Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2015, Article ID 356146, 7 pages
http://dx.doi.org/10.1155/2015/356146

Research Article

A Novel Dynamic Method in Distributed Network Attack-Defense Game

Liu Xiaojian[1] **and Yuan Yuyu**[2]

[1]*College of Computer Science and Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2]*College of Software Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China*

Correspondence should be addressed to Liu Xiaojian; chn1989lxj@163.com

Received 5 January 2015; Revised 4 March 2015; Accepted 4 March 2015

Academic Editor: Hui Zhang

We analyze the distributed network attack-defense game scenarios, and we find that attackers and defenders have different information acquisition abilities since the ownership of the target system. Correspondingly, they will have different initiative and reaction in the game. Based on that, we propose a novel dynamic game method for distributed network attack-defense game. The method takes advantage of defenders' information superiority and attackers' imitation behaviors and induces attackers' reaction evolutionary process in the game to gain more defense payoffs. Experiments show that our method can achieve relatively more average defense payoffs than previous work.

1. Introduction

Modern organizations embed information and communication technologies (ICT) into their core processes as means to facilitate the collection, storage, processing, and exchange of data to increase operational efficiency, improve decision quality, and reduce costs [1]. In this way, distributed system is becoming widely used. Despite the significant benefits of distributed system, the system also places the processing tasks at the risk due to "distributed vulnerability." Traditional approaches to improve security generally consider only system vulnerabilities and attempt to defend all the attacks through system upgrading. No matter if the assuming attacks come, the defending resources have to be inputted. In distributed system, these keeping upgrading approaches will result in a huge waste of defending resource. Regarding this, game theory has been applied in network security.

In traditional game theory, equilibrium is achieved through players' analysis and reasoning based on common view about game rules, players' reason, and payoff matrix. Generally, the game players are the interactional individuals. Even as group-player, the members should be consubstantial with the same rational characteristics, strategies, and payoffs. However, this strong rational assumption of traditional game theory is receiving more and more criticism from game theory experts and economists [2].

In reality, there exist a large number of game problems between individual-player and group-player. For example, in distributed network attack-defense game scenarios, system officers, as defenders of the system, are consubstantial and can be regarded as individual-player (we use singular form to indicate individual-player and use plural form to indicate group-player). The defender has more information about system, game structure, and payoff matrix. Even if they temporarily lack knowledge, the defender has more resources to fill in the blank. So the defender is easier to make rational decision. On the other hand, attackers are regarded as group-player, because of their different information acquisition abilities and rational characteristics. In the game process, attackers will perform in an incomplete rational way and tend to imitate high payoff strategy behaviors. The process of imitation can be regarded as evolutionary process. As the theory of learning stated, the equilibrium is the results of the long-term process that players with incomplete rationality seek for optimization [3]. In distributed network attack-defense game scenarios, game players, especially attackers as group-player, dynamically adjust their strategies based on game situation and press on towards dynamic equilibrium.

In this paper, we propose a dynamic method in distributed network attack-defense game scenarios. The method takes advantage of defenders' information superiority and attackers' imitation behaviors and induces attackers' evolutionary process to gain more defense payoffs.

The contribution of this paper is as follows. First, we describe distributed network attack-defense game as one-many game, regarding defender as individual-player and attackers as group-player. This way is more realistic. Moreover we formulate the game group-player's behaviors as evolutionary process. Based on the above, we propose a dynamic game method to achieve optimization of defense benefit.

The remainder of this paper is structured as follows. In Section 2, we discuss related work. In Section 3, we describe the problem and distributed network attack-defense game scenarios. In Section 4, we discuss group-players' behaviors in the game and model the behaviors into the imitation evolutionary process. In Section 5, we propose the dynamic game method with a strategy sequence generation algorithm and a parameter analysis method. In Section 6, experiments are performed to verify the proposed method. Finally, in Section 7, we present our conclusions and make recommendations for future works.

2. Related Work

Game theory is a study of mathematical models of conflict and cooperation between intelligent rational decision-makers [4]. In 1928, von Neumann proved the basic principle of game theory, which formally declared the birth of game theory. Due to the superiority of understanding and modeling conflict, game theory has recently been used in the field of computer network security. Reference [5] proposes a model to reason the friendly and hostile nodes in secure distributed computation using game theoretic framework. Reference [6] presents an incentive-based method to model the interactions between a DDoS attacker and the network administrator and a game-theoretic approach to infer intent, objectives, and strategies (AIOS). References [7, 8] also focused on DDos attack and defense mechanisms using game theory. Reference [9] modeled the interactions between an attacker and the administrator as a two-player stochastic game and computed Nash equilibrium using a nonlinear program. However, these researches all assume that both players in the game are consubstantial even individuals. Obviously this assumption cannot cover all the realistic situations. This paper extends this assumption to one-many game to be more realistic.

In the field of dynamic game, [10, 11] focused on the same scenarios as this paper. Reference [10] modeled the interaction of an attacker and the network administrator as a repeated game and found the Nash equilibrium via simulation. Reference [11] models the interaction between the hacker and the defender as a two-player, zero-sum game and explained how min-max theorem for this game is formulated. They concluded by suggesting that to solve this problem linear algorithms would be appropriate. Reference [12] modeled the mission deployment problem as repeated game and computed Nash equilibrium using improved PSO. They all do not consider the attackers' group behaviors. This paper precisely takes advantage of the attackers' group behaviors and in this way defender can gain more payoffs. More related works about applying game theory in network security can be referred to [13].

3. Distributed Network Attack-Defense Game

Given the flexibility that software-based operation provides, it is unreasonable to expect that attackers will demonstrate a fixed behavior over time [14]. Instead, on the one hand, attackers dynamically change their strategy in response to the dynamics of the configuration of the target system or defense strategy. On the other hand, relative to the defenders, attackers vary in degree of information acquisition abilities and rational characteristics.

We simplify attackers into two categories: senior attacker and junior attacker. Senior attacker has greater ability to acquire game information than junior attacker. As a result, senior attacker can react as soon as game situation changes and junior attacker generally follows senior attacker's behavior because of his weaker information acquisition ability.

Different from attackers, defenders, as system officers, are consubstantial and have more information about system, game structure, and payoff matrix. Even if they temporarily lack knowledge, they have more resources to fill in the blank. So the defenders are easier to gain the whole view of game situation.

Similar to Stackelberg model [15], there are senior and junior players in the distributed network attack-defense game. Moreover, distributed network attack-defense game is one-many game, as is stated above. Attackers are group-players, containing a minority of senior players and a majority of junior players. Defender is individual and senior player.

In distributed network attack-defense game, there are three game stages classified based on players' behaviors.

Stage 1. Attackers, as group-players, select different pure strategies randomly and format the proportion distribution of various kinds of pure strategies. Generally, the first game stage will not last too long and it will be terminated by defender's behavior.

Stage 2. Defender, as individual-player, behaves based on the proportion distribution of attack strategies. In our opinion, defender can gain more payoffs through misleading and guiding attacker group distribution structure, as in Section 5.

Stage 3. Senior attackers react to the game situation, and junior attackers follow senior attacker's behaviors to gain more payoffs. Junior attackers' behavioral pattern can be modeled as imitation dynamics model, as in Section 4.

Then, the game situation will repeat between the second stage and the third stage infinitely, unless in some special situation which we will discuss in Section 5.1.

4. Imitation Dynamics Model

As discussed above, attacker group presents imitation dynamics pattern in distributed network attack-defense game. Different from general imitation dynamics model, minority of senior attackers can lead the imitation actions. In this section, we model attacker imitation dynamics in distributed network attack-defense game considering the effect of senior attackers.

Stage 1. As attackers select pure strategies randomly, proportion distribution of various kinds of pure strategies obeys uniform distribution. Let attacker's pure strategy space be S^a $(S^a1, \ldots, S^an)$ and let the number of the attackers be N. The Proportion Vector (PV) of attacker group choosing strategy S^ai at time t is denoted by $P^ai(t)$. In this stage, $P^ai(t)$ is equal to $1/n$. n is the number of attack strategies. In the attacker group, the proportion of senior attackers is denoted by θ. So there are $P^ai(t) \cdot \theta$ senior attackers choosing S^ai. Similarly, defender's pure strategy space is denoted by S^d $(S^d1, \ldots, S^dn)$ and the game situation when attacker chooses S^ai and defender chooses S^dj is denoted by S_{ij}, corresponding to attacker's payoff $S_{ij} \cdot U^a$ and defender's payoff $S_{ij} \cdot U^d$.

Stage 2. Defender behaves based on the proportion distribution of attack strategies. There are two cases to be considered: first defense behavior and follow-up defense behavior. Before the first time defender behaves, senior attackers randomly choose attack strategies and the distribution of senior attackers obeys uniform distribution like junior attackers. After the first time defender behaves, senior attackers always concentrate on the best response strategy no matter how defense strategy changes because of their quick reaction capability and the distribution of senior attackers obeys concentrated distribution.

Stage 3. Senior attackers react to the game situation immediately. Let senior attackers react in vector at time t be $\alpha(t)$. In the first defense behavior case, uniform distribution of the senior attackers concentrates on the best response attack strategy, suppose S^ai:

$$\alpha(t) = \left(-P^a1(t) \cdot \theta, \ldots, \left(1 - P^ai(t)\right) \cdot \theta, \ldots, -P^an(t) \cdot \theta\right). \tag{1}$$

In the follow-up defense behavior case, suppose that best response attack strategy changes from S^aj to S^ai. Then concentrated distribution of senior attackers accordingly changes from S^aj to S^ai:

$$\alpha(t) = (0, \ldots, \theta, \ldots, -\theta, \ldots, 0). \tag{2}$$

Let $\beta(t)$ be the PV after senior attackers' reaction at time t:

$$P^a(t+1) = \beta(t) = P^a(t) + \alpha(t). \tag{3}$$

For junior attackers, they imitate senior attacker's behaviors to gain more payoffs in the imitation probability λ. The distribution of junior attackers concentrates on the best response strategy gradually. Let imitation vector be $\gamma(t)$.

Table 1: Game payoff matrix.

		Defender		
		S^d1	S^d2	S^d3
Attacker	S^a1	4, 1	5, 5	3, **6**
	S^a2	2, 2	1, **9**	**4**, 2
	S^a3	**5**, 3	**7**, 4	3, **5**

Similar to the first defense behavior case, uniform distribution of the junior attackers concentrates on the best response attack strategy, suppose S^ai:

$$\gamma(t) = \left(-P^a1(t) \cdot \lambda, \ldots, \left(1 - P^ai(t)\right) \cdot \lambda, \ldots, -P^an(t) \cdot \lambda\right). \tag{4}$$

In the follow-up defense behavior case, suppose that best response attack strategy changes from S^aj to S^ai. Then concentrated distribution of junior attackers accordingly changes from S^aj to S^ai:

$$\gamma(t) = \left(0, \ldots, +P^aj(t) \cdot \lambda, \ldots, -P^aj(t) \cdot \lambda, \ldots, 0\right). \tag{5}$$

Correspondingly, the Proportion Vector (PV) of attacker group is updated as

$$P^a(t+1) = P^a(t) + \gamma(t). \tag{6}$$

Imitation probability λ is affected by additional game information obtained by junior attackers beyond their own information acquisition ability. In this paper, we assume that the additional game information is obtained from two aspects. One is revealing game information initiatively by defender. The more game information is revealed, the higher value of λ can be. So λ can reach maximum value of 1 if plenty of game information was revealed by defender. The other aspect is internal communication among attacker group which is the natural attribute of group and cannot be controlled by external behaviors. So λ has a constant minimum value, suppose λ_0. As a result, the following is obtained:

$$\lambda_0 < \lambda < 1. \tag{7}$$

As mentioned above, defender has a partially ability to control junior attackers' imitation rate through revealing game information purposefully. The game information revealing strategy will be discussed in Section 5.2.1.

5. Dynamic Game Method

We now present a dynamic game method for achieving the optimization of defense benefit. The proposed method is a two-step procedure which involves defense strategy sequence generation algorithm (SSGA) (Section 5.1) and parameter analysis method (Section 5.2) used to set parameters in dynamic game method.

Consider a simple game payoff matrix L as in Table 1.

```
Input: A game situation $S_{ij}$ and a game payoff matrix $M$
Output: A suitable ring containing $S_{ij}$ as key inducing point
(1) Initial $R(SP(S^d key, S^d assist), S_k, S_a)$;
(2) If $S_{ij}$ is Vertex then
(3)       return null;
(4) else
(5)     $R \cdot SP \cdot S^d key = S^d j$;
(6)     $R \cdot S_k = S_{ij}$;
(7)     $a \leftarrow$ the line of vertex of row $j$;
(8)     for ($m = 1$; $m <= n$; $m$++)
(9)         if $S_{im}$ is Vertex && $S_{am} \cdot U^d > S_a \cdot U^d$
(10)            $R \cdot SP \cdot S^d assist = S^d m$;
(11)            $R \cdot S_a = S_{am}$;
(12)        else continue;
(13)    end for
(14) end if
(15) return $R$;
```

Algorithm 1: *Ring_Idenfy*(S_{ij}, M).

Obviously, defender wishes to keep game situation in $S_{22} = (S^a 2, S^d 2)$ within which he can gain global best payoff of 9. However, this desire seems unrealizable since if defender chooses strategy $S^d 2$, attackers will choose strategy $S^a 3$ as response to gain more payoffs. What we propose is a novel dynamic game method to keep game situation in global best situation as long as possible in which way defender can gain more payoffs.

5.1. Strategy Sequence Generation Algorithm. Strategy sequence generation algorithm (SSGA) produces a strategy pair which will be chosen in sequence circularly by defender to keep game situation in global best situation. Two parameters will be attached to the strategy pair and we will discuss them in Section 5.2.

We firstly define some notions which are necessary in SSGA.

Vertex. It is the best response game situation of attackers. In Table 1, $S_{31} = (S^a 3, S^d 1)$, $S_{32} = (S^a 3, S^d 2)$, and $S_{23} = (S^a 2, S^d 3)$ are vertices. Obviously, there is one and only one vertex in a row of game payoff matrix and, in imitation process, attacker group will gather to the vertex of the row. In this way, we can redefine Nash equilibrium as game situation which is both the vertex and the best response game situation of defender.

Inducing Point. It is game situation which is not *Vertex* and has *Vertex* in the same line. Among inducing points, two inducing points are determined seriously by SSGA: *key inducing point* with higher defense payoff which defender wishes to keep as long as possible, for example, $S_{22} = (S^a 2, S^d 2)$ in Table 1, and *assist inducing point* which is used to adjust the contribution of attacker group and assist to keep game situation in key inducing point. We have the following trivial result of the number of inducing points in a game payoff matrix:

$$N^2 - \sum_{Xi>0} \left[(Xi - 1) \cdot N + Xi \right], \qquad (8)$$

where Xi is the number of vertices in ith line in game payoff matrix.

Ring. A triple $Ring((S^d key, S^d assist), S_k, S_a) \cdot (S^d key, S^d assist)$ is a defense strategy pair which will be chosen in sequence circularly; S_k is inducing point of the ring which is in the same line of vertex of $S^d key$; S_a is inducing point which is in the same line of vertex of $S^d assist$. The defense payoffs of S_k, S_a decide which one is key inducing point and which is the order of strategy pair. In Table 1, $((S^d 2, S^d 3), S_{22}, S_{33})$ is a ring of the responding payoff matrix.

The number of rings in a game payoff matrix can be computed as

$$\mathrm{C}_N^2 - \sum_{i}^{N} \mathrm{C}_{Xi}^2. \qquad (9)$$

It is easy to prove that, unless all the vertices concentrate upon one same line, there must exist at least one ring. A ring identification algorithm is as in Algorithm 1.

In lines 9–11, we select higher defense payoff inducing point and corresponding vertex as the ring result in accordance with original intention.

Based on ring identification algorithm, a global ring selecting algorithm is as in Algorithm 2 to work out a global best ring.

The global ring selecting algorithm works out a ring R which is used in the following method discussion. However, let us consider a special case in which the game has Nash equilibrium with corresponding defense payoff larger than key inducing point's defense payoff. In this case, it is easy to make the conclusion that Nash equilibrium is the better choice. So in this paper, we do not consider this case.

5.2. Parameter Analysis Method. Based on the above discussion, a dynamic game scheme is *DGS* (*Ring*, *Leakage_factor*, and *Duration)*, meaning that how long the time to hold each

```
Input: A game payoff matrix $M$
Output: A global best ring
Initial $L \leftarrow$ the sequence of inducing point in descending order of $S_{ij} \cdot U^d$
Initial $^*p = L$;
While $p$ != null
    If $Ring\_Idenfy(p, M)$ != null
        return $Ring\_Idenfy(p, M)$;
    else
        $p = p.next$;
    end if
end while
return null
```

Algorithm 2: $G\_ring\_select(M)$.

strategy in strategy *Ring* is with which degree of information leakage. Since we have discussed *Ring* in the last section, in this section, we discuss the parameters in the dynamic game scheme, mainly *Duration* and *Leakage_factor*.

5.2.1. Leakage Factor. The parameter *Leakage_factor* indicates to what degree defender should reveal information in each strategy duration to induce the behavior of attacker group. As definition of *Ring* in Section 5.1, there are two strategies in a *Ring*, corresponding to two inducing points. Therefore, the parameter *Leakage_factor* should also have two subparameters.

Leakage_Factor. A two-tuple *Leakage_factor* (L_k, L_a) is a pair of percentage figures corresponding to each strategy in *Ring* and also key inducing point and assisting inducing point. Note that the percentage figures are independent of each other, since they are used during different strategy durations. *Leakage_factor* equaling 0 means that defender does not reveal game information intentionally; oppositely, *Leakage_factor* equaling 1 means that defender reveals plenty of game information; others mean that defender reveals game information partially.

As mentioned above, imitation probability λ is affected by revealed game information. The more game information is revealed, the higher value of λ will be, meaning higher imitation speed of junior attackers. Obviously, we can simply suppose that there is positive correlation between λ and *Leakage_factor*. Since the functional relationship $\lambda = f(Leakage\_factor)$ is not the focus of this paper, we just have the following assumptions:

$$\begin{gathered} f(L) = \lambda_0, \quad \text{if } L = 0 \\ f(L1) \geq f(L2), \quad \text{if } L1 \geq L2 \\ f(L) = 1, \quad \text{if } L = 1. \end{gathered} \tag{10}$$

There are two cases to be considered: duration of $S^d key$ and duration of $S^d assist$.

In duration of $S^d key$, the concentrated distribution of junior attackers changes game situation from key inducing point S_k to the *Vertex* of the same row. Based on our purpose, we wish to keep game situation in key inducing point as long as possible. As the result, defender should decrease *Leakage_factor* to 0 by revealing no game information intentionally, corresponding to minimum imitation probability of λ_0 and the lowest imitation speed of junior attackers.

In duration of $S^d assist$, the concentrated distribution of junior attackers changes game situation from assist inducing point S_a to the *Vertex* of the same row. Based on our purpose, assist inducing point is used to adjust the contribution of attacker group and assist in keeping game situation in key inducing point. So we wish the concentrated distribution of junior attackers ready rapidly to be induced to key inducing point. As a result, defender should increase *Leakage_factor* to 1 by revealing plenty of game information, corresponding to maximum imitation probability of 1 and the highest imitation speed of junior attackers.

5.2.2. Duration. The parameter *Duration* indicates how long the time to hold each strategy in strategy *Ring* is. Similar to *Leakage_factor*, the parameter *Duration* should also have two subparameters.

Duration. A two-tuple *Duration* (D_k, D_a) is a pair of durations corresponding to each strategy in *Ring* and also key inducing point and assisting inducing point.

Before analyzing the parameter of *Duration*, a computational method of the average payoff of game players should be given. Let $E(t)$ be average payoff of players at time t. $E(t)$ can be deduced through payoff variation. Suppose the best response attack strategy changes from $S^a j$ to $S^a i$:

$$E(t) = E(t-1) + (Ui - Uj) \cdot P^a j(t-1) \cdot \lambda, \tag{11}$$

where the second part indicates the payoff increment by junior attackers imitation behavior which means there is the proportion $P^a j(t-1) \cdot \lambda$ of attackers changing strategy from $S^a j$ to $S^a i$, the corresponding payoff increment. The Proportion Vector (PV) strategy $S^a j$ varies as

$$P^a j(t) = P^a j(t-1) \cdot \lambda. \tag{12}$$

Let $E(t0) = e0$ be the initial payoff. The average payoff of players at time t is as follows:

$$\begin{aligned} E(t) &= e0 + \frac{(Ui - Uj)\cdot Pj(t0)\cdot\lambda\cdot\left(1-(1-\lambda)^{t}\right)}{1-(1-\lambda)} \\ &= e0 + (Ui - Uj)\cdot Pj(t0) \\ &\quad - (Ui - Uj)\cdot Pj(t0)\cdot(1-\lambda)^{T}. \end{aligned} \tag{13}$$

Then the sum of player payoff in the duration of T can be deduced as

$$\begin{aligned} SoE(T) &= e0\cdot T + (Ui - Uj)\cdot P^{a}j(t0)\cdot T \\ &\quad - \frac{(Ui - Uj)\cdot P^{a}j(t0)\cdot(1-\lambda)\cdot\left(1-(1-\lambda)^{T}\right)}{1-(1-\lambda)}. \end{aligned} \tag{14}$$

Suppose that there is a dynamic game scheme $DGS(((S^{d}key, S^{d}assist), S_k, S_a), (L_k, L_a), (D_k, D_a))$ and let the cost of changing defense strategy be C. In duration of $S^{d}assist$, defender lets $Leakage\_factor$ change to 1 by revealing plenty of game information, corresponding to maximum imitation probability of 1 discussed above which means attackers converge instantaneously. So we suppose that D_a is 0 and that defender gains no payoffs in duration of $S^{d}assist$. Then the average of defender payoff in the duration of a $Ring$ can be

$$AoR = \frac{(SoE(D_k) - 2 * C)}{D_k}. \tag{15}$$

We can achieve the highest AoR by controlling the only variable D_k through solving the equation of $d(AoR)/d(D_k) = 0$.

6. Experimental Results

6.1. Numerical Example. In this section, we provide a numerical test to illustrate the implementation of the proposed method. In the example, we suppose that the game payoff matrix, the imitation probability, and the cost of changing defense strategy are determined since these are not the focus of this paper. Let λ_0 be 0.1 and the game payoff matrix as Table 1.

Using SSGA, we figure out a pair of defense strategies and a dynamic game scheme $(((S^{d}2, S^{d}3), S_{22}, S_{33}), (L_k, L_a), (D_k, D_a))$. As mentioned above, we want to keep game situation in S_{22} as long as possible. So let $L_k = 0, L_a = 1$ and correspondingly $\lambda = \lambda_0$ and $\lambda = 1$. As a result, the dynamic game scheme should be $(((S^{d}2, S^{d}3), S_{22}, S_{33}), (0, 1), (D_k, 0))$. The influence of D_k on AoR is as in Figure 1.

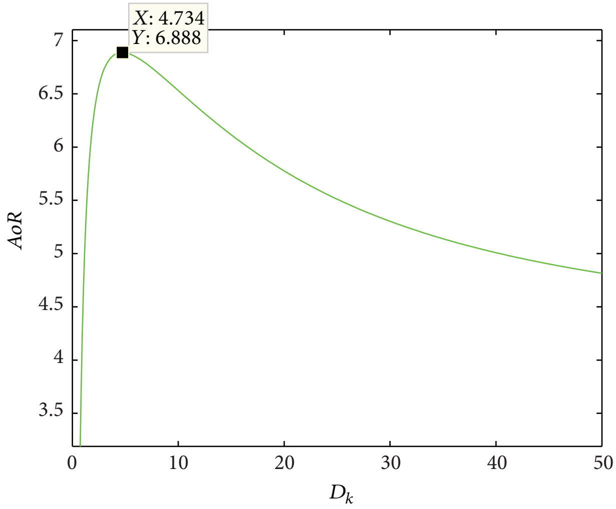

Figure 1: The influence of D_k to AoR.

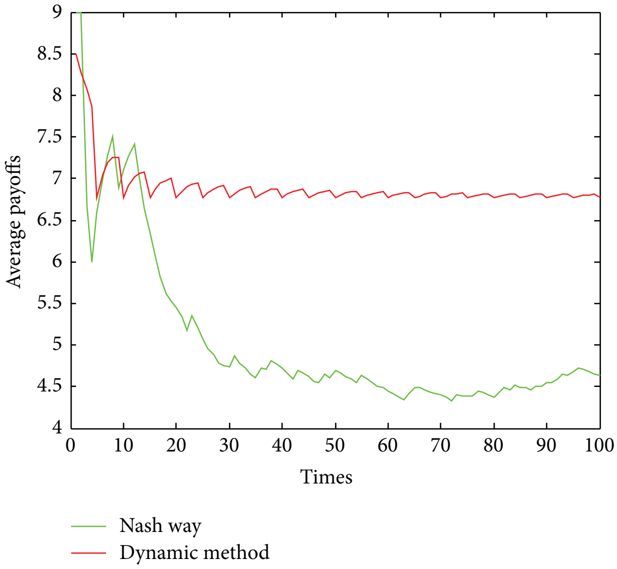

Figure 2: The comparison of average payoffs.

The result of the equation $d(AoR)/d(D_k) = 0$ is $D_k \approx 4.734$. When $D_k < 4.734$, defender changes strategies frequently by which lots of costs $C = 2$ are introduced. So we can see in Figure 1 that, with the increase of D_k, AoR grows rapidly. When $D_k > 4.734$, the cost of changing defense strategy is not main impact factor on AoR anymore because of low frequency of defense strategy replacement. In this case, attackers change their convergence from S_{22} to S_{32} gradually in the process where defender's payoff decreases. That means that longer duration results in low AoR, as seen in the figure.

6.2. Effectiveness. In this section, we verify the effectiveness of proposed method. Reference [12] proposed a game strategy optimization approach solving mission deployment problem. A Nash way to choose game strategy is figured out using particle swarm optimization (PSO). Although reference [12] had different assumption and problems with this paper, the method itself is comparable. We compare the average defender payoffs achieved by two methods, shown in Figure 2.

We can see in Figure 2 that the graphic of dynamic method shows the vibration waveform and amplitude decreases. In every vibration cycle, average payoffs increase firstly with a declining slope. This is because of the fact that the dynamic regulation of attacker group leads to the decreasing growth rate of defender payoff. Then average payoff decreases rapidly caused by the cost of changing strategies. In Nash way, the average payoff fluctuates seriously in the earlier stage because the average payoff is still unstable as average values [12]. Then, after about 30 times, the average payoff is tending towards stability, about 4.5. It is clear that the dynamic method can achieve obviously higher average payoff. The Nash way seeks for an optimization approach by safeguarding a Nash equilibrium game situation. This is driven by minimizing the possible losses. On the other hand, in this paper, our dynamic method applies a different thinking by seeking for the global best payoff in the game. So our method can greatly improve the payoffs.

7. Conclusions

In this paper, we model distributed network attack-defense game as one-many game and formulate the game group-player's imitation behaviors as evolutionary process. Taking advantage of defenders' information superiority and attackers' imitation behaviors, we propose a dynamic game method to help defender gain more payoffs through inducing attackers' evolutionary process. The experiments prove the effectiveness of the proposed method. In our future research, we will apply the proposed method in other areas to verify the effectiveness, such as state estimation, dynamics control, resources allocation, or information management [16–18].

On the other hand, this paper is based on the assumption that players in the game are seeking for the increasing of their own payoffs and do not care about opponents'. However, in the reality, there are different types of attack. For example, there exists such case where attackers are seeking for destroying opponent's system. In this kind of attack, attackers concentrate more on the decreasing of opponent's payoffs than the increasing of their own payoffs. So the attack type will affect defense mode. Our future work will be driven towards these problems.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work is supported by Project 042500318 which is supported by National Nature Science Foundation of China.

References

[1] M. R. Grimaila, R. F. Mills, M. Haas, and D. Kelly, *Mission Assurance: Issues and Challenges*, Air Force Institute of Technology, Center for Cyberspace Research, Wright-Patterson AFB, Ohio, USA, 2010.

[2] K. Binmore, "Foundation of game theory," in *Advances in Economic Theory: Sixth World Congress*, J. Laffont, Ed., vol. 1, pp. 1–31, Cambridge University Press, Cambridge, UK, 1992.

[3] D. Fudenberg and D. K. Levine, "Learning in games," *European Economic Review*, vol. 42, no. 3–5, pp. 631–639, 1998.

[4] R. B. Myerson, *Game Theory*, Harvard University Press, Cambridge, Mass, USA, 1991.

[5] P. F. Syverson, "Different look at secure distributed computation," in *Proceedings of the 10th IEEE Computr Security Foundations Workshop (CSFW '97)*, pp. 109–115, IEEE, June 1997.

[6] P. Liu, W. Zang, and M. Yu, "Incentive-based modeling and inference of attacker intent, objectives, and strategies," *ACM Transactions on Information and System Security*, vol. 8, no. 1, pp. 78–118, 2005.

[7] J. Mirkovic and P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, 2004.

[8] J. Xu and W. Lee, "Sustaining availability of web services under distributed denial of service attacks," *IEEE Transactions on Computers*, vol. 52, no. 2, pp. 195–208, 2003.

[9] K.-W. Lye and J. M. Wing, "Game strategies in network security," *International Journal of Information Security*, vol. 4, no. 1-2, pp. 71–86, 2005.

[10] T. Alpcan and T. Başar, "A game theoretic analysis of intrusion detection in access control systems," in *Proceedings of the 43rd IEEE Conference on Decision and Control (CDC '04)*, pp. 1568–1573, December 2004.

[11] X. Z. You and Z. Shiyong, "A kind of network security behavior model based on game theory," in *Proceedings of the 4th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT '03)*, pp. 950–954, IEEE, August 2003.

[12] L. Xiaojian, Y. Yuyu, F. Binxing, and G. Yi, "A strategy optimization approach for mission deployment in distributed systems," *Mathematical Problems in Engineering*, vol. 2014, Article ID 404681, 8 pages, 2014.

[13] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS '10)*, pp. 1–10, IEEE, Honolulu, Hawaii, USA, January 2010.

[14] M. H. R. Khouzani, S. Sarkar, and E. Altman, "A dynamic game solution to malware attack," in *Proceedings of the IEEE INFOCOM*, pp. 2138–2146, April 2011.

[15] K. Basu, "Stackelberg equilibrium in oligopoly: an explanation based on managerial incentives," *Economics Letters*, vol. 49, no. 4, pp. 459–464, 1995.

[16] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys*, vol. 45, no. 3, article 25, 2013.

[17] C. Leboucher, R. Chelouah, P. Siarry, and S. le Ménec, "A swarm intelligence method combined to evolutionary game theory applied to the resources allocation problem," *International Journal of Swarm Intelligence Research*, vol. 3, no. 2, pp. 20–38, 2012.

[18] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Game theory meets information security management," in *ICT Systems Security and Privacy Protection*, vol. 428 of *IFIP Advances in Information and Communication Technology*, pp. 15–29, Springer, Berlin, Germany, 2014.