WUJNS
Wuhan University Journal of Natural Sciences

Vol.11 No.3 2006 617-620

Article ID:1007-1202(2006)03-0617-04

Network Security Transmission Based on Bimatrix Game Theory

☐ ZHENG Ying, HU Hanping†, GUO Wenxuan

Institute of Image Recognition and Artificial Intelligence, Huazhong University of Science and Technology, Wuhan 430074, Hubei, China

Abstract: Based on the bimatrix game theory, the network data transmission has been depicted in a game theory way: the actions of the attacker and defender (legitimate users) are depicted within a two-person, non-cooperative and bimatrix game model, this paper proves the existence of the Nash equilibrium theoretically, which is further illustrated by the experimental results.

Key words: security transmission; game theory; bimatrix game; Nash equilibrium

CLC number: TP 393

Received date: 2005-09-20

Foundation item: Supported by the National Nature Science Foundation of China (90104029) and the Specialized Research Fund for the Doctoral Program of Higher Education (20050487046)

Biography: ZHENG Ying(1980-), male, Ph. D. candidate, research direction: network security. E-mail:phoolcee2004@yahoo.com.cn

† To whom correspondence should be addressed. E-mail:hphu@mail.hust.edu.cn

0 Introduction

Many researchers have studied network security using game theory. Ref. [1] proposes a network security behavior model based on game theory, describes the actions, strategies and utilities qualitatively, but fails to addresses a concrete case study; In order to make data transmission more secure, many protocols and arithmetic are proposed in Ref. [2]-[9]. Ref. [10] puts forward a stochastic routing protocol: routers randomly choose a next-hop node to prevent data from attacks during transmission and minimize the transmission cost; Ref . [11] analyzes how to distribute network traffic in peer-to-peer transmission to achieve minimum cost and avoid being attacked.

In real life, the attacker and defender may obtain different and incomplete information[12,13], even both sides evaluate their utilities in a different way. this paper puts forward a game theoretical model of security transmission based on bimatrix utility matrix. In this model, the attacker tries to maximize his utility via attacking some node along the transmission path, while the user attempts to choose a most suitable path from the network topology to achieve minimum cost.

1 A Network Game

The network topology:$G=(N,L)$, the set of nodes $N=\{1,2,\cdots,n\}$, the set links $L=\{1,2,\cdots,l\}$; data is transferred from node $o(o\in N)$ to node $d(d\in N)$.

1.1 Framework of Game

Defense strategy $a^{(1)}$: The strategy space is the set of available paths connecting node o and d:$C^R=\{r_1,r_2,\cdots,r_m\}$

(assume the number is m).

Attack strategy $a^{(2)}$: The set of all nodes in the network $N=\{a_1,a_2,\cdots,a_n\}$. we explain the utility functions in the following.

Defender utility $\boldsymbol{A}_{m\times n}=[u^{(1)}(r_i,a_j)]_{m\times n}$: The average transmission time $\bar{T}$ of path r_i when no attack happens minus the transmission time when a certain amount of data are transmitted along r_i.

$$u^{(1)}(r_i,a_j)=\bar{T}-(\bar{T}(r_i)+\theta(r_i,a_j)\beta(a_j)\bar{T}_0),\quad 0<\beta(a_j)\leqslant 1,$$
$$\theta(r_i,a_j)=\begin{cases}1, & \text{if } a_j\in r_i\\ 0, & \text{if } a_j\notin r_i\end{cases}\tag{1}$$

where $\beta(a_j)$ denotes the degree of importance of node a_j. $\bar{T}(r_i)$ denotes the time it takes to transmit data through path r_i when no attack happens. $\bar{T}_0$ denotes the average transmission delay.

Attacker utility $\boldsymbol{B}_{m\times n}=[u^{(2)}(r_i,a_j)]_{m\times n}$: The delay time of defender's data transmission by the attacker and the payoff of attacking this node, the more the node's importance is, the more payoff the attacker needs.

$$u^{(2)}(r_i,a_j)=\theta(r_i,a_j)\beta(a_j)\bar{T}_0-\beta(a_j)C_0\tag{2}$$

C_0 represents the unit cost for the attacker, namely the minimum cost of implementing an attack; $\theta(r_i,a_j)\beta(a_j)\bar{T}_0$ denotes the attacker's benefit, while $\beta(a_j)C_0$ denotes the attacker's cost, $\theta(r_i,a_j)\beta(a_j)\bar{T}_0-\beta(a_j)C_0$ represents the attacker's utility when assaulting a certain node.

Definition of node's importance $\beta(a_j)$: Take Fig. 1 for example, assume data are transmitted from source o to destination d. For the nodes on the transmission path, the smaller the number of least hops between the node and the source or destination node is, the more important this node is.

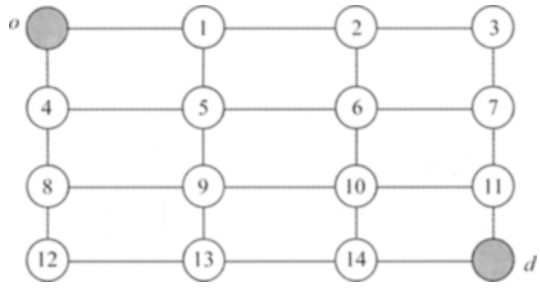

Fig. 1 Network topology

1.2 Existence of Nash Equilibrium

The strategy discussed is the mixed strategy: the defender chooses transmission path in C^R based on a certain probability distribution; while the attacker assaults nodes in N according to one probability distribution.

Definition of two-person bimatrix equilibrium: in $\tilde{A}=(\boldsymbol{X},\boldsymbol{Y};\boldsymbol{A},\boldsymbol{B})$, if there is a mixed strategy pair $(\bar{\boldsymbol{x}},\bar{\boldsymbol{y}})\in(\boldsymbol{X}\times\boldsymbol{Y})$ satisfying:

$$\begin{cases}\bar{\boldsymbol{x}}\boldsymbol{A}\bar{\boldsymbol{y}}\geqslant\boldsymbol{x}\boldsymbol{A}\bar{\boldsymbol{y}}, & \boldsymbol{x}\in\boldsymbol{X}\\ \bar{\boldsymbol{x}}\boldsymbol{B}\bar{\boldsymbol{y}}\geqslant\bar{\boldsymbol{x}}\boldsymbol{B}\boldsymbol{y}, & \boldsymbol{y}\in\boldsymbol{Y}\end{cases}\tag{3}$$

Proof: assume $(\boldsymbol{x},\boldsymbol{y})$ is one mixed strategy pair in $\boldsymbol{\Gamma}=(\boldsymbol{X},\boldsymbol{Y};\boldsymbol{A},\boldsymbol{B})$, and

$$\begin{cases}c_i=\max\{\boldsymbol{A}_{ig}\boldsymbol{y}^{\mathrm{T}}-\boldsymbol{x}\boldsymbol{A}\boldsymbol{y}^{\mathrm{T}},0\}\\ d_j=\max\{\boldsymbol{x}\boldsymbol{B}_{gj}-\boldsymbol{x}\boldsymbol{B}\boldsymbol{y}^{\mathrm{T}},0\}\end{cases}\tag{4}$$

For strategies of $\boldsymbol{x}$ and $\boldsymbol{y}$, c_i denotes the degree of improvement of the improvable parameter i of $\boldsymbol{x}$. d_j denotes the degree of improvement of the improvable parameter j of $\boldsymbol{y}$. then we get

$$x_i^{(1)}=\frac{x_i+c_i}{1+\sum_k c_k},\quad y_j^{(1)}=\frac{y_j+d_j}{1+\sum_k d_k}\tag{5}$$

if $(\boldsymbol{x},\boldsymbol{y})$ is not the equilibrium point, which indicates that there exists some strategy $\bar{\boldsymbol{x}}$ satisfying $\bar{\boldsymbol{x}}\boldsymbol{A}\boldsymbol{y}^{\mathrm{T}}>\boldsymbol{x}\boldsymbol{A}\boldsymbol{y}^{\mathrm{T}}$ or $\bar{\boldsymbol{y}}$ satisfying $\boldsymbol{x}\boldsymbol{B}\bar{\boldsymbol{y}}^{\mathrm{T}}>\boldsymbol{x}\boldsymbol{B}\boldsymbol{y}^{\mathrm{T}}$, assume the strategy $\bar{\boldsymbol{x}}$ exists without a loss of generality. As $\bar{\boldsymbol{x}}\boldsymbol{A}\boldsymbol{y}^{\mathrm{T}}$ is the weighted average of all the $\boldsymbol{A}_{ig}\boldsymbol{y}^{\mathrm{T}}$, then there must be an index i satisfying $\boldsymbol{A}_{ig}\boldsymbol{y}^{\mathrm{T}}>\boldsymbol{x}\boldsymbol{A}\boldsymbol{y}^{\mathrm{T}}$. Namely as $c_i>0$ and all c_k is non-negative, $\sum_k c_k>0$, because $\boldsymbol{x}\boldsymbol{A}\boldsymbol{y}^{\mathrm{T}}$ is the weighted average of all $\boldsymbol{A}_{ig}\boldsymbol{y}^{\mathrm{T}}$, the weighted coefficient is x_i, then we infer that there is an index (denoted as i) satisfying $x_i>0$, $\boldsymbol{A}_{ig}\boldsymbol{y}^{\mathrm{T}}\leqslant\boldsymbol{x}\boldsymbol{A}\boldsymbol{y}^{\mathrm{T}}$, $c_i=0$, and then $x_i^{(1)}=\frac{x_i}{1+\sum_k c_k}<x_i$, this indicates $\boldsymbol{x}^{(1)}\neq\boldsymbol{x}$. Similarly, for $\boldsymbol{x}\boldsymbol{B}\bar{\boldsymbol{y}}^{\mathrm{T}}>\boldsymbol{x}\boldsymbol{B}\boldsymbol{y}^{\mathrm{T}}$, it can prove that $\boldsymbol{y}^{(1)}\neq\boldsymbol{y}$. Then it can be concluded that $(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(1)})=(\boldsymbol{x},\boldsymbol{y})$ is the sufficient and essential term for $(\boldsymbol{x},\boldsymbol{y})$ to be the equilibrium point. Because all the strategies make up a closed, limited and protruding set, and the transformation $T(\boldsymbol{x},\boldsymbol{y})=(\boldsymbol{x}^{(1)},\boldsymbol{y}^{(1)})$ is continuous, there must be a stable point, namely the equilibrium point for the transformation T[12].

2 Numerical Results and Analysis

In the experiment, we set the network topology as shown in Fig. 1. For the defender, the 5 spare paths are presented as below:

$r_1: o\to 1\to 2\to 3\to 7\to 11\to d$;
$r_2: o\to 1\to 5\to 6\to 10\to 14\to d$;
$r_3: o\to 1\to 2\to 6\to 10\to 11\to d$;
$r_4: o\to 4\to 8\to 12\to 13\to 14\to d$;
$r_5: o\to 4\to 5\to 9\to 10\to 14\to d$

From Eq. (1) and Eq. (2), we can obtain the utility matrix of both sides shown as below:

$$\boldsymbol{A}=\begin{pmatrix}36 & 39 & 42 & 45 & 45 & 45 & 39 & 45 & 45 & 45 & 36 & 45 & 45 & 45\\ 36 & 45 & 45 & 45 & 42 & 42 & 45 & 45 & 45 & 42 & 45 & 45 & 45 & 36\\ 36 & 39 & 45 & 45 & 45 & 42 & 45 & 45 & 45 & 42 & 36 & 45 & 45 & 45\\ 45 & 45 & 45 & 36 & 45 & 45 & 45 & 39 & 45 & 45 & 45 & 42 & 39 & 36\\ 45 & 45 & 45 & 36 & 42 & 45 & 45 & 45 & 42 & 45 & 45 & 45 & 45 & 36\end{pmatrix}$$

$$\boldsymbol{B}=\begin{pmatrix}8.1 & 5.4 & 2.7 & -0.9 & -0.3 & -0.3 & 5.4 & -0.6 & -0.3 & -0.3 & 8.1 & -0.3 & -0.6 & -0.9\\ 8.1 & -0.6 & -0.3 & -0.9 & 2.7 & 2.7 & -0.6 & -0.6 & -0.3 & 2.7 & -0.9 & -0.3 & -0.6 & 8.1\\ 8.1 & 5.4 & -0.3 & -0.9 & -0.3 & 2.7 & -0.6 & -0.6 & -0.3 & 2.7 & 8.1 & -0.3 & -0.6 & -0.9\\ -0.9 & -0.6 & -0.3 & 8.1 & -0.3 & -0.3 & -0.6 & 5.4 & -0.3 & -0.3 & -0.9 & 2.7 & 5.4 & 8.1\end{pmatrix}$$

$$\boldsymbol{p}^{*}=(0.519\,103\ 0.222\,283\ 0.080\,833\ 0.034\,293\ 0.143\,488)$$

$$\boldsymbol{q}^{*}=\begin{pmatrix}0.223\,774 & 0.025\,416 & 0.000\,794 & 0.150\,953 & 0.010\,925 & 0.028\,258 & 0.153\,537\\ 0.038\,113 & 0.014\,354 & 0.044\,810 & 0.187\,424 & 0.028\,678 & 0.047\,490 & 0.045\,472\end{pmatrix}$$

we define the β value of nodes (see Table 1).

In Figs. 2-5, the $k_i(i=1,2,3,4)$ represents defender payoff, attacker payoff, defender payoff at NE, attacker payoff at NE.

Table 1 Node's importance value

Node id	1	2	3	4	5	6	7	8	9	10	11	12	13	14
β	0.9	0.6	0.3	0.9	0.3	0.3	0.6	0.6	0.3	0.3	0.9	0.3	0.6	0.9

Figure 2 and Figure 3 display the utility distribution of the attacker and defender when both sides adopt different mixed strategies. According to Eq. (3), we simulated the strategies of both sides and got the mixed Nash Equilibrium strategies $\boldsymbol{p}^{*}$, $\boldsymbol{q}^{*}$ for the attacker and defender respectively.

At this point, the utilities for the defender and attacker are (41.250 727, 3.024 620). Figure 4 and Figure 5 dis-

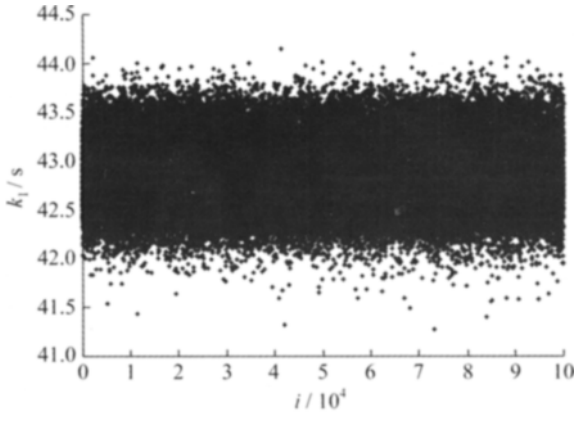

Fig. 2 Defender payoff

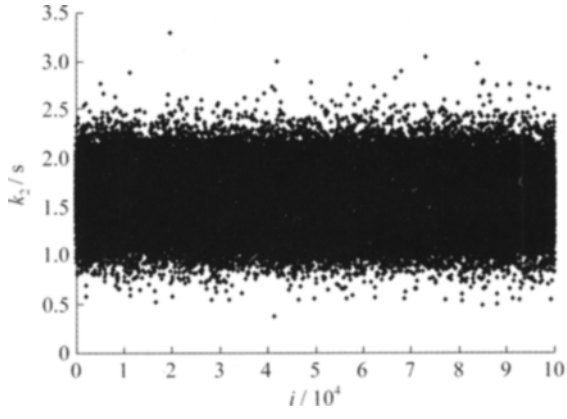

Fig. 3 Attacker payoff

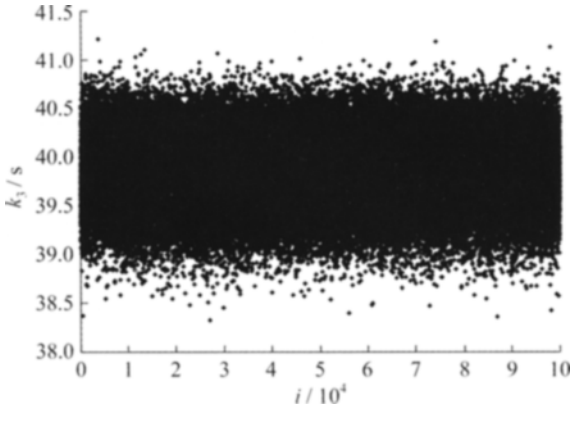

Fig. 4 Defender payoff at NE

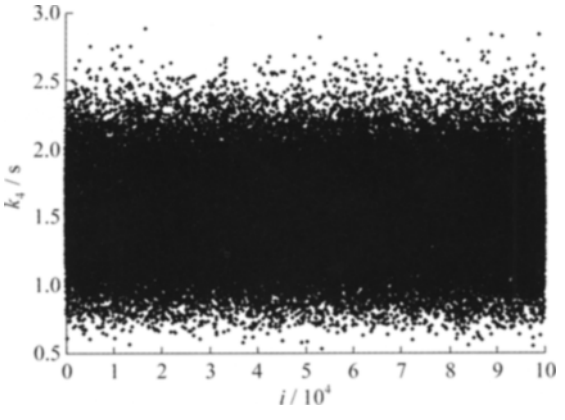

Fig. 5 Attacker payoff at NE

play the attacker's (defender's) utility when the strategy of defender (attacker) changes provided that the attacker (defender) keeps his strategy at the Nash Equilibrium point. The maximum utility of the defender is 41.062 797, and the attacker's maximum utility is 2.820 441.

From the experiment, it can be seen that there exists a saddle point ($\boldsymbol{p}^*$, $\boldsymbol{q}^*$) in this game, because of no more income, neither the defender nor the attacker will change his strategy at the point, on the other hand, it can be concluded from the proof of the existence of Nash equilibrium, there exists likely more than one saddle point in this game process, it just depends on the selection of the defender or the attacker's initial mixed strategy.

3 Conclusion

This paper analyzes the actions of both the attacker and defender during the network data transmission in a game theory way, and proposes a security transmission model based on nonzero-sum utility matrix. According to the incompleteness and asymmetry of the information of the attacker and defender, we define the utility matrix of both sides, which is in agreement with the psychology of the attacker and defender in real network environment. Furthermore, we prove the existence of the Nash Equilibrium point theoretically, which is also illustrated by the experiment.

References

[1] Xia Zhengyou, Zhang Shiyong. A Kind of Network Security Behavior Model Based on Game Theory [J]. *Parallel and Distributed Computing, Applications and Technologies*, 2003,**20**(4):950-954 (Ch).

[2] Szczerba R J, Galkowski P, Glicktein I S, *et al*. Robust Algorithm for Real-Time Route Planning [J]. *Aerospace and Electronic Systems, IEEE Transactions*, 2000,**11**(3):318-335.

[3] Lee J, Kim Y, Lee H S. Fast Route Recovery Methods for Cellular IP Access Network [J]. *Vehicular Technology Conference*, 2005,**4**(1):2580-2584.

[4] Wang Z, Crowcroft J. Quality of Service Routing for Supporting Multimedia Applications [J]. *IEEE Journal on Selected Areas in Communications*, 1996,**14**(7):1228-1234.

[5] Saltzer J, Reed D, Clark D. End-to-End Arguments in System Design [J]. *AMC Trans on Computer Systems*, 1984,**2**(4):195-206.

[6] Xiao Xipeng, Lionel M N. Internet QoS: A Big Picture [J]. *IEEE Network*, 1999,**13**(2):8-18.

[7] Dafermos S, Sparrow F T. The Traffic Assignment Problem for a General Network [J]. *J Res National Bureau Standards-B Math Sci*, 1969,**73B**(2):91-118.

[8] Korilis Y A, Lazar A. On the Existence of Equilibria in Noncooperative Optimal Flow Control [J]. *J ACM*, 1995,**42**(3):584-613.

[9] Srikant R, Whitt W. Simulation Run Lengths to Estimate Blocking Probabilities [J]. *ACM Trans Modeling Comp Sim*, 1996,**6**(1):7-52.

[10] Bohacek S, Hespanha J, Obraczka K, *et al*. Enhancing Security via Stochastic Routing [J]. *Computer Communications and Networks*, 2002,**14**(21):58-62.

[11] La R J, Anantharam V. Optimal Routing Control: Repeated Game Approach [J]. *IEEE Transactions*, 2002,**27**(3):437-450.

[12] Zhang Weiying. *Game Theory and Information Economics* [M]. Shanghai: Shanghai People's Publishing House, 1996 (Ch).

[13] Lye Kongwei, Wing J M. Game Strategies in Network Security [J]. *International Journal of Information Security*, 2005,**4**(1-2):71-86.

□