Available online at www.ijpe-online.com

International Journal of Performability Engineering

Vol. 13, No. 5, September 2017, pp. 763-774
DOI: 10.23940/ijpe.17.05.p19.763774

An Analytical Method for Dynamic Evolution of Attack Process based on Markov Game

Weicheng Yan, Lingyan Li*

School of Management, Xi'an University of Architecture & Technology, Xi'an 710055, Shaanxi, China

Abstract

Because of the randomness of attacker and defender's strategy selection, the state variation during the network attack process must be a random process. So, the network attack and defense process can be abstracted a confrontation of multi-state based on different gains matrix. This paper describes the random of attack and defense strategy selection with Markov decision, and extends the Markov game model from single-state to multi-state and multi-agent. After that, it proves the existence of equilibrium strategy and gives the solving method of nonlinear programming. Finally, deduction and simulation analysis of the practical example indicate that this model's method is correspond to the actual application and the evaluation result is accurate, so it can be used to have a more detailed simulation to network attack and defense process in reality.

Keywords: Attack and Defense Evolution; Evolution Game; Markov Game; Network Attack Model; Network Security

(Submitted on January 29, 2017; Revised on April 12, 2017; Accepted on July 23, 2017)

1. Introduction

With the revolution of information technology, some new technologies such as the computer, network communication have made the world's operation model change fundamentally, especially in recent years. The in-depth research and industrialization on cloud computing, big data, internet of things and other internet concepts has made the control of the information become a new strategic contention point. In February 2014, the establishment of the "central network security and information technology group" marks the awakening of national consciousness of the Internet in China, and demonstrates the importance of national information security strategy. However, with the opening of the network and the simplification of the new attack methods, lots of well-organized and profitable organization will cause serious damage to the country's information infrastructure, especially some high level facilities. How to protect the network space has become a hot research topic in the security field, and a problem to be solved in the new century with the nuclear issue.

At the beginning, the hotspot for network security problems is how to build an absolute security system, and reduce the vulnerability of the design to ensure the confidentiality, integrity and availability of the system, which can be regarded as the first phase of network security research. But people soon realized that an absolute security system is impossible in practice, and malicious intrusion must exist in the reality. People began to think about building a safety assistant system (for example: IDS system), the basic goal of which is to detect and take appropriate measures when the intrusion occurs. Since the technical report of Anderson that was published in 1980, intrusion detection has a great development, but in general it can be divided into two parts: anomaly detection and misuse detection [13]. Intrusion detection model is the earliest method proposed by Dorothy Denning, current development version remains the little refinement in this foundation, which can be regarded as the second phase of network security. Intrusion detection technology has been widely used, but in principle it can only detect the sample attack, and does not work for complex situation such as covert attacks which is bypass the firewall, and multi-step attacks, etc. Under the situation of the increasingly serious network attacks, IDS is very difficult to guarantee real-time

* Corresponding author. Tel.:1-375-987-9522; fax: 0-298-552-0042.
E-mail address: 284993092@qq.com.

detection and alarm, so the focus of research turns to the active analysis from passive defense. This proposal marks the beginning of the third stage, such as vulnerability risk assessment model, situational awareness model, etc. The active analysis method is developed from hacker technology, whose intention is to carry out the overall security evaluation and make defensive strategies before attacks happen, or to ensure that the network can still provide scheduled service functions under damaged attack. Active evaluation model is a hot research topic, and it is also a promising research direction. It mainly includes two steps: model construction and analysis method construction. The process of model construction is aimed to abstract the elements of network and risk assessment and show them in the form of particular language, the present work of it is focused on the attack graph model. Analysis method construction includes two kinds: qualitative analysis and quantitative analysis. The focus of qualitative analysis is logical association problem among vulnerabilities, which usually gets the entire possible attack path through visual analysis for attack scenarios. The quantitative analysis, which describes the security situation of the network in the digital calculation method, generally quantifies some factors with the process of model construction [2]. But most of the models are still an experimental behavior in the small scale of network, and there are lots of steps to meet the security analysis requirements for complex network, such as the description of attack intention, large-scale system applications, and so on. Therefore, combining with complexity science should make a great development in this field such as dynamic network [8], control theory [9], etc.

During the computer network attack and defense process, there must be a confrontation in multi-system states and the gain matrix for each state is different. The random of attack or defense strategy selection will lead to the random of the state change of network system, which is described with Markov decision process in this paper, a new Markov evolutionary game security analysis model with multi-state and multi-agent is proposed, after the definition of formal modeling, this paper also gives out a solving strategy of attack and defense game progress by nonlinear programming methods. Finally, using this model to have a simulation analysis and deduction on a typical enterprise network's attack and defense process, the result shows that the model by this paper is more consistent with the practical application, the evaluation result is more accurate, and it is helpful to the development of the research on the attack and defense game.

2. Related research

With the deepening of research on computer network security, it has integrated multi-disciplines. Formal model analysis methods have been widely used in the evaluation process of different systems. The active network security analysis framework (such as attack model, vulnerability assessment, etc.), whose purpose is not eliminating the vulnerability but guiding the network administrator to find an effective balance point between "safe" and "function" before the attack, is different from the passive detection technology (such as IDS, firewall, virus detection, etc.). However, there is a big difference between the security problem caused by the artificial attack and the traditional system failure problem, and there are many new challenges in the field. According to the analysis of the existing literature, the network security evaluation mainly includes the following four steps.

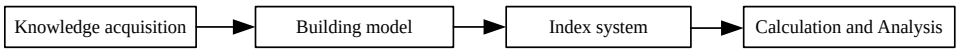


Figure 1. Main steps of network security evaluation

2.1. Vulnerability scanning or knowledge acquisition

Vulnerability scanning is the initial phase of security analysis, whose intention is to detect whether there is an open hole or a simple attack path in the system through a vulnerability scan tool, such as host based scanning tool COPS, network based scanning tool Nessus, etc. A list of vulnerabilities or a clearly brief report cannot solve the vulnerability-associated problems. With the development of research and in-depth analysis, the information collection objects gradually increase; network topology, key assets, services, and other related knowledge have been incorporated into the scope of the acquisition [3,6,17]. The direct effect of this procedure on network security analysis is not obvious, but this step is the most basic link in the evaluation of the network security model. The initial knowledge acquisition process is manual, but so far it has basically reached automation. In recent three years, there are few studies on this aspect; most of articles say that it can get the required information with automated tools [3,24].

2.2. Formal modeling

Formal modeling is the most important step of network security analysis and evaluation, which is mainly divided into two kinds: building based on rules and building based on abstract model. Initial modeling approach is based on rules, whose core

idea is to extract the features of the attack case and express them to the regular expression, then match the rule expression and the target system one by one for safety analysis. This approach can be said to be a continuation of the work of vulnerability scanning or a special application of intrusion detection idea in active safety analysis [6, 17, 24]. Naturally, there are defects too. The generating process of the rule becomes the restriction point, for the collation of the vulnerability rules can only be carried out locally and is not suitable for the overall detection of the network. Currently, mature network security scanning tools are most based on the rules, and the accumulation of these rules is also the basis of the abstract model analysis method (such as the rule description of the atomic attack in the attack graph). Current research is transforming to the abstract model analysis method.

Attack tree model is proposed by Scheier in 1999, it can be seen as an extension of the fault tree; its advantage is easy to understand, but the describe ability is very limited. A serial attack tree construction method is proposed by Luo et al. [16]; attack tree model greatly reduces the complexity of the attack. Attack graph model first proposed by Swilerin in1998 is the most widely used method at present. Sheyner uses model checking method to generate attack graph; based on graph theory, using attack as the center, Yun proposes a tool to generate attack graph. There is also literature focused on the large-scale construction and visualization of attack graphs [28]. Ma proposes a distributed parallel processing attack graph construction method, which can reduce the resource loss to a certain extent [19]. Early attack graph tends to be static attack graph construction [3], but it easily leads to the explosion of the state space. As the research goes deeper and deeper, the attack graph tends to be causal attack graph, in which the edges represent the connection between nodes or the logic relation of the atomic attack, the expansibility of causal attack graph is better than static attack graph and easier to apply to large scale network. At present, most researches do some improvements on the original model to enhance the description ability [14], or to merge with other disciplines to enhance the analysis ability [15,21].

Similar to attack graph, Dacier abstracts the node in the graph as the authority state, and proposes a privilege graph model [5]. Based on this, Ortalo establishes a Markov model and gives out the security evolution process of system [20], and then Dr. Wang refines this [26]. But privilege graph model is difficult to describe the dependency relationship among states or random events, so the subsequent expansion of this model has little impact on the results of the study.

For the first time, Kemmerer proposes the state transition graph, in which each node represents a temporary state of the system, and each edge represents state transition and transfer process, lots of models are extended based on this such as probabilistic model, semi Markov process model, etc. The advantage of the state graph is its description ability, but all of them must face the state space explosion problem, the existing solution to this challenge is still just passable [3, 28].

Attack graph (tree) model, Privilege graph model and State graph model are three classic models. Among them, the research on attack graph model is the most popular one, lots of scholars' research is about attack graph, one of the important directions is the combination with some advanced stochastic models, such as Petri net, game theory, Bayesian network, etc. But the improved model cannot eliminate the limitation of the typical model fundamentally, and there is no good way to solve the limitation of the large-scale network in the attack graph generation.

2.3. Establishment of safety evaluation index system

Formal model is an abstraction of the elements in the network. On the basis of this, to achieve the purpose of security evaluation and analysis of the network, it also needs to define and quantify the security indicators. In a sense, this is the detailed classification of the elements in the model, and also the precondition of safety evaluation. The research of network security index is mainly from two aspects, which are security attribute and attack behavior.

Research from the perspective of security attributes which originated from reliability, reliability or other classical concepts of the traditional industrial production system, is more focused on the definition and interpretation of network security, and trying to exhaust classification of network security attributes, giving out a clear meaning for each classification and the mathematical definition for each attribute. Chen and Shu have made an effective analysis of the relationship between the attributes [3]. Wang proposes an attack technology classification method, which can meet the Amoroso classification standard and has a certain improvement in accuracy [27]. Most of the papers have focused on one of the attributes of security, but the security of the network is clearly a combination of some or all of the attributes. The advantages of this method is that it can draw lessons from the existing theoretical deduction and mature application, but the existing indicators are too absolutely quantitative, and the actual meaning of each indicators are also to be researched.

Research from the perspective of attack behavior uses attack as the center, it classifies and quantify the important factors in the process of attack, so there is a strong relationship between the method of classification and the idea of model construction. According to the statistics and analysis of the existing papers, there are 3 elements (attack severity, probability of attack occurrence/attack success, attack gain) used in the most of model, and they basically formed a certain standard.

The precondition for quantification of attack severity is the qualitative classification of attack types; there are lots of ways to classify attacks. At present, the six-tuple representation method with strong practicability proposed by Christy is accepted by most people. Based on the qualitative classification method, quantification method divides the attacks into a number of grades and quantifies the severity of each grade. This method is generally associated with the IDS alarm mechanism and widely used in intrusion detection system. CVSS vulnerability evaluation mechanisms widely used in the attack model, which evaluates public vulnerability in three ways: basic evaluation criteria, life cycle assessment and environmental assessment, the final result of the operation is a 0-1 value, and the higher the score, the greater the threat of vulnerability.

The purpose of quantification for probability of attack occurrence/attack success is measuring the likelihood of the occurrence of an attack and the success of the attack. There are a lot of false and useless information during attack, information provided by the host and safety equipment is often imprecise, which bring great difficulties to the comprehensive estimate of the information fusion model. Now Expert's subjective probability estimation method is mainly used in each experimental model. Bias network can express the probability of uncertainty knowledge effectively, so the research based on Bias's estimation method has made some progress [13].

The quantification of attack gain is an important part in the evaluation of attack effects. Generally, the first step is to quantify destructive level of attack (such as: the Root privilege of a service is obtained through attack), then give out the quantitative value according to the qualitative classification. At present qualitative classification of atomic attacks is an important means of security analysis, but the quantify process is still the hotspot and difficulty of the research. The research can be carried out from two angles: the attacker and the defender. From the view of the attacker, it is the return of the attack at a certain attack cost and from the defender's; it is the loss of the system at a certain defense cost. Usually the attack gains are less than the loss of the network system, but for simplicity, most of the models use the defense losses as attack gains.

2.4. Model solving and security analysis

According to the summary of the first three analysis steps, the process of knowledge acquisition for building models has been able to achieve automation; the process of building model can be for the abstract of small scale experimental network basically; the qualitative classification and quantitative process of safety evaluation index can also be used in some special practical application; but in the final step, the model solving and security analysis is still in the true sense of the exploration phase. All models just give some suggestions under the assumed conditions, the horizontal comparison among the models is not significant, and there is no accepted systematic theory method.

Based on the quantification of security attributes, Strutt proposes a new evaluation method firstly, in which the risk is defined as the product of the attack probability and the quantification value of the vulnerability security, this kind method is more concerned with the formula calculation process based on the security indicators, and dependent slightly on the formal model [23]. Zhu gives out a hierarchical evaluation and calculation method [32]; Chen gives a model which can do real time assessment and online monitoring of immune detection [3]; the risk propagation algorithm proposed by Feng also has certain reference significance [7]; the attack intention analysis model proposed by Ma tries to get rid of the dependence on CVSS and fusion potential threat, whose result is more reasonable within the constraints [18]; Cheng proposes a polymerization method which can fuse the basic points of common vulnerability scoring system and then evaluate the security of the whole network [4].

Network integration analysis based on attack model is currently a hot research topic, and dozens of articles are found in key journals each year, such as analysis based on attack graph which is a more accurate method to calculate the reach ability of the attack [2,12,14,15,19]; Roschke intends to generate alarm dependency graph through the parallel framework and parallel implementation of the analysis process, if the loop problem is considered at the same time, it will have a further effect [22]; Albanese discusses the solution of optimal complement indemnity for property dependent attack graph [1]. Also, there has the paper focusing on multi-stage or multi-step attack [10], most of these analyses are around three aspects, which are Attack reach ability [14,16,24], Minimum attack cost [3] and Maximum attack gain [13,28]; Gao firstly uses the attack graph model in the analysis of the safety risk of the industrial control system, which is a practical example given for the application of the

attack graph model [8].

By the research on communication network or military, the survivability research of the network system will become the main direction, which intends to describe the ability of performing critical tasks under attack [3]. However, the survival analysis of the application system is not mature; the survivability evaluation of network security is still stuck in the theoretical definition and the qualitative definition. Wang proposes a framework for survivability analysis, but the description of the state transformation of each node limit the large-scale promotion [25]; the penetration test attack model can be used in the process of penetration testing and describe the stability of attack proposed by Luo [5]; the research of Zhou is helpful to detect recommended attack and then improve the robustness of the collaborative recommendation system and ensure the credibility of the system recommendation [29,30].

This section effectively summarizes the main steps of using attack model for network security analysis, the main functions and effects of each step and the research status and difficulty of each step, etc. The result shows that there are serious challenges to solve the current situation of network security, but using stochastic model to analyze is a very promising direction, there already are some effective results in knowledge acquisition, model building and index quantification.

3. Formal modeling

During network attack and defense, there must be some characteristics such as non-cooperation and strategy dependence and so on, so game theory has always been an important research direction of network security, most of the combination of game theory and IDS technology is one time game analysis. This paper pays more attention to the combination of game theory and active defense or situational awareness technology. Based on attack graph, a new defense graph model is proposed, in which the security evaluation and defense algorithm is given out based on the game theory at the same time [11], but the model cannot distinguish the difference between attack strategy and utility, and it is difficult to be applied to large scale complex networks. Based on the spread of vulnerability, Liang uses Markov game to analyze the quantitative relationship between the vulnerability and dynamic effects of behaviour selection on network security, which intends to find the greatest threat node or path to improve security, but there is also the problem of state space explosion and low efficiency [20]. After an effective summary of existing network attack and defense security evaluation model, Fu proposes an attack and defense game strategy model based on stochastic Petri net, the result of it has certain practicality, but it can only analyze the status of attack and defense at a certain moment [23]; Zhu demonstrates the existence and uniqueness of Nash equilibrium, points on the non-cooperative evolutionary game in the process of attack and defense [31], but the result of which is more concerned with the objective explanation of the phenomenon rather than the safety evaluation method. In summary, at present most of the studies on attack and defense game stay in the stage of technical improvement, which means the simple application of game analysis method in a formal model. Because of the lack in macro and depth discussion, the research work is limited to the traditional game research framework, it can only do research on the attack and defense strategy for static network at a certain time, however network attack and defense certainly is a process of multi-state transfer (such as the example in Figure2, at the initial time the attacker E has access privilege to node N_1 and N_7, A do some defense measures on N_4, the system switches to state S_1; in S_1A add defense on node N_5, but the defense failed, attacker expand his rights, system switches to state S_2; after a finite step of game, system reach state S_n). This requires the establishment of a new model based on the accurate description of the state transition.

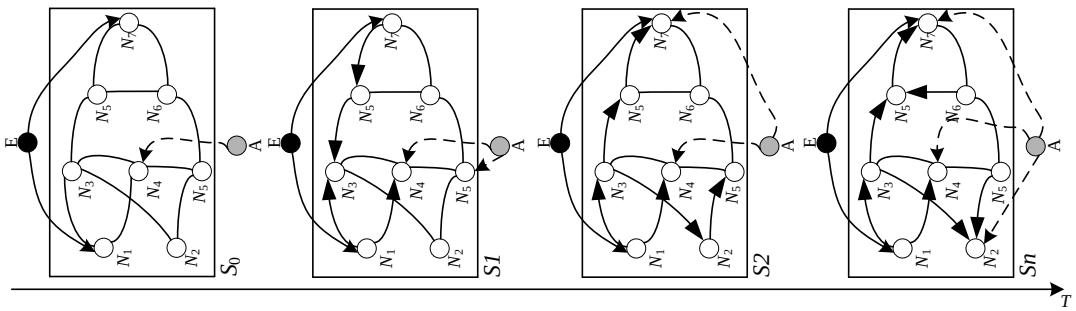


Figure 2. The example of Markov game progress in network attack and defense

3.1. Basic Definition

*Definition 1:*The independent computing device in the network system is called the network node, which is denoted as *v*; the applications, operating systems, services, etc. provided by network node *v* are called network component node, which is denoted as *M*, *M*=(*v*, s) represents a network node *v* provides a network component *S;* $A_\alpha : C \to 2^\alpha$ represents a list of properties owned by the network component *C*, $\alpha$is the collection of all attributes of the network component (both normal and vulnerable).

Definition 2: The relationship represents that a network component has access or connection relationship to another network component. M_l= (M_{xi}, M_{yj}, *l*) is a directed weighted link, which shows that the component *i* in network node *x* has relationship *l* on component *j* in network node *y*.

Definition 3: Attack network can be simplified to a directed weighted graph *G*(*C*,*E*),|*C*|=*n* shows the number of network components collection; *E* is a set of directed links, the weight *w* at the link represents the risk gain from component *i* to component *j* due to the presence of access connection relationship.

Definition 4: Markov evolutionary game model for dynamic network attacks safety analysis is a six-tuple *MG*= {*Q*, *S,R,P,T,Y*}, in which:

(1) *Q*= {1,2,…,*n*}is the collection of players, this paper only considers that there are only one attacker and one defender, which means |N|=2, if more than one attacker or defender, then merge them to one.

(2) *S*={S_1,S_2,…,S_k}is the collection of game state in the process of attack and defense, each state here is an attack graph in a certain time slice as defined in definition 3, the transformation between the state is caused by the change of access privilege or connection relation between different components.

(3) *R*= {R_A, R_{SD}}is the strategy of attacker and defender, |R_A|=*m* is the set of attack strategy, $R_k^{a_i}$ represents that the attacker use the i_{th} attack strategy in state S_k and $\sum_k \cup_{i=1}^{m} R_k^{a_i} = R_A$, |$R_D$|=*n* is the set of defense strategy, $R_k^{d_j}$ represents that the defender use the j_{th} defense strategy in state S_k and $\sum_k \cup_{j=1}^{n} R_k^{a_j} = R_D$.

(4) This paper divides the transition probability *P* into 3 types: $P(a_i|s_k)$(the occurrence probability of atomic attack a_i in state s_k), $P(s_k|a_i)$(the probability of atomic attack a_i success and transfer to the state s_k), $P(a_i|o_i)$(the defense probability that defender monitoring event o_i can prove an atomic attack a_i happened),so $P \to S \times P(a_i|s_k) \times P(s_k|a_i) \times P(a_i|o_i) \times S \in [0,1]$, various probability values in this paper refer to the empirical value method used by Chen [3]. In order to highlight the impact of attacks, "OR" is used for operation between two probabilities.

(5) $T_n = S_i \times R \times S_j \in (-\infty, +\infty)$represents the gain function of player *n* when it transfers from state S_i to state S_j, gain function is the gain value for attack or defense in each game stage. The calculation formula of gain function for attacker or defender can refer to the method used [11].

(6) *Y* is the criterion function, which is used to judge the strategy of attacker or defender. This paper uses the discounted expectation criterion function for definition: $Y(S,R) = T(S,R) + \lambda \sum_{S'} P(S,R,S')Y(S')$, which means that the criterion function is the sum of the current gains for both attack and defense ($T(S,R)$) and future discount gains ($\lambda \sum_{S'} P(S,R,S')Y(S')$), λ is the discount rate (because there is a great relationship between the gain and the attack step, here use λ represent the difference between the future gain value and the current gain value).

3.2. Solving Method

During the game progress between attacker and defender, suppose that every player will try his best to maximize his criterion function, for the model *MG*={*Q*,*S*,*R*,*P*,*T*,*Y*}, when in state S_k, the strategy for attacker and defender is $R_k^a = \{R_k^{a_1}, R_k^{a_2}, ..., R_k^{a_m}\}$ and $R_k^d = \{R_k^{d_1}, R_k^{d_2}, ..., R_k^{d_n}\}$ separately, then the definition and the necessary and sufficient condition of equilibrium strategy can be derived from the general matrix game, if $(R_k^{a^*}, R_k^{d^*})$ is the equilibrium strategy, then for each R_k^a, R_k^d should meet the formula below:

$$Y(R_k^a, R_k^{d^*}) \le Y(R_k^{a^*}, R_k^{d^*}) \le Y(R_k^{a^*}, R_k^d) \tag{1}$$

From the whole process of the game, the equilibrium strategy of *MG* is that each sub game has achieved the Markov strategy combination of Nash equilibrium, because the impact of the sub game is contained in the transformation state during the progress. If the opponent chooses Markov strategy, then the other player should have a corresponding optimal Markov strategy. So, if $R^* = \{R_0^*, R_1^*, ..., R_{N-1}^*\}$ is the equilibrium strategy of some player n in *MG* model defined in this paper, then for any time t the following formula is meet:

$$Y_t^{R^*}(n) = T_t(S_t, R_i^*(n)) + \sum_{j=1}^{S} \lambda_t P_t(S_t, R, S_j) Y_t^{R^*}(n_j) \tag{2}$$

If both the attacker and defender select their behaviour based on the requirement of equilibrium strategy, we can use the method in the proposed by Wang to predict the probability vector of the attacker and the defender, and then get the solving result of equilibrium strategy by Shapley algorithm [25]. But this kind of process is difficult, so the *MG* model is transformed into a nonlinear programming problem for solving in this paper.

Theorem: For a given Markov evolutionary game analysis model *MG*= {*Q*,*S*,*R*,*P*,*T*,*Y*}, if its Markov strategy is f^* and stable gain value is Y^*,then the necessary and sufficient condition for the conclusion that f^* and Y^* are the equilibrium strategy is that f^* and Y^* are the optimal values of the following nonlinear programming.

$$\begin{cases} \min \sum_{n\in Q}\sum_{S_k\in S}[Y_k^n - T_k^n(f) - \lambda\sum_{S_{k'}} P(S_k, f, S_{k'})] \\ Y_k^n \geq T_k^n(f) - \lambda\sum_{S_{k'}} Y_{k'}^n P(S_k, f, S_{k'}) \qquad \forall n \in N, \forall S_k \in S, \forall R_a \in R_k^{a_n} \\ \sum_{\forall R\in R_k^n} f_k^n(R) = 1 \qquad \forall n \in Q, \forall S_k \in S \\ f_k^n(R) \geq 0 \qquad \forall n \in Q, \forall S_k \in S, \forall R \in R_k^{a_n} \\ Y \in \{Y_k^n \mid n \in Q, S_k \in S\} \\ f \in \{f_k^n(R_a) \mid n \in Q, S_k \in S, R_a \in R_k^{a_n}\} \end{cases} \tag{3}$$

Proof: (1) Proof of necessity. The last two conditions in nonlinear programming is the description of the independent variables. Therefore, it is only necessary to prove the first three conditions and the optimal value. Supposing that on the condition that discount rate is λ, Markov strategy f^* and stable gain value Y^* are existed, due to the stability of the Markov strategy f^*, the 2th, 3th constraint conditions in nonlinear programming is naturally true.

Because in the equilibrium state, every player ($n \in N$) will follow the Markov decision-making process with a discount rate λ, so $\forall n \in N$, if the strategy f' of other players n' is determined, then the decision of player n is the maximum value strategy in Markov decision process, that is

$$\forall S_k \in S, \forall R_a \in R_k^n, Y_k^n \geq T_k^n(f) - \lambda\sum_{S_{k'}} Y_{k'}^n P(S_k, f, S_{k'}) \tag{4}$$

At the same time, if f is the optimal stable strategy for a single player, then

$$\forall S_k \in S, Y_k^n = T_k^n(f) - \lambda\sum_{S_{k'}} Y_{k'}^n P(S_k, f, S_{k'}) \tag{5}$$

According to Formula 1 and 2, the objective function value of nonlinear programming is 0, so (f^*,Y^*)is the optimal value of nonlinear programming.

(2) Proof of sufficient. Supposing that (f^*,U^*) is the optimal value of nonlinear programming, according to the above derivation process, the objective function value of the nonlinear programming is 0, under the constraint conditions, for each player n in game, the equilibrium strategy f^n and Y^*must meet the requirements of Formula 1 and 2. Therefore $\forall n \in N$, when the strategy of the other players is determined, strategy f^n must be the optimal strategy which meet the Markov process. Thus f^* is the equilibrium strategy of the model *MG*.

4. Application Example and analysis

4.1. Application and Verification

This research gives out a typical Web service application system, in which the accuracy of the proposed model and algorithm will be verified. Experimental network topology is shown in Figure3, Web Server is Apache server; SQL server provides database services for Apache, and provides RPC service for accessing by outside area, two host machines H1 and H2 in intranet security zone can run Email, Ftp and SSH program.

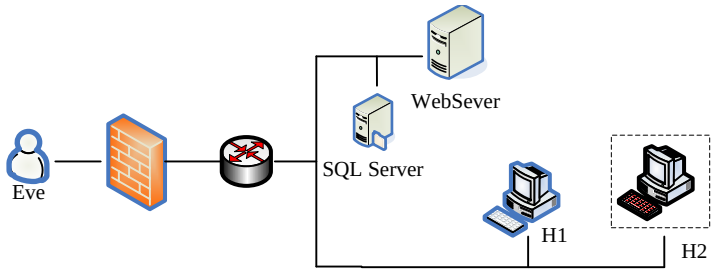
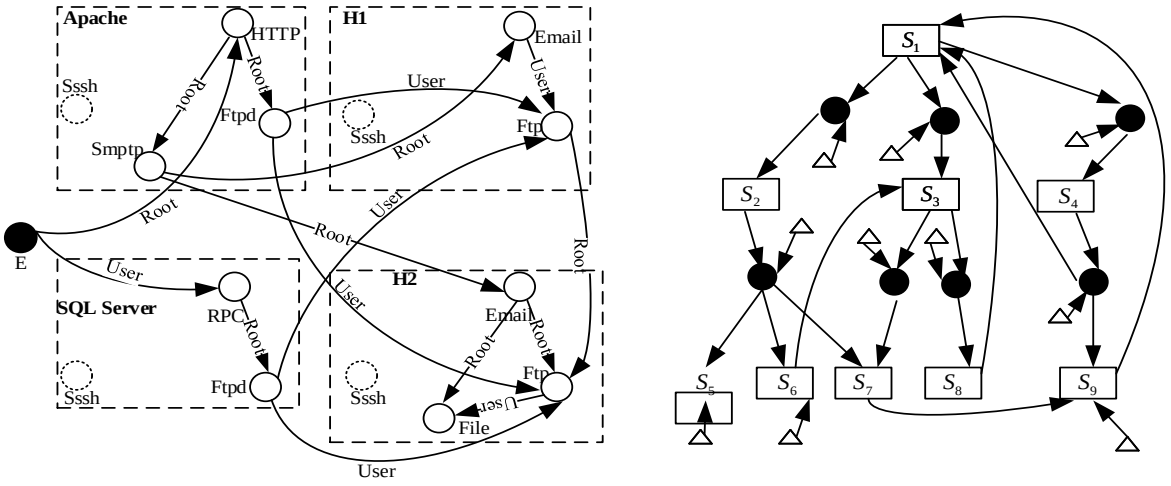


Figure 3. Topological graph of the experimental network

According to the pre-design isolation principle, the user in outside area can access any service on the Apache server and RPC services on SQL server. Apache server can access SQL server or any other working machine. SQL server can access any working machine, host H1 can access the Apache server and host H2 can access SQL server, besides that the working machine can be accessed from each other. The vulnerability information of each area obtained by the Nessus vulnerability scanner is shown in table 1.

Table 1. The vulnerability information in experimental network

Segment	Host	CVENumber	AC Value
Outside area	Apache	CVE-2011-3607	L
Outside area	Apache	CVE-2009-3095	L
Outside area	Apache	CVE-2002-0682	H
Isolation area	SQL Server	CVE-2008-4250	M
Isolation area	SQL Server	CVE-2005-2558	H
Isolation area	H1、H2	CVE-2011-0203	M
Isolation area	H1、H2	CVE-2008-0110	L
Isolation area	H1、H2	CVE-2010-0816	H



(a) The initial state of the experimental network system(S_1) (b) State transition graph of experimental network

Figure 4. State transition graph of experimental network access privilege

In this research, the attack graph is refined to the component level. Here in the experimental network, the connection relation between the component nodes is ignored, and the access privilege between the different components is mainly

considered. In the initial state (normal state S_1), the initial access privilege of the experimental network is shown in Figure4 (a). In this experiment, the set of state S={S_1(normal state), S_2(get Root privilege by attacking Apache), S_3(get User privilege by attacking Apache), S_4(get Access privilege by attacking Apache), S_5(get User privilege of File by attacking SQL Server), S_6(get User privilege by attacking SQL Server), S_7(attack the FTP component on working host),S_8(attack the Outlook component on working host), S_9(get the Root privilege by attacking working host)}, the transition between states is shown in Figure4(b) (The black dot between transfer state represents attack process, triangle symbol represents defense process). This paper uses the expert experience method proposed by Chen to determine the transition probabilities between states, results showed in the following table 2(where $P(S_i, \theta_i^{a_m}, \theta_i^{d_n}, S_j)$ represents the probability from state i transfer to state j when the attacker use attack strategy m and the defender use the strategy n).

Table 2. State transfer probability of the experimental network

P(1,1,3,2)=0.9	*P(1,2,2,3)=0.5*	*P(1,3,2,3)=0.2*	*P(2,1,1,5)=0.6*	*P(2,1,2,6)=0.3*
P(3,1,1,7)=0.1	*P(3,2,1,8)=0.6*	*P(4,1,1,1)=0.5*	*P(4,1,1,9)=0.1*	*P(5,1,1,1)=0.3*
P(2,2,2,7)=0.4	*P(7,3,3,9)=0.1*	*P(1,3,2,1)=0.1*	*P(9,3,1,1)=0.1*	*P(6,2,3,3)=0.3*

The attack and defense strategy sets of the experimental network are shown in table 3.The loss of the system is used as attacker gain. Combined with quantitative ideas in network attack and defense [7], we can get the gain matrix of both attack and defense in each state for the experimental network, as shown in figure 6.

Table 3. The attack and defense strategy for each state in experimental network

S_1	S_2	S_3
R^a={Privilege promotion attack, Remote command injection attack, Evasion information abnormal attack}	R^a={RPC buffer overflow attack, Function buffer overflow, No attack}	R^a={FTP director traversal attack, Outlook URI attack, No attack}
R^d={Patch upgrade, Close service, No response}	R^d={Patch upgrade, Close service, No response}	R^d={Patch upgrade, Close service, No response}
S_4	S_5	S_6
R^a={Response integer overflow attack, No attack, No attack}	R^a={Data acquisition, Failure data, No attack}	R^a={Crack password, No attack, Delete data}
R^d={Patch upgrade, Close service, No response}	R^d={Patch upgrade, Close service, No response}	R^d={Patch upgrade, Close service, No response}
S_7	S_8	S_9
R^a={Data acquisition, Mail attack, No attack}	R^a={Data acquisition, No attack, No attack }	R^a={Steal data, No attack, No attack}
R^d={Delete data, Close service, No attack}	R^d={Delete data, Mounting antisniffer device, No response}	R^d={Delete data, Mounting antisniffer device, No response}

$$
\begin{pmatrix} & R_1^{d_1} & R_1^{d_2} & R_1^{d_3} \\ R_1^{a_1} & 70 & 85 & 90 \\ R_1^{a_2} & 45 & 60 & 50 \\ R_1^{a_3} & 10 & 20 & 15 \end{pmatrix}
\begin{pmatrix} & R_2^{d_1} & R_2^{d_2} & R_2^{d_3} \\ R_2^{a_1} & 20 & 30 & 15 \\ R_2^{a_2} & 15 & 20 & 10 \\ R_2^{a_3} & 0 & 30 & 0 \end{pmatrix}
\begin{pmatrix} & R_3^{d_1} & R_3^{d_2} & R_3^{d_3} \\ R_3^{a_1} & 5 & 8 & 5 \\ R_3^{a_2} & 5 & 8 & 5 \\ R_3^{a_3} & 0 & 8 & 0 \end{pmatrix}
$$

$$
\begin{pmatrix} & R_4^{d_1} & R_4^{d_2} & R_4^{d_3} \\ R_4^{a_1} & 5 & 5 & 5 \\ R_4^{a_2} & 0 & 0 & 0 \\ R_4^{a_3} & 0 & 0 & 0 \end{pmatrix}
\begin{pmatrix} & R_5^{d_1} & R_5^{d_2} & R_5^{d_3} \\ R_5^{a_1} & 20 & 25 & 20 \\ R_5^{a_2} & 35 & 35 & 30 \\ R_5^{a_3} & 0 & -10 & 0 \end{pmatrix}
\begin{pmatrix} & R_6^{d_1} & R_6^{d_2} & R_6^{d_3} \\ R_6^{a_1} & 70 & 95 & 80 \\ R_6^{a_2} & 0 & -25 & 0 \\ R_6^{a_3} & -10 & -20 & 0 \end{pmatrix}
\tag{6}
$$

$$
\begin{pmatrix} & R_7^{d_1} & R_7^{d_2} & R_8^{d_3} \\ R_7^{a_1} & 10 & 15 & 10 \\ R_7^{a_2} & 5 & 5 & 5 \\ R_7^{a_3} & 5 & 0 & 0 \end{pmatrix}
\begin{pmatrix} & R_8^{d_1} & R_8^{d_2} & R_8^{d_3} \\ R_8^{a_1} & 5 & 5 & 5 \\ R_8^{a_2} & 0 & 0 & 0 \\ R_8^{a_3} & 0 & -20 & 0 \end{pmatrix}
\begin{pmatrix} & R_9^{d_1} & R_9^{d_2} & R_9^{d_3} \\ R_9^{a_1} & 10 & 5 & 8 \\ R_9^{a_2} & 0 & 0 & 0 \\ R_9^{a_3} & 0 & -15 & \end{pmatrix}
$$

According to the solving method for M model in section 3.2, it can be transformed into a nonlinear programming (λ=0.7), as shown in Figure 7. For the nonlinear programming, the equilibrium strategy of each state can be achieved by MATLAB or other tools easily. The result is shown in table 4.

$$
\begin{cases}
\min\{[y_1-(70R_1^{a_1}R_1^{d_1}+85R_1^{a_1}R_1^{d_2}+90R_1^{a_1}R_1^{d_3}+45R_1^{a_2}R_1^{d_1}+60R_1^{a_2}R_1^{d_2}+50R_1^{a_2}R_1^{d_3}+10R_1^{a_3}R_1^{d_1}+20R_1^{a_3}R_1^{d_2}+15R_1^{a_3}R_1^{d_3}]-0.7(0.9y_2+0.5y_3+0.2y_4)] \\
[y_2-(20R_2^{a_1}R_2^{d_1}+30R_2^{a_1}R_2^{d_2}+15R_2^{a_1}R_2^{d_3}+15R_2^{a_2}R_2^{d_1}+20R_2^{a_2}R_2^{d_2}+10R_2^{a_2}R_2^{d_3}+30R_2^{a_3}R_2^{d_2})-0.7(0.6y_5+0.3y_6+0.4y_7)] \\
[y_3-(5R_3^{a_1}R_3^{d_1}+8R_3^{a_1}R_3^{d_2}+5R_3^{a_1}R_3^{d_3}+5R_3^{a_2}R_3^{d_1}+8R_3^{a_2}R_3^{d_2}+5R_3^{a_2}R_3^{d_3}+8R_3^{a_3}R_3^{d_2})-0.7(0.1y_7+0.6y_8)] \\
[y_4-(5R_4^{a_1}R_4^{d_1}+5R_4^{a_1}R_4^{d_2}+5R_4^{a_1}R_4^{d_3})-0.7(0.5y_1+0.1y_9)] \\
[y_5-(20R_5^{a_1}R_5^{d_1}+25R_5^{a_1}R_5^{d_2}+20R_5^{a_1}R_5^{d_3}+35R_5^{a_2}R_5^{d_1}+35R_5^{a_2}R_5^{d_2}+30R_5^{a_2}R_5^{d_3}+10R_5^{a_3}R_5^{d_2})-0.7(0.3y_1)] \\
[y_6-(70R_6^{a_1}R_6^{d_1}+95R_6^{a_1}R_6^{d_2}+80R_6^{a_1}R_6^{d_3}-25R_6^{a_2}R_6^{d_2}-20R_6^{a_3}R_6^{d_2})-0.7(0.3y_3)] \\
[y_7-(10R_7^{a_1}R_7^{d_1}+15R_7^{a_1}R_7^{d_2}+10R_7^{a_1}R_7^{d_3}+5R_7^{a_2}R_7^{d_1}+5R_7^{a_2}R_7^{d_2}+5R_7^{a_2}R_7^{d_3}+5R_7^{a_1}R_7^{d_1})-0.7(0.1y_9)] \\
[y_8-(5R_8^{a_1}R_8^{d_1}+5R_8^{a_1}R_8^{d_2}+5R_8^{a_1}R_8^{d_3}-20R_8^{a_2}R_8^{d_2})-0.7(0.1y_1)] \\
[y_9-(10R_9^{a_1}R_9^{d_1}+5R_9^{a_1}R_9^{d_2}+8R_9^{a_1}R_9^{d_3}-15R_9^{a_2}R_9^{d_2})-0.7(0.1y_1)]\} \\
y_1-(70R_1^{d_1}+85R_1^{d_2}+90R_1^{d_3})-0.7(0.9y_2)\ge 0 \\
y_1-(45R_1^{d_1}+60R_1^{d_2}+50R_1^{d_3})-0.7(0.5y_3)\ge 0 \\
y_1-(10R_1^{d_1}+20R_1^{d_2}+15R_1^{d_3})-0.7(0.2y_4)\ge 0 \\
y_2-(20R_2^{d_1}+R_2^{d_2}+15R_2^{d_3})-0.7(0.6y_5)\ge 0 \\
y_2-(15R_2^{d_1}+20R_2^{d_2}+10R_2^{d_3}+30R_2^{d_2})-0.7(0.3y_6)\ge 0 \\
y_3-(5R_3^{d_1}+8R_3^{d_2}+5R_3^{d_3}+5R_3^{d_1}+8R_3^{d_2}+5R_3^{d_3})-0.7(0.1y_7+0.6y_8)\ge 0 \\
y_4-(5R_4^{d_1}+5R_4^{d_2}+5R_4^{d_3})-0.7(0.5y_1+0.1y_9)\ge 0 \\
y_5-(20R_5^{d_1}+25R_5^{d_2}+20R_5^{d_3})-0.7(0.3y_1)\ge 0 \\
y_6-(70R_6^{d_1}+95R_6^{d_2}+80R_6^{d_3}+25R_6^{d_2}+20R_6^{d_2})-0.7(0.3y_3)\ge 0 \\
y_7-(10R_7^{d_1}+15R_7^{d_2}+10R_7^{d_3})-0.7(0.7y_9)\ge 0 \\
y_8-(5R_8^{d_1}+5R_8^{d_2}+5R_8^{d_3})-0.7(0.1y_1)\ge 0 \\
y_8-(20R_8^{d_2})-0.7(0.1y_9)\ge 0 \\
y_9-(10R_9^{d_1}+5R_9^{d_2}+8R_9^{d_3}-15R_9^{d_2})-0.7(0.1y_1)\ge 0 \\
\sum_{i=1}^{3}R_k^{a_i}=1,\sum_{j=1}^{3}R_k^{d_j}=1 \\
R_k^{a_i}\ge 0, i=1,2,3;\ \ R_k^{d_j}\ge 0,\ j=1,2,3
\end{cases}
\tag{7}
$$

Table 4. The result of evolutionary game for experimental network

State	Attack strategy	Defense strategy	Attack gain	Defense gain
S_1	[0.65,0.35,0]	[1,0,0]	3215.8	-356.1
S_2	[0.3,0.3,0.4]	[0.9,0.03,0.07]	189	-654
S_3	[0.45,0.35,0.2]	[0.33,0.33,0.33]	125	-231.8
S_4	[1,0,0]	[1,0,0]	100	-100
S_5	[0.55,0.45,0]	[0.34,0.34,0.33]	480.1	-405.6
S_6	[0.25,0,0.75]	[0.43,0.46,0.01]	20	-60
S_7	[0.5,0.5,0]	[0.33,0.33,0.34]	215.8	-222
S_8	[1,0,0]	[0,1,0]	87	-37
S_9	[1,0,0]	[0,1,0]	58	-65

4.2. Result Analysis

Analysis (1): attack path analysis. Suppose that the target of attacker is the file data on the host H2, if the attacker gets the access privilege of target file, then the attack finish. From the analysis of the upper section we can know there are two attack paths: (a) $\{R_1^a, R_1^d\},\{\{R_2^a, R_3^a\},\{R_2^d, R_3^d\}\},\{\{R_5^a, R_6^a, R_7^a, R_8^a\},\{R_5^d, R_6^d, R_7^d, R_8^d\}\}$, that is E launches an attack from vulnerability on Apache component, then get the User privilege of SQL Server, finally achieves the purpose of attack through the vulnerability of the host node; (b) $\{R_1^{a_3}, R_1^d\},\{R_4^a, R_4^d\},\{R_9^a, R_9^d\}$. That is, the attacker get the User privilege of the component by the abnormal attacks on Apache, and then get the Access privilege of the file by the vulnerability on FTP component in the same way.

Analysis(2): analysis of attack and defense strategy selection. For the attack path (b), through the game analysis resulting on the state S_1, we can know that the probability on Apache exception attacks is 0($P(R_1^{a_3})$=0), so don't pay too much attention

to this path. For the attack path (a), according to the results of game analysis in table 5, in state S_1, the probability of both ($R_1^{a_1}$ =privilege promotion attack) and ($R_1^{a_2}$ =remote command injection attack) are very large, the defender will choose the 1th strategy ($R_1^{d_1}$ =patch upgrade), because $P(R_1^{d_1})$=1, but the defense gain is very low. Attacks on Server SQL are sample and common, and the possibility to choose various attack methods are similar, but the defense gain is very high. In the final step, the gain and chosen probabilities for each attack method on host nodes has little difference, so it can be concluded that the defense should focus on the patch upgrade on database server in intranet security zone, rather than on the Apache server as the analysis showed before.

5. Conclusions

The main contributions of this paper are: (i) Refine the description node in the attack graph to the component level, which makes description ability of the model more accurate and breaks through the limit of the static analysis and evaluation when using the traditional attack graph for analysis. Fusing component attack graph and Markov game, this paper proposes a new Markov evolutionary game security analysis model with multi-state and multi-agent, which can carry out a very good characterization on dynamic evolution mechanism, such as the mind for both attack and defense, non-cooperative and stochastic etc. in the process. (ii) For the probability of single step attack/detection, an operable calculation method is given out, based on the attack and defense gain function and the discounted expectation criterion function, this paper defines the objective function for the Markov evolutionary game security analysis model. Besides on the definition of equilibrium strategy, it is proved that the model must have Nash equilibrium under the mixed strategy. (iii) In order to simplify the solving method of the proposed model, an equivalent nonlinear programming method is given out after the rigorous theoretical proof. The detailed example and simulation progress shows the basic application progress of the model and the result of balanced strategy for both attack and defense; the result shows that the model is effective.

The successful application of the complex dynamic network theory to the network attack graph analysis model is one of the directions that the author has been working on, further research directions include: how to get the effective defense scheme according to game results, construct the data set which is suitable for large-scale network risk assessment analysis, and verify the rationality and validity of the model proposed in this paper further.

Acknowledgements

This work was supported by the Science and technology research plan of Ministry of Housing and Urban-Rural Development of the People's Republic of China under Grant No. R12016026L; the social sciences of Shaanxi Province under Grant No. 2015R006; The Science and technology plan of Xian under Grant No. 2016041SF/RK04(5).

References

1. M. Albanese, S. Jajodia and S. Noel, "Time-efficient and cost-effective network hardening using attack graphs", in *IEEE/IFIP International Conference on Dependable Systems and Networks*, pp.1-12, 2012.
2. X. J. Chen, B. X. Fang, Q. F. Tan and H. L. Zhang, "Inferring attack intent of malicious insider based on probabilistic attack graph model", *Chinese Journal of Computers*, vol. 37, no.1, pp.62-72, 2014.
3. Y. Y. Chen and H. C. Shu, "The algorithm model for cumulative vulnerability risk assessment", *International Journal of Internet Protocol Technology*, vol. 8, no. 2, pp.150-157, 2014.
4. P. Cheng, L. Wang, S. Jajodia and A. Singhal, "Aggregating CVSS Base Scores for Semantics-Rich Network Security Metrics", *Reliable Distributed Systems*, vol.90, no.1, pp.31-40, 2012.
5. M. Dacier. "Towards quantitative evaluation of computer security", Ph. D. dissertation of Institute National Polytechniquede Toulouse, France, 1994.
6. N. Feng, H. J. Wang and M. Li, "A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis", *Information Sciences*, vol. 256, no. 1, pp.57-73, 2014.
7. X. Feng, D. Wang, M. Huang and J. Li, "A mining approach for causal knowledge in alert correlating based on the Markova property", *Journal of Computer Research & Development*, vol. 51, no. 11, pp.2493-2504, 2014.
8. L. Gao, J. Yang and G. Qin, "Methods for pattern mining in dynamic networks and applications", *Journal of Software*, vol. 24, no. 9, pp.2042-2061, 2013.
9. L. L. Hou, S. Y. Lao, Y. D. Xiao and B. Liang, "Recent progress in controllability of complex network", *Acta Physical Sinica*, vol. 64, no. 18, pp.188901-188901, 2015.
10. L. Hu, N. N. Xie, Nurbol, Z. Y. Liu and S. Chai, "A multi-stage attack scenario recognition algorithm based on intelligent planning", *Acta Electronica Sinica*, vol. 41, no. 9, pp.1753-1759, 2013.
11. W. Jiang, B. X. Fang, H. L. Zhang, "Evaluating Network Security and Optimal Active Defense Based on Attack-Defense Game Model", *Chinese Journal of Computers*, vol. 4, no. 1, pp. 817-827, 2009.

12. M. Keramati, A. Akbari, & M. Keramati, "CVSS-based security metrics for quantitative analysis of attack graphs", in *Proc. of International Conference on Computer and Knowledge Engineering*, pp.178-183, 2013.
13. Z. Y. Li, J. S. Wang, Y. Q. Xu and Y. M. Wang, "Complex network attack effect based on dynamic Bayesian network", *Journal of Nanjing university of Posts and Telecommunications (Natural Science Edition)*, vol.35, no.5, pp.67-73, 2015.
14. W. X. Liu, K. F. Zheng, Y. Hu and B. Wu, "Approach of goal-oriented attack graph-based threat evaluation for network security", *Journal of Beijing University of Posts & Telecommunications*, vol. 38, no. 1, pp.82-86, 2015.
15. W. X. Liu, K. F. Zeng and B. Wu, "Alert processing based on attack graph and multi-source analyzing", *Journal of Communications*, vol. 31, no. 9, pp.135-144, 2015.
16. S. L. Luo, L. Zhang, L. Guo, G. L. Yan, Z. Liu and Y. P. Zhao, "An original effective method for modeling the attack tree", *Transactions of Beijing Institute of Technology*, vol. 33, no. 5, pp.500-504, 2013.
17. Z. Y. Luo, B. You, J. Z. Xu and Y. Liang, "Automatic recognition model of intrusive intention based on three layers attack graph", *Journal of Jilin University*, vol. 44, no. 5, pp.1392-1397, 2014.
18. C. Ma, C. Wang, D. Zhang, & Y. Li, "A dynamic network risk assessment model based on attacker's inclination", *Journal of Computer Research & Development*, vol. 52, no. 9, pp.2056-2068, 2015.
19. J. C. Ma, J. Y. Sun, Y. J. Wang, B. K. Zhao, & S. Chen, "Study of attack graph construction based on distributed parallel processing", *Acta Armamentarii*, vol. 33, no. 1, pp.109-115, 2012.
20. R. Ortalo, Y. Deswarte, M. Ka âniche, "Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security", *IEEE Transactions on Software Engineering*, vol. 25, no. 5, pp. 633-650, 1999.
21. N. Poolsappasit, R. Dewri and I. Ray, "Dynamic security risk management using Bayesian attack graphs", *IEEE Transactions on Dependable & Secure Computing*, vol. 9, no. 1, pp.61-74, 2011.
22. S. Roschke, F. Cheng and C. Meinel, "High-quality attack graph-based ids correlation", *Logic Journal of IGPL*, vol. 21, no. 4, pp.571-591, 2013.
23. J. E. Strutt, J. D. Patrick and N. D. E. Custance, "A risk assessment methodology for security advisors", in *Proc. of International Carnahan Conference on Security Technology*, pp. 225-229, 1995.
24. Z. H. Tian, Y. U. Xiang-Zhan, H. L. Zhang, & B. X. Fang, "A real-time network intrusion forensics method based on evidence reasoning network", *Chinese Journal of Computers*, vol. 37, no. 5, pp.1184-1194, 2014.
25. C., Wang Q. Miao, & Y. Dai, "Network survivability analysis based on stochastic game model", *Multimedia Information Networking and Security*, vol. 48, no. 11, pp.99-104, 2012.
26. L. D. Wang, "A quantitative computer system and network security risk assessment method", Ph. D. dissertation of Harbin Institute of Technology, 2002.
27. X. Wang, B. Sun, Y. Liao, & C. Xiang, "Computer network vulnerability assessment based on Bayesian attribute network", *Journal of Beijing University of Posts and Telecommunications*, vol. 38, no. 4, pp.110-116, 2015.
28. Y. Yun, X. Xu, Z. Qi, & X. Wu, "Attack graph generation algorithm for large-scale network system", *Journal of Computer Research & Development*, vol. 50, no.10, pp.2133-2139, 2013.
29. Q. Q. Zhou, F. Z. Zhang, W. Y. Liu, "Detecting unknown recommendation attacks based on bionic pattern recognition", *Ruan Jian XueBao/Journal of Software*, vol. 25, no. 11, pp.2652−2665, 2014.
30. Q. Zhou and F. Zhang, "Ensemble approach for detecting user profile attacks based on bionic pattern recognition", *Journal of Computer Research & Development*, vol. 51, no. 4, pp.789-801, 2014.
31. J. M. Zhu, B. Song and Q. F. Huang, "Evolution game model of offense-defense for network security based on system dynamics", *Journal on Communications*, vol. 35, no. 1, pp.54-61, 2014.
32. L. N. Zhu, Z. C. Zhang and L. Feng "Research on hierarchical network security threat situation assessment", *Application Research of Computers*, vol. 28, no. 11, pp.4303-4302, 2012.

Weicheng Yan is a Ph.D. candidate from the School of Management, Xi'an University of Architecture & Technology, Xi'an, China. His research interests include network security, system engineering, etc.

Lingyan Li graduated from the School of Management, Xi'an University of Architecture & Technology, for the degree of Bachelor, Master and Ph. D. She visited the University of Florida in the U.S.A. as a visiting scholar from 2013 to 2014. Now she is an associate professor and Master supervisor in Xi'an University of Architecture & Technology. Her current research interests include network security, complex system modeling, etc.