# Attack Probability Controllability Analysis Model Based on Attack Graph

Yan Li, Chunzi Wang, Jingfeng Shao, Bin Zhang

***Abstract*—**How to improve the accuracy of network security evaluation and promote its practicability under large-scale network is the focus of the research in the field of network security. This paper detailed summary the research status and progress in network security situational awareness. After that, provides a new model which refines the attack graph node to component level and describes the interaction process between the components in the attack step in the form of a directed weighted graph to improve coarse grain size and limitations of the current attack graph; At the same time, Through mathematical calculation, come out the standard condition of probability controllability or partial probability controllability for complex attack network, and proved the relationship between the probability controllability and the traditional controllability, besides give out the concrete method for controlling network and defense node selection; The analysis results and the examples show that, if valid defense existed, the complex networks can still provide normal service function in the case of attack and damage, the method proposed in this paper can greatly improve the precision of network security defense.

***Keywords*—**attack graph, probability controllability, complex network, network security, vulnerability analysis.

## I. INTRODUCTION

In the context of the information revolution, broadband network has become a strategic public infrastructure of national economic and social development, with the popularization of internet application, the operation mode of the current world has changed radically, but the various types of network security incidents also began to see in the newspaper frequency, the "Prism plan" happened in June 2013 makes the information security issues from the economic benefits driven mainly to the national security level. At present, the overall network defense capabilities against the risk of national organizations attack is still relatively weak [1]. How to prevent the organized malicious network attacks has become a hot research topic in the security field, and it has become a difficult problem in the new century with the nuclear issue together.

At the beginning, the hotspot for Network security problems is how to establish 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[2], malicious intrusion must exist in the reality, so that people began to think about building a safety assistant system (for example: IDS system), the basic goal is to detect and take appropriate measures when the intrusion occurs, since the technical report of Anderson in1980[3], intrusion detection has a great development, but in general it can be divided into anomaly detection and misuse detection[4], intrusion detection model is the earliest proposed by Dorothy Denning[5], current development is remains of little refinement in this foundation, which can be regarded as the second phase of the study 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 attacks such as covert attacks which is bypass the firewall, multi-step attacks, etc. Under the situation of the increasingly serious network attacks, IDS is very difficult to guarantee real-time detection and alarm, so the focus of research turn to the active analysis from passive defense, the concept proposal marks the beginning of the third stage, such as vulnerability risk assessment model [6], situational awareness model [7], etc. which 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 in in the form of particular language, the present work focuses on the attack graph model[8]; analysis method construction includes two species: qualitative analysis and quantitative analysis, the focus of qualitative analysis is logical association problem among vulnerabilities, which usually gets all the possible attack path through visual analysis of attack scenarios[9]. The quantitative analysis generally quantify

This work was supported in part by The Fund Project for Science and technology research and development plan of Shaanxi Province under Grant No. 2013K1117; Xi'an Polytechnic University doctoral research start-up fund

Yan Li is with the School of Management, Xi'an Polytechnic University, xi'an 710048, Shaanxi, China (corresponding author; e-mail: 233381112@qq.com).

Chunzi Wang is with the School of Management, Xi'an Polytechnic University, xi'an 710048, Shaanxi, China.

Jingfeng Shao is with the School of Management, Xi'an Polytechnic University, xi'an 710048, Shaanxi, China.

Bin Zhang is with the School of Management, Xi'an University of Architecture & Technology, xi'an 710048, Shaanxi, China.

some factors with the process of model construction, which describe the security situation of the network in the digital calculation method [10]. But most of the models are still an experimental behavior in the small scale of network; there are lots of steps to meet the security analysis requirements for complex network, such as the description of attack intention and large-scale system applications, and so on. Therefore, Combine with complexity science such as dynamic network [11], control theory [12], etc. should make a great development in this field.

Based on the component attack graph, this paper proposes an analytical framework for probabilistic controllability of complex networks via attacks. The main contributions are: (1) to refine and improve the description ability of attack graph model; (2) the criterion condition of probability control of complex network via attacks, and demonstrate the relationship between probability controllability and traditional structure controllability; (3) it is proved that the network can have anti attack ability under the limited defense.

## II. RELATED RESEARCH

With the deepening of the research on computer network security, it has integrated multi discipline. Formal model analysis methods have been widely used in the evaluation process of various systems [6, 13], the active network security analysis framework (such as attack model, vulnerability assessment etc.) is different from the passive detection technology (such as IDS, firewall, virus detection, etc.), its purpose is not eliminate the vulnerability, but guide the network administrator to find a effectively balance point between "safe" and "function" before the attack. 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 [6]. According to the analysis of the existing literature, the network security evaluation mainly includes the following four steps.


Fig 1 Main steps of network security evaluation

(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, such as host based scanning tool COPS[14], network based scanning tool Nessus[15], etc.. A list of vulnerabilities or a brief report clearly cannot solve the vulnerability associated problems, with the development of research and in-depth analysis, the information collection objects gradually increased, network topology, key assets, services, and other related knowledge have been incorporated into the scope of the acquisition[10,18,20]. 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, so far has basically achieved automation [16], In recent three years, there are few studies on this aspect, most of the articles get the required information with automated tools[10,16,19].

(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 rule 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 then to the regular expression, after that match the rule and the target system one by one to safety analysis, this approach can be said to be a continuation of the work of vulnerability scanning [17] or application of intrusion detection in active safety analysis [18-20], naturally, there are similar defects, the generating process of the rule becomes the restriction point, the collation of the vulnerability rules can only be carried out locally, which is not suitable for the overall detection of the network, currently mature network security scanning tools are most based on the rules [21-22], the accumulation of these rules is also the basis of the abstract model analysis method (like the rule description of the atomic attack in the attack graph [8,28]). Current research is transforming to the abstract model analysis method[6,22].

Attack tree model is proposed by Scheier [23] in 1999, it can be seen as an extension of the fault tree, its advantage is intuitive and easy to understand, but the describe ability is very limited, A serial attack tree construction method is proposed in paper [24], which greatly reduces the complexity of the attack. Attack graph model first proposed by Swiler in 1998 [8] is the most widely used method at present, Sheyner[25] uses model checking method to generate attack graph; Based on graph theory, Ammann [26] uses forward search method to generate attack graph from initial state; Use attack as the center, paper [27] propose a tool to generate attack graph. There is also paper focused on the large-scale construction and visualization of attack graphs presented [28,40]; paper [29] proposed a distributed parallel processing attack graph construction method, which can reduce the resource loss to a certain extent; Early attack graph tends to state attack graph construction [8,10,25-27], but easily lead to the explosion of the state space, As the research goes deeper and deeper, the attack graph tends to causal attack graph[30], 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 and more easy application for large scale network, At present most research are improvements to the original model in order to enhance the describe ability [31], or to merge with other disciplines to enhance the analyze ability [32-33].

Similar to attack graph, Dacier[34] abstract the node in the graph as the authority state, and propose the privilege graph model, based on this, Ortalo[35] establishes a Markov model and give out the security evolution process of system, Dr. Wang Lidong [33] refines this. 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[37] proposed a 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 model are extended based on this such as probabilistic model[38], semi Markov process model[39] etc.. The advantage of the state graph is its describe ability, but all of them must face the state space explosion problem, already existing solution to this challenge[10,40] are still just passable.

Attack graph (tree) model, Privilege graph model and State diagram model are three classic models, among them, the research on attack graph model is the most popular one, lots of scholars research is for attack graph, one of the important directions is the combination of some advanced stochastic models, Such as: Petri net[41-42], game theory[43-44], Bayesian network[45-47] 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.

(3)Establishment of safety evaluation index system

Formal model is an abstraction of the elements in the network, on this 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. To some extent, this is the detailed classification of the elements in the model, and also the premise 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, Originated from the traditional industrial production of reliability, reliability and other concepts, it is more focused on the definition and interpretation of network security, try to exhaustive classification of network security attributes, gives out a clear meaning for each classification and gives out the mathematical definition for each attribute. Lin[6] has made an effective analysis of the relationship between the attributes. Wang[51] propose an attack technology classification method which can meet the Amoroso classification standard, and has a certain improvement in accuracy. Most of the papers has 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 can draw lessons from the existing theoretical deduction and mature application, but the existing indicators are too absolute quantification, the actual meaning of each indicators are also to be a research.

Research from the perspective of attack behavior, use attack as the center, and quantitative classification 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 used almost in most of the model analysis and basically formed a certain standard or standard, they are attack severity, probability of attack occurrence \probability of attack success, attack gain.

The premise for quantification of attack severity is the qualitative classification of attack types, there are lots of ways for classification of attacks, at present, the one that accepted by most people and with strong practicability is the six tuple representation method proposed by Christy[48], on the basis of qualitative classification method, which divides the attacks into a number of grades and quantify the severity of the threat[50,55]. This method is generally associated with the IDS alarm mechanism and widely used in intrusion detection system; CVSS vulnerability evaluation mechanism [43,49] is widely used in the attack model, which evaluates every 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, the higher the score, the greater the threat of vulnerability.

The purpose of attack occurrence/successful probability quantization is measures the likelihood of the occurrence of an attack and the success of the attack. There are a lot of false and useless information in the progress of network 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[10,13,43,44] 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[45-46] has made some progress.

The quantification of attack gain is an important component in the evaluation of attack effects, generally the first step is qualitative destructive level of attack (such as: the Root privilege of a service is obtained through attack[8-9]), and then according to the qualitative classification, gives out the quantitative value. At present qualitative classification of atomic attacks is an important means of security analysis, but the quantify process is the hotspot and difficulty of the research. the research can be carried out from two angles of the attacker and the defender, from the point of view of the attacker it is the return of the attack at a certain attack cost, from the defender 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, for simplicity, most of the models use the defense losses as attack gains [50].

(4)Model solving and security analysis.

According to the summary analysis of the first 3 steps, the process of knowledge acquisition for building models has been able to achieve automation; the process of formal modeling can realize the abstract of small scale

experimental network basically; the qualitative classification and quantitative process of safety evaluation index can also be used in the 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 between the models is not significant, and there is no systematic accepted theory method.

Based on the quantification of security attributes, Strutt[52] proposed 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 of method is more concerned with the formula calculation process based on the security indicators, and less dependence on the formal model. Paper [53] give out a hierarchical evaluation and calculation method, Li[54] gives a kind of model which can do real time assessment and online monitoring of immune detection, The risk propagation algorithm proposed by Zhang[55] also has certain reference significance, the attack intention analysis model proposed by Ma[56] try to get rid of the dependence on CVSS and fusion potential threat, whose result is more reasonable within the constraints. Paper [57] proposes a polymerization method which can fuse the basis points of common vulnerability scoring system and then evaluate the security of the whole network.

Network integration analysis based on attack model is currently a hot research topic, dozens of articles are found in key journals each year, such as analysis based on attack graph[10,29,31,33], advanced model fusion analysis[42], [43,44,50], [45,47] and so on. In the past three years, Kerumati[58] proposes a more accurate method to calculate the reachability of the attack; Roschke[46] intent 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; Paper [59] discusses the solution of optimal complement indemnity for property dependent attack graph; Also has the paper focusing on multi-stage or multi step attack[60]; most of these analyses are around three aspects, which are Attack reachability[19,24,31], Minimum attack cost [10,33] and Maximum attack gain [40,43,45], Gao[61] firstly use the attack graph model in the analysis of the safety risk of the industrial control system, a practical example is given for the application of the attack graph model.

By the research on communication network or military, the survivability research of the network system will become the mainstream direction[6], which is intended to describe the ability to perform critical tasks under attack. 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. Paper [62] propose a framework for survivability analysis, but the description of the state transformation of each node limit the large-scale promotion; the penetration test attack model proposed by Paper [42] can be used in the process of penetration testing and describe the stability of attack; the research of Zhou[63-64] is helpful to detect recommended attack and then improve the robustness of the collaborative recommendation system and ensure the credibility of the system recommendation.

This section effectively summary the main steps 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. Based on the current research of attack graph, reference to the concept of complex network controllability, this paper attempt to improve the modeling capability of large scale complex attack networks, gives out the attack condition of arbitrary network, and does the theoretical argument for network anti attack ability under attack, finally carries on the example comparison.

## III. FORMAL MODELING

### *A. Attack network*

**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, which is denoted as *C*, $C_{vs}=(v,s)$ 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 connection relationship to another network component. $E=(C_{xi}, C_{yj}, l)$ 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 is *n*; *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.

In this way, the process of attack can be interpreted as the progress that attacker go through one or more network components and gradually expand the scope of the impact to obtain income. Supposed that, $\theta$ is the impact value of the attacker's attitude for network component *c*, so $\theta_t=\{\theta_1(t), \theta_2(t),\ldots, \theta_n(t)\}$ is the attitude value vector of network components, $\theta_i(t)\in[-1,+1]$ is the attack effect attitude of network component *i* at time *t*, positive value indicates that it can be attacked, the greater the value, the more likely be

attacked(+1 shows that one component can be fully controlled, attacker has the Root privilege for example), negative value indicates that it cannot be attacked easily due to the presence of defense measures, etc.( -1 shows that one component is completely uncontrollable, attack path is not reachable for example).

### *B. Transition matrix*

In traditional attack graph model, the principle of maximum probability is generally followed[10,40,45], that is rationally the attacker will select the path with the maximum probability in attack progress, however in actual, attack must be the progress of many times of infiltration and temptation, which is not always from the path of the greatest success probability. Together with vulnerability, normal or authorized connection relationship also has influence during the progress, so in this paper, the changes in the impact of attacks of component *i* is defined as the sum of all the effects on *i*.

**Definition 4:** $\lambda_{ij}$ represents the impact value from network component *i* to network component *j*, $\lambda_{ij}=\dfrac{w(i,j)}{\sum_{m\in N(j)} w(m,j)}$, $N(j)$ represents the inside edge collection of neighbor nodes of component *j* in attack network, $w(i,j)$ represents the weight between *i* and *j*.

At the time $t$+1, $\theta_i(t+1)=\theta_i(t)+\sum_{j=1}^{n}(\theta_j(t)-\theta_i(t))\varphi^{\mathrm{T}}$, $\varphi=\lambda_{ij}$ is the impact value defined in Definition 4, $\varphi^{\mathrm{T}}$ is the matrix transpose. Affected by a number of neighbor nodes, the attitude change value of the component *i* is $\triangle\theta_i(t)=\sum_{j=1}^{n}(\lambda_{ji}(\theta_j(t)-\theta_i(t)))$, Let L as the Laplasse matrix and $\Delta\theta(t)=\mathrm{L}\times\theta(t)$, so $\theta(t+1)=\theta(t)+\Delta\theta(t)=\theta(t)+\mathrm{L}\times\theta(t)=(\mathrm{I}+\mathrm{L})\theta(t)$, finally $\theta(t)$ can be expressed as $\theta(t)=(\mathrm{I}+\mathrm{L})^t\theta(0)$.

Now the progress that the attacker launch an attack through the initial access components can be expressed as $\Re=\mathrm{I}+\mathrm{L}=R_{ij}\in\mathrm{T}^{n\times n}$, this paper use $\Re$ to represent the Transtion-probablity matrix of attack network, obviously the sum of elements in each row is 1, and the matrix is a random matrix.

DeGroot model[12,65] can describe the process of information exchange and consensus, the change progress in this paper can also be described by the rules in the same way. $\Re$ is a random matrix, it can also be as the one-step transition probability matrix, According to the Markov chain limit theorem we can infer that[65], if the attack network is strongly connected and non-periodic, the attack impact of each node in the network will converge to a certain value.

## IV. PROBABILITY CONTROLLABILITY

In attack network defined in this paper, each network component node has an initial value for the attack impact. With the attacker's action, the interaction between the neighbors and the time passes, the impact attitude of each component from attacker will change. In short, the attacker wants to control some component nodes, and then to achieve the desired state. Follow the basic describe way of network control characteristics, this paper defines the initial attack node as source node (here suppose there is only an attacker, that means only one source node, if multiple attackers exist, merge them into one node), the direct access node of source node is named drive node.

### *A. Fully probability control*

Attack network fully probability control means that the impact attitude value of all the nodes in the attack network will converge to be same with target attitude value of source node.

**Theorem 1:** In the attack network $G(C,E)$, suppose that $D\subset C$ is a collection of drive nodes, then the condition of fully probability control of $G$ is that there is a directed path for($\forall i\in C\backslash D$ , $\exists\, j\in D$ , $j\rightarrow i$).

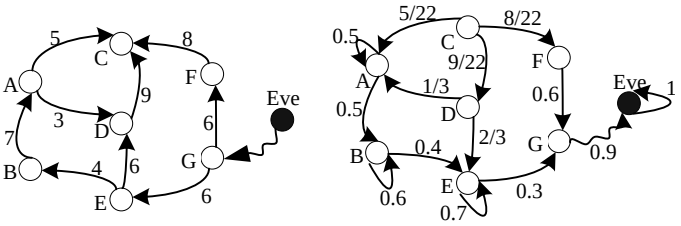
The intuitive understanding of Theorem 1 is that if the source node cannot access some component nodes, then these components will not be affected by the attack. From an attacker's point of view, the network is not controllable, this is consistent with the definition of attack reachability in attack graph[8-10]. The following is a theoretical proof.

**Proof:** According to the definition of fully probability control, there is at least a direct path from source node to any node *j* in collection *D*. obviously if the directed path for ($\forall i\in C\backslash D$ , $\exists\, j\in D$ , $j\rightarrow I$) exists, then the source node can reach every components in network. So theorem 1can be proved only by the convergence of transtion-probablity matrix.

The transtion-probablity matrix $\Re$ is a Markov chain based on one step transtion-probablity matrix, there is at least one direct path from source node to any component, then there is at least one direct path from any component to source node in Markov chain. That is, the Markov chain is a chain of absorption (the probability from any state *S* to source node is greater than 0: $P^n>0$). After the evolution of finite steps, the impact attitude of any component node will be the same with source node. **Proof finished.**

In figure 2, Fig (a) is an example of a sample attack network, Eve is the source node (attacker node), Fig (b) is the Markov chain based on one step transtion-probablity matrix of Fig (a). In Fig (a), there is at least one direct path from source node to any component node, in the corresponding Markov chain (Fig (b)), there is at least one direct path from any component node to source node Eve, that is $\forall i\in C$, $P_{iEve}^{n}>0$, and each temporary state will converge to the same as the source node. If the attacker Eve select E as the drive node in Fig (a), because the node E

cannot reach node F and G, the corresponding Markov chain can be divided into 3 kinds, they are {Eve},{A,B,C,D,E},{G}, in which{A,B,C,D,E}is a temporary state, after finite steps it will arrive at {Eve} or {G} at a positive probability, therefore when E is selected as the drive node, the attack network is not fully probability control.



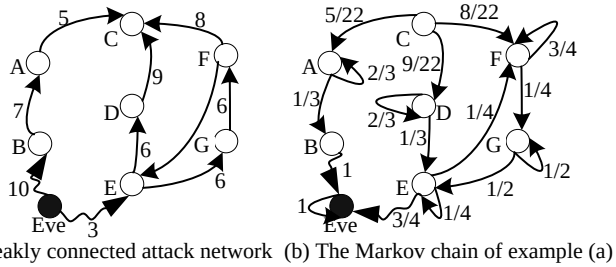

(a) A example of attack network (b) The Markov chain of example (a)

Fig2 An example of attack network and its Markov chain

If strongly connected, there is a direct path from any component node in attack network G to any other component node, so according to theorem 1, the condition of fully probability control is that any component can be the selected drive node.

If weakly connected, the attack network can be divided into two, they are a finite number of closed sets (in this paper the closed set is the smallest closed set[66]) and a set of nodes which is not in closed sets. In figure 3, Fig (a)is another example, Fig (b) is the corresponding Markov chain of Fig (a), the nodes can be divided into three set, they are two closed sets $CS_1$={B},$CS_2$={E,F,G}and the set of the nodes {A,C,D}which is not in the closed set, According to the closed set definition[66], if the source node can reach any node in the closed set, then there is a direct path from the closed set to the source node in the corresponding Markov chain. So, for the weakly connected attack network, we should select drive node in each closed set to make the network be fully probability control. For example, in Figure 3 (b), there are 2 closed sets, any component node in the 2 closed sets can be selected as the drive node, such as B and E.

**Inference 1:** When strongly connected, the minimum number of drive nodes to achieve fully probability control is 1, when weakly connected, the minimum number of drive nodes to achieve full probability control is *k*, and *k* is the number of minimal closed sets in the network.




(a) weakly connected attack network (b) The Markov chain of example (a)

Fig3 An example of weakly connected attack network

In ideal environment, if the basic physical network is fully connected, the initial energy of the attacker can be arbitrarily small, in a finite number of steps he can achieve the expected purpose of the attack, but if the selected drive node has bigger influence, the process of attack will be more easily, in the attack network model proposed in this paper, that means the convergence rate of whole network will be faster. This fact will be verified in the following example.

### *B. Partly probability control*

In the fully probability control, suppose that each node in the network can be directly affected by the source node (attacker), but this is not possible in a realistic computer network, there must be some measures to prevent an attacker from reaching the target, such as Access restrictions, Implementation of defensive measures, Physical link disconnection etc. This section will discuss the controllability in this situation.

In the definition of attack network, we use a negative number to represent a component node which is not easy to be attacked, and use the absolute value of the negative number to indicate the extent. Suppose that threshold $\delta(\delta<0)$ is the minimum value that attacker cannot control, that means that if the attitude of a component node *i* is less than $\delta$ ($\theta_i<\delta$), then the component is not controllable (from the attacker's point of view, it can not to be attacked); if the attitude of a component node *i* is more than $\delta$ ($\theta_i>\delta$) and after evolution the attitude is positive, then the component is controllable; if the attitude of all component nodes is positive, then the whole network is partly probability control.

**Definition 5:** An attack network $G(C,E)$, $D\subset C$ is the set of drive nodes, the initial attitude of source node is positive, $U\subset C\backslash D$ , $\forall i\in U$ , $\theta_i<\delta$ , $|U|=m$ , $\forall j\in C\backslash U$, after a finite step evolution, if $\theta_j^n>0$, then the attack network is partly probability control.

Take the weakly connected attack network in Fig (3) for example again, if the node B is not controllable, node E in close set {E, F, G} is controllable, all nodes in the close set {E, F, G} will converge. According to this classification, the nodes can be divided into {B} (immune closed set), {E, F, G} (control closed set), and {A, C, D} (not in closed set). Generally the random matrix of transition probability can be simplified as $\Re=(\Re_I,\Re_N,\Re_C)$ , in which $\Re_I$ is the transfer matrix for immune closed set node, it represents the impact of nodes that is not controlled by the source node; $\Re_N$ is transfer matrix for the nodes that is not in the close set, it represents the impact among nodes; $\Re_C$ is transfer matrix for the nodes that is in the close set, it represents impact from directly attacked nodes by the source node to the other nodes. Obviously the condition for the partly probability control defined in Definition 5 is that the attack impact of nodes in $\Re_C$ is more than defense impact of nodes in $\Re_I$ ( $\lim_{k\to\infty}(\Re_C)^k>\lim_{k\to\infty}(\Re_I)^k$ ).

**Theorem 2:** The corresponding transition matrix $\Re$ of attack network in definition 5 is convergent, and the sufficient condition for partly probability control is $(1-\Re_N)^{-1}(\Re_C-\Re_I)>0$.

**Proof:** Proof of convergence. For simplified matrix $\Re=(\Re_I,\Re_N,\Re_C)$, the corresponding Markov chain has two absorbing states, they are controllable state and immune state, and all the nodes will reach one of the states in a positive probability, also the two closed sets are strongly connected and non-periodic, so the matrix $\Re$ is convergent [67].

Proof of sufficient. The transition matrix $\Re_N(|\Re_N|=n)$ for the nodes that is not in the close set is a sub stochastic matrix. Suppose that in $\Re_N$, the set in which the sum of each row is less than 1 is $B_1$, the set in which the sum of each row is equal to1is $B_2$, The result of mathematical formula is $\forall i \in B_1, 0 \le \sum_{j=1}^{n} R_{ij} < 1, \ \forall i \in B_2 \sum_{j=1}^{n} R_{ij} = 1 |B_1|+|B_2|=n$, if in the adjacency matrix graph of $\Re_N$, any node in $B_2$ can access the node in $B_1$, then when $k\to\infty$, $(\Re_N)^k\to 0$. Here, we do not prove the correctness of the conclusion [65, 67], only give examples of its specific application.

In Fig (3), suppose that B is an immune node, E is a controllable node, then the sub random matrix of nodes {A,C,D,F,G}which is not in close set is shown in $\Re_N$ in Fig (4), $B_1$={1,3,5}, $B_2$={2,4}, in Fig (4) T is the directed adjacency graph of $\Re_N$, and any node in $B_2$ can reach the node in $B_1$, so when $k\to\infty$ , $(\Re_N)^k\to 0$. Similar results can be obtained for repeated calculations on $\Re_N$ .

$$\Re_N=\begin{pmatrix} 2/3 & 0 & 0 & 0 & 0 \\ 5/22 & 0 & 9/22 & 8/22 & 0 \\ 0 & 0 & 2/3 & 0 & 0 \\ 0 & 0 & 0 & 3/4 & 1/4 \\ 0 & 0 & 0 & 0 & 1/2 \end{pmatrix}, \quad T=\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Fig4 the sub stochastic matrix and adjacency matrix for directed graph of {A,C,D,F,G}

Similarly suppose that D is an immune node, E is a controllable node in Fig (3), then the sub random matrix of nodes{A,B,C,F,G}which is not in close set is shown in $\Re_N$ in Fig (5), $B_1$={3,5} , $B_2$={1,2,4}, in Fig (5) T is the directed adjacency graph of $\Re_N$, and the node 2 in $B_2$ cannot reach any node in $B_1$, in this case, when $k\to\infty$, $\lim_{k\to\infty}(\Re_N)^k$ is shown in Fig (5), $(\Re_N)^k$ will not converge to 0.

$$\Re_N=\begin{pmatrix} 2/3 & 1/3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 5/22 & 0 & 0 & 8/22 & 0 \\ 0 & 0 & 0 & 3/4 & 1/4 \\ 0 & 0 & 0 & 0 & 1/2 \end{pmatrix}, \quad T=\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \lim_{k\to\infty}(\Re_N)^k=\begin{pmatrix} 0 & 0.8 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0.3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Fig5 the sub stochastic matrix and adjacency matrix for directed graph of {A,B,C,F,G}

According to the results of convergence, in the normal state, the random matrix of attack network will converge to a stable state, $\lim_{k\to\infty}\Re^k=\left((\Re_I)^k,(\Re_N)^k,(\Re_C)^k\right)$ because $\lim_{k\to\infty}(\Re_N)^k$ and $\lim_{k\to\infty}\Re^k$ is idempotent, so:

$$\lim_{k\to\infty}(\Re_C)^k=\lim_{k\to\infty}(I+\Re_N+(\Re_N)^2+\cdots+(\Re_N)^{k-1})\Re_C=(I-\Re_N)^{-1}\Re_C$$

$$\lim_{k\to\infty}(\Re_I)^k=\lim_{k\to\infty}(I+\Re_N+(\Re_N)^2+\cdots+(\Re_N)^{k-1})\Re_C=(I-\Re_N)^{-1}\Re_I$$

∵the condition for partly probability control is $\lim_{k\to\infty}(\Re_C)^k > \lim_{k\to\infty}(\Re_I)^k$, $\therefore (I-\Re_N)^{-1}\Re_C > (I-\Re_N)^{-1}\Re_I$, From this we can know that the sufficient condition for partly probability control is$(1-\Re_N)^{-1}(\Re_C-\Re_I)>0$. **Proof finished.**

In attack network, the effect of different nodes on the spread of attack is different, the proving process of theorem 2 is not only given a sufficient condition for partly probability control, and it also provides some methods for the selection of the attacker's direct attack node (drive node): repeat the calculation on the random matrix $\Re$ and the initial attitude $\theta$ to get the weight of each node, when $\lim_{k\to\infty}(\Re_C)^k > \lim_{k\to\infty}(\Re_I)^k$, select the node which is connect to probability immune node as the drive node, for better attack effect, select the largest weight node in the adjacent nodes of probability immune node, if there is more than one node directly connected to probability immune node, then select the out-degree bigger one.

### *C. Compared with the structural controllability*

Paper [68] published the research of structural controllability of complex network firstly in《Nature》, after that, research on this has entered a high point. Controllability study is based on the classical control theory, the theory of linear system ($\frac{dx(t)}{dt}=A\bullet x(t)+B\bullet u(t)$) is generally used for this study, external controller achieve his control objectives through the control input vector node (matrix *B*) and the interaction among the nodes (matrix *A*).

Structural controllability and the probability controllability of complex network model via attack provided by this paper both want to discuss the evolution process when the controller (source node) perform actions

by driving the node and the conditions required to control the evolution process. But the focus of structural controllability is controllable conditions in theory rather than specific methods or measures. During the attack, attacker will adjustment his target and means. Therefore, the focus of this paper is more about whether the evolution of the results will result in loss and attitude trends in the degree of loss, arrive at any state is not needed.

In structural controllability, the controllability condition of complex network is the full rank (Rank($C$)=$n$) of the control matrix, but in this paper, the condition of fully probability control or partly probability control is $\lim_{k\to\infty}(\Re_C)^k > \lim_{k\to\infty}(\Re_I)^k$. It can be learned that if a network is structure controllable, the model proposed in this paper will be established, but vice versa. It can be said that the model proposed in this paper is a special case of structural controllability in network attack and defense.

## V. EXPERIMENTS AND ANALYSIS

In order to verify the correctness of the proposed model and analysis method. Firstly, a typical example of Web information system is constructed according to the traditional approach of attack graph analysis, topology structure is shown in Fig6, The environment used in the experiment is Intel i5-2430M@2.40G processor, 4G memory, Windows7, the algorithm is realized by C#.

In Fig6, there are 4 servers in the experiment, 10.10.0.10 is web server, windows operating system, which provide service through three network components: IIS, Apache and FTP, The Internet users can access one of them through the firewall; 10.10.0.11 is database server, windows operating system, and has SQL server and RPC two network components; 10.10.0.12 is mail server, windows operating system, provides Email and Rshd service; 10.10.0.13 is file server, Linux operating system, provides Telnetd and Ftp services.

According to the set of network security rules, internet users can access IIS and Apache service on Web server, 10 server can be remote to the database server and mail server, apache component can access the Email service on 12 server, IIS component can access the Sever SQL database on 11 server, the Ftp service on 10 server can interact with the Ftp component on the file server, The Rpc component on the database server and the Rshd component on the mail server can be remote to the Telnetd component on Linux server.

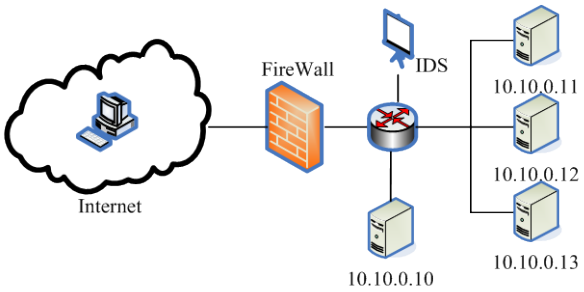
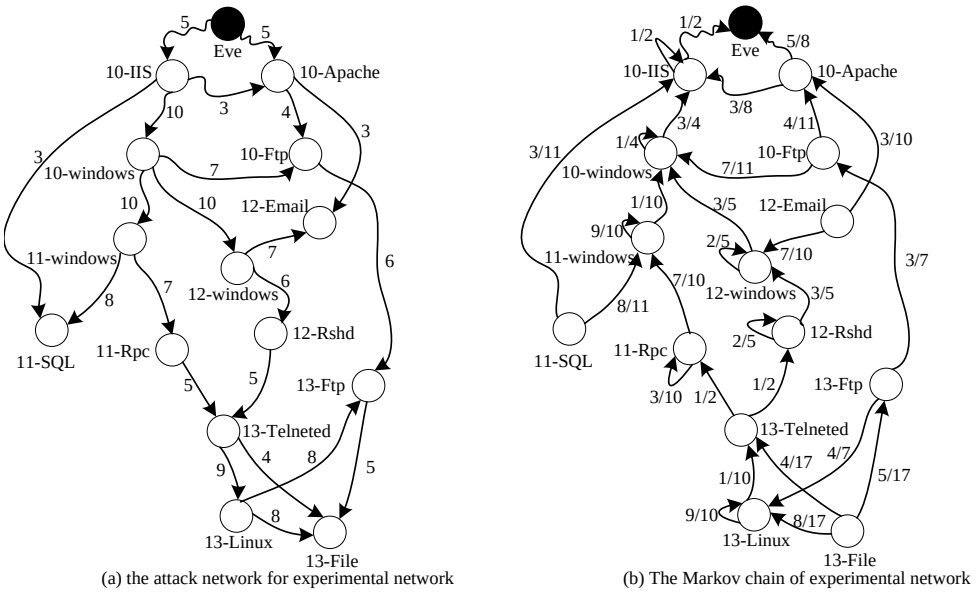



Fig6 Topological map for experimental network

Suppose there is a Null.htw vulnerability on the IIS component, through which attacker can get the host Root permissions, there is a remote command injection vulnerabilities on Apache and there is Outlook URI vulnerabilities on the Email component, There are FTP directory traversal vulnerabilities on both 13 and 10 Ftp component, there is RPC request buffer overflow vulnerability on Rpc component, Rshd component allows the user to perform remote shell commands with Root identity, the Telneted component has an input validation error that allows the visitor to obtain remote administrator rights.

In this example, we refer to the attack and defense strategy and its quantification results in paper [50], and use this as the attack gain for each link, The graphical description of the experimental attack network is shown in Figure 7 (a), According to the calculation method in definition 4, the Markov chain of the experimental attack network is shown in Figure 7 (b).




(a) the attack network for experimental network (b) The Markov chain of experimental network

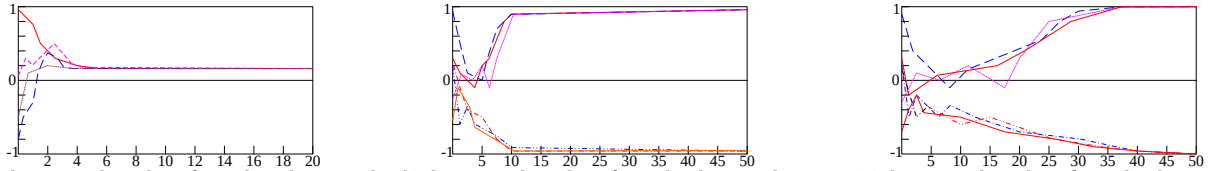
Fig7 the graphical results for experimental network

In Fig7 (b), besides the attack node (source node) Eve, there are two minimal closed sets:{10-IIS} and {10-Apache}. According to the inference 1, the number of driving nodes for fully probability controllability is equal to the number of minimal closed sets, so if Eve selects 10-IIS and 10-Apache as the drive nodes, then entire network can be fully controlled (Theorem 1).

In fully probability controllability, the impact of each node in the network is different. One way to calculate the influence of each node is to get the limit $\lim_{k\to\infty}\Re^k$ of the transition matrix $\Re$, another way is make the multiplication on initial impact vector and transfer matrix repeated as shown in Fig8. The calculation results show that the effect of three nodes 10-IIS, 11-Windows and 10-Windows is larger, according to the attack graph shown in Figure 7 (a), there are 15 paths from Eve to 11-SQL or 13-File, in which 13 will through the three nodes. Figure 9 shows the different convergence rate in different states. Without attack, components in network will affect each other, the convergence process and rate is shown in Figure 9 (a), Figure 9 (b) and Figure 9 (c) show the number of rounds needed for network convergence when 10-IIS and 10-Apache are selected as the drive node respectively. From the results, we can see that the greater the impact of the driving node, the faster the convergence of the network and the easier the attacker to achieve the purpose of controlling the entire network. In the early analysis of attack graph [8-9], the attack path through 10-IIS and 10-Apache will be treated equally, but from the analysis of this paper, the harm degree by the 10-IIS is greater, the rational defender should take this as the starting point to carry on the defense measure.

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10-IIS | 0.8 | 1/2 | 1/2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1.51 |
| 10-Windows | 0.9 | 0 | 3/4 | 1/4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1.05 |
| 10-Apache | 0.8 | 5/8 | 3/8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.2 |
| 10-Ftp | 0.3 | 0 | 0 | 7/11 | 4/11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.26 |
| 11-Windows | 0.9 | 0 | 0 | 1/10 | 0 | 0 | 9/10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1.38 |
| 11-SQL | 0.5 | 0 | 3/11 | 0 | 0 | 0 | 8/11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11-RPC | 0.3 | 0 | 0 | 0 | 0 | 0 | 7/10 | 0 | 3/10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.54 |
| 12-Windows | 0.9 | 0 | 0 | 3/5 | 0 | 0 | 0 | 0 | 0 | 2/5 | 0 | 0 | 0 | 0 | 0 | 0 | 0.75 |
| 12-Email | 0.3 | 0 | 0 | 0 | 3/10 | 0 | 0 | 0 | 0 | 7/10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12-RSHD | 0.3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3/5 | 0 | 2/5 | 0 | 0 | 0 | 0 | 0.57 |
| 13-Telneted | 0.9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1/2 | 0 | 0 | 1/2 | 0 | 0 | 0 | 0 | 0.1 |
| 13-Linux | 0.3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1/10 | 9/10 | 0 | 0 | 0.75 |
| 13-File | 0.3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4/17 | 8/17 | 0 | 5/17 | 0 |
| 13-Ftp | 0.6 | 0 | 0 | 0 | 0 | 3/7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4/7 | 0 | 0 | 0.09 |
| Eve | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1.7 |

Fig8 the calculation process of influence weight for each node



(a) the required number of rounds without attack (b) the required number of rounds when attack 10-IIS (c) the required number of rounds when attack 10-Apache

Fig9 the convergence rate of experimental network under different conditions

In the above fully probability controllability analysis, do not consider the impact of the attack and defense measures, which means the impact of the attacker can be transmitted directly between the nodes, but the actual situation is far from this. Existing models use some other methods to describe the uncertainty, such as Attack success probability [10,45,47], Offensive and defensive game [43-44,50], Correlation analysis [31,53,55] and so on, most of them get the harm degree of each attack sequence or the importance of some key nodes, etc. the selection of defense nodes, especially the effect after defense is rarely analyzed and discussed. Defense for each vulnerability is impossible, so the focus of this paper is that under the limited defense, how is the network's security state.

In the simulation example shown in figure 6, defense measures can be divided into 5 kinds, they are (a) 10-IIS, 10-Windows defense, (b) 10-Apache defense, (c) 11-Windows defense, (d) 12-Windows defense, (E) 13-Linux defense. Suppose that the attitude of attacker is 0(that means the threshold δ=-1) when defense exists. According to theorem 2, the calculation results of partly probability control under different defense measures can be get (as shown in Table 1), According to the calculation results only 10-IIS, 10-Windows defense can prevent the attacker to achieve the results of partly probability control. The graphical results of attack networks in Fig7 (a) shows that if the attacker cannot affect the 10-Windows, 10-IIS two nodes, most of the attack path will be interrupted. The results from table 1 also shows that 10-Apache defense cannot play the desired effect, which is different from the classical attack graph analysis model [8-9], it is because the 10-Apache defense will be much less affected than the attacker's attack on10-IIS. So in Fig6 the optimal defense strategy of the experimental network is repair Null.htw vulnerabilities on 10-IIS component, for other components, just need to update the patch properly, and ensure the access policy is correct.

Table1 the calculation results of partial probability control under different defense measures

| Controllable nodes | Defense nodes | $B_1$(the set that the sum of each row is less than 1) | $B_2$(the set that the sum of each row is equal to 1) | Conclusion |
|---|---|---|---|---|
| 10-Apache | 10-IIS、10-Windows | 10-Ftp、11-Windows、11-SQL、12-Windows、12-Email | 11-RPC、12-RSHD、13-Telneted、13-Linux、13-File、13-Ftp | No |
| 10-IIS | 10-Apache | 10-Windows、10-Ftp、11-SQL、12-Email | 11-Windows、11-RPC、12-Windows、12-RSHD、13-Telneted、13-Linux、13-File、13-Ftp | Yes |
| 10-IIS、10-Apache | 11-Windows | 10-Windows、10-Ftp、11-SQL、11-RPC、12-Email | 12-Windows、12-RSHD、13-Telneted、13-Linux、13-File、13-Ftp | Yes |
| 10-IIS、10-Apache | 12-Windows | 10-Windows、10-Ftp、11-SQL、12-Email、12-RSHD | 11-Windows、11-RPC、13-Telneted、13-Linux、13-File、13-Ftp | Yes |
| 10-IIS、10-Apache | 13-Linux | 10-Windows、10-Ftp、11-SQL、12-Email、13-File、13-Ftp | 11-Windows、11-RPC、12-Windows、12-RSHD、13-Telneted | Yes |

At present, there is not a common data set or test model for the horizontal comparison among different models. Almost every article will illustrate the validity of the model and analysis method as this section shows. Compared with the early attack graph model [8-9], the construction process of the model proposed in this paper can be completed with the vulnerability scanning tool, no more algorithm is needed to do the conversion process of pre-condition and post-condition. At the same time, each node in the attack graph is the component of the network host, which is a natural abstraction based on rights relations and connection relations. Compared with the paper [31],[33],[47] etc., it is more concise and clear, and there is no ambiguity, no need to carry on the individual description to each element in the chart. The results of paper [10],[40] is state attack graph, although some simplified algorithm is put forward at the same time, for large scale network security analysis, there will be the risk of state space explosion. Based on the logical cause and effect relationship, this model is more suitable for large scale networks, because the time complexity is polynomial time on both model generation and model calculation or analysis (time complexity is $O(n^2)$). More important is that this model can give the key point of defense when get the conclusion whether the network is safe, sufficient conditions for partly probability control can give a theoretical and accurate solution whether a defense measures can meet the security policy.

## VI. CONCLUSIONS

This paper divides the process of network security analysis based on formal model into 4 main steps, does detailed summary of the current research status for each step, and makes clear that using stochastic model for network security analysis will be the main direction. Referring to the concept of complex network controllability, this paper refine the granularity of the description of the traditional attack graph to component

level, and use a directed weighted graph to represent the diffusion process of an attacker's rights; after the definition of attack network and transfer matrix, this paper also give out the criterion condition for fully probability control or partly probability control, and discuss the relationship between probability controllability and traditional structure controllability; finally show the basic process of the model by a typical experiment and simulation experiment, The analysis results show that with polynomial time complexity it can be used to analyze the security of large scale network, provide an effective selection of defense nodes, and do validation of the effectiveness of the defense strategy.

In this paper, we use intrusion detection data set for attack analysis first time, but there are obviously a lot of shortcomings when using the classic data set for attack model algorithm validation, besides most of the quantitative results used in this paper are based on expert experience, so it will be the important research direction on constructing a data set suitable for large-scale network risk assessment analysis and objective quantification of the attack attributes.

## REFERENCES


[1] "China information Almanac" editorial board. China information Almanac 2014. Electronic Industry Publishing. 2015.

[2] Miller. B. P, Koski. D, Lee, CJin Pheow, et al, A Re-examination of the Reliability of UNIX Utilities and Services. Technical Report, Department of Computer Sciences, University of Wisconsin, 1995.

[3] Anderson JP. Computer security threat monitoring and surveillance. Technical Report, Contract 79F26400. Fort Washington, Pennsylvania, James P. Anderson Company, 1980.

[4] Li Zhoujun, Zhang Junxian, Liao Xiangke, Ma Jinxin. Survey of Software Vulnerability Detection Techniques. *Chinese Journal of Computers*. 2015, 4(38): 717-731.

[5] Srnaha, S. E. Haystack: an intrusion detection system. In; Orlando ed. Proceedings of the 4th Aerospcce Computer security Applications Conference. Washington. DC; IEEE Computer Society Press, 1988. 37-44.

[6] Lin Chuang, Wang Yang, Li Quanlin. Stochastic Modeling and Evaluation for Network Security. *Chinese Journal of Computers*. 2005, 28(12): 1943-1956.

[7] Bass T, Gruber D. A glimpse into the future of ID. http://www.usenix.org/ publications/login/ 1999-9/features/future.html.

[8] PHILLIPS C A, SWILER L P. A graph-based system for network vulnerability analysis[A]. New Security Paradigms Workshop. 1998.71-79.

[9] Ritechey R, Ammann P. Using Model Checking to analyze network vulnerabilities. *Proceedings of the 2000 IEEE Symposium on Research on Security and privacy*. Oakland, California, USA, 2000:156-165

[10] Chen Xiao-Jun, Fang Bin-Xing, Tan Qing-Feng, Zhang Hao. Inferring Attack Intent of Malicious Insider Based on Probabilistic Attack Graph Model. *Chinese Journal of Computers*, 2014, 37(1):62-72.

[11] Gao L, Yang JY, Qin GM. Methods for pattern mining in dynamic networks and applications. Ruan Jian Xue Bao. *Journal of Software*, 2013,24(9):2042-2061.

[12] Hou Lü-Lin, Lao Song-Yang, Xiao Yan-Dong, Bai Liang. Recent progress in controllability of complex network. *Acta Physica Sinica*, 2015, 64(18): 188901-188901.

[13] Xing Xu-Jia, Lin Chuang. A Survey of Computer Vulnerability Assessment[J]. Chinese Journal of Computers. 2004, 27(1): 1-11.

[14] FARMER D, SPAFFORD E H. The Cops Security Checker System[R]. Technical Report CSD-TR-993. Department of Computer Sciences, Purdue University. 1991.

[15] Renaud Deraison. Nessus Scanner. http://www.nessus.org [EB/OL].2004.

[16] Mao Handong, Chen Feng, Zhang Weiming, Zhu Cheng. Advances in network Multi-attack modeling. *Computer Science*. 2007:11(34):50-61.

[17] Ritchey R., O'Berry B., Noel S.. Representing TCP/IP connectivity for topological analysis of network security. *Proceedings of the 18th Annual Computer Security Applications Conference*, San Diego, California, 2002, 25~31

[18] Luo Zhiyong, You Bo, Xu Jiazhong, Liang Yong. Automatic recognition model of intrusive intention based on three layers attack graph. Journal of Jilin University (Engineering Edition), 2014, 44(5): 1392-1397.

[19] Tian Zhihong, Yu Xiangzhan, Zhang Hongli, Fang Binxing. A Real-Time Network Intrusion Forensics Method Based on Evidence Reasoning Network. *Chinese Journal of Computers*. 2014, 37(5): 1184-1194.

[20] Feng Xuewei, Wang Dongxia, Huang Minhuan, Li Jin. A Mining Approach for Causal Knowledge in Alert Correlating Based on the Markov Property. *Journal of Computer Research and Development*, 2014, 51(11): 2493-2504.

[21] Ramakrishnan C.R., Sekar R.. Model-based analysis of configuration vulnerabilities. *Journal of Computer Security*, 2002, 10(1/2): 189~209

[22] Qu G., Jayaprakash, Ramkishore M., Hariri S., Raghavendra C.S.. A framework for network vulnerability analysis. *Proceedings of the 1st IASTED International Conference on Communications, Internet, Information Technology*, St.Thomas, Virgin Islands, USA, 2002, 289~298

[23] Scheier B. Attack trees: modeling security threats. Dr Dobb's Journal, 1999, 12(24): 21-29.

[24] Luo Senlin, Zhang Lei, Guo Liang, et al. An original effective method for modeling the attack tree. *Transactions of Beijing Institute of Technology*, 2013(5):500-504.

[25] Sheyner O, Haines J, Jha S. Automated generation and analysis of attack graphs. *Proceedings of the IEEE Symposium on Security and Privacy*. Oakland: IEEE Computer Society Press, 2002. 273-284.

[26] Ammann P, Wijesekera D, Kaushik S. Scalable graph-based network vulnerability analysis. *Proceedings of the 9th ACM Conference on Computer and Communications Security*. Washington, D. C., USA: ACM Press, 2002. 217-224.

[27] Swiler L.P., Phillips C., Ellis D., Chakerian S.. Computer attack graph generation tool. *Proceedings of the DARPA Information Survivability Conference and Exposition II*, Anaheim, CA, 2001, 307~321

[28] Homer J, Varikuti A, Ou X M, McQueen M A. Improving attack graph visualization through data reduction and attack grouping. *Proceedings of the 5th International Workshop on Visualization for Computer Security(VizSec2008)*. Cambridge, MA, USA, 2008. Belin Heidelberg, Germany: Springer Verlag,2008:68-79

[29] Ma Jun-chun, Sun Ji-yin, Wang Yong-jun, Zhao Bao-kang, Chen Shan. Study of Attack Graph Construction Based on Distributed Parallel Processing. *Acta Armamentarii*, 2012, 33(1): 109-115.

[30] Ingols K, Chu M, Lippmann R, Webster S, Boyer S. Modeling modern network attacks and counter measures using attack graphs. P*roceedings of the 25th Annual Computer Security Applications Conference*. Honolulu, Hawaii, USA,2009:117-126

[31] Liu Weixin, Zeng Kangfeng, Wu Bin. Alert processing based on attack graph and multi-source analyzing. *Journal of communications*, 2015(9):135-144.

[32] Poolsappasit N, Dewri R, Ray I. Dynamic security risk management using Bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, 2012,9(1): 61-74.

[33] Liu Wei-xin, Zheng Kang-feng, Hu Ying et al. Approach of Goal-Oriented Attack Graph-Based Threat Evaluation for Network Security. *Journal of Beijing University of Posts and Telecom*, 2015, 38(1): 82-86.

[34] Dacier M.. Towards quantitative evaluation of computer security[Ph. D. dissertation]. Institut National Polytechnique deToulouse, France, 1994

[35] Ortalo R., Deswarte Y., Kaaniche M.. Experimenting with quantitative evaluation tools for monitoring operational security. IEEE Transactions on Software Engineering, 1999, 25(5):633~650

[36] Wang Lidong. A quantitative computer system and network security risk assessment method. Harbin Institute of Technology. 2002.

[37] Porras P A,Kemmerer R.A penetration state transition analysis:a rule-based intrusion detection approach. *Proceeding of the Eighth Annual Computer Security Applications Conference*, 1992:220-229.

[38] Stevens F., Courtney T., Singh S., Agbaria A., Meyer J.F., Sanders W.H., Pal P.. Model-based validation of an intrusion-tolerant information system. *Proceedings of the23rd Symposium on Reliable Distributed Systems ( SRDS 2004)*, Florianópolis, Brazil, 2004, 184~194




ISSN: 1998-4464

[39] Madan B., Go eva-Popstojanova K., Vaidyanathan K,Trivedi K.S.. A method for modeling and quantifying the security attributes of intrusion tolerant systems. *Performance Evaluation*, 2004, 56(1~4): 167~186
[40] Ye Yun, Xu Xishan, Qi Zhichang, et al. Attack graph generation algorithm for large-scale network system. *Journal of Computer Research and Development*, 2013,10:2033-2139.
[41] McDermott J.. Attack-potential-based survivability modeling for high-consequence systems. *Proceedings of the 3rd IEEE International Workshop on Information Assurance*, Callege Park, Maryland, USA, 2005, 119~130
[42] Luo Senlin, Zhang Chi, Zhou Mengting, Pan Limin. Researches on Penetration Attacking Model Based on Timed Petri Nets. *Transactions of Beijing Institute of Technology*, 2015,35(1):92~96.
[43] Wang Yuanzhuo, Lin Chuang, Cheng Xueqi, et al. Analysis for network attack-defense based on stochastic game model. *Chinese Journal of Computers*, 2010(9):1748-1762.
[44] Zhang Y, Tan XB, Cui XL, Xi HS. Network security situation awareness approach based on Markov game model. *Journal of Software*, 2011, 22(3):495−508.
[45] Li Zongyu, Wang Jinsong, Xu Yanqi, Wang Yuanming. Complex network attack effect based on dynamic Bayesian network. *Journal of Nanjing university of Posts and Telecommunications (natural Science edition)*, 2015, 35(5): 67-73.
[46] Roschke S, Cheng F, Meinel C. High-quality attack graph-based IDS correlation. *Logic Journal of the IGPL*, 2013, 21(4I):571-591.
[47] Wang Xiujuan, Sun Bo, Liao Yanwen, Xiang Congbin. Computer Network Vulnerability Assessment Based on Bayesian Attribute Network. *Journal of Beijing University of Posts and Telecommunications*, 2015, 38(4): 110-116.
[48] J.Christy. Cyber Threat & Legal Issues. *Shadowcon Conference*. USA: 1999.
[49] CVSS. Common Vulnerability Scoring System. http://nvd.nist.gov/cvss.cfm, 2008.
[50] Jiang Wei, Fang Bin-Xing, Zhang Hong-Li. Evaluating Network Security and Optimal Active Defense Based on Attack-Defense Game Model. *Chinese Journal of Computers*. 2009, 4(1):817-827.
[51] Wang Jinrong, Fang Dingyi, Chen Xiaojiang, Wang Huaijun, He Lu.Taxonomy of Software Attack Technique Oriented to Automated Modeling. *Journal of SiChuan University: Engineer Science Edition*. 2015,47(Z1):91~98.
[52] Strutt JE, Patrick JD, Custance NDE. A risk assessment methodology for security advisors. *Proceedings of the 29th IEEE Annual Int'l Carnahan Conference on Security Technology*. Sanderstead: IEEE Computer Society Press, 1995. 225-229.
[53] Chen XZ, Zheng QH, Guan XH, Lin CG. Quantitative hierarchical threat evaluation model for network security. *Journal of Software*, 2006, 17(4): 885−897.
[54] Li Tao. Detection of network security risk based on immunity. Science in China Ser. E Information Sciences. 2005, 35(8): 798-816.
[55] Zhang YZ, Fang BX, Chi Y, Yun XC. Risk propagation model for assessing network information systems. *Journal of Software*, 2007, 18(1): 137−145.
[56] Ma Chunguang, Wang Chenghong, Zhang Donghong, Li Yingtao. A Dynamic Network Risk Assessment Model Based on Attacker's Inclination. *Journal of Computer Research and Development*, 2015, 52(9): 2056-2068.
[57] Cheng Pengsu, Wang Lingyu, Jujodiu S, et a1. Aggregating CVSS hose scores for sematics-rich network security Metrics. *IEEE 31st Symposium on Reliable Distributed Systems(SRDS)*, 2012: 31-40.
[58] Kerumati M,Akburi A, Kerumati M. CVSS-based security metrics for quantitative analysis of attack graphs. *2013 3th International Conference on computer and Knowledge Engineering(ICCKE)*, Mashhad: IEEE 2013:178-183
[59] Albanese M, Jajodia S, Noel S.Time efficient and cost-effective network hardening using attack graphs. *Proceedings of the 42nd Annual IEEE/IF1P International Conference on Dependable Systems and Networks*. Boston: IEEE Computer Society, 2012.1-12.
[60] Hu Liang, Xie Nan-nan, Nurbol, Liu Zhi-yu, CHAI Sheng. A Multi-Stage Attack Scenario Recognition Algorithm Based on Intelligent Planning. *Acta Electronica Sinica*, 2013, 41(9): 1753-1759.
[61] Gao Meng-zhou, Feng Dong-qin, Ling Cong-li, Chu Jian. Vulnerability analysis of industrial control system based on attack graph. *Journal of Zhejiang University (Engineering Science)*, 2014, 48(12): 2123-2131.
[62] Jha, Wing J. Survivability analysis of networked system[C]. *Proceedings of the 3rd International Conference on Software Engineering*. Washington, DC, 2001. 307-317.
[63] Zhou QQ, Zhang FZ, Liu WY. Detecting unknown recommendation attacks based on bionic pattern recognition. *Ruan Jian Xue Bao/Journal of Software*, 2014, 25(11):2652−2665.
[64] Zhou Quanqiang and Zhang Fuzhi. Ensemble Approach for Detecting User Profile Attacks Based on Bionic Pattern Recognition. *Journal of Computer Research and Development*, 2014, 51(4): 789-801.
[65] DeGroot M H. Reaching a Consensus. *Journal of the American Statistical Association*. 1974. 69(346):118-121
[66] Golub B, Jackson M O. Native learning in social networks: Convergence, influence and wisdom of crowds. *Coalition Theory Network*. 2010, 2(1): 112-149
[67] Jackson M O, Social and Economic Network. Princeton: Princeton University Press. 2008
[68] Liu Y Y, Slotine J J, Barabasi A L, Controllability of complex networks. *Nature*, 2011.473(3):167-173

**Yan Li** was born on Jan.12 1984.He received the PhD degree in information management and information system from Xi'an University of Architecture & Technology of China. He is an assistant professor at Xi'an Polytechnic University, China. His major research interests include information security and big data analysis.

**Chunzi Wang** was born on Jun.8 1983. She received the PhD degree in management science and engineering from Xi'an University of Architecture & Technology of China. She is an assistant professor at Xi'an Polytechnic University, China. His major research interests include information security and system modeling.

**Jingfeng Shao** was born on Sep.11 1980. He received the PhD degree in Traffic information engineering and control from Chang'an University of China. He is an assistant professor at Xi'an Polytechnic University, China. His major research interests include Data warehouse and data mining and information retrieval.

**Bin Zhang** was born on May.10 1984. He is a PhD student in information management and information system from Xi'an University of Architecture & Technology of China. His major research interests include information security and situational awareness.