A Novel Grey Game-Theoretic Model for Intrusion Detection in Vehicular Ad Hoc Network

Cheng Tan, Hao Sun, Ning Cao, Lihui Sun, Cheng Li
Department of Applied Mathematics, Northwestern Polytechnical University, Xi’an, 710129, China
E-mail: tancheng_tank@yahoo.cn

Abstract—**Ensuring security plays a significant role in maintaining the stable operation of vehicular ad hoc network (VANET). Actually, it’s impracticable to evaluate the precise value of packets’ transmission success rate within a short time due to the uncertainty of environmental information collected. To reduce the influence of these errors on detection scheme, we develop the two-person zero-sum classical game into a two-person zero-sum intrusion detection grey game for formulating the confrontation behavior between intrusion detection system (IDS) and malicious node. Finally, we introduce an implementation architecture of our intrusion detection scheme and illustrate the feasibility of our model by simulation. Simulation results reflect some properties of our model, which conclude that IDS can resist malicious attacks more effectively through modifying some parameters.**

Keywords-VANET; intrusion detection system; game theory; two-person zero-sum grey game

I. INTRODUCTION

In recent years, a rapid growth in the number of vehicles contributes to more and more attention to VANET (vehicular ad hoc network), of which the basic idea is that a certain range of vehicles communicate with each other or road infrastructure for exchanging information about speed, location, sensor data, etc. Security problems mainly embody that some key positions tend to be attacked by invasive nodes, resulting in paralysis of the entire network.

In order to protect nodes from been attacked by malicious packets, intrusion detection is of the essence, and there exist a great quantity of works on researching intrusion detection currently. Detection in [1] was achieved by sampling a portion of the packets transiting through selected network links. The total number of the sampled packets can’t exceed a constant known as sampling budget. [2] and [3] have dug a little deeper in environmental design on the basis of [1]. Mehrandish et al. built a model where a group of attackers cooperated in sending malicious packets, while [3] discussed that an attacker would distribute its attack scheme over multiple packets, with each one possibly choosing to traverse a different route. Cluster was studied in [4] and [5] to describe a group of nodes, where a leader node was elected to be engaged in the intrusion detection service on behalf of the whole cluster. A Bayesian game model was established in [5], [6] and [7]. Furthermore, the authors of [6] estimated the behavior between attacker and IDS (intrusion detection system) by synthesizing static and dynamic Bayesian game, which was summarized into a Bayesian hybrid detection approach. [7] adopted the idea of signaling game for constructing a stage game and a multi-stage dynamic intrusion detection game between the malicious and Cluster Header IDS.

However, our model based on uncertain information has a substantial distinction in comparison with models in [5], [6] and [7], which derive from the idea of incomplete information. The uncertainty in this paper is embodied in the incompleteness of information collected by IDS, while the incomplete information in above works reflects the diversity of some player’s type relative to other players. Both of them have conveyed an idea of fuzzy computing. As a rule, most researchers tend to solve the problem of the Bayesian game with the method of Harsanyi transformation. At the same time, we present a grey payoff matrix [8] in our model, i.e., each element of IDS’s payoff matrix is a grey number. To the best of our knowledge, no existing works have studied the problem of intrusion detection by establishing a two-person zero-sum grey game model.

II. SYSTEM MODEL

Our model originates from the scene where IDS installed in BS detects the packets transmitted among vehicles running on highway. The detection is carried out on the link formed between two nodes. For simplicity, we consider merely the subnet $N=(V_0, E)$ extending from the malicious node S to the victim node D, where V_0 is the set of nodes as well as E is the set of links in N.

We assume that S generates n malicious packets aiming to attack node D during the network lifetime T, and the topological structure of N remains roughly unchanged during T, namely, there is no obvious change on any node’s position relative to positions of other nodes in N. We denote by f_e the transmission success rate of packets on link $e \in E$, and let d_e denote IDS’s detection rate on e.

In N, each node produces packets except D and each receives and forwards packets except S. For simplicity, we ignore that D forwards packets produced by nodes in N, nor do we consider the interactions between nodes in N and nodes outside N. Additionally, the amount of packets transmitted on e exerts a significant influence on d_e according to [1], [2], [3]. Generally speaking, more packets passing through e leads to a smaller d_e.

In our two-person zero-sum game model, S and IDS are the two players. For the sake of attacking node D, what S wants to do is to choose a route for each malicious packet

Published by Atlantis Press, Paris, France.

(all choices are independent of each other). Let l be the amount of routes from S to D, and then S has l^n strategies in all. Restricted by high speeds of vehicles and poor detection technology, IDS can't finish detecting all links in N within T . Without loss of generality, let k be the amount of links that IDS detect in T , then there exists altogether $C_{|E|}^{k}$ strategies for IDS.

III. Game Theory for Intrusion Detection

In this section, we focus on the intrusion detection problem with game theory. Two-person zero-sum game is common in game theory [9], whose successful application in many areas such as politics, economics, computer science, military affairs and etc, paves the way for its significant role in game theory. According to two-person zero-sum game theory, the sum of payoffs for the two players is equal to 0 on condition that player Ⅰ chooses his u th strategy and player Ⅱ chooses his v th strategy. As a foreshadowing, we first present an ideal two-person zero-sum classical game model where f_e is an explicit value, and then introduce our grey model. We suppose all nodes in N cooperate in forwarding packets, which implies that there exists no behavior of losing packets factitiously.

A. Two-person Zero-sum Classical Game

Ideally, we just regard the payoff function of IDS for simplicity. Especially, the extent of damage to D varies with the type of malicious packet. For this reason, let M be IDS's expected payoff, M_1^r be IDS's payoff caused by the loss of S's r th malicious packet, M_2^r be IDS's payoff for detecting S's r th malicious packet, and M_3^r be IDS's loss created by attack of the r th malicious packet. We define IDS's cost for detection on e by c_e^d , c_r^a represents S's attack cost by its r th malicious packet, and E^d is the set of links that IDS selects for detection, then

$$M=\sum_{r=1}^{n}(M_1^r p_1^r+M_2^r p_2^r-M_3^r p_3^r+c_r^a)-\sum_{e\in E^d}c_e^d\ , \qquad (1)$$

where p_1^r is the probability that the r th malicious packet drops before reaching D due to noise, p_2^r is the probability that the r th malicious packet get detected on its transmission route, and p_3^r is the probability that D is attacked by the r th malicious packet. Particularly, $p_1^r+p_2^r+p_3^r=1$.

As for its r th malicious packet, S will choose a route P_r for transmission. Assume a_r is the length of P_r (i.e., the sum of links on P_r), and

$$E_{P_r}^d=\left\{e_{i_1^r}^r,e_{i_2^r}^r,\cdots,e_{i_{k_r}^r}^r\right\}$$

is the set of links IDS selects for detection on P_r such that $\left|E_{P_r}^d\right|=k_r$. As mentioned in Section Ⅱ, the number of links selected by IDS from P_1 to P_n by time T is

$$k=\left|E^d\right|=\left|\bigcup_{r=1}^{n}E_{P_r}^d\right|.$$

Given f_t^r and $d_{i_s^r}^r$, representing packets' transmission success rate on link e_t^r and IDS's detection rate on link $e_{i_s^r}^r$ respectively, p_1^r , p_2^r and p_3^r can be obtained, thus,

$$\begin{cases} p_1^r=\sum\limits_{j=1}^{a_r}\left(1-f_j^r\right)\prod\limits_{t=0}^{j-1}f_t^r\prod\limits_{s=1}^{m+1}\left(1-d_{i_{s-1}^r}^r\right), \\ p_2^r=\sum\limits_{m=1}^{k_r}d_{i_m^r}^r\prod\limits_{t=0}^{i_m^r}f_t^r\prod\limits_{s=1}^{m}\left(1-d_{i_{s-1}^r}^r\right), \\ p_3^r=1-p_1^r-p_2^r, \\ i_m^r\le j<i_{m+1}^r. \end{cases} \qquad (2)$$

To balance (2), we set $d_0^r=0$, $f_0^r=1$, $i_0^r=0$, $i_{k_r+1}^r=a_r+1$.

We suppose that IDS is player Ⅰ, and the malicious node S is player Ⅱ. $S_1=\{\alpha_1,\alpha_2,\cdots,\alpha_p\}$ is set of Ⅰ's pure strategies, and $S_2=\{\beta_1,\beta_2,\cdots,\beta_q\}$ is set of Ⅱ's pure strategies ($p=C_{|E|}^k$, $q=l^n$). We shall use X to denote the set of mixed strategies for Ⅰ, and let Y be the set of Ⅱ's mixed strategies, thus

$$X=\left\{x\in\mathbb{R}^p\mid x_u\ge 0,u=1,2,\cdots,p,\sum_{u=1}^{p}x_u=1\right\},$$

$$Y=\left\{y\in\mathbb{R}^q\mid y_v\ge 0,v=1,2,\cdots,q,\sum_{v=1}^{q}y_v=1\right\}.$$

If Ⅰ chooses a mixed strategy $x\in X$ and Ⅱ chooses a mixed strategy $y\in Y$, then the expected payoff for Ⅰ will be

$$E(x,y)=\sum_{u=1}^{p}\sum_{v=1}^{q}x_u M_{uv}y_v\ .$$

Intuitively, M_{uv} is Ⅰ's payoff when Ⅰ chooses its u th strategy and Ⅱ chooses its v th strategy, which can be obtained by (1) and (2). As we have seen, the normal form of a finite two-person zero-sum game can be reduced to a matrix $A=(M_{uv})_{p\times q}$, with as many rows as Ⅰ has strategies and as many columns as Ⅱ has strategies. Then in matrix notation, $E(x,y)=xAy^T$.

B. Two-person Zero-sum Grey Game

As far as we know, the transmission success rate of packets changes along with temperature, humidity, speeds of vehicles, emergence of physical barriers and signal interference sources, and etc. For these reasons, we can't afford to give an explicit value of f_e . If we estimate a value for packets' transmission success rate on each link, it will probably exert a grave error on IDS's detection strategy by building a two-person zero-sum classical game. To address this issue, we use $f_e(\otimes)$ to express packets' transmission success rate on e . Note that $f_e(\otimes)\in[\underline{f}_e,\overline{f}_e]$, whose upper bound and lower bound are $\overline{f}_e$ and $\underline{f}_e$, respectively. Put this back into (1) and (2), then we have

$$M(\otimes)=\sum_{r=1}^{n}\left[M_1^r p_1^r(\otimes)+M_2^r p_2^r(\otimes)-M_3^r p_3^r(\otimes)+c_r^a\right]-\sum_{e\in E^d}c_e^d \qquad (3)$$

and

$$\begin{cases} p_1^r(\otimes) = \sum_{j=1}^{a_r}\left(1 - f_j^{\,r}(\otimes)\right)\prod_{t=0}^{j-1} f_t^{\,r}(\otimes)\prod_{s=1}^{m+1}\left(1 - d_{i_{s-1}^r}^{\,r}\right), \\ p_2^r(\otimes) = \sum_{m=1}^{k_r} d_{i_m^r}^{\,r}\prod_{t=0}^{i_m^r} f_t^{\,r}(\otimes)\prod_{s=1}^{m}\left(1 - d_{i_{s-1}^r}^{\,r}\right), \\ p_3^r(\otimes) = 1 - p_1^r(\otimes) - p_2^r(\otimes), \\ i_m^r \le j < i_{m+1}^r, \end{cases} \tag{4}$$

where $f_0^{\,r}(\otimes) = f_0^{\,r} = 1$, $p_1^r(\otimes) \in [\underline{p}_1^r, \overline{p}_1^r]$, $p_2^r(\otimes) \in [\underline{p}_2^r, \overline{p}_2^r]$, $p_3^r(\otimes) \in [\underline{p}_3^r, \overline{p}_3^r]$ and $M(\otimes) \in [\underline{M}, \overline{M}]$.

We start to set up a two-person zero-sum grey game model, where IDS's and S's sets of pure and mixed strategies remain the same as those in the classical model. Analogously,

$$E(x,y) = \sum_{u=1}^{p}\sum_{v=1}^{q} x_u M_{uv}(\otimes) y_v = xA(\otimes)y^T$$

is IDS's expected payoff, where $A(\otimes) = [M_{uv}(\otimes)]_{p\times q}$.

Definition 1 Let $\Gamma = (X, Y, A(\otimes), E)$ be a two-person zero-sum grey game with mixed strategies. $V^{\Gamma}(\otimes)$ is said to be the value of Γ, if and only if it holds that

$$\max_{x\in X}\min_{y\in Y} E(x,y) = \min_{y\in Y}\max_{x\in X} E(x,y) \underline{\underline{\Delta}} V^{\Gamma}(\otimes) . \tag{5}$$

All pairs of (x,y) satisfying (5) are called equilibrium solutions of Γ, and corresponding x and y are Ⅰ's and Ⅱ's optimal mixed strategy respectively.

For two-person zero-sum classical game with mixed strategies, there exists an equilibrium solution. As for two-person zero-sum grey game with mixed strategies, we have the following conclusion.

Theorem 2 In the game $\Gamma = (X, Y, A(\otimes), E)$, there exists at least an equilibrium solution (x,y) .

Proof: See [8] for the method of proof. ■

C. The Optimal Strategy

Let $V_x^{\Gamma}(\otimes)$ be IDS's expected gain-floor, i.e.,

$$V_x^{\Gamma}(\otimes) = \min_{v}\sum_{u=1}^{p} x_u M_{uv}(\otimes) .$$

In the same way, $V_y^{\Gamma}(\otimes)$ is S's expected loss-ceiling, and

$$V_y^{\Gamma}(\otimes) = \max_{u}\sum_{v=1}^{q} M_{uv}(\otimes) y_v .$$

What we need to do next is to solve the following two linear programming problems, thus,

$$\max V_x^{\Gamma}(\otimes)$$

$$s.t.\begin{cases} \sum_{u=1}^{p} x_u M_{uv}(\otimes) \ge V_x^{\Gamma}(\otimes), & v = 1,2,\cdots,q \\ \sum_{u=1}^{p} x_u = 1, \\ x_u \ge 0, & u = 1,2,\cdots,p \end{cases} \tag{6}$$

and

$$\min V_y^{\Gamma}(\otimes)$$

$$s.t.\begin{cases} \sum_{v=1}^{q} M_{uv}(\otimes) y_v \le V_y^{\Gamma}(\otimes), & u = 1,2,\cdots,p \\ \sum_{v=1}^{q} y_v = 1, \\ y_v \ge 0. & v = 1,2,\cdots,q \end{cases} \tag{7}$$

If $\underline{M}_{uv} > 0$ for $1 \le u \le p$ and $1 \le v \le q$, it suffices to see that $V_x^{\Gamma}(\otimes) > 0$ and $V_y^{\Gamma}(\otimes) > 0$. At this point, we see the following theorem.

Theorem 3 Let $\Gamma_1 = (X, Y, A_1, E_1)$ and $\Gamma_2 = (X, Y, A_2, E_2)$ be two-person zero-sum classical games, where $A_1 = (M_{uv})_{p\times q}$, $A_2 = (M_{uv} + M_0)_{p\times q}$, and M_0 is a constant. $R(\Gamma_1)$ and $R(\Gamma_2)$ are sets of equilibrium solutions in Γ_1 and Γ_2 . Then,

$$R(\Gamma_1) = R(\Gamma_2), \quad V^{\Gamma_2} = V^{\Gamma_1} + M_0 .$$

Proof: See [9] for the method of proof. ■

In fact, we need to convert $A(\otimes)$ into a white matrix for solving (6) and (7). Let $\tilde{A}(\theta) = (\tilde{M}_{uv})_{p\times q}$ ($0 \le \theta \le 1$) be the white matrix of $A(\otimes)$ such that $\tilde{M}_{uv} = (1-\theta)\underline{M}_{uv} + \theta\overline{M}_{uv}$ for $1 \le u \le p$ and $1 \le v \le q$. The error can reach a smaller value through choosing an appropriate θ in an allusion to the specific circumstance (in theory, we can minimize the mean absolute error by setting $\theta = 0.5$). Let $\Gamma(\theta) = (X, Y, \tilde{A}(\theta), E)$, $V_x^{\Gamma(\theta)} = \min_{v}\sum_{u=1}^{p} x_u \tilde{M}_{uv}$, $V_y^{\Gamma(\theta)} = \max_{u}\sum_{v=1}^{q} \tilde{M}_{uv} y_v$, $\tilde{M}_{uv}^{+} = \tilde{M}_{uv} + M_0$ for $1 \le u \le p$ and $1 \le v \le q$, where

$$M_0 = \begin{cases} 1 - \min\limits_{1\le u\le p, 1\le v\le q} \tilde{M}_{uv}, & \text{if } \min\limits_{1\le u\le p, 1\le v\le q} \tilde{M}_{uv} \le 0 \\ 0, & \text{otherwise} \end{cases}$$

then $\sum_{u=1}^{p} x_u \tilde{M}_{uv}^{+} = \sum_{u=1}^{p} x_u \tilde{M}_{uv} + M_0 \ge V_x^{\Gamma(\theta)} + M_0$.

Let $\tilde{x}_u = \dfrac{x_u}{V_x^{\Gamma(\theta)} + M_0}$ for $1 \le u \le p$, then $\sum_{u=1}^{p} \tilde{x}_u = \dfrac{1}{V_x^{\Gamma(\theta)} + M_0}$.

As $V_x^{\Gamma(\theta)} + M_0 > 0$, (6) equals to

$$\min \sum_{u=1}^{p} \tilde{x}_u$$

$$s.t.\begin{cases} \sum_{u=1}^{p} \tilde{x}_u \tilde{M}_{uv}^{+} \ge 1, & v = 1,2,\cdots,q \\ \tilde{x}_u \ge 0. & u = 1,2,\cdots,p \end{cases} \tag{8}$$

Analogously, $\tilde{y}_v = \dfrac{y_v}{V_y^{\Gamma(\theta)} + M_0}$ for $1 \le v \le q$, and (7) equals to

$$\max \sum_{v=1}^{q} \tilde{y}_v$$

$$s.t.\begin{cases} \sum_{v=1}^{q} \tilde{M}_{uv}^{+} \tilde{y}_v \le 1, & u = 1,2,\cdots,p \\ \tilde{y}_v \ge 0. & v = 1,2,\cdots,q \end{cases} \tag{9}$$

We can obtain the optimal solutions of (8) and (9), namely $\tilde{x}^*$ and $\tilde{y}^*$, by Simplex Method. Note that (9) is the dual programming of (8), and vice versa. In light of Theorem 3,

$$V^{\Gamma(\theta)} = \frac{1}{\sum_{u=1}^{p} \tilde{x}_u^*} - M_0 = \frac{1}{\sum_{u=1}^{q} \tilde{y}_u^*} - M_0 , \tag{11}$$

and equilibrium solutions of $\Gamma(\theta)$ are

$$x^* = \frac{\tilde{x}^*}{\sum_{u=1}^{p} \tilde{x}_u^*} , \ y^* = \frac{\tilde{y}^*}{\sum_{u=1}^{q} \tilde{y}_u^*} . \tag{12}$$

With the calculated results, IDS intends to detect k proper links in order to protect D from being attacked by S as much as possible. Through the theoretical analysis above, we find our model shows greater flexibility than classical model, where IDS can update its payoff matrix by changing θ .

IV. Implementation Architecture of Intrusion Detection and Performance Evaluation

In our model, a radar is fixed on BS for target locating. Through broadcasting electromagnetic waves to vehicles and then analyzing those waves that bounce back, BS can quickly determine the locations of vehicles running on highway and build up a structure diagram of N . The temperature sensor and humidity sensor are also necessary to collect environmental information around. Because of the existence of a few physical barriers and signal interference sources, the information processing module can only roughly evaluate packets' transmission success rate on vehicle-to-vehicle link, which violates the true value of f_e more or less. Considering this, we employ an interval grey number $f_e(\otimes)$ for compensation. After CPU processes these data, IDS will obtain its optimal mixed strategy through decision center. In Fig. 1, we present the concrete implementation architecture of our intrusion detection scheme.

Now we present an example to illustrate our model. As described in Fig. 2, there are 4 nodes (namely, S, A, B, D) located in different areas, where S is malicious and D is the victim. In addition, 5 directed links (i.e., e_1, e_2, e_3, e_4, e_5) are accordingly formed by these nodes. Let $n=1$ and $k=1$, then what S wants to do is to choose a route from SAD, SABD and SBD, while IDS should conduct the detection work on one of these links at the same time. IDS's detection rate on each link is 0.8, 0.8, 0.7, 0.6, 0.7, respectively. Besides, $f_1(\otimes) \in [0.7, 0.9]$, $f_2(\otimes) \in [0.6, 0.8]$, $f_3(\otimes) \in [0.7, 0.8]$, $f_4(\otimes) \in [0.5, 0.8]$, $f_5(\otimes) \in [0.8, 0.9]$, $c_1^d = c_4^d = c_5^d = 4$, $c_2^d = 5$, $c_3^d = 3$, $c^a = 6$, $M_1 = M_2 = 10$, $M_3 = 20$.

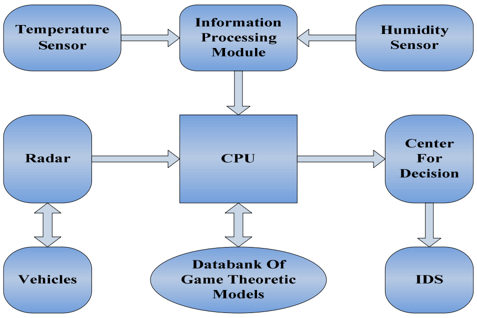

Figure 1. The implementation architecture in our scheme.

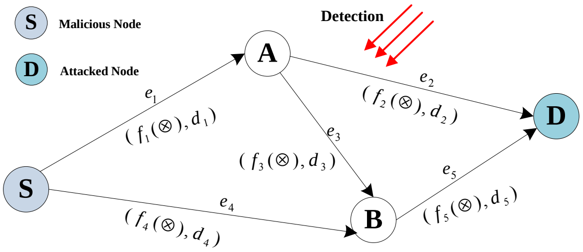

Figure 2. An illustrative example of intrusion detection.

Under this setting, Fig. 3 and Fig. 4 depict IDS's and S's optimal strategies under different θ respectively. It can be observed that IDS never selects e_2, e_3 and e_4 for detection, and S never routes its malicious packet on SABD. Through analyzing, we find that the packet must pass through e_1 whether S chooses SAD or SABD, and likewise, e_5 is the intersection of SABD and SBD. Consequently, IDS can detect the packet on e_1 or e_5 with higher probability than on e_2 , e_3 and e_4 . Moreover, S is unwilling to choose SABD because both e_1 and e_5 are involved on SABD. As θ varies from 0 to 1, IDS is increasingly willing to select e_1 , while S increasingly tends to choose SBD in order to avoid being detected. Particularly, the flattening of the curves reflects the relative stability of the optimal strategies for IDS and S under different θ .

Let α and β be the growth ratio of IDS's detection cost and detection rate on each link. Set $\beta = 0$, then we can see from Fig. 5 that IDS's payoff reaches 2.309 at $\theta = 1$ and –3.536 at $\theta = 0$ when $\alpha = 0.5$. As for $\alpha = -0.5$, its payoff reaches 6.309 at $\theta = 1$ and 0.464 at $\theta = 0$. It indicates that IDS tends to detect links with lower detection fares to obtain a higher payoff. Then we set $\alpha = 0$, and the surface in Fig. 6 implies that a higher β leads to a larger payoff for IDS when θ is fixed. When $\beta = 0.25$, IDS's detection rates on five links are, in order, 1, 1 , 0.875, 0.75, 0.875. In this case, the optimal expected payoff for IDS is 5.455 when $\theta = 1$ and 0.480 when $\theta = 0$. While $\beta = -0.5$, i.e., the detection rate on each link reduces by 50%, IDS's optimal expected payoff turns to be 2.018 and –5.568 when $\theta = 1$ and $\theta = 0$. Therefore, it is profitable for IDS to improve the level of detection capability.

In order to effectively resist attacks from malicious nodes, a good idea is to stimulate IDS to conduct more active detection work. Based on these simulation results above, IDS can obtain a higher payoff through reducing detection cost and raising detection rate, and then IDS has more incentive to detect malicious packets. In a nutshell, to improve and upgrade detection technology of IDS is an urgent problem to tackle in order to effectively intercept malicious attacks.

V. Conclusion

As a principal component of intelligent transportation system, VANET will show its more and more powerful

Published by Atlantis Press, Paris, France.

function in future. Consequently, how to maintain the security operation of VANET through intrusion detection has been a popular research topic these years. First, we propose a basic model for intrusion detection between IDS and S. To reduce the influence of errors, we have analyzed the interactions between IDS and S with two-person zero-sum intrusion detection grey game. Further, we present an implementation architecture of our intrusion detection scheme. At last, we verify the feasibility and effectiveness of our model through simulating experiments. Simulation results illustrate some properties of our model, that is, IDS can intercept malicious attacks more effectively through modifying some parameters.

ACKNOWLEDGMENT

This research was supported by NSF of China (No. 71171163 and No. 71271171).

REFERENCES

[1] M. Kodialam and T. V. Lakshman, "Detecting Network Intrusions via Sampling: A Game Theoretic Approach," Bell Laboratories Lucent Technologies, April 2003.

[2] M. Mehrandish, H. Otrok, M. Debbabi, C. Assi and P. Bhattacharya, "A Game Theoretic Approach to Detect Network Intrusions: The Cooperative Intruders Scenario," Proc. 49th annual of IEEE GLOBECOM, San Francisco, IEEE press, 2006.

[3] M. Mehrandish, C. Assi and M. Debbabi, "A Game Theoretic Model to Handle Network Intrusions over Multiple Packets," In Proc. of IEEE International Conference on Communications (ICC), Turkey, June 2006.

[4] H. Otrok, N. Mohammed, L. Wang, M. Debbabi and P. Bhattacharya, "A game-theoretic intrusion detection model for mobile ad-hoc networks," Journal of Computer Communications, 31(4):708–721, 2008.

[5] Y. Liu, C. Comaniciu and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," ACM International Conference Proceeding Series, Vol. 199, 2006.

[6] N. Mohammed, H. Otrok, L. Wang, M. Debbabi and P. Bhattacharya, "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET," IEEE Transactions on Dependable and Secure Computing, vol. 99, no. 1, 2008.

[7] S. Shen, Y. Li, H. Xu, Q. Cao, "Signaling game based strategy of intrusion detection in wireless sensor networks," Computers & Mathematics with Applications 62:2404–2416, 2011.

[8] D. Luo, "Study on the Analytic Methods for Grey Decision-Making," Nanjing University of Aeronautics and Astronautics, N941, 120100, 1028709 04-0001, October 2004.

[9] G. Owen, Game Theory, third edition, Academic Press, London, 1995.

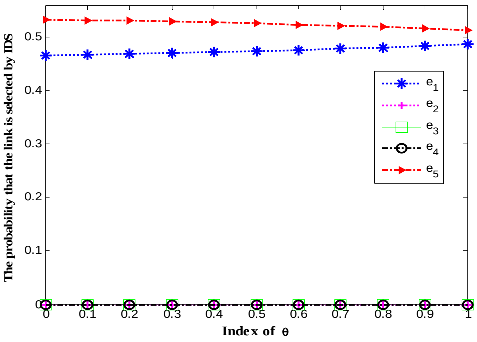

Figure 3. IDS's optimal mixed strategy.

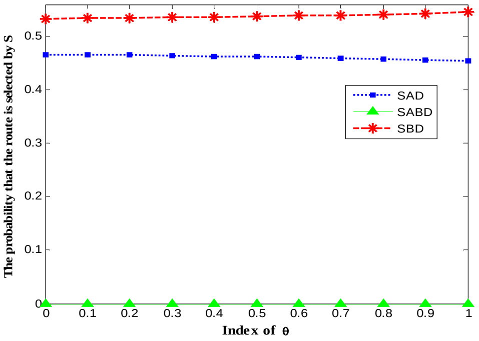

Figure 4. S's optimal mixed strategy.

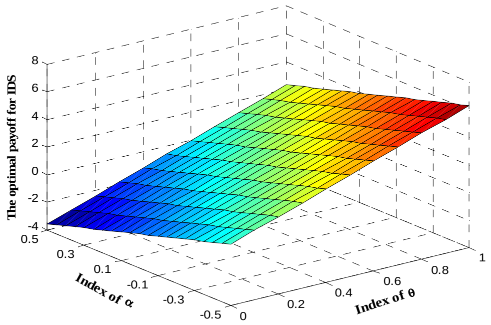

Figure 5. IDS's optimal expected payoff on α .

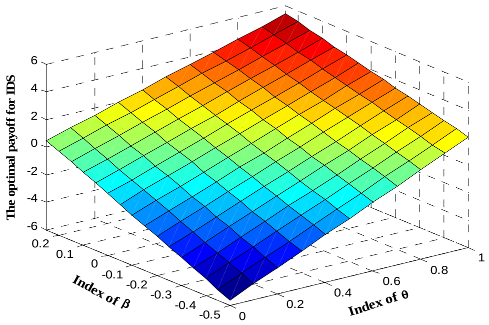

Figure 6. IDS's optimal expected payoff on β .

Published by Atlantis Press, Paris, France.