http://ansinet.com/itj

ITJ

ISSN 1812-5638

# INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (24): 8123-8128, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.8123.8128


# Modeling Mental Attributions of Defense Decision of Networks Security Based on AML

[1]Zhao Dongmei, [2]Liu Jinxing and [3]Zhang Yanxue
[1]College of Information Technology, Hebei Normal University,
Shijiazhuang 050024, China
[2]Department of Airborne Weapon, The First Aeronautics College of PLAAF,
XinYang 464000, China
[3]College of Mathematics and Information Science, Hebei Normal University,
Shijiazhuang 050024, China

**Abstract:** Under the complex, dynamic and uncertain networks threat environment, the network defense decision must be made effectively so that the limited network defense resource, such as firewall, honeypot, reacting resource, etc., can be distributed effectively, the primary information asset can be protected and the mainly network part can be operated effectively. The mental attributions are the foundation of making network defense decisions. In this study, we try to model the mental attribution of the defense decision by means of visualization method, to establish a foundation for developing the network defense decision system. First, the mental factors of the automatics decision are classified from information, motivation and operation of the decision based on the requirements of networks security defense; and then, based on the traditional BDI-Agent (Belief, Desire and Intention), a BGP-Agent model is presented, which has the three types of mental attributions, i.e. the belief, goal and defense plan. Finally, the mental attributions of the network defense decision and the relationship among the mental attributions are modeled by the Agent diagram and the mental diagram with the Agent Modeling Language (AML).

**Key words:** Mental attribution, network defense decision, information security, AML

## INTRODUCTION

As networks getting complicated, the information asset and the operation of the network are threaten by all manner of network attack, such as worm, Trojan horse, hacker and distributed denial of service etc. Under the complex network threat environment, the limited network defense resource can't defend all types of network attack and protect all information assets and keep all parts of the network operation effectively. For this reason, how to dispose and distribute the limited network defense resource effectively is crucial to protect the more important information assets and keep the critical subsystem of the network operation effectively. The study of network defense decision has been pay attention by network security researchers and the Artificial Intelligence has been applied in making network defense decision (Liu, 2011; Lussier, 2009; Yuill *et al*., 2005).

In the current, the research results about the network defense decision mainly include the network attack and defense game based on the game theory (Burke, 1999; Lye and Wing, 2002; Hausken and Levitin, 2009), such as modeling on action of attacker and defender (Burke, 1999), the optimal strategies of the attacker and the defender (Lye and Wing, 2002) and the selecting method of the optimal defense strategies (Hausken and Levitin, 2009). The game theory can provide the optimal defense strategies for the defender, but its decision is based on the perfect information about the attacker. But the information of the attacker is mostly imperfectly in most situations. This shortcoming determines the limitation of the game theory applied in making network defense decision. It is necessary to find an effective decision for the network defense for the large scale network.

Agent theory has been applied in making automatics and distribution decision in many fields, such as intelligent robot, mechanical design and navigation and aerospace and etc. and has been applied in network security defense, such as intrusion detection (Boukerche *et al*., 2007; Zaki and Sobh, 2004), modeling network security defense model (Boukerche *et al*., 2007) etc.

**Corresponding Author:** Liu Jinxing, Department of Airborne Weapon, The First Aeronautics College of PLAAF, XinYang 464000, China

Based on the agent theory and its application results in other fields, we propose a network security defense decision method, i.e. a BGP-Agent (Belief, Goal and Plan) for network defense decision, so that the network defense decision can be made under the uncertain and complex network threat environment. For this purpose, we analyze the mental factors of making the defense decision based on the Agent and classify the mental attributions contributed to the decision and model the mental attritions by means of visualization method, so that the shortcoming of the traditional modal logic i.e. difficult to be understand by the software developer, can be overcome.

AML (Agent Modeling language) is a semi-formal visual modeling language for specifying, modeling and documenting systems that incorporate concepts drawn from multi-agent systems theory (Trencansky and Cervenka, 2005), which is a comprehensive and versatile extension to UML 2.0 designed to address the specific qualities offered by multi-agent systems (MAS) that are difficult, or impossible, to model with more traditional modeling languages such as UML.

The application of the AML shows its advantage in modeling decision system based on agent (Cervenka and Trencansky, 2004). With the agent diagram and the mental diagram, the mental attritions can be described effectively and will provide a foundation for develop actual software.

## MENTAL ATTRIBUTION OF NETWORK DEFENSE DECISION

**Mental factor:** Based on the mankind mental features, the mental decision is a process from the gain information, determine goal, to plan operation. The mental factors of the network defense can be divided into the information, motivation and the operation.

**Information factor:** The information factor is the base of the decision. For the network defense decision, information needed by making decision includes the network environment, defense capability and the defense goal information.

The network environment information means the information about the network threats, such as the type, number of the virus etc.

The defense capability means the capability of the network defense resource disposed in the network, such as the firewall antivirus software etc.

The defense goal means the information of defended network assets and the network operation system.

**Motivation factor:** The motivation factor means the defense purpose of the network defense decision. Under the network environment, the threats are uncertain, dynamic and complex. The network defense decision must has the decidable defense target and the un-decidable target, i.e. the expect defense target for the important network assets and random defense target for the unpredictability attacking.

**Operation factor:** The operation factor means the result of the defense decision, which include the actual defense plan, such as the distribution result of the network defense resource etc.

**Mental attribution of the defense decision:** Based on the traditional BDI-Agent, we propose a BGP-Agent structure for the network defense decision, i.e. the agent has the mental attribution of the Belief, Goal and the Plan. The structure of the agent of the network defense decision is shown as Fig. 1.

The agent structure modeled by the agent diagram of AML (Fig. 1) describes the mental attributions of the agent, i.e., the belief, goal and the plan, where the belief describes the information state of the agent and the goal and the plan describes the motivation and the operation state of the agent respectively.

The feature of the agent diagram of the AML is similar to the class diagram of the UML, which mainly includes the attributions and the operation of the agent.

The logic controls relations are depicted by the logical contribution of the AML, shown in Fig. 2.

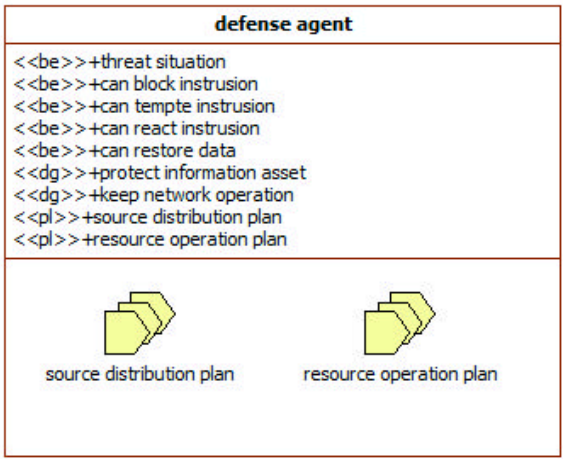


Fig. 1: BGP-agent

| Contribution | logic interpretation | Description |
|---|---|---|
| C ⟶⟶B | C⇒ B | C is sufficient for B |
| C ⟶⊣⟶B | C⇐ B | C is necessary for B |
| **C⟷B** | C⇔ B | C is equivalent with B (C is sufficient necessary for B) |

Fig. 2: Logical contribution

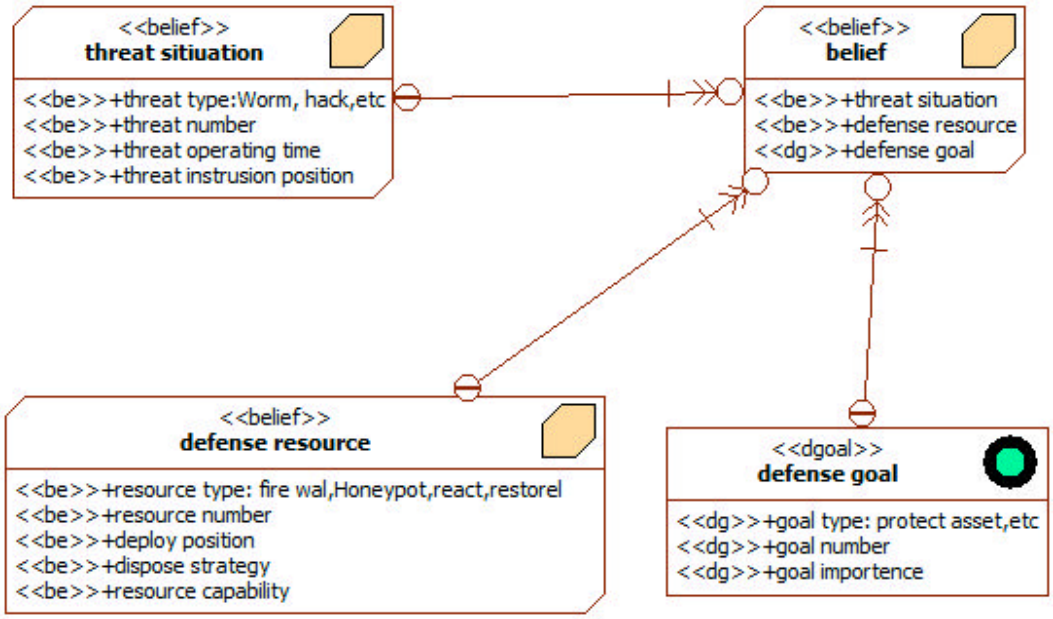


Fig. 3: Model of belief

## MODELING THE MENTAL ATTRIBUTIONS OF THE NETWORK DEFENSE DECISION

**Model of the belief:** The model of the belief described by AML is shown as Fig. 3. In the Fig. 3, the threat situation, defense resource and the decidable defense goal are contributed to the belief. These are the sub-belief and modeled by the mental diagram.

The logical relation among these sub-beliefs is "and" relation and each sub-belief is the post-condition of the belief and their attributions are given.

**Model of the goal:** The model of defense goal can be divided into two types goal according to defense purpose, i.e., the protecting the information assets and the keep the network operation effectively (Fig. 4).

Each goal is composed of several un-decidable sub goals, since in uncertain network environment, the network threat is unknown and the sub-goal is un-decidable. Their logical relation is also shown.

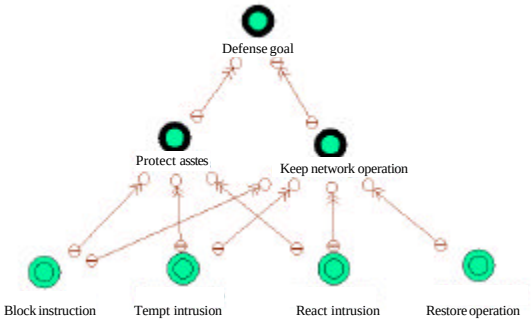


Fig. 4: Model of defense goal

The model of the goal "protect assets" is shown as Fig. 5. And that of "keep network operation" is shown as Fig. 6.

In Fig. 5 and Fig. 6, the model of the goals is described by the attributions, commit time, pre-, post-condition and cancel condition.

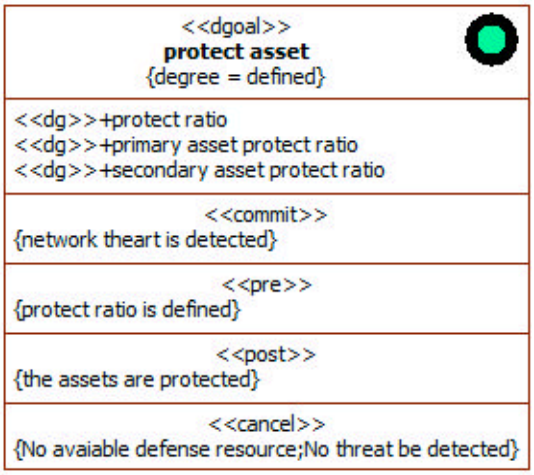


Fig. 5: Model of protect assets

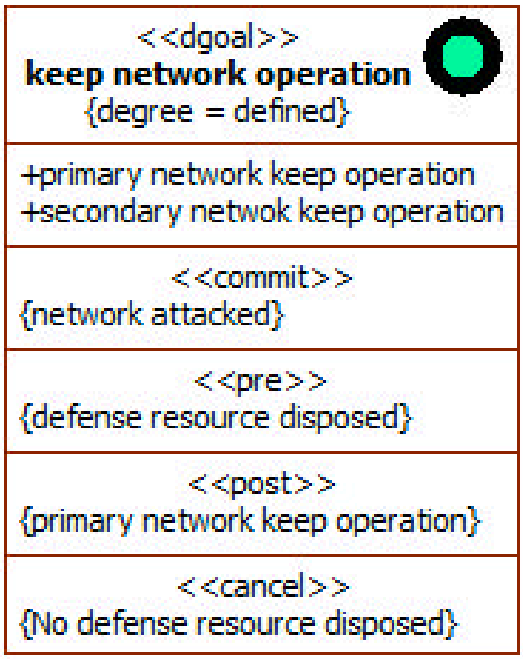


Fig. 6: Model of keep network operation

**Model of plan:** The defense plan is used to achieve the defense goal. In this study, we divide the defense plan into two types of plan, i.e., defense resource distribution and the resource operation. Which are shown in Fig. 7 and 8.

In Fig. 7 and 8, the model of the plan are similar to the goal model mentioned above. The difference between them is that the operation condition and the attribution are different.

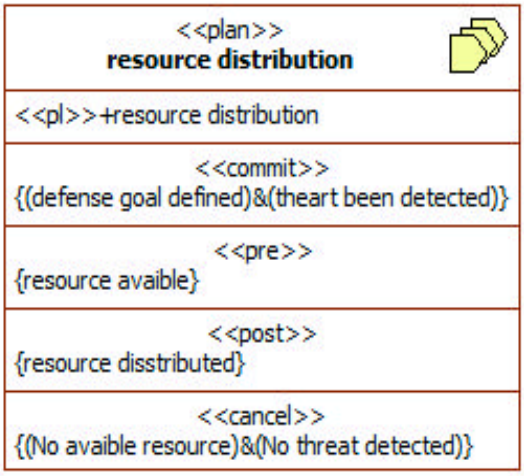


Fig. 7: Model of resource distribution

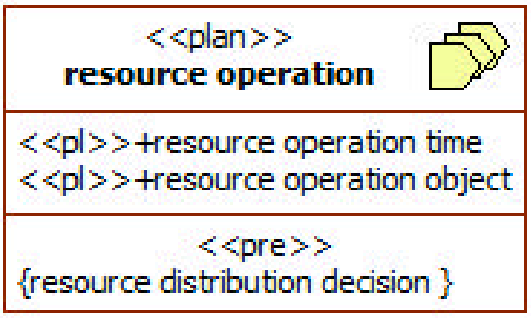


Fig. 8: Model of resource operation

**Relationship among the mental attributions:** The relationship among the mental attributions describes their dependency relationship during the whole network operation lifetime. From the relationship, the change of the attributions can be gained.

**Plan reason:** The defense plan can be reasoned according to the belief and the goal (Fig. 9).

In Fig. 9, the plan is reasoned according to the information of intrusion threat, available resource and the protect assets. Their logical relation is "and" relation.

**Belief change:** The belief is determined by the information of the network situation and the defense goal. Each of these changes will change the belief of the network defense decision. The effecting factors to the belief are shown as Fig. 10.

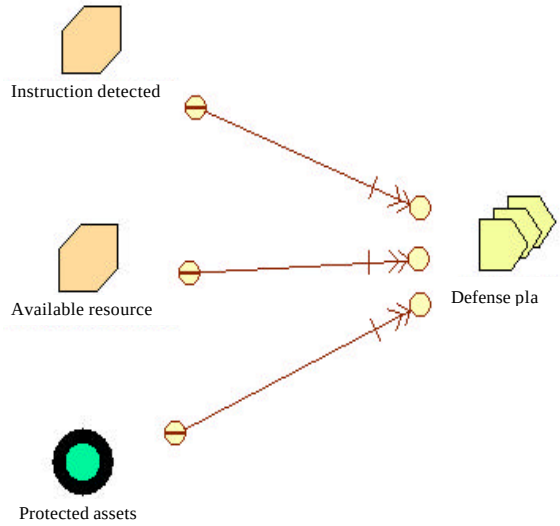


Fig. 9: Plan reasoning

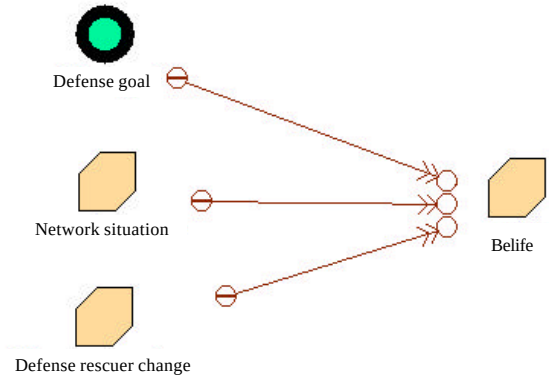


Fig. 10: Belief change

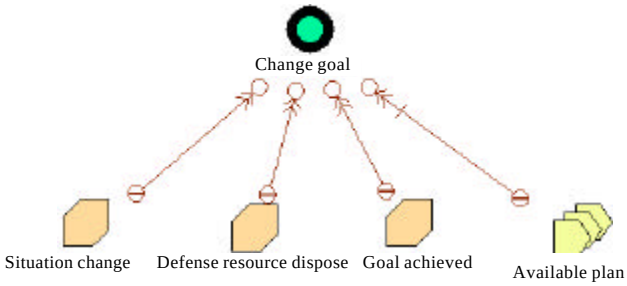


Fig. 11: Goal change

In Fig. 10, the logic relation of each effecting factors is "or "relation. One of the factor can change the state of the belief.

**Goal change:** The defense goal is determined by the information of the threat, defense resource dispose, achieved goal and the available plan (Fig. 11). The logic

relation among them is that the form three factors are "or" relation and that of form three factors and the plan are "and" relation.

## CONCLUSIONS

In this study, we try to explore the modeling method for the network defense decision. By the method studied in this study, the mental attributions of the network defense can be described by means of visualization method. Which can provide the visualization description for the software engineer, so that they can understand the development requirement and design their program. And the relative code, such as C++ can be generated by the relative tool. The workload of the software engineer will be reduced.

## ACKNOWLEDGMENTS

The authors would like to thank the reviewers for their detailed reviews and constructive comments, which have helped improve the quality of this syudy. This work was supported in part by Hebei Science Fund under Grant No F2013205193 and supported in part by Hebei science supported planning projects No. 12213514D.

## REFERENCES

Boukerche, A., R.B. Machado, K.R.L. Juca, J.B.M. Sobral and M.S.M.A. Notare, 2007. An agent based and biological inspired real-time intrusion detection and security model for computer network operations. Comput. Commun., 30: 2649-2660.

Burke, D.A., 1999. Towards a game theory model of information warfare. Technical Report: AFIT/GSS/LAL/99D-1. Air Force Institute of Technology.

Cervenka, R. and I. Trencansky, 2004. Agent modeling language: Language specification. Version 0.9, Technical Report, Whitestein Technologies.

Hausken, K. and G. Levitin, 2009. Minmax defense strategy for complex multi-state systems. Reliab. Eng. Syst. Saf., 94: 577-587.

Liu, S.J., 2011. Study on military networks defense in-depth model based on closed-loop control. Comput. Sci., 38: 96-98.

Lussier, J.J., 2009. Computer network defense roadmap. May, 2009, Department of the Navy|Chief Information Officer.

Lye, K.W. and J.M. Wing, 2002. Game strategies in network security. May, 2002, Technical Report CMU-CS-02-136, Pittsburgh, USA.

Trencansky, I. and R. Cervenka, 2005. Agent Modeling Language (AML): A comprehensive approach to modeling MAS. Informatica, 29: 391-400.

Yuill, J., F. Feer and D. Denning, 2005. Designing deception operations for computer network defense. http://www.sigsac.org/ccs/CCS2005/tutorial/Tutorial-2.pdf

Zaki, M. and T.S. Sobh, 2004. A cooperative agent-based model for active security systems. J. Network Comput. Appl., 27: 201-220.