Research of Artificial Intelligent Plan Recognition Method in the Multi-Agents Conditions

Lei Wang

Border Control Department, The Chinese People's Armed Police Forces Academy, Langfang 065000, China

WangLeiwjxy@QQ.com

Keywords: Artificial Intelligent Plan Recognition, Plan Recognition Method, Virtual State Graph.

Abstract. This paper bases on the formal theoretical research of this plan recognition model, it preliminary studied the plan recognition technology; it is based on the functional characteristics from intelligent plan recognition theory, which one of the most important hotspots in the research field of artificial intelligence. It can analyze the presumable multi-target states that will be achieved by attacker and it can effectively identify the final target state attacker may achieve. Therefore, it can realize the response process to the invasive action of the attacker.

Introduction

Intelligent plan recognition is a very important in the field of artificial intelligence research direction, and adversarial planning recognition at present as intelligent planning research in the field of an important branch, is still in a preliminary study on the international stage.

This paper is from above aspects starts with, for plan recognition technology of itself features, in specific of attack event in the application planning recognition theory, through constructed reasonable of planning recognition model and on has observation to of some behavior (adversarial Agent executive of action) to forecast attack behavior by to achieved of all possibilities target State, then from find and found attack who attack behavior by to achieved of eventually target State, eventually reached in current attack process in the on attack who attack behavior for effective recognition and response of purposes. This paper is based on plan recognition model of virtual state diagram is the use of "virtual State" to mean "attack" a specific attack, the "attack". It can act and the object state determines, on the basis of "crisis" to achieve constantly tracking the attackers through the entire attacking process that must be completed for each critical step in. Such recognition in some attacks has not been caused before substantial harm, the ability to recognize and take appropriate response measures in real-time.

Basic Concepts

Intelligent plan recognition. Intelligent plan recognition is the final goal of a series of parts have been observed under Agent issued or executed, trivial, fragmented actions to infer the Agent to achieve the whole process of planning which it is to execute.

The Plan Recognition Method Based on Virtual State Graph

The introduction of plan recognition method function. This paper uses to construct the "virtual state diagram" to describe the specific attacks and attackers' state (or target). Thus, SSGPRM attacks can be expressed by apparent attackers (hostile action) and a wide range of possibilities may achieve the target state recognition to determine whether the attack occurred, which makes the attacker before reaching the final goal state feature, SSGPRM will be able to achieve the effect of recognizing and responding to attacks.

The formal description of the virtual state graph. This paper puts the possibility of target an attack process of virtual state graph in the attack action based on the generated is expressed as a form

of three triples: $=G_n=<S_i, A_i, P(\lambda_{G_{n_{line_i}}})>$ (i =1,2,... n; n=1,2, n,... , m). Among them, 'G_n' it said is a process of attack behavior under the action of the T_i time step to cause effect (behavior arc) abstract form multiple possibilities of target state nodes generated when; 'S_i' in the T_i time step triggered precondition (behavior arc) when an initial state (when i=1. The initial state of the attack process is the initial state of attacks), namely from the state, after the attack action can lead to various possibilities of the target state; 'A_i' represents a different kind of trigger state varies between aggressive behavior; and 'λ' called crisis coefficient, it shows the relationship between the ultimate goal state node of node and the target state attacks launched an attacker role in the realization of the attacker trying to attack before to achieve; '$P(\lambda_{G_{n_{line_i}}})$' represents the first column I (section I, the time step) the possibility the target G_n generated attack action with respect to the final purpose of state crisis degree node has its own, namely its own crisis degree.

It is also not difficult to see, in a virtual state graph, for the time step of the state, from the initial state to the current state of the ultimate goal (intermediate state) relative crisis value approaches 1, i.e.:

$$\sum_{n=1}^{m} P(\lambda_{G_{n_{line_i}}}) \rightarrow 1(P(\lambda_{G_n}) \in [0, 1], i=1,2,\cdots,n) \tag{1}$$

Overall Architecture Based on Virtual State Graph Plan Recognition Method

In this paper, on the basis of the proposed virtual state graph, by constructing a structured model to implement the attacker behavior under the action of the attack on the target system to realize the target state of the analysis and judgment, and ask the security administrator sends the corresponding alarm information. The system model is mainly composed of the following most:

Preprocessing Module. Preprocessing Module is responsible for processing and filtering operation on the read data, it can be thought of as the data acquisition. It is responsible for the data collection form analysis, removes some redundant and useless information in the process of analysis, event recognition and will be hostile action for the attackers and forwarded to the hostile reasoning machine for processing.

Adversarial Inference Engine. Adversarial Inference Engine is a core component of the operation. The main function of this module is to complete the preprocessing module passes have been identified as aggressive behavior of hostile action analysis and processing. It will first with hostile knowledge base on the aggressive behavior of the preprocessing module submitted for analysis, to forecast the possibility of aggressive behavior in a plurality of target state may implement the present time step I, and describe the method, according to the virtual state diagram formalization unified namely: three triples form

$$G_n=<S_i, A_i, P(\lambda_{G_{n_{line_i}}})> \quad (i=1,2,\ldots,n;\ n=1,2,\ldots,m) \tag{2}$$

In the adversarial knowledge base search match the attack target state all the possibilities.

Adversarial Knowledge Base. Adversarial Knowledge Base is one of the core modules of it, it stored two main types of knowledge: one is the so-called open hostility in the field of software and hardware related knowledge, such as specific intrusion detection problem in a series of related definitions, in the field of relevant facts and theory; Another kind is some knowledge engineers and experts in the field of so-called personal knowledge and experience, the experience is an expert in the field after years of business practice and gradually accumulated over a long period of time.

Decision Response Engine. The basic functions of decision engine response is to send alarm information to security administrators , including the attack on the current planning process as well as a variety of attacks to identify the state and parameter identification after the success.

Experimental Results and Analysis

The Description of Experimental Problem . The plan recognition method developed in this paper in 1 before the start of the attack process by loading data to AKB, and then through the aggressive behaviors of action recognition in 1 and then judge the effectiveness of its action. It can through to state a variety of possibilities to realize the goal of its crisis degree configuration of current attack state and aggressive behavior, so as to realize in the current process of attack, the attacker sentenced to effectively achieve through aggressive behavior role desire to achieve the ultimate goal of state fault; if in aggressive behavior possibility of target state to 1 of its crisis degree the configuration process, the emergence of relative degree is equal to the crisis of value, so, it is possible to cause the current level of knowledge of AKB is unable to complete the valid identification of aggressive behavior in the process of the current attack. At this time, plan recognizer will give up the current information, the realization of which in the current process of the attack on the basis of the final target state planning process to process 2 to attack plan recognition, and by AKB loading, expanding the virtual state graph. When through the state a variety of possibilities to continue to attack the target prediction process 2 attack behavior under the action of its own crisis degree configuration, so as to recognize the many possibilities of target state attack process 2 attack behavior may reach, to derive the maximum relative crisis has the possibility of target value, so it believes that in the current attack in the process, the plan recognition method for effective recognition of specific attacks attack behavior.

The Analysis of Experimental Results. In this paper, intelligent plan recognition method based on the implementation which is a new model for plan recognition, it will be applied to a specific plan recognition technology in the attacks. We focus on a specific incident, the plan recognition method conduct the necessary tests. It is shown in table 1.

Table 1 the test results

Attack Number	Attack Process 1					Attack Process 2			
	P1	P2	P3	Max(P)	action	P1	P2	Max(P)	action
1	0.1	0.2	0.3	0.834;0.667;0.500	P1	0	0	0	null
2	0.3	0.4	0.2	0.667;0.556;0.778	P2	0	0	0	null
3	0.5	0.4	0.3	0.584;0.667;0.750	P1	0	0	0	null
4	0.7	0.7	0.7	0	null	0.3	0.4	0.572;0.429	P1
5	0.4	0.3	0.4	0	null	0.7	0.2	0.223;0.778	P2
6	0.5	0.5	0.9	0	null	0,8	0.9	0.530;0.471	P1

In this test, this paper collected six sets of data, respectively. Among them, in the first three sets of data in attack process 1 is random sampling, and then three groups 2 and purposeful selection is a process for attack. Selection reasons of such data to a different configuration of its own crisis degree by attacking process, thus will attack to attack process of 2, 2 and then transferred to the attack process of effective plan recognition, and the attack process 2 data selection is random.

From table 1, it is not difficult to see, whether in the attack process of 1 or in the attacking process of 2, all possibility of target state which can be generated in aggressive behavior under the action of its own crisis degree value is small, so the maximum relative crisis value it is likely to be large; on the other hand, in view of the events occurred in the attack the current time step, the maximum relative crisis degree value of the possibility of the target state is bigger also, and also explains the possibility of the target state is more likely is the ultimate goal to achieve the desired state of the attacker in the current process of attack. This reasoning results are consistent and our test results. In addition, since the state variety of possibilities to target an attack during the attack action which may arise as a result of its own crisis of value allocation is different, will have different maximum relative crisis degree, that directly affect the effect of plan recognition. Therefore, we only according to the domain expert knowledge and experience and scientific and reasonable configuration of all possibilities of the target state its own crisis of value, can before the attacker to achieve the ultimate goal, to minimize the time

cost for the bottom line, identification of all possibility of target state may realize the attacking behaviors of malicious attackers, and before the attacker to achieve the ultimate goal state to the security administrator issued the corresponding alarm information.

Conclusions

In this paper to develop a model of system has a strong ability of problem description. Based on the abstract analysis of the attacks, found the attack way to achieve the ultimate goal of state is a show nearly process per column. And on this basis, the attack is decomposed into several attacks in the process of collection, and through the process of each attack the ultimate goal of the analysis of the condition node, so as to realize the effective recognition of the attacker attacks, namely, the identification process of adversarial plan; This paper also in formal theoretical research on the basis of the study of its planning recognition model has carried on the preliminary design, and in a closed in a virtual environment for specific attacks on the plan recognition model carried out the necessary tests. Find the smart plan recognition technology applied to the identification of a specific attack does exist in the process of its own advantages. That is to say, it can be before the system is the substantial harm according to the analysis of the adversarial plan recognition method produce the alarm information, thus realize the effective recognition and response of the attacker attacks.

Acknowledgements

This paper is supported by the Young Teachers' Scientific Research Project, The Chinese People's Armed Police Forces Academy: The Research and Implementation for Public Security Border Drug Case Data Analysis System Based on GIS.

References

[1] Yin Ming-Hao, Gu Wen-Xiang, Liu Ri-Xian, Liu Xiao-Long, Using regressive graph as a novel paradigm in plan recognition[C]. ICMLC2003.

[2] Gu Wen-Xiang, WangLei, Li Yong-Li, Research for Adversarial Planning Recognition and Reply in the Complex Domains and the more Agents Conditions[C]. Proceeding of 2005 International Conference on Machine Learning and Cybernetics(EI),2005:225-230.

[3] Lei Wang, Research of Plan Recognition Model in Specifical Intrusion Detection Problem, Information Technology,2009.

[4] Lei Wang,Research and Implementation of Plan Recognition Model Based on Action State Graph, Northeast Normal University[Master Paper],2007.

[5] Kangheng Wu, Yunfei Jiang, Planning with Domain Constraints Based on Model-Checking, Journal of Software Vol.15,No.11,2004.

[6] Hengtai Ma, The Model And Practice of Distributed Intrusion Detection System Basing on Agent, Institute of Software, Chinese Academy of Sciences(ISCAS), 1st,December,2000.