modeling and inference of attacker intent, objectives, and strategies. ACM Transactions on Information and System Security, 8(1):1–41.

[7] X. Wang and M. Reiter. Defending against denial-of-service attacks with puzzle auctions. In Proceedings of IEEE Security and Privacy, 2003.

[8] J. Xu and W. Lee. Sustaining availability of web services under distributed denial of service attacks. IEEE Transactions on Computers, (4):195–208.

[9] B. Littlewood, S. Brocklehurst, N. Fenton, P. Mellor, S. Page, D. Wright, J. Dobson, McDermid J., and D. Gollmann. Towards operational measures of computer security. Journal of Computer Security, 2:211–229, Oct 1993.

[10] R. Ortalo and Y. Deswarte. Experimenting with quantitative evaluation tools for monitoring operational security. IEEE Transactions on Software Engineering, 25(5):633–650, Sept/Oct 1999.

[11] B B. Madan, K. Vaidyanathan, and K.S. Trivedi. Modeling and quantification of security attributes of software systems. In Proceedings of the International Conference on Dependable Systems and Networks (DSN'02), 2002.

[12] Karin Sallhammar, Bjarne E. Helvik and Svein J. Knapskog. On stochastic modeling for integrated secruity and dependability evaluation. The Journal of Networks (JNW, ISSN 1796-2056), Vol. 1, No. 5

[13] Karin Sallhammar and Svein J. Knapskog. Using Game Theory in Stochastic Models for Quantifying Security. In Proceedings of the 9th Nordic Workshop on Secure IT-systems. 2004

[14] Chuang Lin, Yuanzhuo Wang, Yang Wang. A Stochastic game nets based approach for network security analysis, In Proc. of the 29th International Conference on Application and Theory of Petri Nets and other Models of Concurrency, Concurrency metHods: Issues aNd Applications 2008 Workshop (Invited paper), 2008:21-33.

[15] Yuanzhuo Wang, Chuang Lin, Kun. Meng. Security analysis of enterprise network based on stochastic game nets model: In proc, international conference on communicaations (ICC), 2009 , in print.

[16] A. Kats and J. F. Thisse , unilaterally competitive games, International Journal of Game Theory, (1992) 21: 291-299.

[17] L S. Shapley, Stochastic games, Proceedings of the National Academy of Science USA, vol. 39, pp. 1095–1100, 1953.

[18] Ciaodo G, Muppala J, and Trivedi K S, SPNP: Stochastic Petri Net Package, in: Proc. Petri Nets and Performance Models, 1989, 142-151.

Yuanzhuo Wang, born in 1978, Ph.D. He is an assistant researcher in Tsinghua University, He is a IEEE member and a senior member of China Computer Federation. received the B.S. degree and M.S. degree in computer software and engineering from Deparament of Computer Science, School of Information Technology and Engineering, Yanshan University. His current research interests include stochastic Petri nets, stochastic game nets, network security analysis, performance evaluation,. So far he has published over 40 papers.

Chuang Lin is a professor and the head of the Department of Computer Science and Technology, Tsinghua University, Beijing, China. He received the Ph.D. degree in Computer Science from Tsinghua University in 1994. In 1985-1986, he was a Visiting Scholar with the Department of Computer Sciences, Purdue University. In 1989-1990, he was a Visiting Research Fellow with the Department of Management Sciences and Information Systems, Graduate School of Business, University of Texas at Austin. In 1995-1996, he visited the Department of Computer Science, Hong Kong University of Science and Technology. His current research interests include computer networks, performance evaluation, network security analysis, logic reasoning, and Petri net theory and its applications. He has published more than 200 papers in research journals and IEEE conference proceedings in these areas and has published three books.

Professor Lin is a senior member of the IEEE and the Chinese Delegate in TC6 of IFIP. He serves as the Technical Program Vice Chair, the 10th IEEE Workshop on Future Trends of Distributed Computing Systems (FTDCS 2004); the General Chair, ACM SIGCOMM Asia workshop 2005; the Associate Editor, IEEE Transactions on Vehicular Technology; and the Area Editor, Journal of Parallel and Distributed Computing.