Network Security Situation Assessment Method Based on Markov Game Model

Xi Li[1], Yu Lu[1], Sen Liu[2] and Wei Nie[3]
[1]Information Engineering Department
Ordnance Engineering College
Shijiazhuang 050003, China
[2]The 54th Research Institute of CETC
Shijiazhuang 050200, China
[3]College of Information Engineering
Shenzhen University
Shenzhen 518060, China
[e-mail: wei.nie@szu.edu.cn]
*Corresponding author: Wei Nie

Received May 10, 2017; revised September 23, 2017; revised October 30, 2017; accepted January 18, 2018; published May 31, 2018

Abstract

In order to solve the problem that the current network security situation assessment methods just focus on the attack behaviors, this paper proposes a kind of network security situation assessment method based on Markov Decision Process and Game theory. The method takes the Markov Game model as the core, and uses the 4 levels data fusion to realize the evaluation of the network security situation. In this process, the Nash equilibrium point of the game is used to determine the impact on the network security. Experiments show that the results of this method are basically consistent with the expert evaluation data. As the method takes full account of the interaction between the attackers and defenders, it is closer to reality, and can accurately assess network security situation.

Keywords: network security, situation assessment, Markov Decision Process, Game theory

This research was supported by the National Natural Science Foundation of China [No. 61271152] and the Natural Science Foundation of Hebei Province, China [No. F2012506008].

http://doi.org/10.3837/tiis.2018.05.027 **ISSN : 1976-7277**

1. Introduction

In recent years, with the rapid development of Internet technology, the means of attack are becoming more and more diverse, and security incidents are increasing substantially. The research direction of network security has changed from single security problem to overall situation of global network. The concept of situation assessment originates from military requirements. As an integral part of data fusion, situation awareness is an important part of decision making process[1].As the core of network security situation awareness, network security situation assessment is to analyze and comprehend the security status of the network.

Recent years, domestic and foreign scholars have made a lot of research on network security situation assessment. Boyer S[2] designs a situation assessment framework based on D-S evidence theory. This method does not need to know the probability distribution of variables accurately, but it has a large amount of calculation and has a potential problem of combination explosion; Ramaki A A[3] proposes a risk assessment method based on Bayesian networks. The method has better convergence and fault tolerance. Even in a large network application environment, it can rely on better performance to handle large amounts of data. However, it still needs proper training to obtain the corresponding parameters; Wang C H[4] designs a kind of alert correlation system. The system does not need predefined knowledge database and configuration information of network, it can discover the causal relationship between attack behaviors and identify unknown attack behaviors. But, it cannot handle the behavior of IDS omission; Jinxia Wei[5] proposes a dynamic classification network security defense strategy model by analyzing the security situation of complex computer network. The model can solve a safety problem that the static defense cannot cope with tactics and lack of dynamic change; Xie Lixia[6] proposes a network security situation awareness method based on neural network. She designs a BP neural network structure to meet the evaluation requirements, realize the nonlinear mapping relationship between the first level indicators and the second, and use the hierarchical matrix to accomplish the first level situation evaluation. Li F W[7] proposes a network security situation assessment method based on Hidden Markov model. The method can trace the dynamic characteristics of numerical fluctuations conveniently and intuitively, and realize the effective prediction of the security status; Wen Z C[8] proposes a network security situation prediction method based on Hidden Markov model. The method analyzes the change rules and predicts the trend of development by describing the dependence of the security situation at different times; Xi R R[9] proposes a method for determining the state transition matrix based on the game of safety incidents and protective measures. This method is used to solve the problem that the state transition matrix of hidden Markov model is often obtained by experience. Guan-Yu Hu[10] proposes a forecasting model of network security situation based on the hidden belief rule base model. In order to train the parameters of model, a revised covariance matrix adaption evolution strategy (CMA-ES) algorithm is further developed by adding a modified operator.

At present, most of the researches about network security situation assessment just focus on the network attack behavior, the vulnerability of its own system and so on, and ignore the defense measures. As we knew that the same network attack has different threat level to different network. For the same attack using different defense, the final result of the damage will be a lot of difference. The network security situation assessment method proposed by this paper, takes full account of the network offensive and defensive actions adopted by the two sides, and gives a comprehensive evaluation.

2. Improved Situational Assessment Framework

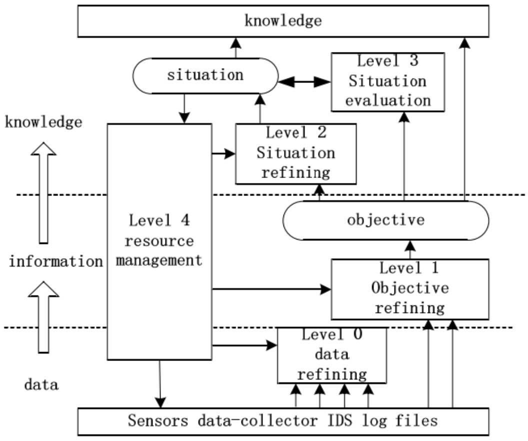

knowledge
situation
Level 3 Situation evaluation
knowledge
Level 2 Situation refining
Level 4 resource management
objective
information
Level 1 Objective refining
Level 0 data refining
data
Sensors data-collector IDS log files

Fig. 1. Network security situation assessment framework based on data fusion

In 1999, Bass T proposed the concept of network security situation awareness firstly and the security situation assessment framework based on data fusion such as **Fig. 1**[11,12]. The framework is divided into "data-information-knowledge" three processing levels. The underlying security event is the data source. The object base is extracted from data and object reconstruction, and loaded into situation reconstruction and threat assessment. Finally, the top-level situation information is extracted. The framework provided a good theoretical basis and guidance for the follow-up NSSA(Network Security Situation Awareness) study.

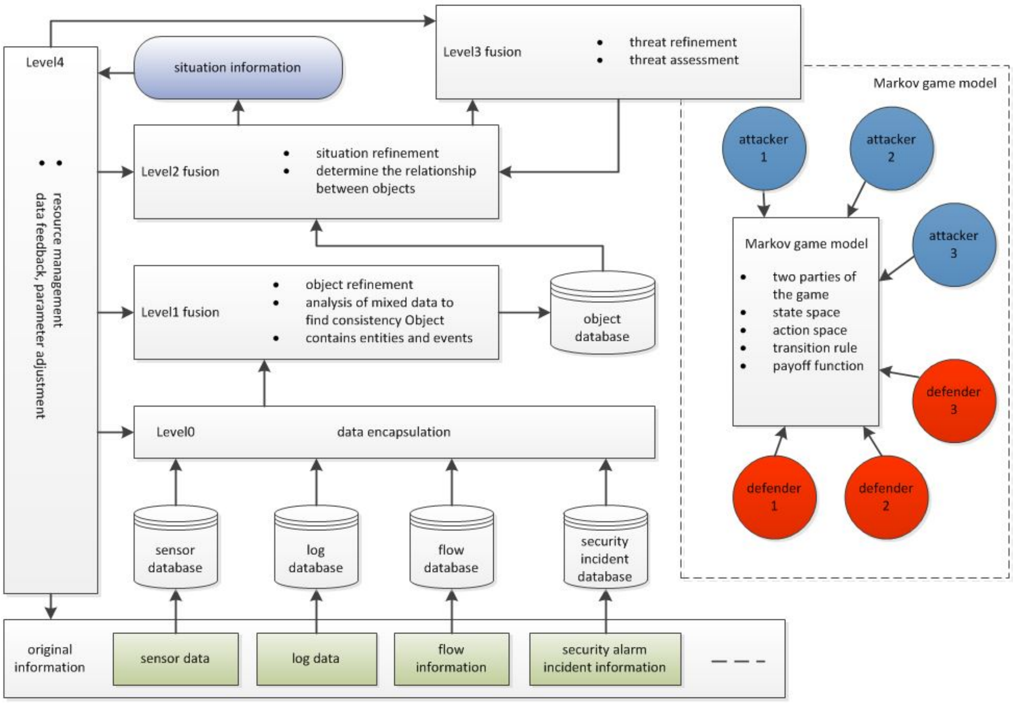


Fig. 2. Situational assessment framework based on Markov Game model

This paper proposes a kind of network security situation assessment framework based on Markov Game model, with referencing multiple models[13,14,15,16,17],as shown in **Fig. 2**. The framework uses Markov Game model to achieve the refinement and evaluation of network threats in Level3, which is the core of the framework. Game theory can well reflect the substantive characteristics of the attackers and the defenders. Their behaviors are closely related, which will have impacts on the network security situation. Markov Decision Process can reflect the uncertainty of network attack and defense. The fusion of Level3 can refine the situation judgement of Level2, and take into account the network defensive behaviors to make a comprehensive assessment.

3. Markov Game Model

The Markov Game model proposed in this paper consists of two sides of the game, the state space, the behavior space, the transition probability and the pay function.

3.1 Two Sides of the Game

In this model, the attackers (blue team) and the defenders (red team) are the two sides of the game. The attackers exploit the vulnerabilities to attack the network in order to steal information and destroy the network. The defenders are the network administrators, who use strengthening program to reduce the destructiveness of threats and cut off their transmission path, thereby enhancing the security of the system.

3.2 State Space

All the possible states of network nodes compose the state space. For the network node *i*, whose state vector at time *k* is S_{i^k} .

$$S_{i^k} = (w, p, a)^T$$

where *w* is the working status of the node *i*, *p* is the protection status, *a* is the status of being attacked, and *T* is the transpose operator. The values of *w* can be "normal", "response slow", "malfunction", "crashed" and so on. The values of *p* can be "firewall", "IDS", "email-filter", "and IDS firewall" and so on. The values of *a* can be "NULL", "attack Web", "bombing email", "DOS" and so on. Then, the state space of the whole network at time *k* is S_k .

$S_k = [S_{1^k}, S_{2^k}, S_{3^k}, \cdots, S_{n^k}]$, *n* is the number of nodes in the network.

3.3 Action Space

The behaviors of all the network security participants constitute action space(strategy set). At each moment, the different nodes will take the appropriate action according to the obtained information. For example, the blue team may take overflow buffer behavior, if buffer overflow vulnerability is detected. The blue team may take "attempted-admin" or "attempt-dos" according to the established strategy of the attack. The red team may take "firewall strategy adjustment" behavior, if IDS detected attacks. **Table 1** is a part of the network attack behaviors take out from the snort manual[18].

Table 1. Snort Default Classifications

Classtype	Description	Priority
attempted-admin	Attempted Administrator Privilege Gain	high
attempted-user	Attempted User Privilege Gain	high
inappropriate-content	Inappropriate Content was Detected	high
policy-violation	Potential Corporate Privacy Violation	high
shellcode-detect	Executable code was detected	high
successful-admin	Successful Administrator Privilege Gain	high
trojan-activity	A Network Trojan was detected	high
web-application-attack	Access to a potentially vulnerable web application	high
unusual-client-port-connection	A client was using an unusual port	medium
attempted-dos	Attempted Denial of Service	medium
attempted-recon	Attempted Information Leak	medium
rpc-portmap-decode	Decode of an RPC Query	medium
system-call-detect	A system call was detected	medium
protocol-command-decode	Generic Protocol Command Decode	low
network-scan	Detection of a Network Scan	low
string-detect	A suspicious string was detected	low
tcp-connection	A TCP connection was detected	Very low
……	……	……

3.4 Transition Rule

The system state transition rule describes as $R(S_{k+1}|S_k, u_k^{blue}, \mathrm{u}_k^{red})$,where S_{k+1}, S_k are system states at time *k* and *k*+1 respectively, u_k^{blue} , u_k^{red} are the overall decisions of the two sides at time *k*. For each network node, the state of time *k*+1 is determined by three aspect:1) state at time *k*; 2) control strategies of the two sides; 3) the attack/defense efficiency.

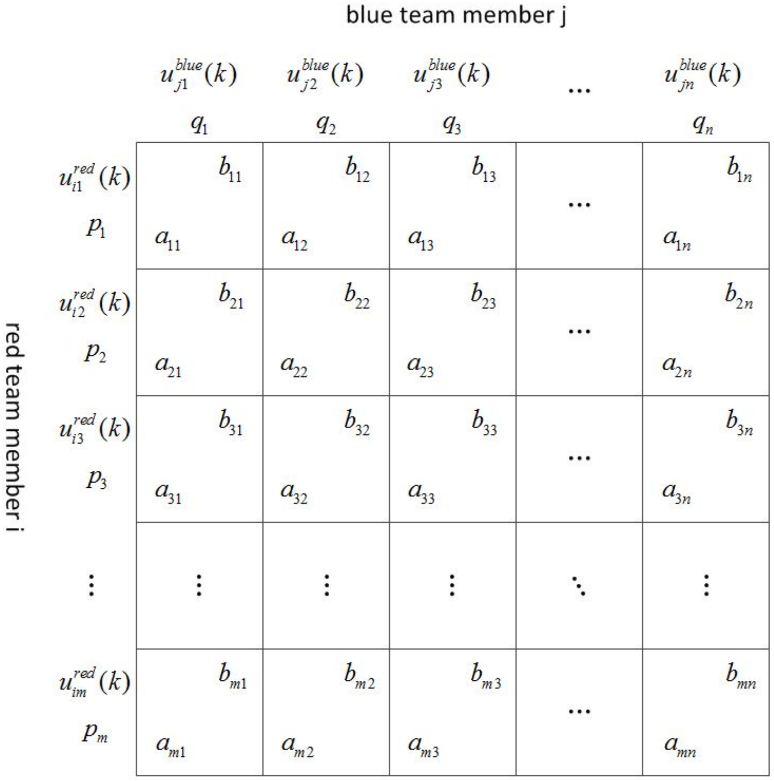
3.5 Payoff Function

The game between red team and blue team is a kind of mixed strategy game, and the payoffs of the two sides are their expectation payoffs. **Fig. 3** is the game matrix of red team member i and blue team member j at time k.

$u_i^{red}(k)$ is the probable behavior of red team member *i* at time *k*, p is the probability to take this action, $\sum_{i=1}^{m} p_i = 1$, $p_i \geq 0$; $u_j^{blue}(k)$ is the probable behavior of blue team member *j* at time *k*, q is the probability to take this action, $\sum_{i=1}^{n} q_i = 1$, $q_i \geq 0$; a_{ij} is the payoff of *i*, when *i* takes the behavior of $u_{ii}^{red}(k)$ and j takes $u_{jj}^{blue}(k)$. At the same time, the payoff of *j* is b_{ij}. Then, the expectation payoff of *i* and *j* can be obtaind by formula(1) and (2).

$$\pi_i^{red}(p,q,k) = \sum_{i=1}^{m}\sum_{j=1}^{n} p_i q_j a_{ij} \tag{1}$$

$$\pi_j^{blue}(p,q,k) = \sum_{i=1}^{m}\sum_{j=1}^{n} p_i q_j b_{ij} \tag{2}$$



blue team member j

red team member i

$$\begin{array}{c|c|c|c|c|c}
 & \begin{matrix} u_{j1}^{blue}(k) \\ q_1 \end{matrix} & \begin{matrix} u_{j2}^{blue}(k) \\ q_2 \end{matrix} & \begin{matrix} u_{j3}^{blue}(k) \\ q_3 \end{matrix} & \cdots & \begin{matrix} u_{jn}^{blue}(k) \\ q_n \end{matrix} \\
\hline
\begin{matrix} u_{i1}^{red}(k) \\ p_1 \end{matrix} & \begin{matrix} & b_{11} \\ a_{11} & \end{matrix} & \begin{matrix} & b_{12} \\ a_{12} & \end{matrix} & \begin{matrix} & b_{13} \\ a_{13} & \end{matrix} & \cdots & \begin{matrix} & b_{1n} \\ a_{1n} & \end{matrix} \\
\hline
\begin{matrix} u_{i2}^{red}(k) \\ p_2 \end{matrix} & \begin{matrix} & b_{21} \\ a_{21} & \end{matrix} & \begin{matrix} & b_{22} \\ a_{22} & \end{matrix} & \begin{matrix} & b_{23} \\ a_{23} & \end{matrix} & \cdots & \begin{matrix} & b_{2n} \\ a_{2n} & \end{matrix} \\
\hline
\begin{matrix} u_{i3}^{red}(k) \\ p_3 \end{matrix} & \begin{matrix} & b_{31} \\ a_{31} & \end{matrix} & \begin{matrix} & b_{32} \\ a_{32} & \end{matrix} & \begin{matrix} & b_{33} \\ a_{33} & \end{matrix} & \cdots & \begin{matrix} & b_{3n} \\ a_{3n} & \end{matrix} \\
\hline
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
\hline
\begin{matrix} u_{im}^{red}(k) \\ p_m \end{matrix} & \begin{matrix} & b_{m1} \\ a_{m1} & \end{matrix} & \begin{matrix} & b_{m2} \\ a_{m2} & \end{matrix} & \begin{matrix} & b_{m3} \\ a_{m3} & \end{matrix} & \cdots & \begin{matrix} & b_{mn} \\ a_{mn} & \end{matrix} \\
\hline
\end{array}$$

Fig. 3. The game matrix of red team and blue team

Suppose the total number of both sides is x, then the expectation payoff of red team member *i* at time *k* can be expressed as the formula (3).

$$\pi_i^{red}(p) = \sum\nolimits_{u\in U}\left(\prod_{j=1}^{x} p_j(u_j)\right)\omega_i(u) \tag{3}$$

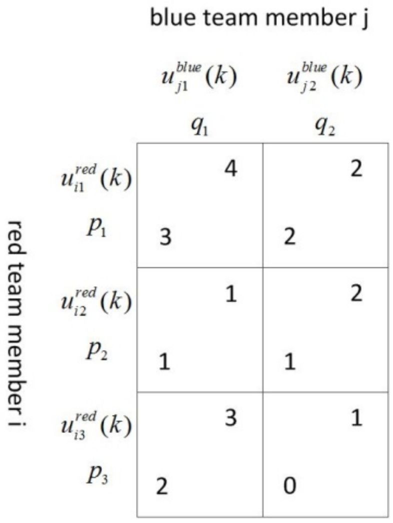
Where $\omega_i(u)$ is the payoff of red team member *i* when all members of both teams take the pure strategy (behavior) combination *u*. $p_j(u_j)$ is the probability of member *j* (*j* may be red team member or blue team member) to take pure strategy u_j. Similarly the expectation payoff of blue team member j at time k can be described by the formula (4).

$$\pi_j^{blue}(p) = \sum\nolimits_{u\in U}\left(\prod_{i=1}^{x} p_i(u_i)\right)\omega_j(u) \tag{4}$$

To determine payoff function is the key to calculate the value of security threat situation assessment. The specific payoffs of both sides are determined by the Nash equilibrium point.

4. Using Markov Game Model to Calculate the Security Threat Situation

Suppose the red team member *i* has three kinds of defense behaviors, $u_{i1}^{red}(k)$, $u_{i2}^{red}(k)$, $u_{i3}^{red}(k)$, blue team member *j* has two kinds of attack behaviors, $u_{j1}^{blue}(k)$, $u_{j2}^{blue}(k)$. The game matrix of *i* and *j* is determined by the offensive and defensive efficiency and other empirical data of the both sides, as shown in **Fig. 4**.



	$u_{j1}^{blue}(k)$ q_1	$u_{j2}^{blue}(k)$ q_2
$u_{i1}^{red}(k)$ p_1	4 3	2 2
$u_{i2}^{red}(k)$ p_2	1 1	2 1
$u_{i3}^{red}(k)$ p_3	3 2	1 0

Fig. 4. Example -- the game matrix of red team and blue team

The expectation payoff of *i* is shown in equation (5):

$$\pi_i^{red} = 3p_1q_1 + 2p_1q_2 + p_2q_1 + p_2q_2 + 2p_3q_1 \tag{5}$$

Because

$$\sum_{i=1}^{m} p_i = 1 \text{ and } p_i \geq 0, \tag{6}$$

$$\sum_{i=1}^{n} q_i = 1 \text{ and } q_i \geq 0, \tag{7}$$

Then

$$p_3 = 1 - p_1 - p_2 \,, \quad q_2 = 1 - q_1 \tag{8}$$

$$\pi_i^{red} = q_1(2 - p_1 - 2p_2) + 2p_1 + p_2 \tag{9}$$

Thus the reaction function of *i* can be obtained, as shown in equation (10):

$$(p_1, p_2) = \begin{cases} (1,0), & q_1 > 0 \\ (1,0), & q_1 = 0 \end{cases} \tag{10}$$

Similarly, the expectation payoff and reaction function of *j* are shown in equation (11) and equation(12):

$$\pi_j^{blue} = q_1(2 - 3p_2) + p_1 + p_2 + 1 \tag{11}$$

$$q_1 = \begin{cases} 1, & p_2 < \frac{2}{3} \\ [0,1], & p_2 = \frac{2}{3} \\ 0, & p_2 > \frac{2}{3} \end{cases} \tag{12}$$

The result is a straight line and a folding surface in the three-dimensional space, as shown in **Fig. 5**.

The reaction function of red team member *i* is red line, and that of j is stepped surface. They have one intersection, $(p_1, p_2, q_1) = (1,0,1)$, which is the Nash equilibrium point. Thus the expectation payoffs of *i* and *j* are:

$$\begin{cases} \pi_i^{red} = 3 \\ \pi_j^{blue} = 4 \end{cases}, \quad (1,0,1) \tag{13}$$

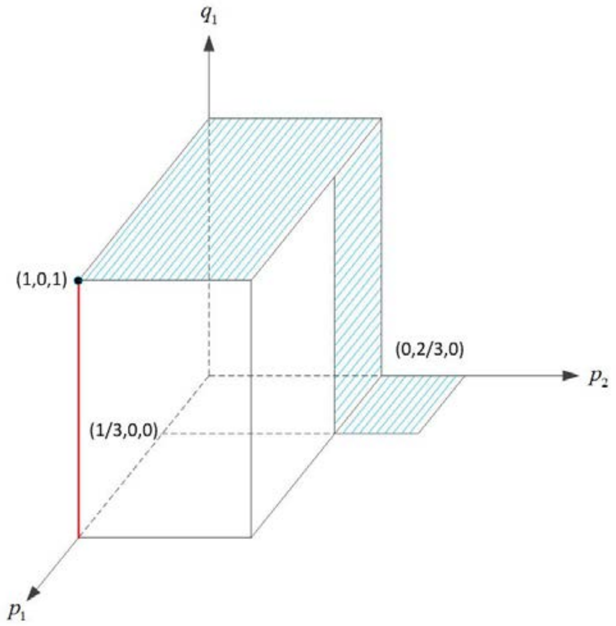


Fig. 5. The solution space of the reaction function of the example

As a finite game, red team and blue team will go to the Nash equilibrium point in the process in order to obtain the maximum benefits each other. Blue team member *j* selects the strategy (1,0), namely takes action $u_{j1}^{blue}(k)$ with 100% chance. At the same time, red team member *i* selects the strategy (1,0,0), namely takes action $u_{i1}^{red}(k)$ with 100% chance. If *i* and *j* are the only members of the both sides, the network security situation value is as the equation (14):

$$\pi_j^{blue} - \pi_i^{red} = 4 - 3 = 1 \tag{14}$$

In order to directly show the process that using Markov Game model to calculate the threat situation assessment, this paper uses the minimum dimension of the high dimension problem. In fact, the both sides' actions(strategy) are not limited to the 2-3 types, and the algebraic method is used to solve the problem of higher dimensional Nash equilibrium.

According to the definition of Nash equilibrium, the purpose of each player is to choose the strategy to maximizes the value of the payoff function. Under the condition of differentiable function, the necessary condition of the extremum is that all partial derivatives of the function are equal to 0.Then,take $p_m = 1 - \sum_{\sigma=1}^{m-1} p_\sigma$ and $q_n = 1 - \sum_{\varsigma=1}^{n-1} q_\varsigma$ into formula (1) and (2), to solve simultaneous equations (15).

$$\begin{cases} \dfrac{\partial \pi_i^{red}}{\partial p_\sigma} = 0, \sigma = 1, \cdots, m-1 \\ \dfrac{\partial \pi_j^{blue}}{\partial q_\varsigma} = 0, \varsigma = 1, \cdots, n-1 \\ p_\sigma \geq 0 \\ q_\varsigma \geq 0 \\ \sum_{\sigma}^{m-1} p_\sigma \leq 1 \\ \sum_{\varsigma}^{n-1} q_\varsigma \leq 1 \end{cases} \tag{15}$$

The solutions are all Nash equilibrium candidate solutions, if the candidate solution is unique, then need to verify the results by two order derivative. If the candidate solution is not unique, this paper uses the Pareto advantage standard and the expert experience to verify and determine the final Nash equilibrium point. For example, assuming that both $(p_1, p_2, q_1) = (1,0,1)$ and $(p_1, p_2, q_1) = (0,0,1)$ are candidate solutions, according to Pareto advantage, both sides will get more payoff if selecting $(p_1, p_2, q_1) = (1,0,1)$, so the result is $(p_1, p_2, q_1) = (0,0,1)$.

5. Situation Assessment Algorithm

Input: sensor data, Log data, Flow information, security alarm events and other types of network security data.

Output: equipment support information network security situation information and all kinds of feedback information.

```
  1) Initialization
  set sensor information database = null, Log information database = null, Flow information database = null, security event library = null, object database = null, situation information = null;
  2) Set up a classification database
  Set up the sensor information database, Log information database, Flow information database and security event database according to the original information;
  3) Level 0 data fusion
  The sensor information database, Log information database, Flow information database and security event library are encapsulated by time parameters.
  4) Level 1 data fusion
  Do consistent analysis of Level 0 output data , and output objects to form Object database;
  set $i = 0$
  5) Level 2 data fusion
  if $i = 0$
Determine the relationship between the Objects, and form a preliminary situation information
  else
      Combine the threat assessment of Level 3 to form the final situation information
      goto 7）
  endif
  6) Level 3 data fusion
  6.1) Markov Game model initialazation
  set $team_{red} = null$ , $team_{blue} = null$ , $S_k = null$ , $action_{red} = null$ , $action_{blue} = null$
  $team_{red}$ 、 $team_{blue}$ are the two sides of the game, $action_{red}$ 、 $action_{blue}$ are the action spaces.
  6.2) Assignment
  Determine $team_{red}$ , $team_{blue}$ , $S_k$ , $action_{red}$ and $action_{blue}$ according to the Level 2 data
  6.3) Threat assessment
  6.3.1) Determine the game matrix according to the Level 2 data and expert experience data
  6.3.2) Use reaction function , algebraic method or other methods to determine the Nash equilibrium.
  6.3.3) Determine threat assessment values
  Use formula (3) and (4) to calculate the payoffs of the game players.
  threat assessment value=$\left|\pi^{blue} - \pi^{red}\right|$ , $\pi^{blue}$ and $\pi^{red}$ are the sum of the payoffs at the time $k$
  6.4) $i = i + 1$ , goto 5);
  7) Entry into Level 4, resources management, feedback data, adjust parameters.
```

6. Experiment and analysis

In order to validate the Markov Game model, this paper constructs a network environment, and the topology structure is shown in **Fig. 6**.

Through pre script, the network attack software is used to attack the network automatically, and the experiment process lasts for 48 hours. The network security situation assessment system based on Markov Game model analyzes and processes data in every 2 hours. In order to verify the accuracy of the Markov Game model, 6 experts are selected to evaluate the network security situation. The expert score is the average value after removing a maximum value and a minimum value. The results of the security situation are shown in **Table 2** and **Fig.7**. By modifying the script, as well as fixing the payoff value, the second experiment is carried out for 48 hours, and the experimental results are shown in **Table 2** and **Fig. 8**.

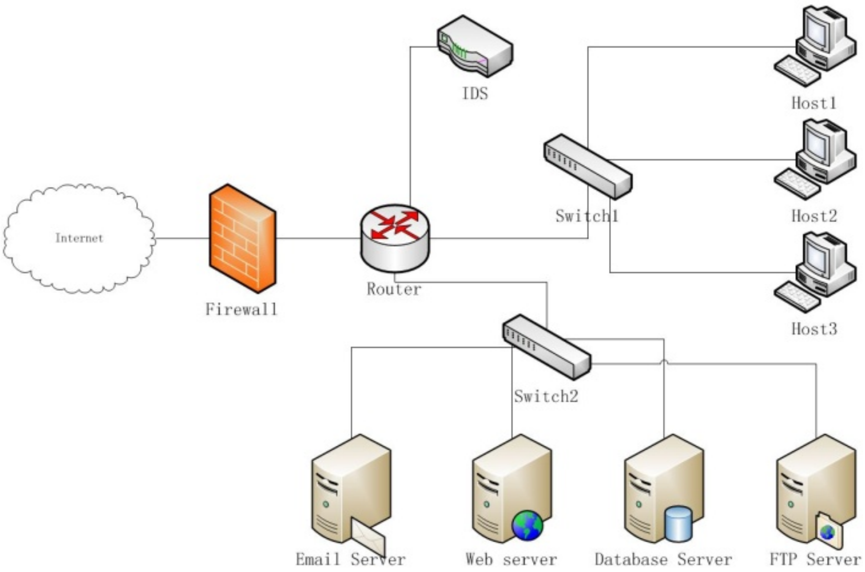


Fig. 6. Diagram of experimental network

Table 2. Results of security situation

sampling point	the first 48 hours		the second 48 hours	
	expert data	system data	expert data	system data
1	12	18	54	52
2	38	27	68	66
3	75	85	78	80
4	23	30	32	33
5	45	50	55	50
6	13	23	52	55
7	85	78	57	60
8	67	64	69	70
9	90	80	87	86
10	67	60	77	80
11	35	30	24	27
12	22	15	30	32
13	78	85	82	80
14	54	58	51	52
15	67	60	81	79
16	37	30	23	21

17	24	30	16	18
18	33	37	43	42
19	21	25	34	31
20	14	20	16	17
21	25	28	25	25
22	36	40	38	37
23	45	39	26	25
24	29	25	24	26

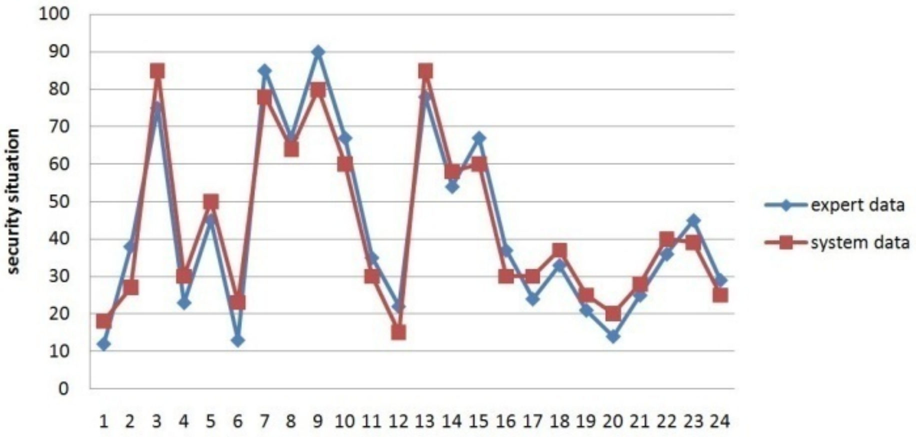


Fig. 7. Results of the first 48 hours of security situation chart

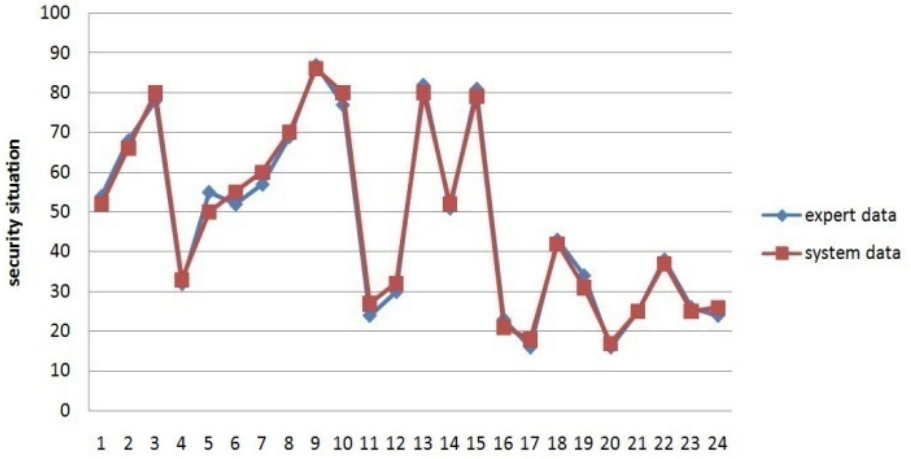


Fig. 8. Results of the second 48 hours of security situation chart

From the experimental results, we can see that the trend of network security situation curve is consistent with the preset attack strength and attack density. In the first experiment, the system evaluation data and expert evaluation data are basically consistent, but there are still some deviations. In the second experiment, the both sides' payoff values of the Markov Game model are modified. It can be seen from the result that the system data and expert data are more consistent after adjustment.

7. Conclusion

The security situation assessment method proposed in this paper combines the Markov Decision Process and the Game Theory. This method reflects the characteristics of network security that the process of network attack and defense is a game with randomness. It can be seen from the experiment that the method can accurately assess the security situation of the network, so as to provide a strong support for network security management. At the same time, the method can also be used to predict the situation of network security, and provide suggestions of security event processing for network managers.

The advantages of this method are as follows:

- The judgment of network security situation is not only to consider the network threat caused by the attackers, but also to take into account the defense measures to weaken the threat. Comprehensive two sides' factors, the network security situation is relatively objective.
- This method can reflect the characteristics of different networks, and the evaluation of network security situation can be more targeted.

The disadvantages of this method are as follows:

- The payoffs of both sides will have a great impact on the evaluation result, but they may be affected by human factors.
- Due to the network attack and the defense sides are not completely rational, this method is difficult to estimate the possible jitter.

In order to improve the accuracy of the method, the next step is to study the game matrix in depth. The reward value in the matrix can be referred to CVSS (Common Vulnerability Scoring System). At present, CVSS has been fully supported by NVD (Nation Vulnerability Database).

References

[1] Gong Z H, Zhuo Y. “Research on Cyberspace Situational Awareness,” *Journal of Software*, vol.21, no.7, pp.1605-1619, 2010. Article (CrossRef Link)

[2] Boyer S, Dain O, Cunningham R. “Stellar: A fusion system for scenario construction and security risk assessment,” in *Proc. of the 13th IEEE Int’l Workshop on Information Assurance*, pp.105−116, 2015. Article (CrossRef Link)

[3] Ramaki A A, Khosravi-Farmad M, Bafghi A G. “Real time alert correlation and prediction using Bayesian networks,” in *Proc. of the ISCISC*, pp.98−103, 2015. Article (CrossRef Link)

[4] Wang C H, Chiou Y C. “Alert correlation system with automatic extraction of attack strategies by using dynamic feature weights,” *Int’l Journal of Computer and Communication Engineering*, vol.5, no.1, pp.1−10, 2016. Article (CrossRef Link)

[5] Jinxia Wei, Ru Zhang , Jianyi Liu, et al. “Defense Strategy of Network Security based on Dynamic Classification,” *Ksii Transactions on Internet and Information Systems*, vol.9, no.12, pp.5116-5134, 2015. Article (CrossRef Link)

[6] Xie L X, Wang Y C, Yu J B. “Network Security Situation Awareness Approach Based on Markov Game Model,” *J Tsinghua Univ (Sci & Technol)*, vol.53, no.12, pp.1750−1760, 2013. Article (CrossRef Link)

[7] Li F W, Sun S, Zhu J, etal. “Situation Assessment Method based on Hidden Markov Model,” *Computer Engineering and Design*, vol.36, no.7, pp.1706-1711, 2015. Article (CrossRef Link)

[8] Wen Z C, Chen Z G. “Network security situation prediction method based on hidden Markov model,” *Journal of Central South University (Science and Technology)*, vol.46, no.10, pp.3689-3695, 2015. Article (CrossRef Link)

[9] Xi R R, Yun X C, Zhang Y Z, etal. "An Improved Quantitative Evaluation Method for Network Security," *Chinese Journal of Computers*, vol.38, no.4, pp.749-758, 2015. Article (CrossRef Link)

[10]Guan-Yu Hu, Zhi-Jie Zhou, Bang-Cheng Zhang, etal. "A method for predicting the network security situation based on hidden BRB model and revised CMA-ES algorithm," *Applied Soft Computing*, vol.48, pp.404-418, 2016. Article (CrossRef Link)

[11] Bass T. "Multi sensor data fusion for next generation distributed intrusion detection systems," in *Proc. of the'99 IRIS National Symp. on Sensor and Data Fusion*. pp.24-27, 1999. Article (CrossRef Link)

[12] Bass T. "Intrusion detection systems and multi sensor data fusion," *Communications of the ACM*, vol.43, no.4, pp.99-105, 2000. Article (CrossRef Link)

[13] Gad A, Farooq M. "Data fusion architecture for maritime surveillance," in *Proc. of the Int'l Society on Information Fusion(ISIF)*, pp.448−455, 2002. Article (CrossRef Link)

[14] Kadar I. "Knowledge representation issues in perceptual reasoning managed situation assessment," in *Proc. of the FUSION*, pp.13−15, 2005. Article (CrossRef Link)

[15] Llinas J, Hall D. "An introduction to multi sensor data fusion," in *Proc. of the ISCAS '98 - Proceedings of the 1998 IEEE International Symposium on Circuits and Systems*, vol. 6, pp.537-540, 1998. Article (CrossRef Link)

[16] Blasch E, Plano S. "DFIG level5 issues supporting situational assessment reasoning," in *Proc. of the FUSION*, pp.35-43, 2005. Article (CrossRef Link)

[17] Zhang Y, Tan X B, Cui X L, etal. "Network Security Situation Awareness Approach Based on Markov Game Model," *Journal of Software*, vol.22, no.3, pp.495-508, 2011. Article (CrossRef Link)

[18] The snort project. "SNORT Users Manual," Article (CrossRef Link)

Xi Li received the M.S. degree from Ordnance Engineering College. Now, he is a Ph.D. Candidates of Ordnance Engineering College. His research interests include network security and information technology of equipment support.

Yu Lu received the Ph.D. from Beihang University. Now, he is a professor of Ordnance Engineering College. His research interests include information security, computer network and cryptograph.

Sen Liu received the M.S. degree from Yanshan University. Now, she is a senior engineer of the 54th Research Institute of CETC. Her research interests include signal processing and information resistance.

Wei Nie received the Ph.D. from the University of Electronic Science and Technology. He is a Lecturer of Shenzhen University. His research interests include network security and optimization theory.