Hindawi
Security and Communication Networks
Volume 2018, Article ID 3652170, 11 pages
https://doi.org/10.1155/2018/3652170

Research Article

An Approach for Internal Network Security Metric Based on Attack Probability

Chun Shan,[1] Benfu Jiang,[1] Jingfeng Xue,[1] Fang Guan,[1] and Na Xiao[1,2]

[1] *Beijing Key Laboratory of Software Security Engineering Technique, Beijing Institute of Technology, 5 South Zhongguancun Street, Haidian District, Beijing 100081, China*
[2] *State Grid Jibei Information & Telecommunication Company, Beijing 100053, China*

Correspondence should be addressed to Jingfeng Xue; xuejf@bit.edu.cn

Received 2 November 2017; Revised 10 February 2018; Accepted 15 March 2018; Published 24 April 2018

Academic Editor: Zheng Yan

A network security metric may provide quantifiable evidence to assist security practitioners in securing computer networks. However, research on security metrics based on attack graph is not applicable to the characteristics of internal attack; therefore we propose an internal network security metric method based on attack probability. Our approach has the following benefits: it provides the method of attack graph simplification with monitoring event node which could solve the attack graph exponential growth with the network size, while undermining the disguise of internal attacks and improving the efficiency of the entire method; the method of attack probability calculation based on simplified attack graph can simplify the complexity of internal attacks and improve the accuracy of the approach.

1. Introduction

With the rapid development of network and information technology, the role of information system in enterprise becomes more and more important. At the same time, the number of attacks from internal network has also increased. Therefore, it is necessary to build an effective security metric technology for the internal network.

According to the definition and analysis of internal attacks provided by Computer Emergency Response Team (CERT) [1], the internal attacks have the transparency to defense intercepts, such as access control or firewalls. Internal attacks also have the camouflage system privileges, high risk to access the core confidential resources easily, and the complexity of gradual attacks. The security metric as a proactive defense technology, whose role is actively analyzing and evaluating what is existing in the current security risks or potential security risks before the attacks. When the attack action occurred, the security metric method needs to analyze and assess the threat of attack incidents, then predict the attack paths, and take appropriate measures to defend [2].

The analysis method in network security can be divided into two types: one is the unknown vulnerabilities in a network, mainly considering the prevention measures; the other one is the known vulnerabilities in a network, repairing the weak parts of the network and improving the security of the whole network. As for the unknown vulnerabilities, the information security experts have already carried out a lot of research; the main methods are as follows:

(i) Analysis protocol vulnerabilities, such as ARP address resolution protocol: researchers try to find out the protocol vulnerabilities, sum up the vulnerability in some areas, give the solutions for the lack of agreement, and achieve the purpose of prevention.

(ii) Analyze the source code of the software: mistakes are unavoidable when programming, such as buffer overflow vulnerabilities. By studying some important codes, researchers take necessary precautions against possible errors and give patches of software, so as to improve the overall safety of software.

Although these methods are effective, they are very abstract and not easy to implement, and the results are relatively few. But if we start from the known network security vulnerabilities, it is relatively easy, for example, all kinds of graph theory based model checking methods, such as attack graph. The attack graph is a kind of graph theory method to judge the network security by studying the nodes and the relationship between nodes in the network. By building the actual network into a theoretical graph theory model, the attack graph can give us many places to think deeply, sometimes with unexpected results. For example, constructing a model from the known aspects to simplify or idealize the actual elements allows us to focus on the most important or important aspects of cybersecurity, ignoring the secondary and quickly determining the security of the network. The attack graph model has great advantages over other assessment models, becoming one of the most widely used and most studied security metrics models.

Although the attack graph can visually indicate the origin and destination of the network attack, it cannot quantitatively describe the network security. In order to conduct quantitative analysis of the possibility of attacks, we introduce the cumulative reachable probability for each node. Above all, we proposed an internal network security metric method based on attack probability to solve the problem of the existing security metrics with attack graph for the internal network.

2. Related Work

The numerous existing researches on network security metrics based on attack graph mainly focus on the representation of attack graph models, the metrics of indicators, and the conclusions of network security metric. Those early researchers conducted research mainly including the following aspects.

The representation of attack graph models. Xie et al. [3] firstly explored three sources of uncertainty in the attack graph, but the attack graph model they established is carrying on probability derivation only when the attack behaviors are determined, resulting in the fact that the probability of uncertainty testing data is not calculated in the final derivation process. Wang et al. [4] proposed the probabilistic attribute description of the attack graph based on the probability of attacks and the cost of the network deployments, using the method of cumulative reachable probability to evaluate the safety of the whole network, but they did not take into account the impacts of other uncertain factors.

The metrics of indicators: Li et al. [5] used CVSS to evaluate vulnerabilities and proposed a general approach for the network security metrics based on vulnerabilities, but they only considered the probability of a single vulnerability node, while ignoring the vulnerability of the vulnerability node in the whole system, especially the indicators between the vulnerability nodes.

The conclusions of network security metric: in terms of attack probability calculation, Wang et al. [6] use Bayesian network algorithm to calculate the risk probability for internal nodes and quantify the node variables, the node variable values, and the conditional probability distribution. Based on the improved likelihood weighting algorithm, the calculation of Bayesian network node parameter is more convenient; the internal threat forecast also is more accurate. However, this approach did not take into account the vulnerability of their own indicators. Zhang et al. [7] proposed satisfying the temporal order of attack evidence, using the Bayesian network algorithm to analyze the security for all attack paths. However, the probability confidence of nodes in the attack graph is complicated and lacks mathematical theory, and the computational model is also too complicated to work efficiently.

We proposed an internal network security metric of the attack probability based on the attack graph model [8] in this paper. Because of the internal attacks' characteristics of camouflage and complexity, we decided to add the monitoring event node and the key-value pair in the attack graph. Compared with other security metrics, our internal network security metric improved the efficiency and the accuracy obviously with the help of attack graph simplification method and cumulative reachable probability calculation method.

3. An Approach for Internal Network Security Metric Based on Attack Probability

3.1. Method Overview. In order to understand the characteristics and the occurrence environment for the internal attacks, first of all, according to the original attack graph and the attack evidence provided by the security monitoring system, we could get the temporal difference relationship of the monitoring event nodes and simplify the attack graph with the temporal difference relationship. Second, we divide the simplified attack graph into key-value pairs and then calculate the probability of the key-value pairs. Third, we calculate the cumulative reachable probability by the method of attack probability calculation we proposed. Finally, the quantitative evaluation of the current internal network is represented by the cumulative reachable probability of target node. The specific steps are shown in Figure 1.

3.2. The Attack Graph Model. Based on the complexity of internal attacks, internal attack events are mostly multistep and continuous attack behaviors. An attack event includes multiple attack subtargets and a series of related subattack events; that is, from a resource node to the next resource, the event requires a minimum set of basic attack actions. In the initial stage, the attacker has a certain system access or operating authority and through an atomic attack can help the attacker to reach the next state node, so as to obtain more resources and permissions to achieve the next attack subtarget. Therefore, in the attack graph model constructed in this paper, the resource state node is mapped to the original attribute node; the attack action node is mapped to the original atomic attack action node. The attack graph model includes the following contents.

(1) The Atomic Attack. An attack action is a different instruction or a set of operations, which could divide into different basic actions. For example, to open a word file, we need two methods. Method 1: open the file by double-clicking it; Method 2: click on the file, and then click "Enter" to open it. These two methods can open the file but are composed of different operations; we will set those different

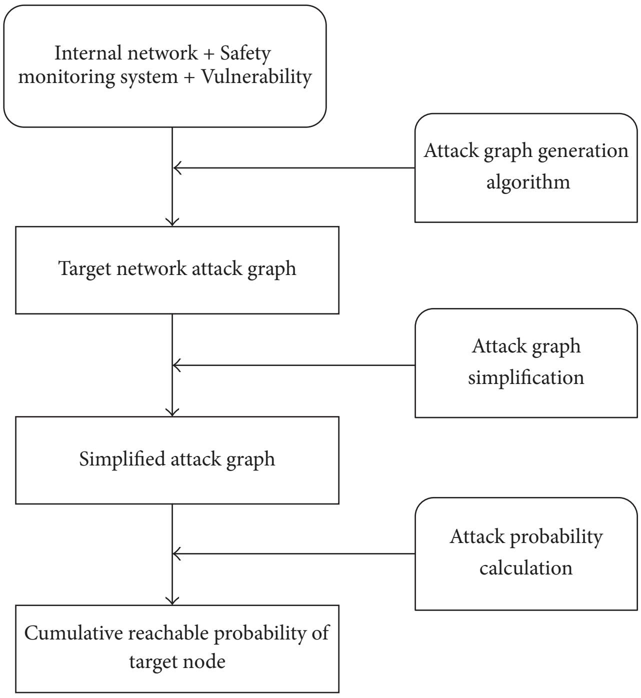

Internal network + Safety monitoring system + Vulnerability
Attack graph generation algorithm
Target network attack graph
Attack graph simplification
Simplified attack graph
Attack probability calculation
Cumulative reachable probability of target node

Figure 1: The schematic diagram of internal network security metric based on attack probability.

but similar function operations or instructions as one basic action.

And from one resource state node to another resource state node, the attacker needs a combination of multiple basic actions to achieve; such a series of basic actions is called the atomic attack. An atomic attack is the minimum set of basic actions that an attacker needs from a resource state node to another resource state node [4].

(2) The Monitoring Event Node. In order to simplify the attack graph, the monitoring event node is introduced in the attack graph model. Because each atomic attack contains a series of the basic attack actions, although the internal attack has camouflage, some basic actions more or less will trigger the security monitoring system, and attacks and other related information will be recorded in alarm log. The set of information recorded in the alarm log is called attack evidence. The monitoring event node refers to the attacker from one resource state to the next resource state, and the implementation of atomic attack triggers the monitoring system, recorded in the alarm log as attack evidence. We use one monitoring event node to record one kind of atomic attack's set of basic actions execute time sequence.

(3) The Attack Graph Model. In order to construct an attack graph model applicable to the internal network security metric, an improved probability attack graph is proposed based on the attribute attack graph [6, 7, 9]. Among them, the nodes represent the conditions of using vulnerability (the necessary resources and permissions of exploiting the vulnerability) and the use of the vulnerability of the atomic attack action; the directed edge represents the dependency between nodes, clearing the probability of attack process distribution conditions can be intuitive to show all the attack paths that may exist in the internal network. The formal definitions of the attack graph and its constraints are as follows.

Definition 1 (attack graph model [7, 10]). $\mathrm{AG} = (S, A, O, E, P)$ is a directed acyclic graph.

(i) S represents the system resource state node set, $S = s_0 \cup s_i \cup s_e$ $(i = 1, 2, \ldots, e)$, where s_0 represents the initial node, describing the resource state that the attacker has occupied at the first time. s_i represents a single resource state node that describes the resources which an attacker gets during an attack. s_e represents the target resource state node that describes the attacker's final attack target.

(ii) A represents the set of attack action nodes, and a_i represents an atomic attack.

(iii) O denotes the set of monitoring event nodes. The value of node o_i can be T or F, which indicates whether the attack behaviors of a_i have been detected. When an attack action a_i occurs, the security monitoring system can capture these actions and provide the appropriate evidence of the attack recorded in the alarm log.

(iv) E represents the set of directed edges between nodes. The attack graph defined in this paper is a directed acyclic graph; the edges between the various nodes are directed edges. $E = E_a \cup E_b \cup E_c$, E_a is $S \times A$, represents the attacker has some resources before they can initiate an attack; $E_b = A \times S$ represents the attacker could get some resources in the condition of the attack action success; $E_c = A \times O$ represents the corresponding attack evidence of the attack action captured by the security monitoring system.

(v) P represents the probability of attack, $P = P_A \cup P_{\mathrm{AS}}$, where P_A represents the probability that the attack behavior a_i occurs after having some resources; that is, the probability of attacking the attack action node, P_{AS}, represents the probability that a_i succeeds into the next resource state s_i, that is, the success probability of attack action.

(4) The Directed Edges Relationship. Considering the attack graph is a directed acyclic graph, it is necessary to effectively define the relationship between the edges which point to the same node, including "AND" and "OR" relationship. The specific content is Definition.

Definition 2 (directed edges relationship).

(i) The "AND" relationship between two state nodes s_i and s_j, indicating that the attacker needs to have both of the resources in order to carry out the next attack.

(ii) The "OR" relationship between two state nodes s_i and s_j, indicating that if the attacker has any of these two resources, he can proceed to the next attack.

```
Procedure IsAvailableMonitor
Input: AO, EO
//AO - Sequence of attack evidence of a monitoring event node in the alarm log;
//EO - Attack evidence sequence of the corresponding atomic attack action
Output: The confidence value of the monitoring event node
Method:
String function(AO)
initialize EO
A= getS(AO)
t=0
S={}
for i=1:EO.size()
    count=0;
    for j=1:A.size()
        n=j, m=i
        while (A(n)==EO(m) && m<=A.size()&&n<=EO.size())
            count++, m++, n++;
    t++;
    S{t}=count
f=max(S)
if (f>= EO.size()) return True;
else return False;
```

Pseudocode 1: The pseudocode of confidence analysis.

(iii) The "AND" relationship between two attack action nodes a_i and a_j, indicating the attacker needs two attack actions to occupy the next state node.

(iv) The "OR" relationship between two attack action nodes a_i and a_j, indicating that the attacker can send any attack to occupy the next state node.

(v) There is a "OR" relationship between two attack action nodes pointing to the same monitoring event node o_i; that is, any attack action can independently trigger o_i.

(5) Temporal Difference Relationship. The temporal difference relationship means that if the monitoring event node a_i is detected by the security monitoring system earlier than the monitoring event node a_j all the time, then we could say the monitoring events a_i and a_j have a temporal difference relationship.

3.3. The Method of Attack Graph Simplification. Although the time complexity of the current attack graph generation algorithm [10] can be controlled in $O(n^2)$ (n is the number of hosts in the network) [11], the network structure becomes more and more complex and the connection between the various terminal nodes becomes more and more close, resulting in an increasingly complex attack graph structure. But the happening probability of some attack paths is very low or does not satisfy the current actual situation. The removal of these paths does not influence the whole metric model, and even their existence only increases the amount of subsequent work. Therefore, we propose the monitoring event node to prune the attack path in attack graph to simplify the whole structure of attack graph.

(1) Pruning Attack Nodes with Confidence Analysis. The alarm log as input, we reference the attack evidence confidence analysis algorithm defined by Wang et al. [6]; the probability of basic action of attack evidence covers the basic action set in atomic attack determining the confidence of monitoring event. For example, assume the basic attacks contained in the atomic attack are $a = \{\mathrm{ba}_1, \mathrm{ba}_2, \mathrm{ba}_3, \mathrm{ba}_4\}$. If the attack evidence provided by the security monitoring system is $a_1 = \{\mathrm{ba}_1, \mathrm{ba}_5, \mathrm{ba}_7, \mathrm{ba}_2, \mathrm{ba}_3\}$, the coverage rate is 0.75, and the attack evidence value of $a1$ is F. Assuming another evidence is $a_2 = \{\mathrm{ba}_7, \mathrm{ba}_1, \mathrm{ba}_2, \mathrm{ba}_3, \mathrm{ba}_5, \mathrm{ba}_4, \mathrm{ba}_6\}$, the coverage rate is 1, and the attack evidence confidence value of a_2 is T. Then we should remove all the attack action nodes of the attack evidence confidence value F. The pseudocode implementation of the algorithm is shown in Pseudocode 1.

The complexity of confidence analysis is $g(n) = O(kn)$, n is the number of atomic attack nodes, and k is the number of basic attacks. Because the number of basic attacks is a constant, we can get $g(n) = O(kn) = O(n)$.

(2) Pruning Paths with Temporal Difference Relationship. According to the alarm log provided by the security monitoring system, we can obtain the temporal difference relationship of the monitoring event node. Then prune the path of the existing attack graph with temporal difference relationship; the attack paths would be deleted which do not match the temporal difference relationship; otherwise the attack paths will be preserved. Finish all these jobs, and the simplified work of the attack graph is completed.

For example, in Figure 2, the cycle a_i is the basic action of attack evidence, the square s_j is the state node of hosts [6], and the cycle o_k is the monitoring event nodes. We could know

```
Procedure IsTemporalDifferenceRelationship
Input: G,Otd,O1,O2,Wo1,Wo2
//Attack graph G; Otd --The temporal difference relationship of the
//monitoring event nodes; O1,O2 -- Two monitoring event nodes of
//temporal difference relationship; Wo1, Wo2 -- Two sets of sequence
//that let the values of O1,O2 are T.
Output: Whether there is a timing difference between Wo1 and Wo2,
"Yes" or "No".
Method:
(01) b←G //The topological sequence of attack action nodes
(02) if((O1→O2)∈ Otd)
(03)     foreach(A1∈Wo1,A2∈Wo2)
(04)         if((A2→A1) ∈ b) return No;
(05)     end for (03)
(06)     return Yes;
(07) else (02)
(08)     return Yes;
(09) end if (02)
```

Pseudocode 2: The pseudocode of confidence analysis.

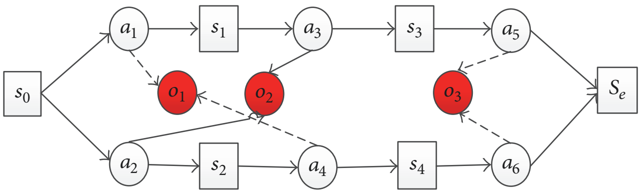


Figure 2: The temporal difference relationship.

there are two paths from the initial state node s_0 to the final target node s_e.

Path 1: $s_0 \rightarrow a_1 \rightarrow s_1 \rightarrow a_3 \rightarrow s_3 \rightarrow a_5 \rightarrow s_e$

Path 2: $s_0 \rightarrow a_2 \rightarrow s_2 \rightarrow a_4 \rightarrow s_4 \rightarrow a_6 \rightarrow s_e$.

If we do not consider the temporal difference relationship between the monitoring event nodes, then the conclusion is that the attack is likely to have two attack paths. But when we consider the temporal difference relationship of the monitoring event nodes, the temporal difference relationship of the monitoring event nodes in Figure 2 is $o_1 \rightarrow o_2 \rightarrow o_3$. Because Path 2 triggers the monitoring event o_2 at the first time, not matching the temporal difference relationship of the monitoring event nodes provided by the security monitoring system, Path 2 should be deleted. Similarly, if the temporal difference relationship is $o_2 \rightarrow o_1 \rightarrow o_3$, delete Path 1 that needs to be deleted. The pseudocode implementation of the algorithm is shown in Pseudocode 2.

The complexity of the temporal difference relationship is decided by the number of attack paths in attach graph which shows that the problem is NP-hard. According to attack graph generation algorithm [10], it can be controlled in $O(n^2)$ (n is the number of hosts in the network).

According to the above definition, we designed the schematic diagram of attack graph simplification in Figure 3.

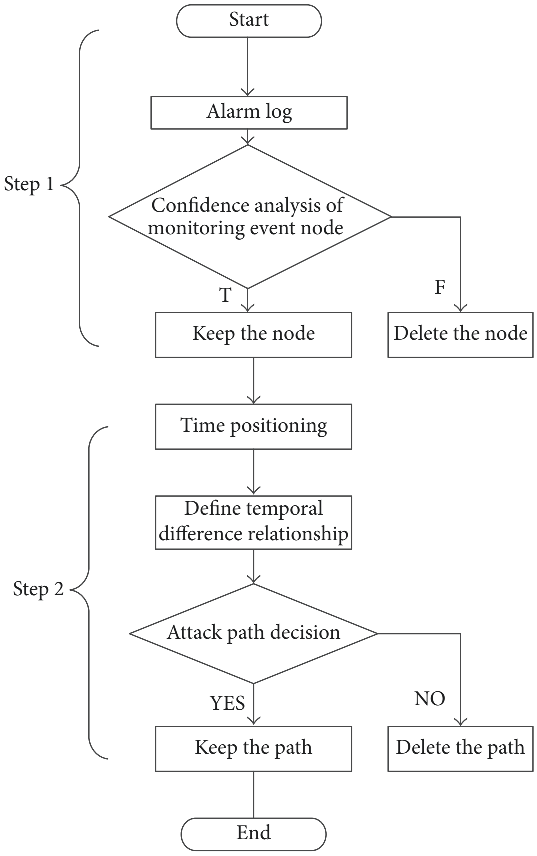


Figure 3: The schematic diagram of attack graph simplification.

The two steps in Figure 3 would simplify attack graph. By the monitoring event nodes confidence analysis and the temporal difference relationship of monitoring events, we can remove the interference attack graph nodes and attack

Table 1: The weight value of hosts.

Name	Host location	Indicator value	Description
H_i	Office network	2	Host is located on the office network, easy to be used
	Core network	1	Host is located on the core network, difficult to be used

paths and improve the efficiency and accuracy of our security metric.

3.4. The Method of Attack Probability Calculation. After the attack graph simplification, each subpath is a subprocess in which the attackers initiate an atomic attack by using the vulnerability state of the current resource state and obtain more resource states after attacking. Therefore, we propose an approach for dividing the attack graph nodes into key-value pairs composed of "resource state node, attack action, and resource state node." The probability of key-value pairs is defined as $P = (P_A, P_{\text{AS}})$. P_A is the probability of attack action, which represents the probability from the first resource state node to the attack action node; P_{AS} means the probability from the attack action node to the next resource state node, also called the probability of attack success.

This paper proposes the cumulative reachable probability calculation method for target node with the simplified attack graph. The specific steps are as follows.

(1) Divide the Key-Value Pairs. According to the dependency relationship between the simplified attack graphs, divide all nodes and edges into the key-value pairs in the form of "resource state node, attack action, and resource state node."

(2) Calculate the Initial Attack Probability. (a) The probability of an attack action is P_A.

The formula is

$$P_A = \frac{\left(V_s + H_i\right)}{12}. \tag{1}$$

H_i represents the weight where the host is located. The location of the host in the internal network is different, so the weight will be different, as shown in Table 1. The internal network is divided into the core network and the office network.

V_S represents its own probability, which indicates the probability of being used vulnerability. According to the CVSS metric method of individual vulnerabilities: Access Vector (AV), Authentication (AU), and Access Complexity (AC) [9] are shown in Table 2.

The formula is

$$V_S = \text{AV} + \text{AU} + \text{AC}. \tag{2}$$

(b) The attack action success probability is P_{AS}, which could assess the success probability for a vulnerability that the attackers use it to attack. The influencing factors include the information of vulnerability (K), the method of atomic attack (M), and whether corresponding attack tool is used (N). Based on the relevant research papers, with reference to the calculation method of the success rate of independent vulnerability from CVSS and Wu et al. [12], consider the following.

Table 2: The CVSS metric method of individual vulnerabilities.

Name	Degree of difficulty	Indicator value	Description
AC	High	1	The vulnerability is very difficult to use
	Medium	2	The vulnerability is a little difficult to use
	Low	3	The vulnerability is easy to use
AU	Multiple	1	The vulnerability is difficult to use
	Single	2	Vulnerability is a little difficult to use
	None	3	The vulnerability is easy to use
AV	Local	1	The vulnerability only can be used locally and difficulty
	Adjacent network	2	The vulnerability can be used and is harder to use
	Network	3	The vulnerability can be exploited remotely and easily

The formula is

$$P_{\text{AS}} = K + M + N, \tag{3}$$

where K is in the range of $\{0, 0.1\}$, indicating whether the vulnerability information is published. The vulnerability has been issued; K value is 0.1; otherwise, the value is 0.

Here, M is in the range of $\{0, 0.2, 0.4\}$, indicating whether the atomic attack method or step is currently available. If the vulnerability has a detailed attack step scheme, then the value of M is 0.4. If there is a simple attack scheme, then M is 0.2. Otherwise, M is 0.

N is in the range of $\{0, 0.2, 0.4\}$, indicating whether the attack tools are required in the atomic attack. If the vulnerability is not required to use the attack tools, N is 0.4. If the vulnerability exploited needs to use the attack tools and the corresponding attack tools are available, N is 0.2; and if you need to use the attack tools, but there are no available attack tools, the value of N is 0.

(3) Calculating the Cumulative Reachable Probability of Attack Action Node P_{AC}. P_{AC} means the cumulative reachable probability of attack action except for the initial node. Due to the complexity of the internal network, we will discuss the classification of the key-value pairs with the directional edges.

(a) The cumulative occurrence probability of common key-value pairs: normally, there is only one directed edge of an action node; that is, after obtaining the resources of one resource node, you can use the vulnerability to attack.

Therefore, when an atomic attack is initiated, the attack probability of all the front nodes is evaluated, and the value

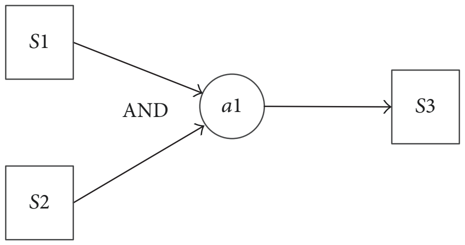


Figure 4: The "AND" relationship between two resource state nodes.

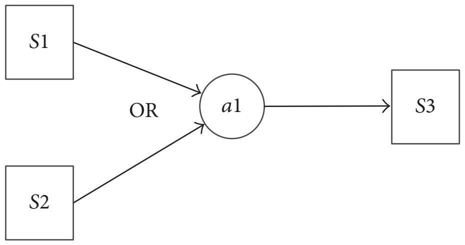


Figure 5: The "OR" relationship between two resource state nodes.

is the cumulative reachable probability of the first resource state node in the key-value pair. Then, we can calculate the cumulative reachable probability of current action node.

The formula is

$$P_{\mathrm{AC}} = P_S \times P_A. \tag{4}$$

P_S represents the cumulative reachable probability of the first resource state node in a key-value pair and P_A represents the probability of the attack action carrying out the attack.

(b) The directed edges to the same attack action with "AND" relationship.

The form is shown in Figure 4.

The formula is

$$P_{\mathrm{AC}} = P_{Si} \times P_{Sj} \times P_A. \tag{5}$$

P_{Si}, P_{Sj} represent the cumulative reachable probability of two resource state nodes pointing to the same attack action.

(c) The directed edges to the same attack action with "OR" relationship.

The form is shown in Figure 5.

The formula is

$$P_{\mathrm{AC}} = \left(P_{Si} \oplus P_{Sj}\right) \times P_A. \tag{6}$$

(4) Calculating the Cumulative Reachable Probability Ps for the Target Node. (a) The cumulative reachable probability of common resource state node. In the usual case, there are only one directed edge points to the resource state node. That means to obtain another resource state node only one vulnerability is needed.

The formula is

$$P_{Si} = P_{\mathrm{AC}} \times P_{\mathrm{AS}}. \tag{7}$$

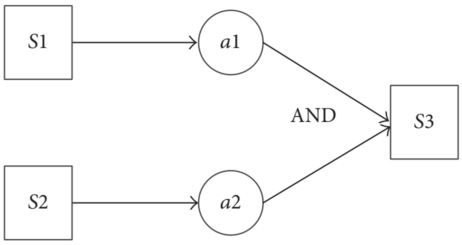


Figure 6: The "AND" relationship between two attack action nodes.

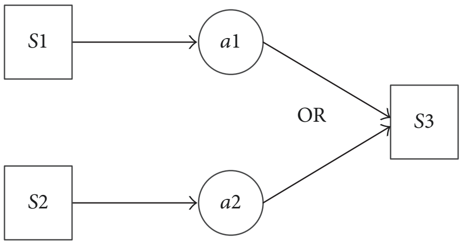


Figure 7: The "OR" relationship between two attack action nodes.

(b) The directed edges to the same resource state node with "AND" relationship, as shown in Figure 6.

The formula is

$$P_{Si} = \left(P_{\mathrm{AC1}} \times P_{\mathrm{AS1}}\right) \times \left(P_{\mathrm{AC2}} \times P_{\mathrm{AS2}}\right). \tag{8}$$

(c) The directed edges to the same resource state node with "OR" relationship.

The concrete form is shown in Figure 7.

The formula is

$$P_{Si} = \left(P_{\mathrm{AC1}} \times P_{\mathrm{AS1}}\right) \oplus \left(P_{\mathrm{AC2}} \times P_{\mathrm{AS2}}\right). \tag{9}$$

The complexity of the method of attack probability calculation is decided by the number of atomic attack nodes. According to attack graph generation algorithm [10], we can get a certain attack graph, so it is countable but is not predictable.

4. Experiment and Analysis

4.1. Experiment Environment. To verify the method proposed in this paper, we build a representative virtual simulation environment of an internal network which comprised hosts with VMware and network devices with GNS3. The key network topology is shown in Figure 8.

The firewall isolates the network structure into two parts, the external network and the internal network. The hosts in office network are as follows: Host 0 is an ordinary computer with Windows system for office users; Host 1 is the DNS server, which provides DNS services for all internal network hosts; Host 2 is the Web server and provides HTTP service for all internal network hosts. The hosts in the core network are as follows: Host 3 and Host 4 provide SSH services, with Linux system; Host 5 is the FTP server; Host 6 is the database SQL server.

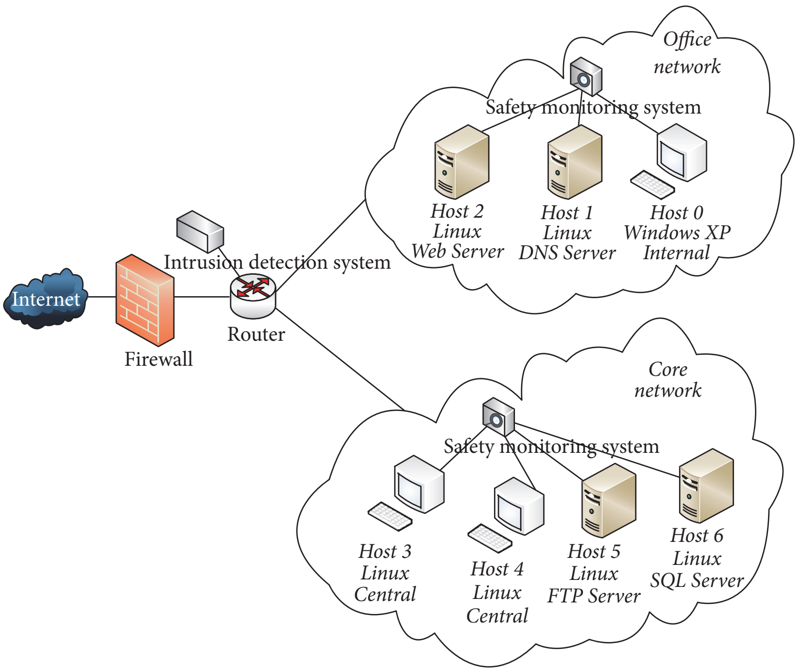


FIGURE 8: The network topology diagram.

TABLE 3: The vulnerability information for each terminal.

Host	Name of software	Vulnerability description	CVE ID
H1	BIND 9	Stack buffer overflow vulnerability	CVE-2015-7547
H2	IIS 7.0	IIS Buffer Overflow Vulnerability	CVE-2008-0075
H3	OPENSSH (SSH2)	Mode information disclosure vulnerability	CVE-2008-5161
		Local privilege elevation vulnerability	CVE-2007-2063
H4	OPENSSH (SSH2)	Mode information disclosure vulnerability	CVE-2008-5161
		Local privilege elevation vulnerability	CVE-2007-2063
H5	Ser-U 10.5.0.19	Read the vulnerability	CVE-2015-7601
		FTP buffer overflow vulnerability	CVE-2015-7768
H6	SQLServer 2005	Buffer Overflow Vulnerability	CVE-2008-0086
		Information disclosure and buffer overflow vulnerability	CVE-2008-0106

The security monitoring system is deployed in the two subnetworks to monitor the hosts; then we could obtain the appropriate attacking alarm log. The specific security monitoring systems include the OSSEC intrusion detection system, which monitors the abnormal activities of the host PC and the Trojan horse and Tripwire security monitoring tools deployed on the file server for system integrity check.

The attacker originally owns the resources as normal staff user on Host 0 in the office network. The final target is to get the root privilege of Host 5 or Host 6 in the core network. At the first time, the corresponding security policies are as follows: (1) the office network Web server Host 2 and DNS server Host 1 provide internal network service for internal users; all internal hosts can connect to the office network by accessing the services on Host 1 and Host 2. (2) Host 4 in the office network is allowed to access the SQL services on Host 6 for specific data but cannot browse all information and could not modify or download; (3) Host 3 and Host 4 in the core network are allowed to access the rest of the terminals and the corresponding services and own the permissions to modify specific data.

We scanned the vulnerabilities on each host with Nessus. The vulnerability scanned results and related information of each host are shown in Table 3.

The security monitoring system was deployed to monitor the hosts; we could obtain the appropriate attacking alarm log. The specific security monitoring systems included the OSSEC intrusion detection system, which monitored the abnormal activities of hosts and the Trojan horse, and Tripwire security monitoring tools are deployed on FTP server and SQL server for system integrity check.

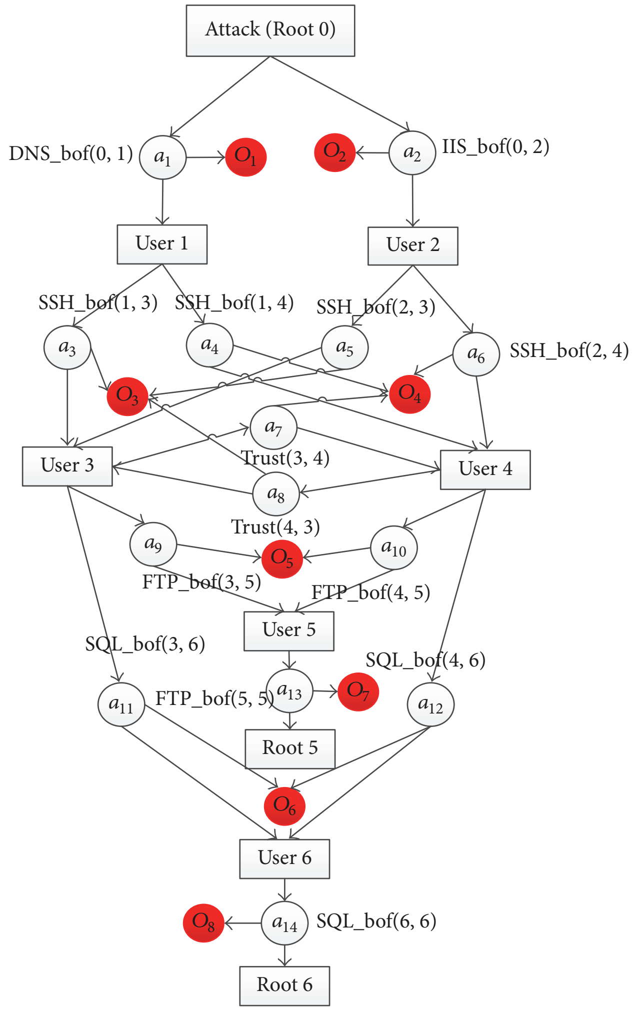


FIGURE 9: The initial attack graph.

4.2. Experiment Verification. After determining the topology of the internal network and the information of each terminal, attack graph automatic generation algorithm would help us to generate the attack graph of the internal network, and the atomic attack edges pointing to the same resource state node all present "OR" relationship. The concrete structure is shown in Figure 9.

In Figure 9, the rectangle represents the resource state node and the resource rights that can be obtained after each atomic attack; the hollow circle represents the atomic attack action node and marked the corresponding terminal vulnerability on the left or right side of the atomic attack; the red solid circle is the monitoring event node.

According to the method of attack graph simplification, we got the simplified attack graph in Figure 10. We can simplify the attack graph with the temporal difference relationship of monitoring event node, removing the attack paths that do not match the temporal difference relationship.

After simplifying the attack graph, we can divide the simplified attack graph into key-value pairs and calculate the cumulative reachable probability for target nodes. The key-value pairs and attack probability are shown in Table 4.

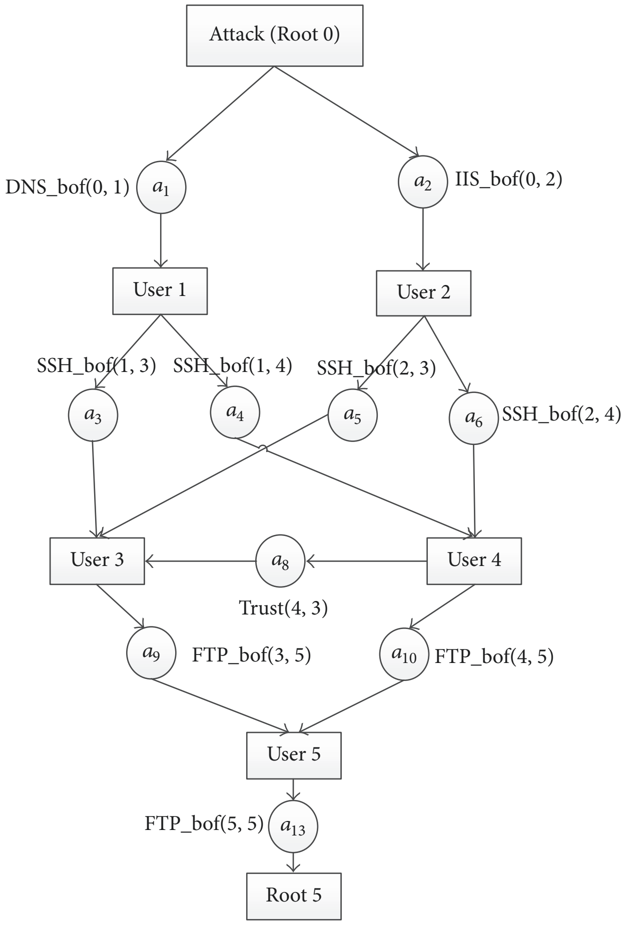


FIGURE 10: The simplified attack graph.

TABLE 4: The key-value pairs with attack probability.

Key-value pair	Attack probability ((P_A, P_{AS}))
(Root 0, a_1, User 1)	(0.83, 0.7)
(Root 0, a_2, User 2)	(0.92, 0.5)
(User 1, a_3, User 3)	(0.67, 0.3)
(User 1, a_4, User 4)	(0.67, 0.3)
(User 2, a_5, User 3)	(0.67, 0.3)
(User 2, a_6, User 4)	(0.67, 0.3)
(User 4, a_8, User 3)	(0.58, 0.5)
(User 3, a_9, User 5)	(0.83, 0.7)
(User 4, a_{10}, User 5)	(0.83, 0.7)
(User 5, a_{13}, Root 5)	(0.83, 0.7)

The cumulative reachable probability values for subresource state nodes and target node are shown in Table 5.

The cumulative reachable probability from H0 to H5 is 3.95% by using the other terminal's vulnerabilities. Compared with the frequency of internal attacks and the safety reports of the enterprise system from daily inspection, the two values are basically in line. Based on such an internal network, where the attacker only has privilege in the office network, the

TABLE 5: The cumulative reachable probability for target nodes.

Subresource state node	Cumulative reachable probability
User 1	0.581
User 2	0.46
User 3	0.117
User 4	0.117
User 5	0.068
Root 5	0.0395

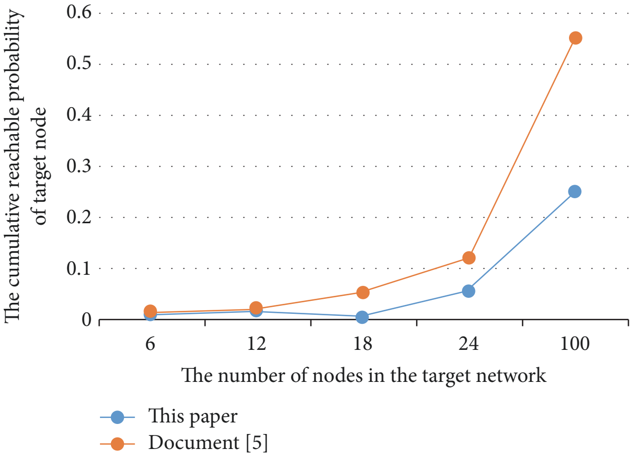


FIGURE 11: The comparison of cumulative reachable probability.

probability of stealing the core data successfully is relatively low.

4.3. Experiment Analysis. In order to assess the accuracy of our method, we performed five times' experiments with different cumulative reachable calculation method of target node on the same internal network. We compared the data based on the attack probability of the attack graph proposed by Li et al. [5] with the data obtained by the method proposed in our paper. The results are shown in Figure 11, the abscissa indicates the number of target network nodes and the ordinate indicates the cumulative reachable probability of target node.

Comparing the data in Figure 11, the cumulative reachable probability of target node changed more smooth and more stable with our method than Li et al. [5] that our security metric should be more accurate than Li et al.'s [5].

At the same time, the approach we proposed could prune the attack graph paths and not only reduce the calculation greatly but also improve the accuracy of the attack graph obviously. Therefore, the computational effort is absolutely less than Document [5], as shown in Figure 12.

5. Conclusion

In our paper, we propose an internal network security metric method based on attack probability to solve the problem of the existing security metrics based on attack graph lacking the applicability of the internal network. We use the monitoring event node and the temporal difference relationship to simplify the attack graph, put forward the concept of the key-value pair to analyze the attack graph, and propose the calculation method of cumulative reachable probability for different kind of target nodes based on vulnerabilities with CVSS metric indicators and the directed edges relationship. The simulation results show that the method of attack graph simplification has a significant improvement in efficiency, and the method of attack probability calculation improves the quantitative analysis accuracy obviously. The next step of the work will focus on the refinement attack probability calculation, finding a more comprehensive internal network to improve the accuracy of the final probability value.

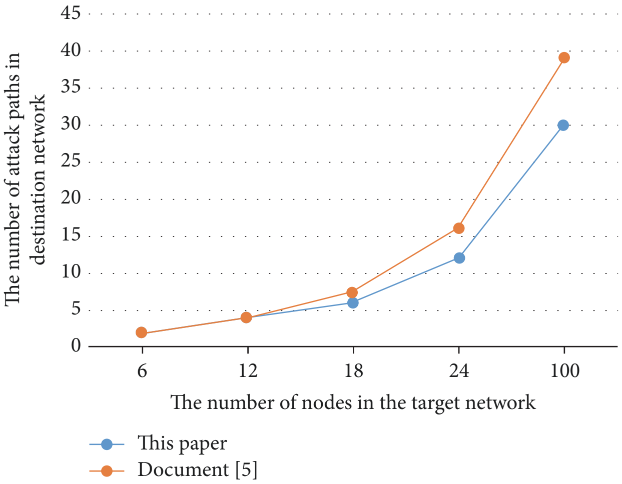


FIGURE 12: The comparison of attack paths.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This article is supported by National Key R&D Program of China (Grant no. 2016YFB0800700) and National Natural Science Foundation of China (Grant no. U1636115).

References

[1] G. Yang, J. Ma, and A. Yu, "Study on internal threat detection," *Journal of Information Security*, vol. 1, no. 3, 2016.

[2] X. Lu, "Research on information system security metrics theory and method," *Computer Science*, vol. 35, no. 11, pp. 42–44, 2008.

[3] P. Xie, J. H. Li, X. Ou et al., "Using Bayesian networks for cyber security analysis," in *Proceedings of the IEEE/IFIP International Conference on Dependable Systems & Networks*, vol. 23, pp. 211–220, 2010.

[4] L. Wang, T. Islam, T. Long et al., "An Attack Graph-Based Probabilistic Security Metrics," in *Proceedings of the Conference on Data & Applications Security XXII*, 5094, pp. 283–296, 2008.

[5] Q. Li, B. Wang, X. Wang et al., “Network security measurement method based on probability of attack graph node,” *Application Research of Computers*, vol. 30, no. 3, pp. 906–908, 2013.

[6] H. Wang, G. Yang, and D. Han, “Study on internal threat prediction based on bayesian networks,” *Application Research of Computers*, vol. 30, no. 9, pp. 2767–2771, 2013.

[7] S. Zhang, G. Li, S. Song et al., “Application of Bayesian Reasoning in the Confidence Calculation of Attack Graph Node,” *Journal of Software*, vol. 21, no. 9, pp. 2376–2386, 2010.

[8] N. Poolsappasit, R. Dewri, and I. Ray, “Dynamic security risk management using Bayesian attack graphs,” *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 61–74, 2012.

[9] X. Chen, B. Fang, Q. Tan et al., “Study on inference algorithm of internal attack intention based on probability attack graph,” *Journal of Computers*, vol. 37, no. 1, pp. 62–72, 2014.

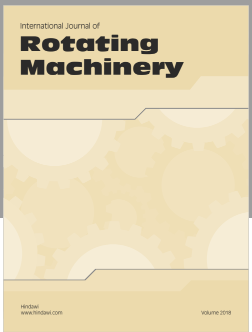
[10] Y. Ye, X.-S. Xu, Y. Jia, and Z.-C. Qi, “An attack graph-based probabilistic computing approach of network security,” *Jisuanji Xuebao/Chinese Journal of Computers*, vol. 33, no. 10, pp. 1987–1996, 2010.

[11] X. Ou, S. Govindavajhala, and A. W. Appel, “MULVAL: a logic-based network security analyzer,” in *Proceedings of the 14th Usenix Security Symposium*, pp. 113–117, Baltimore, MD, USA, 2005.

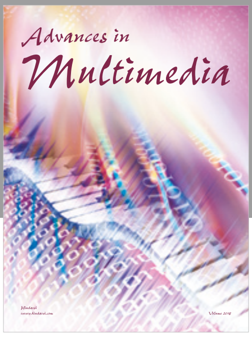
[12] D. Wu, D.-G. Feng, Y.-F. Lian, and K. Chen, “Efficiency evaluation model of system security measures in the given vulnerabilities set,” *Journal of Software* , vol. 23, no. 7, pp. 1880–1898, 2012.

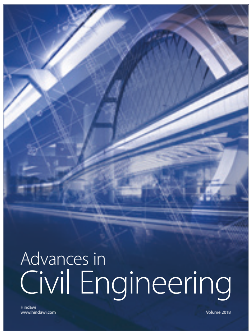
Journal of
Engineering

The Scientific
World Journal

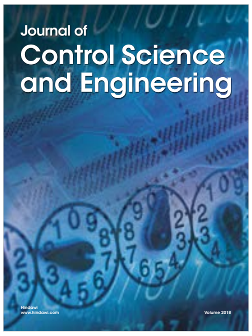

International Journal of
Rotating
Machinery

Journal of
Sensors

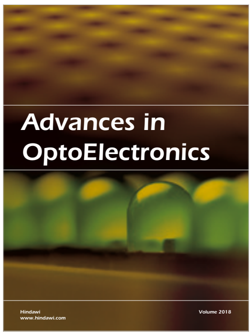

Advances in
Multimedia


Advances in
Civil Engineering

Journal of
Robotics

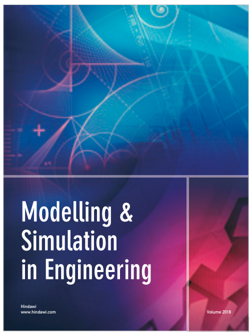

Journal of
Control Science
and Engineering

Journal of
Electrical and Computer
Engineering

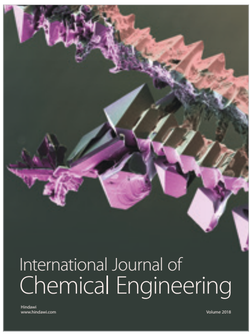

Advances in
OptoElectronics

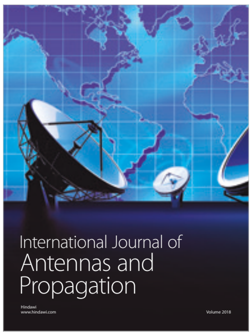
VLSI Design

International Journal of
Navigation and
Observation

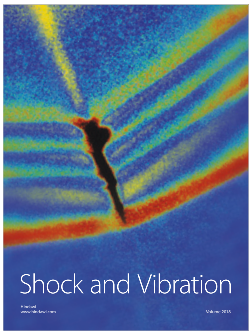

Modelling &
Simulation
in Engineering

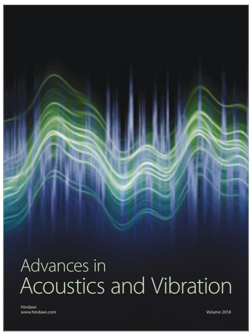
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration