Model of Intrusion Detection Based on the Game Theory

Xiao Heng
Sanya University
Sanya Hainan China
e-mail: girlinwind@163.com

Long Caofang
Sanya University
Sanya Hainan China
e-mail: longcaofang@163.com

Fund Projects: science and technology cooperation project of Sanya (2012YD42)

***Abstract*—With the development of network application, network security is facing greater pressure. Based on the characteristics of intrusion detection in the wireless network of the Ad hoc working group, the article introduces the game theory, proposes a game model of network security, concluds the Nash equilibrium in the stage game, repeats game, the pareto Nash equilibrium, more attack both income and payment, so that they get the best choice.**

Keywords- Ad hoc; game theory; Nash equilibrium; repeated game

I. PREFACE

With the development of network technology, computers and all kinds of mobile communication equipments have brought people incomparable convenience in the use of the information and resources sharing. Accordingly, it also has emerged a series of problems brought by the invasion in the information security. Intrusion detection technology of network security has become an important direction of research.

Intrusion Detection System, IDS analyzes the possible intrusion behaviors from the internal system and all kinds of network resources, extends the ability safety management of system administrators, such as safety audit, monitor, recognition of invasion and response.

According to the system theory and cybernetics, intrusion detection system is actually a detection and control system based on technology and attacks each other between the system and the system in the network space and network attack. MANET, Mobile Ad hoc networks are different from cable network significantly. Therefore, intrusion detection technology of fixed networks should not be applied to directly wireless Ad hoc networks.

Mobile Ad hoc networks are a kind of temporary autonomous network system which is comprised of a number of wireless mobile nodes without control center through the nodes of mutual cooperation network interconnection. Affected by various resource, the loss of response during the incoming the invasion is likely to be worse than that caused by the real attack when the intrusion detection system is difficult to deal with various means of attack.

Introduce the game theory into the intrusion detection system of mobile Ad hoc networks, evaluate cost loss from different strategies, consider limited system resources, look for Nash equilibrium and establish the model of game intrusion detection from both sides of the attack and the cooperation.

II. ESTABLISHMENT OF NETWORK MODEL

A. Game model

Game theory studies the decision of decision-making interacted behavior and the equilibrium problems and make the value of utility maximized.

Game theory has five elements: participants, space of strategies, distribution of probability, information collection and utility function.

Definition: the expansion of the game model of network can be expressed by five elements:

G ={{A, D}, {SA, SD}, {PA, PD}, {IA, ID}, {RA, RD}} (1)

Participants: in formula (1), (A, D} says the decision-making subject as the first element in the game; A stands for network Attacker; D means decision makers of network defenders of IDS response,

Action sequence: the order of participants who make decisions and implement decision activities in the game. At the same time, both sides of decision choose static game, the order of strategy choice of both sides. The latter actors choose dynamic game after detecting the strategy of the other side. The game of the whole network security is repeated and dynamic.

Strategy space: type (1) {SA, SD) stands for the second element strategy space; SA for the strategy of attacker and SD for strategy of defenders. Strategy is a contingent action plan which can be used by participants in the game that can be displayed by vector.

Si means a particular strategy of participants in a game. Strategy set, namely S = {s1, s2,... , si,... , sn}.

Probability distribution: In type (1), (PA, PD} says probability distribution of the third element. The probability distribution matrix P can be represented by distribution matrix that evolves from data of intrusion detector monitoring network providing attack classification information for IDS and detector classification; P (Ai, Dj) says the real data type Ai determined as the probability of type Dj by detector; Each Ai has $\sum_{i=1}^{N}\sum_{j=1}^{N}(PAi，PDj)=1$。

Information set: In type (1), {IA, ID} says the information set of the attacker and defender of the fourth element. The defenders, provided information by the detector,

can't see the attacker's behavior. Dimension of information set of is decided by the number of attack type.

Utility function: In type (1), {RA, RD} says the utility function of the fifth element, namely, the possible gain set of the attacker and the defender after game. In each game, a real number is used for showing the income of both sides in the set. This is also what gamers really care about.

B. Nash Equilibrium

In the standard game participants: G={S1,…,Sn;U1,…Un}, strategy s*i of any game party i is the best the rest of the game, namely, $u_i(s^*_1,\ldots, s^*_i\ldots,s^*_n) \geqq u_j(s^*_1,\ldots,s^*_j\ldots,s^*_n)$ suited for all si∈sj which can be called as a Nash equilibrium for G.

In this model, attack type of the attacker is limited. So is the information dimension correspondingly. So the corresponding strategy game is also limited. According to the existence principle of Nash equilibrium, there exists at least one strategy Nash equilibrium[3] in any limited strategy game. Only when the attacker and the defender achieve Nash equilibrium strategy, can they make the income maximized.

C.Pareto - Nash equilibrium

For most of the Nash equilibrium games, there are multiple Nash equilibrium. Maybe a Nash equilibrium can bring greater benefits to game parties than any other Nash equilibrium. Then each game tends to the Nash equilibrium, realizes Pareto efficiency. Nash equilibrium selected by this method is also known as "Pareto Nash equilibrium".

α*=(a*,b*,…,m*) ,a Pareto Nash equilibrium of multiple game G. If there is no condition ,for all other participants, makes αi(a*,b*,…,m*)>α*(a*,b*,…,m*),that means each component are more than and equal to and at least one component strictly greater.

D. Model of IDS based on the game theory

The intrusion detector distributed in the network uses a detection means to audit network data, detect intrusion, submit the test results and determine whether alarm or not. Then the game model simulates the interaction of the attacker and the defender, weigh the test results and detection efficiency from intrusion detector (the rate of right and wrong of detection), conclude the Nash equilibrium to assist IDS to make reasonable response decision finally.

E.Repeated game

Repeated game means the game with the same structure repeats many times. Every game is called "stage game " or the original game, i.e., equal in the set of participants, strategic space, and revenue function. Equilibrium path of repeated game is made up of action combination series of every gamer and gross income of repeated game can be used for showing overall income.

Establish a limited secondary repeated game model of complete information, set: G={N， S1， S2， U1,U2}. N={A，D}. A represents network attack and D on behalf of IDS, assuming that both sides are reasonable and intelligent enough; S1 and S2 on behalf of the strategy sets of both sides respectively. The network has N nodes.

For any node k have m targets (energy, mobility, etc.) to measure, set a, b, c,... , m.

For any node k, the attacker has two strategies (attack or not attack); The corresponding IDS also has two strategies (defense or not defense).

III. EXPERIMENTAL RESULTS AND ANALYSIS

In order to validate the accuracy of the model proposed in the article, choose GloMoSim platform to test the model. Set the number of node of the attacker and the defender and the position is not fixed. The attackers aim at stealing data as much as possible and destroying the life cycle of the network; the defenders look on collecting data and maintaining survival of the duration network as the goal. Quote two experimental scenes: one is AODV routing protocol with normal intrusion detection system and the other is the improved AODV routing protocol based on the game theory.

Network parameters are Set as follows: application layer for CBR (Constants Bit Rate, fixed code Rate), the transport layer, network layer for the UDP AODV, MAC layer TDMA TDMA and Radio layer for NoNoise without interference noise.

Experimental scene: The area is 500m*500m, the time is sixty seconds, defense node number is ten to twenty and the place is random, assuming that each node can be independent to start IDS. Offense node number ten to twenty and attack node can send attack packets to arbitrary nodes in the covered radius area directly or indirectly and the different size of the packets can be adopted to distinguish different strategies. Data flow types of application layer have 90 articles CBR including 60 articles of attack packets: sent from attack node and received by defense node. Node trajectory is random route. Movement speed is 0~1m/s. Coverage radius is 10m, round for 5 TDMA, initial battery energy for0.1~10J and when node quantity is less than 0.1J it is thought of node failure. Speed of sending data is that every node sends a attack packet at most in each round. Data acquisition speed is 1~5K/Round, maximum data capacity of node is 1M.

Game judgment of both offensive and defensive: attack of each round is determined by the game result whether to issue attack packets and in the same round each attack target is different. When the attack node has launched IDS, regarded as failure, otherwise as successful attack and obtain the corresponding interest such as steal data. etc.

Each round defense node decides whether to start IDS according to the outcome of game. When node receives a attack packet, it is regarded as an attack. If at this time the defender do not start node IDS, it is treated as defense failure and node will pay the relevant cost such as the lost data and energy consumption, etc.

Evaluation goal: when residual node number of the network is less than 10% it is considered network failure, namely, network survival due; Total amount of data is sum volume that all the node has collected data before the network failure; Hyper defense success rate is the mean of a single node defense success rate: single node defense success rate is the proportion between the frequency of node success

of stopping the invasion and the number of node initiating IDS.

Experiment 1: node number is fifty, attack node is 10, energy consumption in per turn Random[0.02~0.1], standby consumption is 0.01, movement speed of "defense" party is 1 m/s, the attacker is 0.5 m/s and the data acquisition speed is 1 k/round.

The experimental results:

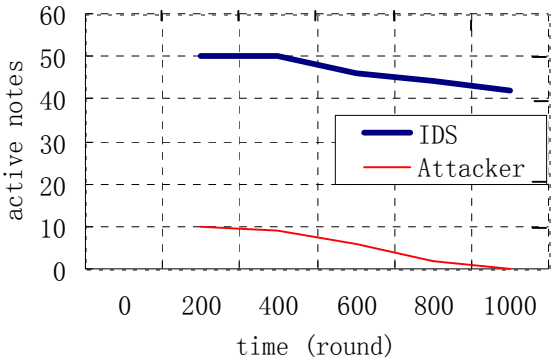

Figure 1. network active node number

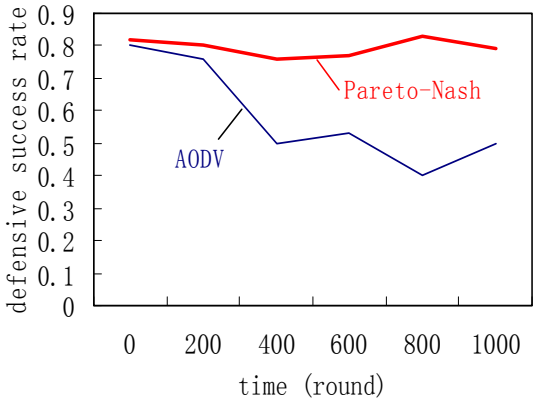

Figure 2. defensive success rate comparison

Experiment 2: node number fifty, attack node fifty, attack node energy consumption Random[0.05~0.1]per turn, defense node energy consumption Random[0.02~0.5] per turn, standby consumption 0.01, movement speed of "defense" party 1m/s, the attacker 0.5m/s and the data acquisition speed 1k/round.

The experiment results:

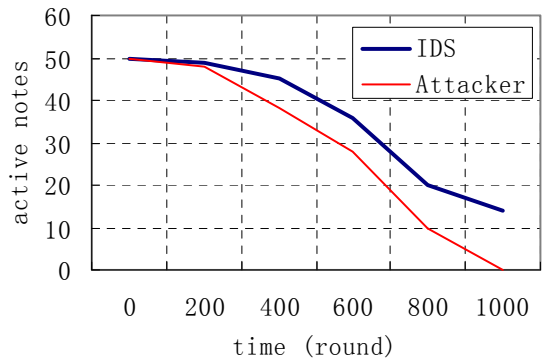

Figure 3. the network active node number

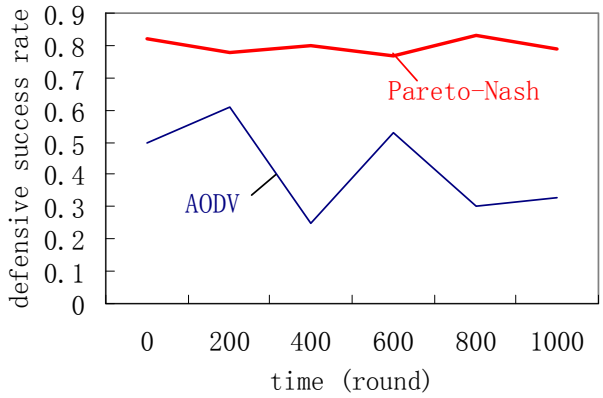

Figure 4. defensive success rate comparison

It can be seen that from node survival in figure 1 and figure 3, the IDS will produce a large number of alarms with the increase of the number of node attack and occurrence of large-scale invasion events, , which will consume a lot of node energy and the network performance drop. The decline can get some relief through the introduction of the game model.

According to the node defense success rate from figure 2 and figure 4, it can be found that without using AODV routing protocol of game model of, as long as there appear doubtful and apparent attack packets, it will start up the IDS for defense with a higher success rate in the top 100 seconds. But at the same time it will make the network node energy decrease and defense state unstable. The employment of the game model of Nash equilibrium can make it stabilized in the ideal level in a certain period.

IV. CONCLUSION

This paper puts forward the Ad hoc intrusion detection model based on the game theory, designs the response scene between the attack and the defender in the Ad hoc network game, compares node survival and success rate of defense in the two scene networks, gets the Pareto Nash equilibrium from repeated game which makes participants make the best choice. Through the experiment, it can be concluded that the

introduction of game theory model can guarantee the income of the IDS after the response after guaranteed, stable and reliable.

REFERENCES

[1] Debar H, Becker M . A neural network component for an intrusion detection system.In: research in Security and privacy, 1992. Proceedings, 1992 IEEE Computer Society Symposium, 240-250

[2] Dong Wushi, Sun Qiang, etc. The Adho networkc power control model based on the game theory. University of Science and Technology Journal of Wuhan , 2009 (17) : 114-122

[3] Dressler F,A Study of Self-organxation mechanisms in Ad Hoc and Sensor nertworks[J].Computer Communications.2008,31； 3018－3130

[4] Raghunath,B.R. Mahadeo,S.N. Network intrusion Detection System Emerging Trends in Engineering and Technology, 2008.ICETET'08:1272-1277.

[5] Software facilitates data recovery and repair of RAR files, Product News Network, 04/10/07.

[6] George Petersen, Hard Disk Drives, Mix, 2006

[author introduction] :

Xiao Heng (1979 -), female, Hengyang Hunan, Sanya university, lecturer, master degree, research direction for the computer network security; tel:18808967875, E-mail: girlinwind@163.com

Long Caofang (1983 -), female, Fuzhou Jiangxi, Sanya university, Teaching assistant, master degree, research direction for the computer network and database application. (Sanya Hainan 572022);tel:15091942530

Fund Projects: science and technology cooperation project of Sanya (2012YD42)