Intrusive Intention Recognition Based on Signaling Game Model

Xiaoning Zhang*, Hengwei Zhang*,†, Pengyu Sun, Jindong Wang

PLA SSF Information Engineering University, Zhengzhou 450001, China

* These authors contributed equally to this work

†Corresponding Author: Hengwei Zhang. Email: zhw11qd@aliyun.com

Abstract. In order to accurately assess the network security situation and identify the intrusive intention of attackers, we propose an intrusive intention identification method based on a signaling game model. Based on the attack path graph, an offensive and defensive signalling game model is established, and the payoffs and costs of attack and defence are quantified using CVSS. By calculating the game equilibrium to quantitatively analyse and predict the attack paths that match the attacker's intent, administrators can be guided to make defensive decisions.

1. Introduction

Intrusive intention recognition is analyzing the detected alarm information to determine the attacker's purpose and assumptions. It is a process of reasonable interpretation of the detected attack data. Recognition based on known attack patterns is an important type of intrusive intention recognition method. This method uses the attack path to enumerate all possible attack behaviors, and identifies the attack intention through path reachability calculation and path analysis. According to the difficulty of vulnerability exploitation, Wang et al. [4] first quantified the network security risk using the probabilistic methods, established a probability model of the attack graph, and used the cumulative probability to calculate the probability of each node in the attack graph. [1] first proposed an intrusive intention recognition method based on attack path graphs, and applied probabilistic reasoning to describe the uncertainty in intention recognition. Hu et al. [2] considered the problem of loops that might be generated by the attack hypothesis of "monotonicity", used Markov chain absorption to describe the attack process, quantified the probability distribution of different attack paths through matrix derivation, and calculated the expected value of the attack path length which assist in identifying threat hosts. Chen et al. [3] proposed a probabilistic attack graph model suitable for internal intrusive intention inference, which reduces the number of untrustworthy alarms and can more accurately infer the attacker's intentions. While all of the above studies take the attacker's perspective, they do not consider the impact of the defender's actions on the attacker's intentions and are lacking in accuracy.

In the process of network attack and defence, the attacker's choice of attack path depends on the adversarial actions of both attackers and defenders and their outcomes. The goal opposition, strategy dependency and non-cooperative relationship between the attacking and defending adversaries fit perfectly with the basic features of game theory [6], so game theory is an effective analysis and decision-making tool in the process of identifying the attacker's intrusion intention. In this paper, we will identify and predict the attacker's intention from a gaming perspective.
2. Attack Path Graph

Attack path graph is a directed graph composed of vertices and directed edges, which can visually display selectable attack paths. By scanning and analyzing the system, most defenders can find all vulnerabilities in the network (excluding 0day vulnerabilities). Based on the network topology, they can connect network nodes that have connectivity relationships and can be infiltrated with vulnerabilities to generate attack path graph.

The process of generating a attack path graph follows the assumptions: ① If the attacker has obtained a higher authority, he will no longer obtain the lower authority of the node; ② The attacker will not invade the node that has obtained the authority again; ③ Every attack step in the node process is necessary and there is no redundancy. The above assumptions can remove redundant paths and loops, simplifying the attack path graph and conforming to the behavioral characteristics of a rational attacker.

Definition 1. Attack path graph can be expressed as

\[
\text{APG} = (H, B, E)
\]

where \(H\) is the set of network nodes, \(B\) is the set of vulnerabilities, and \(E\) is the set of directed edges in the attack graph. A directed edge connects two nodes, which represents the process of starting from one network node and exploiting vulnerabilities to attack the next network node. Figure 1 shows an example of an attack graph, where \(H_0\) represents the network node the attacker has mastered, \(H_t\) represents the target node, and \(B_i\) represents the vulnerability that the attacker can exploit. From Figure 1, we can clearly see all the attack paths from the attacker to the target node.

Figure 1. Example of attack path graph

3. Attack-Defense Signaling Game Model

Assuming that both the attacker and the defender are completely rational, seeking to maximize their own benefits under restricted conditions, the game between the two parties will eventually reach the Nash equilibrium. In an equilibrium state, any participant's income from changing its strategy is less than its income in the equilibrium state. Therefore, the attack path can be effectively predicted based on the game equilibrium solution.

3.1. Definition of attack-defense signaling game model

Definition 2. The attack-defense game model \(G\) can be expressed as

\[
G = (N, T, M, R, S, P, U)
\]

where

① \(N = (N_A, N_D)\) is the set of players in the game, \(N_A\) represents the attacker, which is the signal sender; \(N_D\) represents the defender, which is the signal receiver.

② \(T = (T_A, T_D)\) is the type space of attacker and defender. According to the attacker's ability to obtain information, the type of attacker can be expressed as a set \(T_A = \{t_1, t_2, \ldots, t_n\}\). The type of
defender can be expressed as $T_t = \{t\}$. Attackers with different abilities will choose different attack paths corresponding to their abilities.

③ $M$ represents the signal space of the attacker. The information related to the attacker's type obtained by the defender through scanning detection and log analysis is the attack signal. $M = \{m_1, m_2, \cdots, m_n\}$. Affected by the false signals sent by the attacker and the insufficient ability of the defender to collect and analyze information, the signal received by the defender may not necessarily match the actual type of the attacker.

④ $R=\{A,D\}$ represents the space of action of the attacker and the defender, where $A = \{a_1, a_2, \cdots, a_g\}, D = \{d_1, d_2, \cdots, d_h\}$, $g, h \geq 1$. $a_i$ represents an atomic attack using the vulnerability $B_i$, and $d_j$ represents a defense deployment against the vulnerability $B_j$.

⑤ $S=\{S_A, S_D\}$ is the strategic space between the attacker and the defender.

⑥ $P_d = \{P(t_1), P(t_2), \cdots, P(t_t)\}$ is the defender's prior belief set, which represents the defender's initial judgment of the attacker type $t$.

⑦ $\tilde{P}$ is the posterior belief set of the defender. $\tilde{P}(t_i|m_j)$ represents the posterior probability of the attacker type $t_i$ calculated by Bayes' rule when the defender observes the signal $m_j$.

⑧ $U = \{U_A, U_D\}$ is the set of revenue functions of the attacker and the defender.

3.2. Offensive and defensive strategy benefit

Definition 3. The specific concepts of system damage cost (Dcost), attack cost (Acost) [5], and defense cost (Decost) [6] can be found in literature [5, 6]. Generally, the system loss cost can be used as the defender's loss and the attacker's benefit. This article quantifies the above indicators based on Common Vulnerability Scoring System (CVSS).

① Dcost is determined by the node asset value ($V$) and Impact Sub-Score (ISS) on each attack path, and defines $D_{\text{cost}} = \sum_{i=1}^{n} V_i \times \text{ISS}_i$. The asset value of each node depends on the node type, and is quantified as follows:

| Node type             | Asset value |
|-----------------------|-------------|
| Ordinary host, user host | 50          |
| Ordinary server       | 80          |
| Data server           | 100         |

Impact sub-score $\text{ISS}=1 - \left[ (1 - \text{Confidentiality}) \times (1 - \text{Integrity}) \times (1 - \text{Availability}) \right]$, where the three metrics of Confidentiality, Integrity, and Availability are used to measure the impact of successfully exploiting the vulnerability on the confidentiality, integrity and availability of the affected nodes. The Quantitative criteria in CVSS are as follows:

| Metric               | Influence level          | Numerical Value |
|----------------------|--------------------------|-----------------|
| Confidentiality (C)  | None (N) / Low (L) / High (H) | 0 / 0.22 / 0.56 |
| Integrity (I)        | None (N) / Low (L) / High (H) | 0 / 0.22 / 0.56 |
| Availability (A)     | None (N) / Low (L) / High (H) | 0 / 0.22 / 0.56 |

Table 1. Quantitative criteria for node types

Table 2. Quantitative criteria for ISS metrics
Factors affecting Acost include AV (attack vector), AC (attack complexity), PR (privileges required), and UI (user interaction). Define \( A_{\text{cost}} = \sum_{i=1}^{n} \lambda (1 - AV_i \times AC_i \times PR_i \times UI_i) \), where \( \lambda \) is the correction factor. The quantitative criteria are as follows:

| Influencing factor | Metric | Numerical Value |
|--------------------|--------|-----------------|
| AV                 | Network (N)/ Adjacent (A)/ Local (L)/ Physical (P) | 0.85 / 0.62 / 0.55 / 0.2 |
| AC                 | Low (L) / High (H) | 0.77 / 0.44 |
| PR                 | None (N) / Low (L) / High (H) | 0.85 / 0.62 / 0.27 |
| UI                 | None (N) / Required (R) | 0.85 / 0.62 |

Decost is the sum of the operation cost and the negative cost of the defense strategy. The definitions of operation cost and negative cost can be found in literature [5]. The calculation of defense costs requires further grading and quantification of operation costs and negative costs. Due to space reasons, this article will not describe them again.

Based on the above definition, the expected benefit of the attacker is:

\[
U_{\text{a}}(m_i, d_i, t_i) = \sum_{g, h} (D_{\text{cost}}(a_g, d_h) - A_{\text{cost}}g)
\]

The defender's expectation of benefit in the game is:

\[
U_{\text{d}}(m_i, d_i, t_i) = \sum_{g, h} (D_{\text{cost}}(a_g, d_h) - D_{\text{cost}}h)
\]

Where \( a_g \) is the atomic attack selected by the attacker of type \( t_i \), \( d_h \) is the defensive action chosen by the defender after observing the attack signal, \( A_{\text{cost}}g \) is the operation cost of the attack action \( a_g \), \( D_{\text{cost}}h \) is the operation cost of the defensive action \( d_h \), \( t_i \) is the attacker type, and \( m_i \) represents the attacker signal.

3.3. Perfect Bayesian equilibrium solution

**Definition 4.** The perfect Bayesian equilibrium of the attack-defense signaling game model is composed of the strategy combination \( (m^*(t), d^*(m)) \) and the posterior belief \( \hat{P}(t|m) \) [7], and satisfies the following conditions:

(a) \( m^*(m) \in \arg \max_{m^*} \sum_{t} \hat{P}(t|m)U_{\text{a}}(m, d^*, t) \);

(b) \( m^*(t) \in \arg \max_{m^*} \sum_{m} \hat{P}(m|t)U_{\text{a}}(m, d^*(m), t) \);

(c) \( \hat{P}(t|m) \) is obtained by the defender from the prior probability \( P_D \), the observed signal \( m \), and the attacker's optimal strategy \( m^*(t) \) using Bayes' rule.

In the above definition, (a) represents the optimal action for the signal sent by the attacker when the defender’s posterior belief is \( \hat{P}(t|m) \); (b) represents the optimal attack strategy chosen by the attacker when the defender's optimal action \( d^*(m) \) is predicted; (c) is the process by which the defender calculates the posterior probability \( \hat{P}(t|m) \).

The solution process is as follows:
Algorithm 1

Input: Attack path graph $APG = \{H, B, E\}$; the defender's prior belief $P_D = \{P(t_1), P(t_2), \cdots, P(t_n)\}$;

Output: The path of attack with the highest probability

1: Initialize $(P_D = \{P(t_1), P(t_2), \cdots, P(t_n)\})$

2: $R = \{A, D\}$, $A = \{a_1, a_2, \cdots, a_g\}$, $D = \{d_1, d_2, \cdots, d_h\}$

3: while ($a_g \in A$ && $m_j \in M$ && $d_h \in D$) do

4: $U_A(m_j, d, t) = \sum_{g,h} (D \cos(a_g, d_h) - A \cos t_g)$

5: $U_D(m_j, d, t) = \sum_{g,h} (D \cos(a_g, d_h) - D \cos t_g)$

6: $d^*(m) \in \arg\max_{D_j} \sum_{t} \tilde{P}(t | m) U_D(m, d, t)$

7: $m^*(t) \in \arg\max_{m \in M} U_A(m, d^*(m), t)$

8: End

9: Bayesian $(\tilde{P}(t | m))$;

10: Create $(m^*(t), d^*(m), \tilde{P}(t | m))$

11: Output $(m^*(t), \tilde{P}(t | m))$

12: End

4. Instance Analysis

4.1. Network construction

This paper constructs the network topology as shown in Figure 2, and divides the subnet area through the firewall. The specific access rules between the subnets are as follows:

1. Only user node $H_6$ in the $D_1$ domain can access the SQL database;
2. Each node in the $D_1$ domain can communicate with the server in the DMZ domain;
3. Nodes in the same domain can access each other, and cross-domain access is not supported.

Figure 2. Experimental network topology
4.2. Attack graph generation

We scanned the experimental network for vulnerabilities and obtained vulnerability information for each node, as shown in Table 4.

| Node | Vulnerability number | CVE-ID       | AV  | AC  | PR  | UI  | C   | I   | A   |
|------|----------------------|--------------|-----|-----|-----|-----|-----|-----|-----|
| H1   | B1                   | CVE-2021-28144 | 0.85| 0.77| 0.62| 0.85| 0.56| 0.56| 0.56|
| H2   | B2                   | CVE-2021-26810 | 0.85| 0.77| 0.85| 0.85| 0.56| 0.56| 0.56|
| H4   | B6                   | CVE-2021-29379 | 0.62| 0.77| 0.85| 0.85| 0.56| 0.56| 0.56|
| H4   | B9                   | CVE-2021-31437 | 0.55| 0.77| 0.85| 0.62| 0.56| 0.56| 0.56|
| H4   | B10                  | CVE-2021-3464 | 0.55| 0.77| 0.62| 0.85| 0.56| 0.56| 0.56|
| H4   | B11                  | CVE-2021-29302 | 0.85| 0.44| 0.85| 0.85| 0.56| 0.56| 0.56|
| H5   | B12                  | CVE-2021-28204 | 0.85| 0.77| 0.27| 0.85| 0.56| 0.56| 0.56|
| H6   | B3                   | CVE-2021-28179 | 0.85| 0.77| 0.27| 0.85| 0| 0| 0.56|
| H7   | B7                   | CVE-2021-29083 | 0.85| 0.77| 0.27| 0.85| 0.56| 0.56| 0.56|

In the experimental network, the node H5 with important information can be considered as the target node of the attacker. Figure 3 shows the attack diagram generated by using the scanned vulnerability information, the exploitable relationship between the vulnerabilities, and the network configuration.

Figure 3. Experimental network attack graph

We first calculate the attacker’s attack strategy in the two attack paths from H6 to H5. The two paths are path 1: $H_6 \rightarrow B_9 \rightarrow H_7 \rightarrow B_{11} \rightarrow H_4 \rightarrow B_{12} \rightarrow H_5$; path 2: $H_6 \rightarrow B_9 \rightarrow H_7 \rightarrow B_{12} \rightarrow H_5$. According to the number of affected hosts and the difficulty of the vulnerability attack, it can be assumed that...
low-capable attackers $t_1$ choose path 1 and high-capable attackers $t_2$ choose path 2. Defenders have different defense levels, which can be assumed to be $D_L$ and $D_H$. Each defense level contains defense measures for different vulnerabilities, and the defender sets the corresponding defense level based on the posterior probability of the attacker type. Under different combinations of offensive and defensive strategies, the revenue values of both parties are as follows:

![Image](image.png)

Figure 4. Offensive and defensive strategies and gains

The equilibrium of the game at this stage is calculated as $EQ = ((m_1, m_1) \rightarrow (D_L, D_L), \tilde{P}(t_1 | m_1) = 0.4, \tilde{P}(t_1 | m_2) = 0.5)$ . It shows that at this stage the attacker, regardless of the type, chooses to release the attack signal $m_1$ containing the information about path 1 as the best choice, meanwhile, the defender, observing $m_1$, believes that the probability of the attacker choosing path 1 is 0.4 and the probability of the attacker choosing path 2 is $1 - 0.4 = 0.6$ .

The expectation of gain for the attacker from $H_0$ to $H_5$ can be obtained as $0.4 \times 20.15 + 0.6 \times 21.5 = 20.96$ , the defender's expectation of gain is $0.4 \times 17.02 + 0.6 \times 15.9 = 16.35$ . Substituting its value into the next stage of the calculation of the attack and defence gains when choosing the attack path from $H_0$ to $H_5$ . Two attack paths can be defined from $H_0$ to $H_5$ : path3: $H_0 \rightarrow B_1 \rightarrow H_1 \rightarrow B_2 \rightarrow H_2 \rightarrow B_3 \rightarrow B_4 \rightarrow H_4 \rightarrow B_5 \rightarrow H_5$ , path4: $H_0 \rightarrow B_1 \rightarrow H_1 \rightarrow B_3 \rightarrow H_6 \rightarrow H_5$ . Repeating the calculation process of the first stage, the equilibrium solution of this stage can be obtained as $EQ = ((m_3, m_3) \rightarrow (D_H, D_L), \tilde{P}(t_1 | m_3) = 0.32, \tilde{P}(t_1 | m_4) = 0.6)$ . This means that the attacker's best strategy is to release the signal $m_3$ associated with path 3 regardless of the attacker's type, and upon receiving the signal $m_3$, the defender believes that the attacker has a probability of 0.32 to choose path 3 and 0.6 to choose path 4. The results also show that as the number of games increases, defenders become more aware of the true type of attacker and it becomes easier to derive the true attack path of the attacker.

5. Conclusions

This paper presents a method for identifying attacker’s intrusive intention using a signalling game model. On the basis of the attack path diagram, a quantification of the attack and defence gains is proposed based on the CVSS scoring criteria. Calculating the attacker's optimal attack strategy and the probability of choosing each attack path by solving the Bayesian equilibrium of the signalling game to identify the attacker's intrusion intention. The feasibility and effectiveness of the method is demonstrated through experiments.

Acknowledgments

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

[1] Peng, W., Hu, C.Z., Yao, S.P. (2010) Intrusive Intention Recognition Based on Attack Path Graph. Transactions of Beijing Institute of Technology, 30(009): 1077-1081.

[2] Hu, H., Liu, Y.L., Zhang, H.Q. (2018) Route Prediction Method for Network Intrusion Using Absorbing Markov Chain. Journal of Computer Research and Development, 55(004): 831-845.

[3] Chen, X.J., Fang, B.X., Tan, Q.F., Zhang, H.L. (2014) Inferring Attack Intent of Malicious Insider Based on Probabilistic Attack Graph Model. Chinese Journal of Computers (01): 62-72.

[4] Wang L, Islam T, Long T, et al. (2008) An attack graph-based probabilistic security metric. In: IFIP Annual Conference on Data and Applications Security and Privacy. Berlin. pp.283-296.

[5] Jiang, W., Fang, B.X., Tian, Z.H., Zhang, H.L. (2009) Evaluating Network Security and Optimal Active Defense Based on Attack-Defense Game Model. Chinese Journal of Computers (04): 817-827.

[6] Jiang, W., Fang, B.X., Tian, Z.H., Zhang, H.L. (2010) Research on Defense Strategies Selection Based on Attack-Defense Stochastic Game Model. Journal of Computer Research and Development (10): 1714-1723.

[7] Fudenberg D, Tirole J. (2012) Game theory. Massachusetts Institute of Technology Press, Boston.