Security Analysis for Web Service Behaviors Based on Hierarchical Stochastic Game Model*

LV Junjie¹, WANG Yuanzhuo², LI Jingyuan², MENG Kun³ and LIN Chuang³

(1. Business School, Beijing Technology and Business University, Beijing 100027, China)
(2. Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China)
(3. Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)

Abstract — Model-based quantitative techniques are not commonly used for web service behaviors security evaluation, which have typically been applied to analyze small parts of an overall design. Aiming at the traits of attack behaviors for web services, this paper proposes the hierarchical Stochastic game nets (SGN) model and analysis methods. We give the definitions and important theorems of stochastic game nets, study the modeling algorithm of hierarchical SGN model. A series of simulation results are presented to show that, by applying hierarchical SGN model to describe the attack and defense behaviors in web services, quantifiable results can be successfully obtained for the evaluation of important attributes.

Key words — Hierarchical stochastic game nets, Web service behaviors, Security analysis, Attack, Defence.

I. Introduction

The use of web services is pervasive, and is becoming the key technology for enabling a loosely coupled, language-neutral, platform-independent foundation to link applications across multiple organizations throughout the web. By masking the heterogeneity of the underlying platforms, web services enhance interoperability, and are thus able to support complex business applications which are composed of a series of services. In fact, interoperability among heterogeneous systems is the key promise of web services, from which a bunch of notions are derived. Web services paradigm provides a vast amount of flexibility in the way complex software systems are implemented, especially enterprise services. These services are important concepts, enabling the modularization of functions or capabilities presented as services, to extract abstract activities in complex business processes that can be rearranged in an easy way at any time. The involvement of independent trust domains is also a key aspect regarding security in web services architectures.

Security becomes even more critical for implementations based on web service principles, due to loose coupling of services and applications, and their possible operations across trust boundaries. Nevertheless, the benefits stand against some serious flaws these new technologies bring along, where the most severe issues they bring is web services security. The typical requirements for a secure system are integrity, confidentiality and availability. Any behavior targeting violation of one of the three properties is called an attack, the possibilities for an attack is called vulnerability.

However, no system-level methodology currently exists that can quantify the security level provided by a particular system-level approach. Most attempts at validation of security are qualitative, focusing on the process to build an architecture that is supposed to be secure. Currently, efforts aimed at quantitative validation of security have usually been based on formal methods or informally using “red teams” to try to compromise for a certain goal. Both approaches, although capable of identifying system vulnerabilities, have their limitations, especially when they are applied to large scale architectures.

This paper proposes hierarchical Stochastic game nets (SGN) to analyze security in web processes. SGN differs from other methodologies of security in that it applies stochastic modeling and game theory to analyze security issues, which has certain advantages. For example, the stochastic game nets have a powerful modeling and analyzing ability for complicated and dynamic game problems, which is effective for describing prioritized, concurrent, asynchronous, stochastic and non-deterministic events.

Aiming at the complexity of the security issues of web services, we investigate a special kind of SGN named hierarchical SGN, which has been proved to be effective to simplify an otherwise complicated and large-scale model, and to simplify the analyzing procedure of a game. According to the cases we have studied and analyzed in this paper, we believe that it is appropriate to make stochastic assumptions about: 1) the cause and

* Manuscript Received Nov. 11, 2013; Accepted Dec. 23, 2013. This work is supported by National Natural Science Foundation of China (No.61402022, No.61173008, No.61303244, No.61370132), and Beijing Social Science Foundation (No.14JGB033).
© 2015 Chinese Institute of Electronics. DOI:10.1049/cje.2015.07.002
detection of vulnerabilities; 2) attacker and defender’s behaviors, in terms of the effectiveness of the chosen vulnerabilities and the defender’s responses to the attacks; 3) the transient periods of vulnerabilities. We can therefore apply stochastic theories and methods to solve or simulate the model of web service procedures. By a series of experiments and the following analyses, we have proved that the hierarchical SGN is a powerful weapon for security analyses, especially in complex game behavior relationships.

The rest of the paper is organized as follows. Section II introduces the definitions of stochastic game nets, including the corresponding theorems and corollaries. The modeling and analysis methods based on the hierarchical SGN model for web services are proposed and discussed in Section III. We apply the hierarchical SGN to model the attack and defense behavior in web services, analyzing confidentiality, identity, availability and integrity of web services quantitatively in Section IV, and concludes the paper in Section V.

II. Hierarchical Stochastic Game Nets

Aiming to fulfill the aforementioned requirements, based on the basic definitions of stochastic game nets, we propose a bunch of fundamental characteristics and hierarchical model analysis methods of the hierarchical stochastic game net to support hierarchical analyses of web services security issues.

**Definition 1** A stochastic game net is represented as a nine-tuple model $SGN=(N, P, T, F, \pi, \lambda, R, U, M_0)$ where

1. $N = 1, 2, \ldots, n$ denotes the set of players,
2. $P$ is a finite set of places,
3. $T = T_1 \cup T_2 \cup \ldots \cup T^n$ is a finite set of transitions, where $T^k$ is the set of transitions with respect to players $k$ 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 $P \cup T \neq \emptyset$,
6. $R : T \rightarrow (\mathbb{R}_1, \mathbb{R}_2, \ldots, \mathbb{R}_N) = \{s_1, s_2, \ldots, s_n\}$ is a reward function for the players taking each transition, where $\mathbb{R}_i \in (-\infty, +\infty)$ for $i \in N$,
7. $\lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_\omega\}$ is a set of transition set, where $\omega$ is the number of transitions,
8. $U$ is the utility function of players, and
9. $M_0$ is the initial marking.

In Definition 1, we further explain the firing rule of the SGN. 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 players $k$ for the token $s$. At the beginning, for every token $s$, $h(s) = (0, 0, \ldots, 0)$. A transition $t$ is enabled under a marking $M$ whenever $M(p) \neq \phi, (p, t) \in F$. $M(p)$ denotes the set of tokens under the marking $M$ in the place $p$. 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. Players get the reward $R(t)$ after the firing of the transition $t$ and the reward is recorded in the reward set $h$ of the token. For any $p \in P$, the utility of players depends on the path, the tokens pass and the places. It is convenient to simplify the utility function of players by introducing the utility of places. Let $u^k(p)$ be the utility of players $k$ at place $p$ and $u^0_0(p)$ is its initial utility,

$$u^k_0(p) = \begin{cases} u^k_0(p) + \sum_i E(h_k(s_i)), & \text{token } s_1, s_2 \ldots \\
0, & \text{otherwise}
\end{cases}$$

where $E(h_k(s_i))$ is the expectation of reward of player $k$ for the token $s$ under some routing policy.

We define the utility function of player $k$ as $U^k = f(p)$, where $P$ is the place set, the details of function $f$ will be explained in Section III.

**Definition 2 (Sub-SGN)** given an SGN, set a place $p \in P$ to be the final place. Any source $p_s \neq p \in P$ and $|p_s| = 0, 1, p_s, p$ and all paths from $p_s$ to $p$ in the SGN constitute a submodel Sub, the Sub is a sub-SGN if all places in the Sub have no pre-transitions outside Sub except $p_s$.

**Definition 3 (Strategy)** in an SGN model, a strategy of player $k$ is described as a $p^* = (\pi(t_1^k), \pi(t_2^k), \ldots, \pi(t_n^k))$, where $\pi(t_i^k)$ is the probability that player $k$ takes behavior $t_i$ and $w_j = |T|^j$.

Given an $n$ 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 4 (Nash equilibrium)** given an $n$-players game, a mixed strategy Nash equilibrium (NE) is a set $\pi^* = (\pi_1^*, \pi_2^*, \ldots, \pi_n^*)$ such that $U^k(\pi_1^*, \pi_2^*, \ldots, \pi_{k-1}^*, \pi_k^+, \pi_{k+1}^+, \ldots, \pi_n^*) \geq U^k(\pi_1^*, \pi_2^*, \ldots, \pi_{k-1}^*, \pi_k^*, \pi_{k+1}^*, \ldots, \pi_n^*)$ where $k = 1, 2, \ldots, n$, $\pi^k$ is any alternative mixed strategy of player $k$ except for $\pi^k$.

For an NE $\pi^*$, no player has an incentive to deviate from its mixed strategy given that the others do not deviate. Moreover, there is no mutual incentive for any one of the players to deviate its equilibrium strategies $\pi^* = \pi_1^*, \pi_2^*, \ldots, \pi_n^*$. A deviation is a player to downgrade their optimal expected utility. Hence, the NE is also known as the best response.

**Theorem 1** For an 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 at least a mixed strategy Nash equilibrium.

According to Theorem 1, we know SGN has NE, and always has multiple equilibria. We can use the above characteristics to build a method to address the selection of the “right one” according to the concept of refinements in game theory. For the security analysis of network, participators select their behavior according to the system states, so the rational solution should satisfy Definition 5.

**Definition 5 (Sub-SGN perfect Nash equilibrium)** for an SGN $G$, if $\pi$ is a behavior strategy for SGN and
$p_s$ is the source place of a Sub-SGN $G_{ps}$. $\pi_{ps}$ is the restriction of $\pi$ to the Sub-SGN. A Sub-SGN perfect equilibrium $\pi^*$ of the SGN is a Nash equilibrium of $G$ with the property that $\pi_{ps}$ is a Nash equilibrium of Sub-SGN $G_{ps}$ for all $p_s \in P$.

**Corollary 1** For an SGN, if $|N| < \infty$, and the two sets $P$ and $T$ contain finite elements. Then it has a sub-SGN perfect Nash equilibrium.

From Corollary 1, for an SGN, if there exists a sub-SGN which has only one Nash equilibrium, then the Nash equilibrium is the sub-SGN perfect Nash equilibrium restricting in the sub-SGN. For finding a sub-SGN perfect Nash equilibrium for the complicated SGN model, we propose the hierarchical SGN model method, where we focus on 3 sub-models patterns as of pattern 1–3 in Fig.1-3. To simplify these patterns to the equivalent simple model, three theorems are presented as follows.

![Pattern 1 transform to the equivalent simple model](image1)

**Theorem 2** Given an SGN, for a sub model like pattern 1 in Fig.1, it has an immediate transition $t$ with strategy probability $\pi$ and $n$ time transitions $T_i(1 \leq i \leq n)$ with expected rate $\lambda_i$, where the firing times of $T_i$ are exponentially distributed random variables. Moreover, suppose the player can obtain reward $R_i$ through the firing of the transition $T_i$, and let $T$ denote the equivalent transition, we have

1. The expected rate $\lambda^*$ of the transition $T$ has been expected as $\lambda = 1/\sum_{i=1}^{n} \pi_i/\lambda_i$.
2. The expected expected reward $R^* = \sum_{i=1}^{n} \pi_i \cdot R_i$.

**Theorem 3** Given an SGN, for a sub model like pattern 2 in Fig.2, it has $n$ immediate transitions $t_i$ with strategy probability $\pi_i$ such as $\sum_{i=1}^{n} \pi_i = 1$ and $n$ time transitions $T_j(i = 1, 2, \ldots, n)$ satisfying exponential distribution with expected value $1/\lambda_i$, respectively. Moreover, suppose the player can obtain reward $R_i$ through the firing of the transition $T_i$. Let $T$ denote the equivalent transition, we have

1. The expected rate $\lambda^*$ of the transition $T$ has been expected as $\lambda = 1/\sum_{i=1}^{n} \pi_i/\lambda_i$.
2. The equivalent expected reward $R^*$ of $T$ is $R^* = \sum_{i=1}^{n} \pi_i \cdot R_i$.

**Theorem 4** Given a multi-stage sub model like pattern 3 in Fig.3, it has $n$ immediate transitions $t_i$ with strategy probability $\pi_i$, where $\sum_{i=1}^{n} \pi_i = 1$ and $n$ time transitions $T_i$ satisfy exponential distribution with expected value $1/\lambda_i$, respectively. Suppose that any $T_i$ does not fire more than one time until the transition $t_j$ fires, where $(i = 1, 2, \ldots, n)$. Moreover, the player can obtain reward $R_i$ through the firing of the transition $T_i$. Let $T$ denote the equivalent transition, we have

1. The equivalent rate $\lambda^*$ of the transition $T$ has been expected as $\lambda^* = 2/(\alpha \times (1/\lambda_1 + \sum_{i=2}^{n} 1/\lambda_i))$, where $\alpha$ is an adjustive coefficient related to the behavior arrival rate, $\lambda_m$ is the least rate among the rate set $\{\lambda_1, \lambda_2, \ldots, \lambda_n\}$.
2. The equivalent expected reward $R^*$ of $T$ is $R^* = \beta \cdot \sum_{i=1}^{n} R_i$, where $\beta$ is an adjustive coefficient depending on the arriving tokens in the place $P$.

### III. Hierarchical Modeling and Analysis Method

In this section, we introduce the general method for analyzing security behaviors by SGN\[8\]. We then propose a hierarchical modeling and analysis method for the analyses of the security issues in complex systems.

1. **Construct SGN models**
   1. Constructing the place set $P$. Finding all possible states of considering system, let them be the place set $P$.
   2. Constructing the set of transitions $T$ that consists of all possible behaviors. For all of the game element states, identifying the corresponding game behaviors. Note that there will always be an inaction $\phi$, which represents that a player takes no behavior at all. The behavior set is a complete set of all these behaviors, but every behavior will not necessarily be available in any special state. Let $T_i$ denote the behavior set of player $i$, and transition $T_j = \{t_{j1}, t_{j2}, \ldots\}$ to refer to the set of behaviors available in the state $j$ for player $i$.

2. **Constructing SGN.** For every player $i$, given a place $p_x \in P$, connect $p_x$ and the transition elements of $T_x^i$ by arc respectively. If after the behavior $t^i_{jm}$ (or transition) is performed, the system transforms to the state $p_y \in P$, then connect $t^i_{jm}$ and $p_y$ by arc. By this step, we can construct the SGN of player and use the arc $F$ to denote the consequence between the $P$ and $T$. By combining the same places of all players, we can obtain the whole SGN.

3. **Assigning reward values $R$.** In an SGN model, we assign values $R : T \to (\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_n), \mathcal{R}_i \in (-\infty, +\infty)$, which represent the reward gained by the players when certain behavior is conducted. If the reward is negative, it means that the player has suffered certain 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.

2. **Describe 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 has passed until leaving the SGN. We denote $U^k(\pi, p) = E\{\sum_{i=1}^{P} \delta_t u^k(p_i)\}$ as the utility of player $k, k = 1, 2, \ldots, n$, where $p_i$ is the initial place.
of strategy $\pi$, $\delta_i \in [0, 1]$ is the discount index of place $p_i$ which implies the importance of $p_i$ by identifying a proper value to $\delta_i$. The expectation operator $E$ means that player $k$ adopts strategy $\pi$, i.e., player $k$ chooses behaviors according to the probability distribution $\pi^k(p_i)$ at place $p_i$. According to the flow of tokens the player can receive utility $u^k(p_i)$ at $p_i$, where $E(h_k(s_i))$ is the expectation of the $h_k(s_i)$ where the token $s_i$ flows from $p_1$ to $p_i$ under the strategy $\pi$. In order to determine the optimal defense strategy, we must find the Nash equilibrium $\pi^* = (\pi^1, \pi^2, \ldots, \pi^n)$.

3. 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 or her own utility. By Corollary 1, we can find the Nash equilibrium by solving the sub-SGN with place set $P_{ss}$. Let $p_w$ be the source place of the sub-SGN $ss_i$. The expected utility function $U^k(\pi, p^w)$ denotes a utility of player under the strategy $\pi$ from the sub-SGN. Let $\delta_i \in [0, 1]$ be discount factors, the utility $U^k(\pi, p^w)$ is

$$U^k(\pi, p^w) = E\left[ \sum_{p_i \in P_{ss_i}} \delta_i u^k(p_i) \right]$$

(1)

where $u^k(p_i)$ is calculated by the assumption that the initial token in the place $p_i$ is in the sub-SGN.

By the work of Filar and Vrieze[9], an NE 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 as:

$$\min_{u^1, u^2, \sigma^1, \sigma^2} \left\{ 1^T[u^k - U^k(\pi^1, \pi^2) - \delta P(\pi^1, \pi^2)u^k] \right\}, \quad k = 1, 2$$

(2)

$$R^1(p_i)\pi^2(p_i) + \delta T(p_i, u^1)\pi^2(p_i) \leq u^1(p_i)1,$$

s.t. $\pi^1(p_i)^T R^2(p_i) + \delta \pi^1(p_i)^T T(p_i, u^2) \leq u^2(p_i)1^T,$

$$i = 1, \ldots, |P|$$

where $T(p, u^k) = [[[p(p_1[p, t^1], i^2), \ldots, p(p_1[p, t^1], i^2)]^T u_k^k]_{i^1 \in T^1, i^2 \in T^2}$.

For the players, the global minimum to this non-linear program represents the optimality conditions required, where solution $(U^1, U^2, \pi^1, \pi^2)$ corresponds to a Nash equilibrium of the game.

IV. Security Model and Analyses in Web Services

1. Hierarchical SGN model in web services

In this section, we describe some main security behaviors in web services by a hierarchical SGN model. We show attacker model in Fig.4, and Fig.5 shows the defender’s viewpoint, in which places represent network states containing the symbolic name.

We assume the defender can adopt the corresponding defense approaches for the attacks in Fig.4. As shown in Fig.5, there are a group of defence models {D1, D2, D3, D4, D5, D6, D7, D8, D9}, where the gray transitions denote the attacker’s behaviors, and the white transitions denote the defender’s behaviors. Each transition is labeled with a behavior $(p, r, \lambda)$, where $p$ is the successful probability of the transition and $r$ is the reward, $\lambda$ denotes the behavior ability. The strategy probability $\pi$ can be computed according to Eq.2.

2. Security analysis

We used the software package SPNP (Stochastic Petri net package)[10] to compute the SGN model in Fig.5 and analyzed the security behaviors, mainly concerning confidentiality,
identity, availability and integrity in web services. In Fig.6, we compare the four attributes in a whole, where Fig.6(a) shows confidentiality, identity, availability and integrity change with system time, and Fig.6(b) shows that the four characteristics change if the attack arrival rate increases.

In Fig.6(a), the availability came to a stable stage quickly as system time increases, while confidentiality, integrity and identity keep low and finally go into a comparatively stable value as the attack and defence behaviors proceed. In Fig.6(b), we can see that the four characteristics does not change notably along with the attack rate, where availability does not change at all, and confidentiality, integrity and identity decrease a little and become stable quickly. According to the above analyses of Fig.6, we can find the effects of defence measures to the attack behaviors, where availability keeps high in probability and the others too. This results indicate that a rational attacker prefers to get direct rewards rather than just to disrupt services in web services. On the other hand, attacks to identity are always the pre-conditions of many other attack behaviors. Therefore it is not as important as the other characteristics.

From the above analyses, we show confidentiality, identity, availability and integrity change with system time and attack arrival rate respectively. According to the modeling of typical web attack and defence process, we use hierarchical stochastic game nets to describe a complete web service attack and defence process. By quantitative calculations of the four most important characteristics along with the system time and attack arrival rate, we get a series of useful conclusions as follows. 1) When an attack is in progress, confidentiality, integrity and identity decrease gradually to a small but fixed value, despite of the defence measures. 2) The attack rate has little to do with availability, confidentiality, integrity and identity at the same time. 3) At the beginning, the attack rate affects confidentiality critically; but as system time increases, the attack rate slows down the decreasing rate of confidentiality and integrity. 4) The availability of a web service will reach a stable
value as system time passes; the availability of a web service system relies on its own defence strategies and parameters, and will not be affected by the system time and the attack behaviors. These four findings will greatly support the design and implementation of web services security policies and mechanisms.

V. Conclusion

In this paper, we discussed a new modeling method for analyzing security behaviors of web services by using SGN to describe the attack and defence behaviors. SGN has a powerful modeling and analyzing ability for the complicated and dynamic game problems, by which the complexity of the security issues of web services can be solved properly. Moreover, we proposed a hierarchical SGN modeling and analysis method, including a series of important theorems and corollaries based on which the complicated attack and defence processes were described, and the confidentiality, identity, availability and integrity in web services were analyzed and evaluated quantificationally. Our research findings can be applied to predict the attack behaviors, and the design of defending mechanisms as well.

References


LI Junjie Ph.D., associate professor. Her current research interests include stochastic game model, network security analysis, etc.

WANG Yuanzhuo (corresponding author) Ph.D., associate professor. He is a IEEE member and a senior member of China Computer Federation. His current research interests include social computing, open knowledge network, network security analysis, stochastic game model, etc. (Email: wangyuanzhuo@ict.ac.cn)

LI Jingyuan Ph.D., Senior Engineer at Institute of Computing Technology, Chinese Academy of Sciences. His current research interests include information dissemination in social networks, social network structure and evolution prediction, etc. He is a senior member of China Computer Federation.

MENG Kun Postdoctor Fellow of the Department of Computer Science and Technology, Tsinghua University. His research interests include performance evaluation of computer networks, network security analysis, service computing and stochastic models.

LIN Chuang Professor and Ph.D. supervisor of the Department of Computer Science and Technology, Tsinghua University. His main research interests include performance evaluation, stochastic Petri net and quality of network services. He is a fellow member of China Computer Federation.