Optimal Security Protection Selection Strategy Based on Markov Model Attack Graph

Jinwei Yang1, a, Yu Yang1*
1 School of Information Engineering, Engineering University of PAP, Xi’an, Shanxi, China
a e-mail: daweiwei0416@163.com
*Corresponding author’s e-mail: 836993008@qq.com

Abstract. Intrusion intent and path prediction are important for security administrators to gain insight into the possible threat behavior of attackers. Existing research has mainly focused on path prediction in ideal attack scenarios, yet the ideal attack path is not always the real path taken by an intruder. In order to accurately and comprehensively predict the path information of network intrusion, a multi-step attack path prediction method based on absorbing Markov chains is proposed. Firstly, the node state transfer probability normalization algorithm is designed by using the nil posteriority and absorption of state transfer in absorbing Markov chain, and it is proved that the complete attack graph can correspond to absorbing Markov chain, and the economic indexes of protection cost and attack benefit and the index quantification method are constructed, and the optimal security protection policy selection algorithm based on particle swarm algorithm is proposed, and finally the experimental verification of the model in protection policy decision-making, which can effectively reduce network security risks and provide more security protection guidance for timely response to network attack threats.

1. Introduction
Computer network systems face complex attack events that are essentially due to the vulnerability of computer and network systems in the design, development, operation, and maintenance processes. A network attack is a complex multi-step process in which an external attacker analyzes the interconnected relationships of vulnerabilities in the internal network and then launches a multi-step attack that allows the attacker to take possession of more resources and ultimately cause damage to the attack target. The current challenge and breakthrough of network security is to research new models, technologies and methods for active real-time protection, to judge the current security situation by means of risk assessment, and to implement a security protection system for active defense based on the judgment results. Network Security Situation Awareness (NSSA), as an active network security protection means, realizes cognition, understanding and prediction of network security status and its development trend in the complex and changing network environment, which helps managers to grasp the network security status in time and make an effective prediction of possible future threats. Effective prediction of possible future threats. Among them, the attack graph is a graph theory-based situational awareness approach, which assesses the risk of current network systems based on the attack graph, calculates the optimal security protection strategy and moderately controls the risk and attack loss. In security risk management, each protection measure has a certain protection cost, and the trade-off between benefits and costs is a complex issue. Therefore, under the condition of limited protection cost, how to select the optimal
A protection strategy has become a hot issue of current research. Kerem [1] reviewed the current state of research on attack graphs and pointed out that the reachability analysis and path study of attack graphs is one of the main focuses of attack graph research. Sheyner et al. [2] were the first to combine probability theory with attack graphs, based on Markov decision process, and used conditional transfer probability to analyze nondeterministic nodes and pointed out that attackers tend to choose the path that is most favorable to achieve the attack goal to complete state transfer. Chen et al. [3] introduced transfer probability table in the attack graph model and used cumulative probability to calculate the maximum reachable probability of the target attack node, which is used to identify the attack intent and predict the attack path to assist the study of threat posture. Liu et al. [4] introduced Hidden Markov Model, combined with alarm observation sequence, and used Viterbi algorithm to derive the maximum possible state transfer sequence to achieve attack intent identification, but lacked network-wide risk value quantification. Dai et al. [5] comprehensively considered network defense measures, quantified attack costs and benefits, established a risk flow attack graph model, calculated the risk saturation rate of different intrusion paths and ranked the threats of the paths using fuzzy comprehensive evaluation method. Fredj et al. [6] used absorbing Markov chains to describe the state transfer behavior in the attack graph, and realized attack identification, through alarm correlation Abraham et al. [7] analyzed the variation of attack path length with the release time of vulnerabilities by introducing the vulnerability lifecycle. Ghasemigol et al. [8] proposed a comprehensive prediction algorithm for the uncertainty of attack occurrence probability. Nayot et al. [9] designed a dynamic assessment method of network security risk by blocking the maximum possible attack path.

Combining the above research results found that, although there are many existing studies, but mainly around the ideal attack scenario path prediction research, the default each vulnerability exploit can be successfully implemented, including the maximum possible attack path, the probability of success and the number of paths, however, the ideal maximum possible attack path is not necessarily the attack path used by the attacker, it needs a comprehensive sensory analysis of the probability distribution of attack paths, the number of atomic attacks, and the threat level of nodes to more comprehensively assist security administrators in their decisions.

To solve the above problems, this paper introduces Absorbing Markov Chain (AMC) into the field of attack graph research. Due to the non-sequential and absorbing nature of state transfer in AMC, which is in line with the randomness of network attacks and the reachability of target state nodes, we propose an attack path prediction method based on Absorbing Markov Chain. Firstly, it is proved that the complete attack graph can be mapped to the absorbing Markov chain; further, combining the Common Vulnerability Scoring System (CVSS) [10] and network asset information, the Particle Swarm Optimization (PSO) algorithm is used to achieve a reasonable quantification of attack threats and assist administrators in comprehensively and accurately grasping the changing trends of network security; finally, the effectiveness of the model is verified through experiments.

2. Attack graph based on absorbing Markov chain

Absorbing Markov chain is applicable to the state transfer prediction problem of stochastic model, and the basic idea is to map the attack graph to absorbing Markov chain and build the attack graph model based on absorbing Markov chain. On the one hand, the posteriority-free nature of Markov chain is consistent with the feature that the attack state transfer is only related to the adjacent states; on the other hand, there is at least one termination state of the network attack, which is consistent with the absorbing state of absorbing Markov chain.

2.1 Preliminary Knowledge

Definition 1. Atomic attack \( a \). Refers to a single attack action performed by an attacker in the network, which may be a scan of a host service or an exploit of a host vulnerability, each atomic attack action triggers the attacker to move to an attack state \( S \). The probability of an atomic attack occurring is \( p(a) \).

Definition 2. The attack path (\( AR \)). Refers to the set of directed edges from the attacker's initial state node to the target state node, and the attack path, \( AR = S_1 \rightarrow S_2 \rightarrow \cdots \rightarrow S_n \).
Definition 3. The attack path length (RL). Refers to the number of edges contained in the attack path, \( RL = n-1 \).

Definition 4. Attack success probability \( \text{p}(AR) \). Refers to the probability that all state transfers in the attack path are successful, \( \text{p}(AR) = \text{p}(a_1) \times \text{p}(a_2) \times \cdots \times \text{p}(a_m) \).

Definition 5. The expected length of the attack path \( \text{EARL} \). Refers to the mathematical expectation of the attack steps implemented by the attacker to achieve the attack goal.

Definition 6. Expected number of state visits. The mathematical expectation of the number of visits to a state node in the process of achieving the attack goal.

Definition 7. State node threat ranking. It refers to the ranking of the contribution of different state nodes to achieve the attack target, the higher the node ranking, the greater the threat of the node.

2.2 The concept of attack graph

An attack graph is an effective method for modeling the association of multi-step attack behaviors and describes the attack state transfer process from the attacker's perspective as a directed graph, as shown in Figure 1.

![Fig1. Model of attack graph](image)

Definition 8. The attack graph (AG). It is represented by a quadruple \( AG = (S, A, E, \Delta) \), where \( S \) denotes the set of state nodes, \( A \) denotes the set of atomic attack nodes, \( E \) denotes the set of directed edges between state nodes, and \( \Delta \) denotes the set of state transfer probabilities.

1) \( S = \{S_i \mid i = 1, 2, \cdots, n\} \) denotes the set consisting of \( n \) different state nodes.

2) \( E \subseteq S \times S, \forall e_{i,j} \in E, e_{i,j} \) denotes the edges connecting nodes \( S_i \) and \( S_j \), where \( S_i \) denotes the starting state node of \( e_{i,j} \), \( S_j \) denotes the destination state node of \( e_{i,j} \), and the atomic attack that achieves state transfer \( e_{i,j} \) dependence is \( a \).

3) \( \forall \Delta(e_{i,j}) \in \Delta, \Delta(e_{i,j}) \) denotes the probability \( \text{p}(S_j \mid S_i) \) of an attacker moving from state \( S_i \) to state \( S_j \), and \( \Delta(e_{i,j}) \) is equal to the probability \( \text{p}(a) \) of occurrence of atomic attack \( a \). Vulnerability scanning of the network using vulnerability scanning tools such as Nessus, Retina\(^\text{[11]}\), based on the topology of the deployed network with the collected vulnerability set, combined with MulVAL, an automatic attack graph generation tool, to construct the attack graph, avoiding the complexity of manual construction, is the mainstream construction method at present.

2.3 Relevant definitions of absorbing Markov chains

Definition 9. Markov chain (MC). For a discrete set of random sequences containing a finite number of states \( X = \{x_1, x_2, \cdots, x_n\} \), if each state value is only related to the previous adjacent state value and not to the state before it again, it is called a Markov chain.

\[
p(x_t \mid x_{t-1}, x_{t-2}, \cdots, x_1)
\]  

(1)

Definition 10. The state transfer probability matrix \( P \). The state transfer probability in a Markov chain is represented by the adjacency matrix \( P \), where \( p_{i,j} \) denotes the probability of a state \( x_i \rightarrow x_j \), if \( x_i \rightarrow x_j \) is unreachable, such that \( p_{i,j} = 0 \), and the matrix \( P \) satisfies \( \sum_{j=1}^{n} p_{i,j} = 1, \forall 1 \leq i \leq n \), where
0 ≤ p_{ij} ≤ \mathcal{I}(1 ≤ i, j ≤ n).

Definition 11. Initial state. Denotes the starting state of the attacker, the state node has only outgoing edges and no incoming edges.

Definition 12. Absorbing state. Denotes the target state of the attacker, and the state node has only inflow edges and no outflow edges.

Definition 13. Transition state. The other states in the state sequence, excluding the absorbing state, are called transition states.

Definition 14. Absorbing Markov Chain. The Markov chain containing absorbing states is called absorbing Markov chain, and the corresponding state transfer probability matrix is expressed as:

\[ P = \begin{pmatrix} Q & R \\ 0 & I \end{pmatrix} \]

where Q is a \( t \times t \) matrix, representing the transfer probability between transition states; 0 is a zero matrix; R is a \( t \times r \) non-zero matrix, representing the transfer probability from transition states to absorbing states; I is a \( r \times r \) unit matrix; and the number of all states is \( n = t + r \).

Definition 15. The expected number of attacks \( N \). The expected value of the number of times an attacker visits a transition state \( S_i \) before absorbing it from the transition state \( S_j \) is denoted by \( N_{ij} \), where \( 1 ≤ i, j ≤ t \), let \( N \) be a \( t \times t \) matrix, and assigning \( N_{ij} \) to the element at position \((i, j)\) in the matrix \( N \), then \( N = (I - Q)^{-1} \).

Definition 16. Desired path length matrix \( T \). The attacker starts from the node \( S_i \), the expected value of the total number of transfers (expected path length) before the attacker starts from the node is denoted by \( T_i \). Let \( T \) be a \( t \times 1 \) matrix and \( C \) be a \( t \times 1 \) unit matrix. Assigning the value to the element at position \((i, 1)\) of \( T \), then \( T = N \cdot C \).

3. Security protection policy selection model

3.1 Model Design

Step 1 Risk identification

1) Identify network assets, assign importance to assets, and correlate assets with vulnerability analysis.

2) Use OVAL vulnerability scanner to identify vulnerabilities of network hosts and assign values to the probability of successful exploitation of vulnerabilities using CVSS.

Step 2 Risk Assessment

1) Generate an attack graph using MulVAL tool based on information such as vulnerability, association of vulnerabilities, network configuration, and network connectivity.

2) Describe the uncertainty of the attack behavior through the probability of successful vulnerability exploitation and the probability of successful attack, and build a probabilistic attack graph using AMC for multi-step atomic attacks.

3) The local conditional probability distribution (LCPD) table of attribute state nodes is used in the attack graph model to calculate the corresponding unconditional probability, and then the joint probability of nodes is used to assess the security risk.

Step 3 Security Protection Management

1) Construct the economic indexes of protection cost and attack benefit and the index quantification method.

2) By analyzing the protection cost and attack benefit, the particle swarm algorithm is used to quickly obtain the optimal security protection strategy.
3.2 Risk assessment

3.2.1 LCPD function calculation
A local conditional probability distribution table captures the likelihood of a state node being threatened and it describes the probability distribution of that node given the set of its father nodes.

Definition 17. LCPD function \(^{[12]}\). Suppose the Markov model attack graph is \(MBAG = (S, A, E, R, T, P, M, P_{c}, C)\), \(S_j \in N_{\text{internal}} \cup N_{\text{terminal}}\), and \(S_j\) is the sets of \(S_j\) father nodes denoted as \(S_i \in Pa\left[S_j\right]\), and the vulnerability exploit \(v_i\) is associated with a certain step of atomic attack. The LCPD function of a node \(S_j\) is denoted as \(P\left(S_j \mid Pa\left[S_j\right]\right)\), defined as follows.

1) when \(d_j = \text{AND}\),
\[
P\left(S_j \mid Pa\left[S_j\right]\right) = \begin{cases} 
0, \exists S_i \in Pa[S_j] | S_i = 0 \\
\prod_{S_i \in Pa[S_j]} P(\cap_i v_i), \text{else} 
\end{cases}
\]  

2) when \(d_j = \text{OR}\),
\[
P\left(S_j \mid Pa\left[S_j\right]\right) = \begin{cases} 
0, \forall S_i \in Pa[S_j] | S_i = 0 \\
\prod_{S_i \in Pa[S_j]} P(\cap_i v_i), \text{else} 
\end{cases}
\]

3.2.2 Unconditional probability calculation
Definition 18. Unconditional probability. Suppose each attribute node \(S_j\) and its set of ancestor nodes \(S_j\), whose set of parents is denoted as \(An[S_j] = \{ S_j \in S, j = 1, 2, \cdots, J \}\), then the unconditional probability of \(S_j\) is the joint probability of the current attribute node and its set of all parents, defined as follows.
\[
P(S_j, An[S_j]) = P(S_j \mid Pa[S_j]) \prod_{j=1}^{J} P(S_j \mid Pa[S_j])
\]

3.2.3 Based CVSS transfer probability metric
In this paper, we use the Common Vulnerability Scoring System CVSS provided by the U.S. Institute of Standards and Technology to evaluate the probability of vulnerability exploitation success. A CVSS score is a number in the range of 0 to 10. Each vulnerability consists of three sets of attributes: base, temporal, and environmental. base attributes are related to the probability of exploit success given the characteristics of the exploit. base subsections include: Access Vecto (AV), Access Complexity (AC), and Authentication (Au). The probability of success of an exploit is defined as follows:
\[
P(v_i) = 2 \times AV \times AC \times Au
\]

Fig.2 Attack graph of LLDOS1.0 scenario
4. Experimental Analysis

In this section, the LLDOS1.0 attack scenario in the DARPA2000 dataset provided by Lincoln Laboratory is used as the experimental object, and the literature [13] has mined the complete attack scenario contained in this dataset through clustering-based alert association analysis, as shown in Figure 2, which is widely recognized and gives the following state transfer probabilities, which are drawn upon for experimental analysis.

The transfer matrix $P$ of the absorbing Markov chain is first constructed, and the matrices $N$ and $T$ are further calculated as follows.

$$
P = \begin{pmatrix}
0 & 0.47 & 0 & 0.53 & 0 \\
0 & 0.22 & 0.31 & 0.31 & 0.16 \\
0 & 0 & 0.87 & 0 & 0.13 \\
0 & 0.19 & 0.45 & 0.19 & 0.17 \\
0 & 0 & 0 & 0 & 1
\end{pmatrix},\quad (6)
$$

$$
N = \begin{pmatrix}
1 & 0.84 & 5.38 & 0.98 \\
0 & 1.41 & 5.24 & 0.54 \\
0 & 0 & 7.69 & 0 \\
0 & 0.33 & 5.50 & 1.36
\end{pmatrix},\quad (7)
$$

$$
T = \begin{pmatrix}
8.198 \\
7.200 \\
7.692 \\
7.197
\end{pmatrix},\quad (8)
$$

The absorbing state node is $S_5$, $N_{i,j}$ indicates the number of times the state $S_i$ departs and visits the state $S_j$ before reaching the target state, for example, from the initial state node $S_1$, the number of times it reaches the node $S_2$, $S_3$, $S_4$ is 0.84, 5.38, 0.98, respectively, at which time the transition state node threat ranking is $S_3 > S_4 > S_2$, and the state vulnerability should be fixed $S_3$ first. From the matrix $T$, it can be seen that the expected attack path lengths to reach the target node from different nodes $S_1, S_2, S_3, S_4$ are 8.198, 7.2, 7.692, and 7.197, respectively, and the results show that the attacker who starts from the node $S_1$, the average number of vulnerability attacks implemented to reach the target state node is the most.

Table 1 gives a comparison of the results of the ideal and actual metrics in the LLDOS 1.0 attack scenario, in the ideal case, since there is no repeated state transfer behavior, the statistics yield the number of possible paths is 8, the shortest path length is 2, and the path length types are 2, 3, and 4 the median and average value of all path lengths are 3. The cumulative success probability of the attack intent is 0.14.

| Types                  | Metric                      | Value  |
|------------------------|-----------------------------|--------|
| Ideal Attack Scenario  | Shortest Route Length       | 2      |
|                        | Median of Route Lengths     | 3      |
|                        | Mean Route Length           | 3      |
|                        | Number of Routes            | 8      |
|                        | Mode of Route Lengths       | 3      |
|                        | Cumulative Success Probability| 0.14  |
| Realistic Attack Scenario | Expected Success Probability | 1     |
|                        | Maximum EARI                | 8.198  |
|                        | Minimum EARI                | 7.197  |
In contrast, in the actual case, the desired probability of achieving the attack intent is 1, and the longest and shortest desired path lengths are 8.198 and 7.197, respectively. The former indicates that an average of 8.198 exploit attacks need to be performed to achieve the target, and the latter indicates that the minimum number of exploit attacks required is 7.197, which is clearly larger than the desired path length value and in line with expectations. Therefore, the use of this paper's metric allows scientific assessment of the attacker's current state and accurate prediction of subsequent attacks.

5. Conclusions

Since the attack state transfer process of network intruders is complex, attack path prediction is important for security administrators to intuitively understand the attack process. Considering that the existing methods mainly focus on the ideal attack path, this paper maps the attack graph into an absorbing Markov chain, gives a transfer probability quantification method based on a common vulnerability scoring criterion, and on this basis focuses on the expected number of visits of different state nodes in the actual network environment, which is used to analyze the threat ranking of nodes and calculate the expected attack path length and its probability distribution to assist security The administrator comprehensively analyzes the probability of occurrence of different attack paths and grasps the number of atomic attacks that an attacker may implement, and proposes an optimal security protection policy algorithm based on the PSO algorithm by establishing the economic indicators of protection cost and attack benefit and quantifying the indicators. It also provides guidance for preformulating security protection measures to defend against network intrusion.

Acknowledgements
Fundamental Research Fund of People Armed Police Engineering University: The Key Technology Research on Security Situational Awareness for People Armed Police Force Optical Cable Network

References
[1] Keremk. A taxonomy for attack graph generation and usage in network security [J]. Journal of Information Security and Applications, 2016, 29 (C):27-56
[2] SheynerO, HainesJ, JhaS, et al. Automated generation and analysis of attack graphs[C]//Proc of the 2002IEEE Symp on Security and Privacy. Piscataway, NJ:IEEE, 2002:273-284
[3] CHEN X J, FANG B X, TAN Q F, et al. Inferring attack intent of malicious insider based on probabilistic attack graph model[J]. Chinese Journal of Computers, 2014, 37(1): 62-72.
[4] LIU S, LIU Y. Network security risk assessment method based on HMM and attack graph model[C]//IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, NETWORKING and distributed Computing. 2016:517-522.
[5] FREDJ O B. A realistic graph based alert correlation system[J]. Security & Communication Networks, 2015, 8(15):2477-2493.
[6] DAI F, HU Y, ZHENG K, et al. Exploring risk flow attack graph for security risk assessment[J]. IET Information Security, 2015, 9(6): 344-353.
[7] ABRAHAM S, NAIR S. A predictive framework for cyber security analytics using attack graphs[J]. International Journal of Computer Networks & Communications, 2015, 7(1): 1-17.
[8] GHASEMIGOL M, GHAEMI B A, TAKABI H. A comprehensive approach for network attack forecasting[J]. Computers & Security, 2016,58:83-105.
[9] OU X, GOVINDAVAJHALAS, APPEL A W. MulVAL: a logic-based network security analyzer[C]//14th USENIX Security Symposium. 2005.
[10] MELL P, SCARFONE K, ROMAMOSKY S. Common vulnerability scoring system[J]. IEEE Security & Privacy, 2007, 4(6): 85-89.
[11] Tenable N. Nessus vulnerability scanner [EB/OL]. [2017.06.17]. http://www.tenable.com/products/nessus-home
[12] Sun Shiliang, Huang Rongqing. An adaptive k-nearest neighbor algorithm[C]//2010 7th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD),2010,1:
91-94.

[13] Shin B, Lee J H, Lee T, et al. Enhanced weighted K-nearest neighbor algorithm for indoor Wi-Fi positioning systems[C]//2012 8th International Conference on Computing Technology and Information Management (ICCM), 2012, 2: 574-577