Attack path prediction based on Bayesian game model

Pengyu Sun*, Hengwei Zhang*,† and Chenwei Li
PLA SSF Information Engineering University, Zhengzhou 450001, China
*These authors contributed equally to this work
†Corresponding Author: Hengwei Zhang. Email: zhw11qd@aliyun.com

Abstract: The current network risk assessment model often ignores the impact of attack cost and intrusion intention on network security. In order to better solve the problem of information security defense strategy selection and accurately assess the target network risk, this paper proposes an attack path prediction method based on game model. The atomic attack probability is calculated by vulnerability value, attack cost and attack benefit. The static risk assessment model is established combined with Bayesian belief network quantitative attack graph. And the dynamic update model of intrusion intention is used to realize the effective prediction of attack action under rational assumption, which provides the basis for dynamic defense measures of attack surface. The experimental results verify the feasibility and effectiveness of the model and method.

1. Introduction
With the rapid development of information, network technology and the popularization of all kinds of network infrastructure, network system has become the key support for the effective operation of all walks of life. However, how to grasp the current network security situation in the complex and changeable network environment in real time, how to carry out early warning and protection against the security situation in advance, and how to reduce the damage of network attacks, are the primary tasks of network security work.

The traditional intrusion detection system (IDS) can only analyze the dependency relationship between node vulnerabilities after the attack, and then monitor the attack behavior, which belongs to passive defense [1]. In the 1990s, Phillips et al. [2] firstly proposed the concept of attack graph, which used the configuration information of the attacked nodes, the causal relationship between nodes and the ability of attackers to generate attack graph, and applied it to the analysis of network vulnerability. Attack graph can intuitively display the details of attack behavior which includes target network, vulnerability, attack path, etc. [3], provide support for predicting the attack intention and subsequent attack behavior of attackers, as well as facilitate administrators to deal with sudden network intrusion events in time [4]. Lei Cheng et al. [5] in order to defend the mobile targets in the network and calculate the cost and benefit, established a hierarchical network resource graph by using the attack graph. Combined with the change point detection method, a network mobile target defense effectiveness evaluation method based on the change point detection was proposed, which effectively improves the construction efficiency of the network resource graph.

The above studies have established different network security risk assessment models based on attack graphs, but the assessment indicators of atomic attack probability are too single to truly reflect the possibility of attackers choosing the target network and attack path. This paper establishes a static network intrusion intent analysis model based on Bayesian attack graphs. The main work and
innovations are as follows.  
(1) Considering the complex factors that affect the attacker’s attack behavior, the atomic attack probability is calculated from the three aspects of vulnerability value, attack cost and attack profit, which better reflects the use of the vulnerability in the actual network.  
(2) Combining the Bayesian belief network and the attack graph, a static risk assessment model for attack intention is established. The model is used to work with complex networks with constantly changing security elements, so as to improve the accuracy of risk assessment.  
(3) The attack path is generated and the total reachability probability of the path is calculated to realize the prediction of the attack path, avoiding the influence of the vulnerability of a single network node on the path selection, and improves the accuracy of the prediction.

2. Bayesian attack graph establishment

Attack graph can be divided into state attack graph and attribute attack graph. The state attack cannot cope with the rapid growth of state nodes, and its structure is not intuitive enough, so it is not suitable for large-scale network. Each attribute vertex in the attribute attack graph is an independent security element, which avoids the problem of the state of the explosive state attack graph. Therefore, attribute attack graph has better adaptability to complex large-scale network. In order to calculate the probability of vertex arrival in attack schedule and the possible path of attack, Bayesian belief network is used to describe the causal relationship between attacks. Combined with the graph structure of attack graph, Bayesian attack graph is created to evaluate the risk of target network.

2.1. Bayesian attack graph definition
The $BAG$ (Bayesian attack graph) is a directed acyclic graph, which can be expressed as $BAG = (R, S, E, V, p)$, and the specific definition is as follows.

(1) $R$ is a collection of attribute nodes, divided into three categories, namely $R = R_{start} \cup R_{transition} \cup R_{target}$, where $R_{start}$ is the initiating node of the network attack, $R_{transition}$ is the process node of the attack behavior, and $R_{target}$ is the target node of the attacker. Among them, $R_i = \{0, 1\}$, 1 means that the attacker has successfully used the attribute node vulnerability to occupy the node, and 0 means that the node is not occupied.  

(2) $S = \{S_i | i = 1, 2, \ldots, n\}$ is the set of atomic attacks, which represents the attacker's attack on node vulnerabilities, that is, the migration method of attribute nodes, which can be expressed as $S_i : R_{pre} \rightarrow R_{next}$.  

(3) $E = \{E_i | i = 1, 2, \ldots, n\}$ is the set of directed edges in the attack graph, representing the causal relationship of attack behaviors between attribute nodes, where $(R_{pre}, R_{next}) \in E$ represents a directed edge attacking $R_{next}$ from $R_{pre}$.  

(4) $V$ represents the relationship between the parent and child attribute nodes, which can be represented by the two-tuple $< R_j , d_j >$, $d_j \in \{AND, OR\}$. Among them, $AND$ means that the attack can only be completed when the state of all parent nodes is true; $OR$ means that as long as the status of one of the parent nodes is true.  

(5) $p$ is the static reachability probability of the attribute node in the attack graph.

2.2. Bayesian attack graph structure establishment
The structure of the Bayesian attack graph is similar to that of the general attack graph. This article uses a modeling method to generate the main structure of the attack graph. An example is shown in Figure 1.
In Figure 1, $R_0$ is the initiating node of the attack, $R_1$ and $R_2$ are process attribute nodes, which are the target network nodes of the attacker. $S_1, S_2, S_3, S_4, S_5,$ and $S_6$ are atomic attacks. **AND** means that both the atomic attack and the arrived attack strategy are true, the attack can be realized; **OR** means that as long as one of the atomic attack and the arrived attack strategy is true, the attack can be realized, that is, the two attack paths shown in Figure 1 can complete any one of them. The attack on the target node can be completed.

### 2.3. Bayesian attack graph quantification

The value of vulnerability is related to the complexity and impact of attribute node vulnerability, which is usually quantified the Common Vulnerability Scoring System (CVSS) [6] provided by the National Common Vulnerability Database (NVD) of the United States. In this paper, according to CVSS quantitative standard, vulnerability is quantified by three indicators: availability, impact and scope. If the attacker attacks the vulnerability, the value of the vulnerability will be considered according to the existence and impact of the vulnerability. Therefore, in order to quantify the vulnerability value, we first need to calculate the vulnerability estimation value representing the vulnerability value, and its formula is:

\[
\text{Score} = \begin{cases} 
\min\left(1.08(\text{Exp} + \text{Impact}), 10\right), & \text{Scope}=C \\
\min(\text{Exp} + \text{Impact}, 10), & \text{Scope}=U
\end{cases}
\]

\[
\text{Impact} = \begin{cases} 
7.52((\text{ISC} - 0.029) -3.25 \left((\text{ISC} - 0.02)^{15}\right)), & \text{Scope}=C \\
6.42\text{ISC}, & \text{Scope}=C
\end{cases}
\]

\[
\text{ISC} = 1 - \left((1-C)(1-I)(1-A)\right)
\]

\[
\text{Exp} = 8.22\text{AV} \cdot \text{AC} \cdot \text{PR} \cdot \text{UI}
\]

Among (1), Impact represents the vulnerability impact factor, Exp represents the vulnerability utilization factor, ISC represents the intermediate variable, the constant 10 represents the maximum value of Score, and the other constant coefficients are set by CVSS according to the security policy.

**Definition 1** Vulnerability value indicates the possibility that an attacker exploits a vulnerability for the vulnerability $v_i$, using $\text{value}(v_i)$ to represent its vulnerability value, and the size is related to
the vulnerability score. Since the standard vulnerability score range is \([0,10]\), in order to facilitate subsequent probability calculations, the calculation formula of \(\text{value}(v_i)\) is:

\[
\text{value}(v_i) = \frac{\text{Score}}{10} \times 100\%
\]  

(2)

3. Construction of Bayesian attack and defense game model

3.1. Basic assumptions of the model

In the actual information security attack and defense game, attackers are often the originator of the game. The defenders respond according to the existing strategies. Neither party can observe the actions of the other party before the action, so both sides can be regarded as simultaneous actions. The establishment of the game model of attack and Defense meets the following three basic assumptions.

Assume 1 (Rational people assume) Assume that the attacker and the defender are completely rational, the attacker and the defender choose strategies according to the principle of maximizing their own benefits.

Assume 2 (Benefit assume) It is assumed that the game gains are evaluated based on the economic value of information assets.

Assume 3 (Type assume) Assume that the defender has a priori judgment on the probability distribution of the attacker type, and the defender type is the common information of the attacker and the defender [7].

3.2. Model definition

Generally speaking, the components of an offensive and defensive game mainly include players, strategy and payoff function. The strategy execution effect of both offense and defense is not only related to their own strategy, but also closely related to the other's strategy. This is the principle of “strategic dependence” and the basic characteristic of the game process [8].

Definition 2 ADG(attack-defense game) The information security attack-defense game can be described by the quintuple \(ADG = (N,T,H,P,U)\), and its specific meaning is as follows:

(1) \(N\) represents the collection of players participating in the offensive and defensive game. In the network offensive and defensive game, the participants are the main body of strategy selection and the strategy makers. In most of the network offensive and defensive games, the two sides of the game can be regarded as a two-player game of attacker \(A_a\) and defender \(A_d\).

(2) \(T\) represents the type space of attacker \(A_a\) and defender \(A_d\). Based on the possible actions and benefits of the attacker, and the defender's understanding of the attacker, this article divides the attackers into adventurous attackers \(A_a^h\) and conservative attackers \(A_a^l\). Adventurous attackers are willing to pay more for more frequent and longer attacks in order to obtain a higher attack success rate; but the defender collects relevant information and evidence, and then implements legal accountability or counter attacks. The probability is also higher. Conservative attackers tend to attack at a lower cost, and their attack success rate is relatively low; but the probability of being held accountable by law or countering attacks is also low.

(3) \(H\) is the action space of participants in the network attack and defense game. In this article, define the attacker's action space as the attack strategy set \(AS = \{A_i | 1 \leq i \leq m\}\), and the defender's action space as the defense strategy set \(DS = \{D_j | 1 \leq j \leq n\}\).

(4) \(P\) is the a priori belief space of the attacker and the defender. \(P(A_a^h)\) and \(P(A_a^l)\) are the prior beliefs of the defender on the attacker's type inference, and \(P(A_d)\) is the prior belief of the attacker on the defender's type inference. Among them, \(P(A_a^h) = q\), \(P(A_a^l) = 1 - q\), \(P(A_d) = 1\).
is the profit function of participants \( A_a \) and \( A_d \). The gain reflects the gains and losses of the participants, and the use of different strategies for the game will result in different game results, and the benefits will also be different. Among them, \( u_a \) is the profit function of the attacker, and \( u_d \) is the profit function of the defender.

3.3. Income quantification and calculation method

Quantifying the benefits of both offense and defense is the basis for quantitative calculation and game analysis, and it directly affects the outcome of the game as an input to the offense and defense game model. The implementation of network offensive and defensive actions by the intermediary nodes according to the confrontation strategy requires resource costs such as manpower, material resources and calculations, but at the same time it also generates corresponding security returns, which has economic characteristics. For the defender, the choice of defense strategy must find a balance between cost and reward in order to achieve the overall optimum. Definition related symbols and descriptions are shown in Table 1.

| sign | implication | Measurement method |
|------|-------------|--------------------|
| AC   | Attack Cost | The resources required by the attacker to implement the attack strategy |
| DC   | Defense Cost| The resources required for the defender to implement the defense strategy |
| AR   | Attack Reward| The attacker's reward after a successful attack |
| DR   | Defense Reward| The defender's return after adopting a defense strategy against an attack strategy |
| DL   | Defense Loss | The defender's loss due to the attacker's attack |

According to the above definition, an offensive and defensive game scenario is established. In the following, we will study the method of calculating the benefits of both offense and defense for the game between adventurous attackers, conservative attackers and defenders.

① For adventurous attackers, you can get the income expectations of the attacker and the defender:

\[
u_{a_i}^h = AR_i^h - AC_i^h - DR_i^h \tag{3}
\]

\[
u_{d_i}^h = DR_i^h - AR_i^h - DC_i^h - DL_i^h \tag{4}
\]

Add the above two formulas to get the sum of the benefits in the game scenario:

\[
u_{a_i}^h + u_{d_i}^h = -AC_i^h - DC_i^h - DL_i^h \tag{5}
\]

② For a conservative attacker, you can get the income expectations of the attacker and the defender:

\[
u_{a_i}^i = AR_i^i - AC_i^i - DR_i^i \tag{6}
\]

\[
u_{d_i}^i = DR_i^i - AR_i^i - DC_i^i - DL_i^i \tag{7}
\]

Add the above two formulas to get the sum of the benefits in the game scenario:

\[
u_{a_i}^i + u_{d_i}^i = -AC_i^i - DC_i^i - DL_i^i \tag{8}
\]

It can be seen that in the information security game, the sum of the benefits of the attacker and the defender is negative, that is, the game is a negative sum game. In other words, in each round of the game, regardless of the benefits of both parties, there will inevitably be cost losses. Therefore, the use of higher cost strategies is statistically unfavorable to both parties.
3.4. Bayesian Nash Equilibrium Solution

In the process of offensive and defensive games, each participant $A_{ai}$ hopes to maximize his expected reward $u_a$ given his own type $A_{ai}^h, A_{ai}^l$ and his own prior belief space $P$. Under the guidance of this principle, each participant will eventually reach an equilibrium, named Bayesian Nash equilibrium. Specifically, Bayesian Nash Equilibrium is a combination of strategies and beliefs of all participants. It satisfies the following conditions: Given the probability distribution of their own type and the type of others, the expected utility of each participant has reached Maximization, that is, no one has the enthusiasm to choose other strategies [9]. Therefore, the attack strategy under this equilibrium is the optimal choice conclusion, and the defender should choose the defense strategy corresponding to this attack strategy as the optimal defense strategy.

**Definition 3** In the ADG model, if for any participant $A_{ai}$ and each of his possible types $t_i \in T$, the action $h_i$ selected by the strategy $AS_i^*(t_i)$ can satisfy:

$$\max_{h_i \in H_i} \sum_{t_i} \left\{ u_i \left[ AS_i^*(t_i), \cdots, AS_{i-1}^*(t_{i-1}), h_i, AS_{i+1}^*(t_{i+1}), \cdots, AS_n^*(t_n) \right] p(t_{i-1} \mid t_i) \right\}$$

(9)

The strategy portfolio $AS^* = (AS_1^*, \cdots, AS_n^*)$ is called a Bayesian Nash equilibrium of the ADG model. Among them, $h_i$ represents a certain action in the action space $H$ of participant $A_{ai}$; the belief $p_i(t_{i-1} \mid t_i)$ of participant $A_{ai}$ describes the uncertainty of the possible type $t_i$ of another participant when given his own type $t_i$. In the definition, the sum of the maximum value is the sum of various possible combinations of other participants. Since the defender can only choose one defense strategy at a time, in a network game scenario, the defender predicts various behaviors of the attacker under rational assumptions, and this prediction result is the probability distribution $P_{AS}^*(t) = \left\{ p_{AS_1}(t_1), p_{AS_2}(t_2), \cdots, p_{AS_n}(t_n) \right\}$ in the mixed strategy. The effectiveness expectation of the defender's defense strategy $DS_j^*(t_D)$ in this game scenario can be obtained through the prior probability and return function of each type of defender:

$$u_d = (DS_j^*(t_D)) = \sum_{AS(t)} P(AS(t)) | DS(t) | \sum_{A_{ai}} u_d(A_{ai}, DS_j^*(t_D), AS(t)) P_{AS}^*(t)$$

(10)

After solving the defense effectiveness expectations of all defense strategies of the defender, each defense strategy can be sorted according to the level of defense effectiveness, and the defender can choose the optimal defense strategy in the order of effectiveness from high to low.

4. Case Analysis

In order to verify the effectiveness of the proposed offensive and defensive game model, attack prediction and defense strategy selection method, this paper uses the network topology shown in Figure 2 to simulate offensive and defensive scenarios for experiments.
The attack host is located in the external network, and the target information system is the switching network, including 32 node machines. Three servers are set up to provide SQL service, file service and backup service. IP6 trusts IP5. IP6 is a database server and has all kinds of sensitive information. Due to the existence of firewall, non local hosts can only access servers in DMZ area. IP2 and IP3 can access IP6 data by using network services, but they are forbidden to access other hosts in LAN.

Suppose that an attacker in an external network tries to obtain data from a database server. And the defender's prior belief in the type of attacker is: \( P(A_1^h) = 0.4, P(A_2^h) = 0.6 \), taking the attack of risk-taking attacker as an example, the strategies of risk-taking attacker include buffer overflow attack \( A_1 \) (35,9), Trojan horse attack \( A_2 \) (56,6), computer virus attack \( A_3 \) (28,2) and denial of service attack \( A_4 \) (72,5).

According to the expected income of participants, the income matrix of both sides is calculated as:

\[
\begin{bmatrix}
5.62 & 3.25 & -5.06 & 3.88 \\
4.36 & 3.69 & 0.57 & 2.97 \\
5.87 & 4.41 & -2.83 & 5.69 \\
4.98 & 5.28 & 1.34 & 6.31 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
-15.34 & -12.32 & -6.76 & -23.74 \\
-24.18 & -21.96 & -10.73 & -18.58 \\
-8.65 & -16.44 & 0.25 & -15.21 \\
-10.48 & -8.83 & -11.83 & -16.75 \\
\end{bmatrix}
\]

After quantifying the strategy cost and benefit, the attack and defense game tree is constructed and input into ADG model to calculate the mixed strategy of risk-taking attacker and defender under Bayesian Nash equilibrium.

\[AS^*_h = \begin{bmatrix} A_1 & A_2 & A_3 & A_4 \\ 0.15 & 0.24 & 0.33 & 0.48 \end{bmatrix} \quad DS^*_h = \begin{bmatrix} D_1 & D_2 & D_3 & D_4 \\ 0.005 & 0.342 & 0.213 & 0.154 \end{bmatrix} \]

Therefore, the hybrid strategy \( AS^*_h = (0.15 \ 0.24 \ 0.33 \ 0.48) \) of the risk-taking attacker is a reliable prediction of the attacker's behavior. It can be inferred that the attacker is most likely to take a "denial of service attack". Although the revenue of "denial of service attack" is not the largest, with the lower cost of attack and higher success rate, this strategy has the largest revenue expectation and becomes the most likely strategy for attackers.

5. Conclusion
The experimental results show that the algorithm proposed in this paper can greatly improve the accuracy of attack path prediction and the reliability of network security situation evaluation compared with the traditional network security evaluation methods, because this paper uses the cumulative probability of attack path to predict the most likely attack path. And achieve the inference of the
attacker's attack intention according to the current attack path combined with attack probability, to provide direct and effective help for security managers' decision-making. The effectiveness of the model and method is verified by an example.

Acknowledgments
This work was supported by the National Key Research and Development Program of China under Grant no. 2017YFB0801900.

References:
[1] LUO Z Y, YANG X, SUN G L, et al. Finite automaton intrusion tolerance system model based on Markov[J]. Journal on Communications, 2019, 40(10): 79-89.
[2] PHILLIPS C, SWILER L P. A graph-based system for network vulnerability analysis[C]/1998 Workshop on New Security Paradigms. New York: ACM Press, 1998: 71-79.
[3] WU C S, XIE W Q, JI Y X, et al. Survey on network system security metrics[J]. Journal on Communications, 2019, 40(6): 14-31.
[4] WANG S, TANG G M, WANG J H, et al. Attack scenario construction method based on causal knowledge net[J]. Journal of Computer Research and Development, 2018, 55(12): 2620-2636.
[5] LEI C, MA D H, ZHANG H Q, et al. Performance assessment approach based on change-point detection for network moving target defense[J]. Journal on Communications, 2017, 38(1): 126-140.
[6] JUKKA R. A look at the time delays in CVSS vulnerability scoring[J]. Applied Computing and Informatics, 2019, 15(2): 1-18.
[7] Liu Y, Cristina C, Hong M. A bayesian game approach for intrusion detection in wireless ad hoc networks[C]. In: Proc. of the 2006 Workshop on Game Theory for Communications and Networks, 2006.
[8] Hengwei Zhang, Jian Zhang, Jihong Han. Defensive strategy selection method based on non-cooperative game attack prediction[J]. Computer Science, 2016, 43(01): 195-201.
[9] Jindong Wang, Dingkun Yu, Hengwei Zhang, Na Wang. The method of selecting active defense strategy in static Bayes game[J]. Journal of Xidian University, 2016, 43(01): 144-150.