Journal of Computational Information Systems 6:7(2010) 2199-2211
Available at http://www.Jofcis.com

Dynamic Game Based Intrusion Response Model

Jianqi ZHU[1,2], Yanheng LIU[1,2,†], Xu YANG[1,2], Xin SUN[1,2]

[1]*College of Computer Science and Technology, Jilin University, Changchun 130012, China*

[2]*Key Laboratory of Computation and Knowledge Engineering, Ministry of Education*

Abstract

The severity and number of intrusions on computer networks are rapidly increasing, which requires advances not only in detection algorithm, but also in automatic response techniques. In this paper, a new approach to automatic response called DGII_IDR is presented that employs a game-theoretic response strategy against adversaries. It transforms the incomplete information dynamic game into a complete but imperfect information game by Harsanyi transformation. The optimal response is chosen by the use of perfect Bayesian equilibrium to revise the posterior belief of player's type continuously. Moreover, DGII_IDR solved the conflict between the rational assumption and irrational behavior of attacker/defender by restricting their strategies in game theory. We also show how our game theoretical framework can be applied to configure the intrusion detection strategies in realistic scenarios via a case study and demonstrate the effectiveness of DGII_IDR.

Keywords: Network Securities; DGII_IDR; Game Theory; Harsanyi Transform; Perfect Bayesian Equilibrium; Payoff

1. Introduction

The proliferation of complex and fast-spreading intrusions against computer systems brought new requirements to intrusion detection (ID) and intrusion response (IR). Although the IR component is often integrated with the ID system (IDS), it receives considerably less attention than IDS research owing to the inherent complexity. In recent years the focus has shifted towards the development of sophisticated and automated intrusion response system (IRS) [1-8]. According to different mechanisms, three types of techniques aimed at enhancing automation in the IRS were proposed.

Static mapping: essentially automated manual response system that maps an alert to a predefined response. These systems are easy to build and maintain as pH [1] and BMSL-based response [2] system. However, they are also predictable and therefore, vulnerable to intrusions. Besides, it doesn't take into account the current state of the system and the negative response.

Dynamic mapping: response decision is based on some attack metrics (confidence, severity of attack, etc.). A typical dynamic response mapping model used in adaptive, agent-based intrusion response system (AAIRS) is proposed by Carver [3][4]. In the setting of dynamic mapping an intrusion alert is associated with a set of response actions. The exact action is chosen in real-time based on the characteristics of the attack. By adjusting attack metrics we can provide more flexibility in intrusion response decision. Although this approach provides much more fine-grained and flexible control in response to an attack, it can still be

[†] Corresponding author.
Email addresses: liuyh@jlu.edu.cn (Yanheng LIU), zhujq@jlu.edu.cn (Jianqi ZHU).

July, 2010

potentially exploited by adversary [5]. Besides it seldom considers the negative impact of a response and therefore, the response cost may be greater than the damage cost.

Recently, cost-sensitive response model, which is the only response system that attempts to balance intrusion damage and response cost became more attractive [6-9]. In this case, an intrusion which has a higher response cost than damage cost should usually not be acted upon beyond simple logging. One of the downsides of this approach is the necessity to update cost factor values over time. In most cases this is done manually which puts additional burden on the system administrator.

In order to overcome the shortcomings of aforesaid IRS, a game-theoretic approach called DGII_IDR (Dynamic Game with Incomplete Information based IDR model) is suggested to model the interactions between the attacker and defender. Game theory has been a strong candidate to provide mathematical framework for analysis, modeling, decision, and control processes for computer security [10-14]. However, there has been limited and minimal research in IRS. We formulate the attacker/defender game model in dynamic Bayesian game contexts. The motivation behind our Bayesian game formulation is that generally an attacker/defender game is an incomplete information game where the defender is uncertain about the type of his opponent (regular or malicious). Moreover, the defender can dynamically update his beliefs based on new observations of the opponent's actions and the game history, and therefore can adjust his strategy. Our model has the following features: (1) analyze attacker and defender's behavior and create a response decision model with incomplete information dynamic game in order to update the responses on-the-fly and make quick decision. (2) incorporate some risk factors such as the errors of false negative and false positive etc. in payoff assessment. (3) solve the conflict in game theory between the rational assumption and irrational behavior of players for the first time. (4) propose an improved payoff assessment model for attack-defense game.

The remainder of the paper is organized as follows. Section 2 discusses the related work. Dynamic game model DGII_IDR is given in section 3. Section 4 outlines the payoff assessment approach. Experimental setup and results are given in Section 5. Section 6 concludes the paper with our future work.

Related work. The game theory discipline is to address problems where multiple players with different objectives compete and interact with each other on the same system. In recent years, it is a strong candidate to provide mathematical framework for analysis, modeling, decision, and control processes for computer security. Lye [9] etc. present a game theoretic method for analyzing the security of computer networks, which views the interactions between attacker and administrator as a two-player stochastic game and constructs an assessment model for the network security. Otrok [10] etc. put forward an optimized framework scheme that aims at developing a network packet sampling strategy to effectively reduce the chance of attack using game theory. Fang bin xing [11] etc. present some models including defense graph model, attack-defense taxonomy, cost quantitative method, and attack-defense game model in order to evaluate the security of network information system and give an optimal active defensive selection algorithm. Zhu jian ming [12] presents an evaluation model of information security technologies based on game theory, and the information security technologies include firewall, IDS and intrusion tolerant that construct a three layers architecture. Liu[13] etc. put forward an approach that dynamically adjusts the objects that the host-based IDS (HIDS) monitors according to the expected attacks based on non-cooperative game. Carroll[14] etc. model the interactions between attacker /defender using a signaling game that is a non-cooperative two player dynamic game with incomplete information, and then present the benefits of employing deceptive equilibrium strategies in the defense of computer network.

The common of above researches is the assumption that attacks are rational and intelligent. However, in the real network, attacks are usually irrational that have no concerns about the costs associated with their attacks compared with rational attacks. This paper solves the conflict between the rational assumptions and irrational behaviors of attack-defense game by restricting their strategies.

2. DGII_IDR

The architecture of DGII_IDR model in this paper is shown in Fig.1, which includes modules of the intrusion detection (ID), alert aggregation (AA) and intrusion response (IR). ID includes various types of IDS to generate the intrusion alerts. AA aggregates large numbers of alerts produced by IDS, eliminates redundancy and generates a small amount of high-level alerts. IR produces the optimal response based on dynamic game model. IR includes:

1. Strategy space: both for attacker/defender, different alert correspond to different strategy.

2. Attack threat level set: records the threat levels of occurred attacks, which will be the main basis for evaluating the prior belief in the decision-making stage.

3. System information collection: collects the system information and assesses the weights of the system resources.

4. Payoff assessment: computes the payoffs under different circumstances for both sides.

5. Response decision: driven by the high-level alerts, inquiry the strategies and computes the payoffs for both sides, this module will construct a game scenario to produce the optimal response through the game perfect Bayesian equilibrium. The whole process does not require human intervention, so DGII_IDR is an automated intrusion response system.

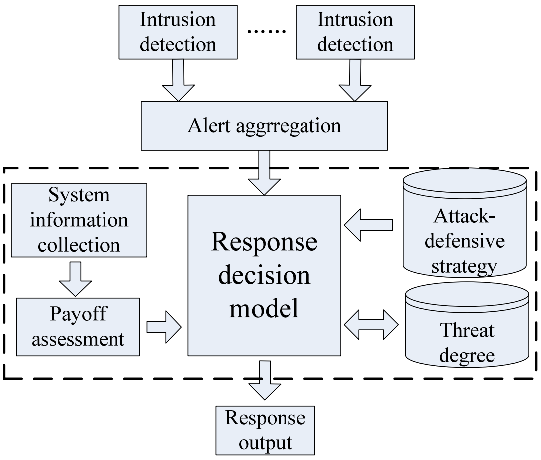

Fig.1 Architecture of DGII_IDR

2.1. Game Scenarios

The strategies of attacker and defender are mutual restraint in the network thus affecting their effectiveness. Game theory is to address problems where multiple players with different objectives compete and interact with each other on the same system, so it can be used to analyze the interactions between the attacker and defender. The motivation behind our game formulation is that generally an attacker/defender game is an incomplete information game where defender is uncertain about the type of his opponent (regular or malicious). A dynamic Bayesian game formulation provides a framework for the defender to select his strategies based on his belief on the type of his opponent. Moreover, dynamic Bayesian game model is more realistic, because the defender can dynamically update his beliefs based on the new observations of opponent's actions and the game history, and then can adjust his strategy accordingly [15].

The response decision model in this paper includes the following elements.

1. Players: including attacker and defender. Attacker mainly refers to malicious network attackers or internet users who make a threat to network security. Defender may be a host equipped with IDS, firewall etc. The defender's type is d_n and the type space is $D=\{d_0,d_1,...,d_{N-1}\}$, card($D$)=$N$. The attacker's type is h_m and the type space is $H=\{ h_0,h_1,...,h_{M-1} \}$, card(H) = M. $\eta_{n,m}=(d_n,h_m)$ is the attacker/defender posture and the posture space is $\eta=\{ \eta_{0,0}, \eta_{0,1},..., \eta_{N-1,M-1}\}$, card(η) = $N\times M$. h_0 represents pseudo-attacker who is actually an ordinary user misjudged by IDS as a malicious attack.

2. Strategy space: The defender's strategy is denoted as r_j and the strategy space is $R=\{r_0,r_1,...,r_{J-1}\}$. The attacker's strategy is a_k and the strategy space is $A=\{a_0,a_1,...,a_{K-1}\}$, a_0 means no attack.

3. Payoff function: The payoffs of both sides are represented by $U_d(\eta_{n,m},r_j,a_k)$ and $U_h(\eta_{n,m},r_j,a_k)$, respectively.

4. Private information: For one thing, player's type is private and transparent to others. For another, player can dynamically update his beliefs based on the new observations of opponent's actions and adjust his strategy accordingly.

5. Prior belief: The prior belief of attacker's type is denoted as $p(h_m)$, and $\sum_{m=0}^{M-1} p(h_m)=1$. The prior belief of defender's type is $p(d_n)$, and $\sum_{n=0}^{N-1} p(d_n)=1$.

6. Posterior belief: $p(d_n|r_j)$ is the posterior belief of defender's type judged by attacker after defender adopts r_j strategy, computed by Bayesian formula.

$$p(d_n \mid r_j) = p(d_n)p(r_j \mid d_n) / p(r_j) \tag{1}$$

Where $p(r_j)$is computed by the total probability formula.

$$p(r_j) = \sum_{n=0}^{N-1} p(d_n)p(r_j \mid d_n) \tag{2}$$

2.2. Rational Assumption and Irrational Behavior

There is a central assumption in game theory: the players are rational and intelligent. A rational player is one who always chooses a strategy which gives the outcome he most prefers. However, in general network game models, most strategies of attacker and defender are set well in advance. They don't update their strategies according to the changes of game scenario. So, the rational assumption in the game theory can't be simply used in the real network game scenario.

In most network game models as [9-14], players with different types have different payoffs. In our DGII_IDR model, their strategies are also different. The strategy spaces of rational and intelligent attacker/defender are *R* and *A*, while to the general attacker/defender, their strategy spaces are a subset of *R* and *A*, which depends on the attacker/defender themselves.

2.3. Attacker's Threat Level

Attacker's threat level and space are denoted as t_v and $T=\{t_0,t_1,\ldots,t_{V-1}\}$, card($T$)=$V$. $p(t_v)$is the probability that attacker's threat level is t_v. The threat level space records the occurred attacks' threat levels, which are stored in the database, will be the main basis for evaluating the prior belief in the decision-making stage. The attackers' threat level information is denoted as $(p(t_0), p(t_1),\ldots, p(t_{V-1}),c)$, $\sum_{v=0}^{V-1} p(t_v)=1$, c is the version and the initial value is 0. The initial values of threat level information are same, which are determined by the occurred ratio of different threat level attacks.

The response decision model will compute the posterior belief and update the threat level by observing the attacker's follow-up action. The revised formula is as (3):

$$p(t_v)=\delta(c)\times p(t_v \mid A_k)+(1-\delta(c))\times p(t_v) \tag{3}$$

Where, $\delta(c)$ is the revision factor in each game step. The attack threat level is used to set the prior belief of the attacker's type in the decision-making model, for example, $p(h_v)= p(t_v)$.

2.4. Optimal Response Decision

Generally, an attacker/defender game is an incomplete information game where the defender is uncertain about the type of his opponent (regular or malicious). Thus, the game rules can't be defined. Harsanyi[16] proposed a virtual player who decides the types of involved players and makes the player only knows his/her own type.

On the basis of the virtual player and Harsanyi transformation [16], in this paper, dynamic game with incomplete information is converted into complete dynamic game but imperfect information. Fig.2 shows the game process, in which virtual player *N* chooses the posture η and inform the players of their types. First, defender responses to the alert and then attacker choose his/her following strategy according to defender's action. During this process, attacker and defender can choose any strategy in their strategy space. As play evolves, observed strategy choices allow players to update their beliefs, and more accurately judge a player's type. Last, the payoffs can be computed based on the posture and their strategies.

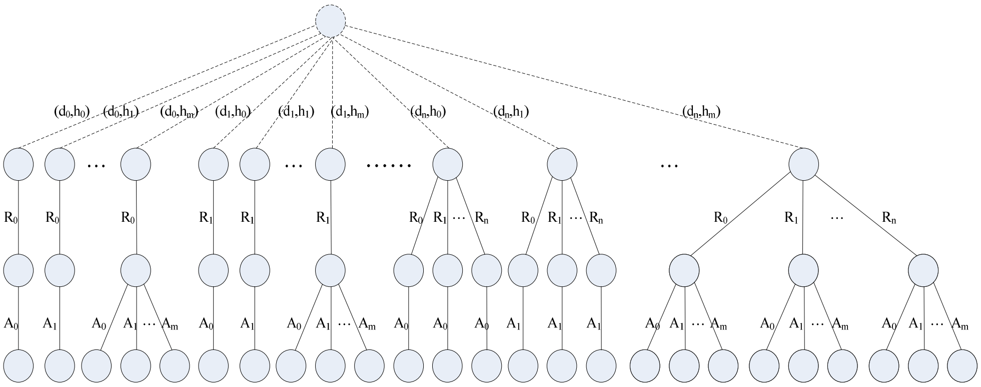

Fig.2 Game Process

Perfect Bayesian equilibrium [17] is composed of a strategy combination $s^*(\theta)=(s_1^*(\theta_1),...,s_n^*(\theta_n))$ and a posterior belief combination $\tilde{p}=(\tilde{p}_1,...,\tilde{p}_n)$, which satisfies the following conditions:

1. (P) For any player *i*, at each information set *h*

$$s_i^*(s_{-i},\theta_i)\in\arg\max_{s_i}\sum_{\theta_{-i}}\tilde{p}_i(\theta_{-i}\mid a_{-i}^h)u_i(s_i,s_{-i},\theta_i),i=1,2,...,n$$

2. (B) $\tilde{p}_i(\theta_{-i}\mid a_{-i}^h)$ is computed by the use of Bayes rule and based on the prior belief $p_i(\theta_{-i}\mid\theta_i)$, observed a_{-i}^h and optimal strategy s_{-i}^*.

The player's type is θ_i, $p_i(\theta_{-i}\mid\theta_i)$ is the prior belief that player *i* with type θ_i think that other *n*-1 players' types are $\theta_{-i}=(\theta_1,...,\theta_{i-1},\theta_{i+1},...,\theta_n)$. S_i is the strategy space of *i*, $s_i\in S_i$ is a specific strategy which depends on θ_i. $a_{-i}^h=(a_1^h,...,a_{i-1}^h,a_{i+1}^h,...,a_n^h)$ is the other *n*-1 players' strategy combination observed by player *i* at the h^{th} information set, which is a part of $s_{-i}=(s_1,...,s_{i-1},s_{i+1},...,s_n)$. $\tilde{p}_i(\theta_{-i}\mid a_{-i}^h)$ is the posterior belief that player *i* think that other *n*-1 players' type are $\theta_{-i}=(\theta_1,...,\theta_{i-1},\theta_{i+1},...,\theta_n)$ after *i* observed a_{-i}^h. $\tilde{p}_i$ is the set of all posterior beliefs $\tilde{p}_i(\theta_{-i}\mid a_{-i}^h)$, that is, $\tilde{p}_i$ includes all the posterior beliefs of player *i* at each *h*. $u_i(s_i,s_{-i},\theta_i)$ is the payoff of player *i*. In DGII_IDR model, we have two players: attacker *h* and defender *d*, their types are h_m and d_n, the prior beliefs are $p(h_m)$ and $p(d_n)$, the strategy spaces of defender and attacker are $R=\{r_0,r_1,...,r_{J-1}\}$ and $A=\{a_0,a_1,...,a_{K-1}\}$, respectively. The posterior beliefs are $p(h_m|A_k)$ and $p(d_n|R_j)$, the payoffs are $U_a(\eta_{n,m},R_j,A_k)$and $U_d(\eta_{n,m},R_j,A_k)$.

(P) is the perfect condition, given the other players' strategies $s_{-i}^*(t_{-i})$ and posterior belief $\tilde{p}_i(\theta_{-i}\mid a_{-i}^h)$ of player *i*, each *i*'s strategies are optimal in the following game from information set *h*. Obviously, the rational and intelligent attacker/defender satisfies above condition. For irrational attacker/defender game, above condition can also be met by restricting their strategies.

(B) is the usage of Bayes rule. The posterior belif of player's type is determined by Bayes rule, the model in this paper conforms to this principle.

3. Payoffs Assessment

Formulating the payoffs assessment is especially important because it can affect the perfect Bayesian equilibrium, therefore affecting the choice of the optimal response strategy. Based on Strasburg's [18] method, an improved IR payoff model is presented that adds some security policy goals (such as administrator or user authorities) to the system resources, and also considers the impact of potential risk factors (errors of false negative and false positive) and attack threat level etc.

3.1. System Resource and Weight

System resources can be broadly viewed as the system assets (e.g., host, network, etc.), services provided by the system (e.g., FTP, HTTP, file system, etc.) and users served by the system. The system security goals can be classified as follows:

1. *Availability*: indicates the requirement of service and information availability upon request.

2. *Integrity*: a guarantee of the consistency and accuracy of the information or the system computing environment as a whole.

3. *Confidentiality*: refers to the imposed restrictions on information flows, e.g., restricted access to data.

The importance of a resource depends on the system security goals which in turn depend on the type of system. Therefore, the resources are assigned weights according to their importance for each system policy goal for a specific system. The overall weight of the system resources, denoted as *W*(*SR*), is computed as a combination of the resource importance for each security goal category SRI_i (*i* is the policy category index) and system specific category weight PCW_i (weight of the *i*-th security category index):

$$W(SR) = \sum_i SRI_i \times PCW_i \tag{4}$$

3.2. Payoffs

The payoff model includes the *damage cost*, *response cost*, *intrusion operation cost* and *intrusion benefit.*

1. *Damage cost*

Damage cost $IDC(\eta_{n,m},A_k)$ assesses the amount of damage that could potentially be caused by the attack.

$$\begin{aligned} IDC(\eta_{n,m},A_k) &= DC(\eta_{n,m},A_k) + damage\ \ \mathrm{cos}t\ \ by\ \ false\ \ negative\ \ rate \\ &= DC(\eta_{n,m},A_k) + \frac{fn(A_k)}{1-fn(A_k)} \times DC(\eta_{n,m},A_k) \\ &= \frac{DC(\eta_{n,m},A_k)}{1-fn(A_k)} \end{aligned} \tag{5}$$

Where, $fn(A_k)$ is the false negative rate of attack A_k, $DC(\eta_{n,m},A_k)$ is the basic *damage cost* caused by A_k *as* (6), which is computed as a combination of $Avail(A_k,SR_i)$ that is the intrusion impact to the resource SR_i and system resource weight $W(SR_k)$, *TL* is the attack threat level.

$$DC(\eta_{n,m},A_k) = TL \times \sum_i (Avail(A_k,SR_i) \times W(SR_i)) \tag{6}$$

2. *Response cost*

Response cost is denoted as $IIC(\eta_{n,m},R_j)$ that is the negative impacts to the system caused by response decision defined as (7).

$$\begin{aligned} IIC(\eta_{n,m},R_j) &= IC(\eta_{n,m},R_j) + response\ \ \mathrm{cos}t\ \ by\ \ false\ \ positive\ \ rate \\ &= IC(\eta_{n,m},R_j) + \frac{fn(A_k)}{1-fn(A_k)} \times IC(\eta_{n,m},R_j) \\ &= \frac{1+2fn(A_k)}{1+fn(A_k)} \times IC(\eta_{n,m},R_j) \end{aligned} \tag{7}$$

Where $fn(A_k)$ is the false negative rate of attack A_k, $IC(\eta_{n,m},A_k)$ is the basic *response cost* to A_k as (8). $Impact(R_i, SR_i)$ is the impact of response R_i on resource SR_i.

$$IC(\eta_{n,m}, R_j) = \sum_i Impact(R_j, SR_i) \times W(SR_i) \tag{8}$$

3. *Attacker's payoff*

Attacker's payoff means the benefits that attacker obtained when he/she is successful, which is closely relative to the damages to IDS. In general, *attacker's payoff* is equal to the *damage cost* of the system. The *payoff* of A_k is denoted as $IR(\eta_{n,m},A_k)$ as formula (9).

$$IR(\eta_{n,m},A_k) = -DC(\eta_{n,m},A_k) \tag{9}$$

Where, $DC(\eta_{n,m},A_k)$ is the basic *damage cost* to the system by A_k.

4. *Operational cost*

The main cost in the operation of an attack, denoted by $AC(\eta_{n,m},A_k)$, is the amount of time and computing resources (such as bandwidth, disk space or CPU time). The costs of general attacks are little, but, for example, Denial of Service (DoS: an attempt by attackers to prevent access to resources by legitimate users for which they have authorization) will occupy huge system resources. So we classify features into two levels, based on their costs:

Level 1: general attack that occupies few system resources.

Level 2: special attack that occupies huge system resources as DOS attack.

The payoffs of our model is as Table 1.

Table 1 Payoffs

Scenario	Payoff
Attack Succeeds	$U_a(\eta_{n,m},R_j,A_k) = AC(\eta_{n,m},A_k) + IR(\eta_{n,m},A_k)$
Attack Fails	$U_a(\eta_{n,m},R_j,A_k) = AC(\eta_{n,m},A_k)$
Defender Reponses & Succeeds	$U_d(\eta_{n,m},R_j,A_k) = IC(\eta_{n,m},R_j)$
Defender Reponses & Fails	$U_d(\eta_{n,m},R_j,A_k) = IC(\eta_{n,m},R_j) + IDC(\eta_{n,m},A_k)$
Defender No Responses	$U_d(\eta_{n,m},R_j,A_k) = IDC(\eta_{n,m},A_j)$

4. Case Study

The network topology used in this case is shown in Fig.3, NIDS is the network intrusion detection system, and the defensive host is equipped with HIDS and DGII_IDR system presented in this paper.

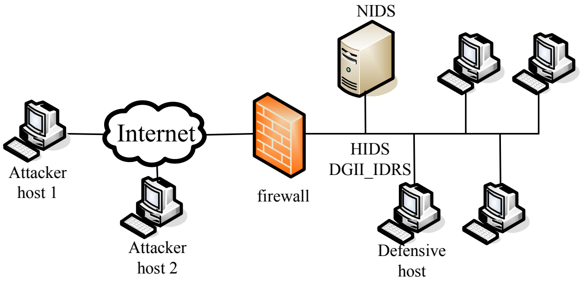

Fig.3 Topology of Proposed Network

Scenario 1: Attacker (host 1) with lower threat level attacks defensive host with the automatic tool, the process is as following:

Sadmind ping vulnerability scanning →Sadmind buffer overflow attack

Scenario 2: Attacker (host 2) with higher threat level attacks defensive host with intelligence.

First attack: Sadmind ping vulnerability scanning in step1, and then chooses one strategy from the strategy space {stopping attack, attack of sandmind buffer overflow immediately, attack of sandmind buffer overflow after time delay (e.g., 10 minutes)} to launch the next attack in step2.

Second attack: 24 hours later, attacker continues attacking to host2. In step1, attacker launches LPD vulnerability scanning, and then chooses one strategy from the strategy space {stopping attack, attack of LPD overflow immediately, attack of LPD overflow after time delay (e.g., 10 minutes)} to launch the next attack.

The type spaces of attacker/defender are shown in Table 2 and Table 3. Attacker's strategy space is $A=\{A_0,A_1,A_2\}$ and defender's strategy space is $R=\{R_0,R_1,R_2\}$, as shown in Table 4. The main resources of SR_1 and SR_2 are affected by the attacks of sandmind and LPD overflow as shown in Table 5. The affection $Avail(A_j,SR_k)$ caused by attack A_j on the system resource SR_k and $Impact(R_i,SR_k)$ caused by response R_i on SR_k are shown in Table 6. The value of basic cost $AC(\eta_{n,m},A_j)$ is shown in Table 7.

Table 2 Attacker's Type

Types	Strategy	*TL*	Descriptions
h_0	$\{A_0\}$	0	Pseudo attacker:ordinary user misjudged by IDS as malicious attack.
h_1	$\{A_1\}$	1	Lower threat attacker:Scripts etc., use the known programs or scripts to attack computers' vulnerabilities randomly, seldom care for the potential dangers.
h_2	$\{A_0,A_1,A_2\}$	1.5	Higher threat attacker:Often accurately and carefully targeted in the selection of a specific aggressive behavior in the attack.

Table 3 Defender's Type

Types	Strategy	Descriptions
d_0	$\{R_0\}$	Lower security defender:No response automatically to any attack
d_1	$\{R_1\}$	Medium security defender:Make a fixed response to attack
d_2	$\{R_0,R_1,R_2\}$	Higher security defender:Intelligent and rational, make different response according to different circumstance.

Table 4 Strategies

Attack Level	Strategy	Defender Level	Strategy
A_0	Stop attacking	R_0	No response
A_1	Launch next attack immediately	R_1	Blockade attacker's IP for 10 mininutes
A_2	Launch next attack at a appropriate time	R_2	Close the attacked service

Table 5 Strategy Space

Resource	Security Policy	Lower Security Defender			Medium Security Defender			Higher Security Defender		
		PCW	SRI	W(SR$_i$)	PCW	SRI	W(SR$_i$)	PCW	SRI	W(SR$_i$)
SR$_1$	availability	1.0	1.0	1.04	0.8	1.0	0.88	0.5	1.0	0.7
	confidentiality	0.0	0.1		0.3	0.1		1.0	0.1	
	integrity	0.4	0.1		0.5	0.1		1.0	0.1	
SR$_2$	availability	1.0	0.2	0.52	0.8	0.2	0.86	0.5	0.2	1.9
	confidentiality	0.0	1.0		0.3	1.0		1.0	1.0	
	integrity	0.4	0.8		0.5	0.8		1.0	0.8	

Table 6 Strategy Space

System Resource	Attack of Sandmind Overflow						Attack of LPD Overflow					
	A_0	A_1	A_2	R_0	R_1	R_2	A_0	A_1	A_2	R_0	R_1	R_2
SR$_1$	0	0	0	0	-10	-30	0	0	0	0	0	-10
SR$_2$	0	-20	-20	0	0	0	0	-18	-18	0	-25	0

Table 7 Strategy Space

	A_0	A_1	A_2
Attack of Sandmind Overflow	0	-1	-4
Attack of LPD overflow	0	-1	-4

The prior belief of defender's type is assumed as $p(\mathrm{d}_0) = 0.2$, $p(\mathrm{d}_1) = 0.2$; $p(\mathrm{d}_2) = 0.6$. The false positive rate of IDS is 0.05 and false negative rate to the attacks of sandmind & LPD overflow is 0.1. The initial values of *TL* is $p(t_0)$=0.05, $p(t_1)$=0.85, $p(t_2)$=0.1. So, the prior belif of attacker's type is $p(h_0) = 0.05$, $p(h_1) = 0.85$, $p(h_2) = 0.1$.

As shown in Fig.3, the defensive host is equipped with HIDS and DGII_IDR system, which can be regarded as a higher security defender and the strategy space is $\{R_0,R_1,R_2\}$.

The following is the game process of Scenario 1.

After receiving the sandmind ping alert from IDS, IDR model calls the information from the strategy spaces, attacker threat level and payoffs model to make decision. Table 8 is the attacker/defender's payoffs, the value of payoff is denoted as the format (*payoff of defender, payoff of attacker*).

Table 8 Attacker/Defender's Payoffs

		h$_0$	h$_1$	h$_2$		
		A_0	A_1	A_0	A_1	A_2
d$_0$	R_0	（0.0）	(-11.56,9.4)	(0,0)	(-17.33,14.6)	(-17.33,11.6)
d$_1$	R_1	(-9.22,0)	(-9.22,-1)	(-9.22,0)	(-9.22,-1)	(-37.89,21.8)
d$_2$	R_0	(0,0)	(-42.22,37)	(0,0)	(-63.33,56)	(-63.33,53)
	R_1	(-7.33,0)	(-7.33,-1)	(-7.33,0)	(-7.33,-1)	(-70.66,53)
	R_2	(-22,0)	(-22,-1)	(-22,0)	(-22,-1)	(-22,-4)

The expected payoff of defender is as Table 9.

Table 9 .Expected Payoff of Defender

Response Strategy	R_0	R_1	R_2
Expected Payoff	-42.22	-13.0805	-22

To sum up, the pure strategy *(R_1,A_1)* is obtained by the perfect Bayesian equilibrium. That is, DGII_IDR system chooses the response R_1 and stops the follow-up attack A_1 successfully.

The following is the game process of scenario 2.

The first attack in scenario 2 is same as in the scenario 1. However, the attacker here is rational and intelligent, who is a higher threat level attacker.

The expected payoff of defender is shown in Table 9, who chooses response R_1 by the perfect Bayesian equilibrium. Assume the revision factor $\delta(c)=1/(c+1)$, c=1, $\delta(1)=1/(1+1)=1/2$. Then the revised belief of defender's type is $p(d_0|R_1)=0$, $p(d_1|R_1)=0.75$, $p(d_2|R_1)=0.25$. The expected payoff of attacker is shown in Table 10.

Table 10 Expected Payoff

Response Strategy	A_0	A_1	A_2
Expected Payoff	0	-1	29.6

In this situation, attacker chooses the follow-up strategy A_2. IDR system doesn't stop this attack; however, the information feedback to the threat level database by response model improves the threat level of this attack.

When the second attack begins, IDS issues LPD alert and IDR model will make response decision after calling the relative information from the database of strategy space, threat level and payoff model. Table 11 is the attacker/defender payoffs.

Table 11 The Attacker/Defender Payoffs

		h_0	h_1		h_2	
		A_0	A_1	A_0	A_1	A_2
d_0	R_0	(0.0)	(-10.4,8.36)	(0,0)	(-15.6,13.04)	(-15.6,10.04)
d_1	R_1	(-9.22,0)	(-9.22,-1)	(-9.22,0)	(-9.22,-1)	(-35.02,19.22)
	R_0	(0,0)	(-38,33.2)	(0,0)	(-57,50.3)	(-57,47.3)
d_2	R_1	(-7.33,0)	(-7.33,-1)	(-7.33,0)	(-7.33,-1)	(-64.33, 47.3)
	R_2	(-18.33,0)	(-18.33,-1)	(-18.33,0)	(-18.33,-1)	(-18.33,-4)

The expected payoff of defender is shown in Table 12.

Table 12 Expected Payoff

Response Strategy	R_0	R_1	R_2
Expected Payoff	-47.5	-38.68	-18.33

Defender chooses the response R_2, c=2, $\delta(2)=1/(2+1)=1/3$, then attacker will revise the type belief of defender as following:

$$p(d_0|R_1)=0, p(d_1|R_1)=0, p(d_2|R_1)=1.00$$

The expected payoff is shown in Table 13.

Table 13 Expected Payoff

Response Strategy	A_0	A_1	A_2
Expected Payoff	0	-1	-4

The strategy (R_2,A_0) is obtained by the perfect Bayesian equilibrium, that is, defender closes LPD service and attacker will stop attacking, which is the most stable and optimal response, and in this case, whatever the attacker/defender changes their strategies, the payoffs will not be increased any more, and defender successfully stop the higher threat attack.

The experiment shows that in the real network, most attacks are lower threats as in case 1, DGII_IDR can make the optimal response to this kind of attack. However, to the higher threat attack as in case 2, DGII_IDR can also make the optimal response by revising the attacker's threat level. To sum up, DGII_IDR can make the optimal response to the most attacks in the network.

5. Conclusions and Future Work

A novel DGII_IDR model based on incomplete information dynamic game is constructed that can make optimal response decision effectively. This model fully considers the response negative impact and strategy changes of attacker/defender and incorporates the false negative and false positive errors as the influence factors in constructing the payoff function. The conflict between the rational assumption and irrational behavior of attacker and defender is solved by restricting their strategy spaces, which balances the response negative impact and intrusion damage, and further enhances the response ability to strategy changes of attacker.

The further work is to enhance the feedback mechanism of DGII_IDR system to bring the results back to the IRS. Incorporate the response success rate etc. to the model so that the response results can affect decision-making and therefore, DGII_IDR model can be well adapted to the changes of network environment and attacks.

Acknowledgement

This work is supported by National Natural Science Foundation of China under Grant No.60973136, China-BC ICSD under Grant No.2008DFA12140 and Erasmus Mundus External Cooperation Window's Project under Grant No.155776-EM-1-2009-1-IT-ERAMUNDUS-ECW-L12.

References

[1] S.A and F.S. Automated response using system-call delays [C]. In Proc of the 9th USENIX Security Symposium: The Advanced Computing System Association, Berkeley, CA, USA, Aug. 2000, pp.185-198.

[2] U.P and S.R. Experiences with specification-based intrusion detection [C]. In Proc of the 4th Int'l Symp on Recent Advances in Intrusion Detection, Berlin: Springer, Heidelberg, Sep. 2001, pp.172-189.

[3] C.A.Carter. Adaptive-based intrusion response [D]. Master's thesis, Texas A&M University, 2001.

[4] R.D.J and e.a. Carter C A. Adaptation techniques for intrusion detection and intrusion response systems [C]. In Proc of IEEE Int'l Conf on System, Man and Cybernetics Information Assurance Workshop, Nashville, TN, USA, Oct. 2000, pp.2344-2349.

[5] W. Lee. Toward cost-sensitive modeling for intrusion detection and response [J]. Journal of Computer Security, 2002, 10(2): 5-22.

[6] I. Balepin and e. a. S. Maltsev. Using specification-based intrusion detection for automated response [C]. In Proc.of the 6th International Symposium on Recent Advances in Intrusion Detection, Pittsburgh, PA, USA, Sep. 2003, pp. 136-154.

[7] N. Stakhanova and e. a. Samik Basu. A cost-sensitive model for preemptive intrusion response systems [C]. In 21st International Conference on Advanced Networking and Applications, Niagara Falls, Ontario, Canada, May 2007, pp. 428-435.

[8] Y. Wu and S. Liu. A cost-sensitive model for preemptive intrusion response systems [C]. In 12th International Conference on Computer Supported Cooperative Work in Design, China, Apr. 2008, pp. 760-764.

[9] K.-W. Lye and J. Wing. Game strategies in network security [C]. In 12th International Conference on Computer Supported Cooperative Work in Design, Copenhagen, Denmark, May 2002, pp. 760-764.

[10] H. Otrok and e. Mona Mehrandish. Game theoretic models for detecting network intrusions [J]. Computer Communications, 2008, 31(10): 1934-1944.

[11] J. Wei, F. B. Xing, T. Z. Hong, and Z. H. Li. Evaluating network security and optimal active defense based on attack-defense game model [J]. Chinese Journal of Computers, 2009, 32(4): 817-826.

[12] Z. Jian-Ming and S. Raghunathan. Evaluation model of information security technologies based on game theoretic [J]. Chinese Journal of Computers, 2009, 32(4): 828-834.

[13] S. Liu, D. Y. Zhang, X. Chu, H. Otrok, and P. Bhattacharya. Game theoretic approach to optimize the performance of host-based ids [C]. In IEEE International Conference on Wireless & Mobile Computing, Networking & Communication,WIMOB'08, Avignon, France, Oct. 2008, pp. 448-453.

[14] T. E. Carroll and D. Grosu. A game theoretic investigation of deception in network security [C]. In Proceedings of 18th International Conference on Computer Communications and Networks,2009, San Francisco, CA, USA, Aug. 2009, pp. 1-6.

[15] E. Rasmusen. Game and Information:An introduction to Game Theory, 4th ed [M]. USA: Wiley-Blackwell, 2006.

[16] J. C. Harsanyi and R. Selten. A generalized nash solution for two-person bargaining games with incomplete information [J]. Management Science, 1972, 18(5): 80-106.

[17] D. Fudenberg and J. Tirole. Perfect bayesian equilibrium and sequential equilibrium [J]. Journal of Economic Theory, 1991, 53(2): 236-260.

[18] C.Strasburg, N.Stakhanova, S.Basu, and J.Wong. The methodology for evaluating response cost for intrusion response systems [R]. Dept. of Computer Science, Iowa State University, MA, Tech. Rep. 08-12, Dec. 2008.

[19] 2000 darpa intrusion detection scenario specific data sets [EB/Q]. http://www.ll.mit.edu/ll.mit.du/SST/ideval/data/2000/2000_data_index.html.