

Mimic Geographic Information System

FAN Yong-wen*, ZHU Wei-jun and BAN Shao-huan

School of Information Engineering, Zhengzhou University, 450001, Zhengzhou, China

Abstract. With the development of the Internet, the geographic information system gets a chance to develop rapidly. Aiming at the security problems of existing geographic information systems, a Mimic Geographic Information System, i.e. M-GIS, based on mimic defense is proposed to improve the security of geographic information systems. The system consists of heterogeneous redundancy geographic information execution bodies pool, request distributor, scheduler and arbiter. Firstly, the scheduler dynamically selects the geographic information execution bodies set for processing, and then makes a mimic decision on the processing results. The experimental results show that the mimic system is more security than traditional system.

1 INTRODUCTION

The rapid development of Internet has provided a great convenience for the communication and acquisition of information in Geographic Information System, i.e. GIS. However, the valuable data of GIS has become the target of hackers, due to the impact of internet security issues. Therefore, it is necessary to take measures to enhance the security of GIS.

At present, experts and scholars from home and abroad are greatly focusing on the security of GIS. Such as, YANG proposed the safety design method of GIS [1]. Kotenko proposed the logical inference framework of GIS security management [2], Wu proposed three-dimensional authorization mechanism of Grid-GIS [3]. TIAN proposed a security solution of GIS based on Web [4]. There are also many studies on the security of GIS. We do not detail it in the interest of brevity.

Although these methods have improved the security of GIS. However, they have some limitations because of the inevitability of system vulnerabilities. Thus, this paper proposes a M-GIS based on mimic defense.

2 PRELIMINARY

2.1 The security of GIS

GIS [5] [6] integrates multi-discipline, such as computer science and geography. The application of GIS has a vast prospect in our life, and its related fields include natural, social and military medical, etc. As shown in Fig. 1, the implementation process of GIS is the process of data processing, collection, analysis and expression.

As shown in Fig.1, the security problems of GIS can be divided into three aspects, which includes data security, application security and system security. To protect data, we can carry all sorts of measures, such as,

encrypting data and cryptographic storage. As for system and application security, the intrusions detection and other measures can be used to improve the security of it.

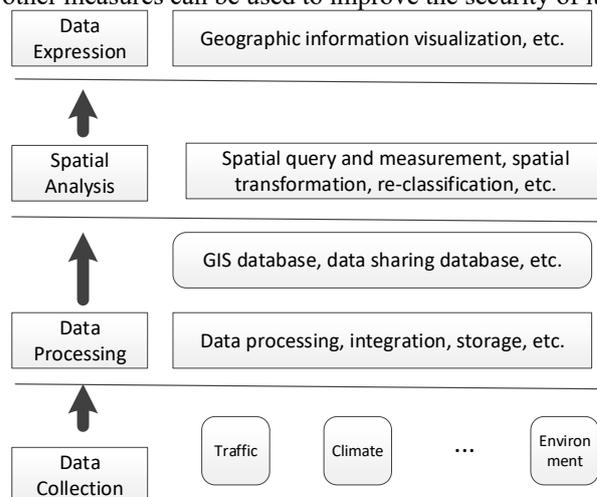


Fig. 1 The processing of GIS

2.2 Mimic defense

Inspired by the biologic mimic, the academician Wu Jiangxing proposed a new dynamic and variable active defense technology, Mimic Defense (MD) [7] [8] [9]. The essence of mimic defense [9] is to conceal its inherent function, and increase the uncertainty of the system and the cost of attacker's attack.

Based on this, the researchers have developed the core architecture of mimic defense, i.e., dynamic Heterogeneous Redundancy (DHR) architecture [10], as shown in Fig. 2. The principle of DHR structure is described as follows:

Firstly, the scheduler dynamically selects online execution bodies set from the execution bodies pools;

* Corresponding author: 316072803@qq.com

Secondly, the input agent distributes tasks to these execution bodies;

Thirdly, the arbiter makes a consistent decision on the processing results;

Finally, the arbiter outputs the result of the decision. And feedback the relevant information to scheduler.

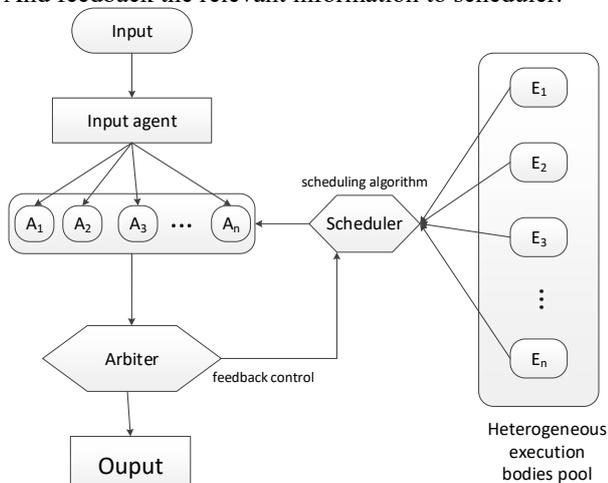


Fig. 2 Dynamic Heterogeneous Redundancy, DHR

Table 1. The application of mimic defense.

Mimic defense	
Applications	Web Server [11]
	Router [12]
	Network Operating System [13]
	DNS [14]
	Password recovery [15]
	Industry Control System [16]

As shown in Table 1, the mimic defense technology based on DHR architecture technology has been applied in many fields.

3 M-GIS

In view of the limitations of the existing protection methods for GIS, a mimic GIS system is proposed in this paper. The combination of mimic defense and multi-modal decision mechanism is used to enhance the security of GIS.

3.1 System architecture

This section will introduce the composition and workflow of the M-GIS.

3.1.1 The composition of M-GIS

As shown in Fig. 3, the M-GIS is composed of heterogeneous redundancy geographic information execution bodies pool, request distributor, scheduler and arbiter. The request distributor is responsible for distributing tasks to the online execution bodies set; the scheduler is responsible for dynamically scheduling the online execution bodies set from execution bodies pools; and the arbiter is responsible for making consistency decision of the processing results. The controller is responsible for dynamic scheduling of execution bodies.

3.1.2 The workflow of the M-GIS

The specific workflow of M-GIS is described as follows:

- (1) The scheduler selects online execution bodies set from the execution bodies pools.
- (2) The request distributor distributes tasks to the online execution bodies set.
- (4) The online execution bodies set process the task and transmit it to the arbiter.;
- (5) The arbiter makes consistency decision according to the result of online execution bodies set.
 - (a) The result will be output, if the result is consistent.
 - (b) Most of the consistent results will be output, if the results are inconsistent. And the feedback result will be given to the scheduler.

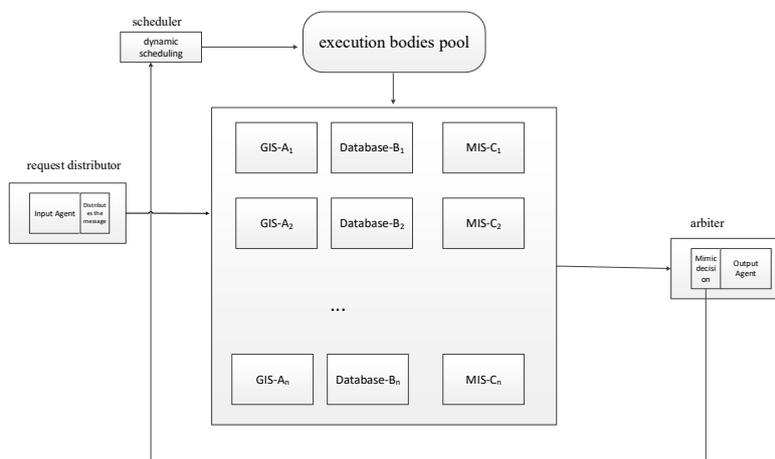


Fig. 3 The Logic diagram of M-GIS

3.2 Feasibility Analysis

The model of M-GIS has been applied in the market. And multiple application markets also bring convenience to the theM-GIS. As shown in Fig. 4, the heterogeneous of M-GIS system can be embodied in three layers: system environment layer, database layer and management information system layer.

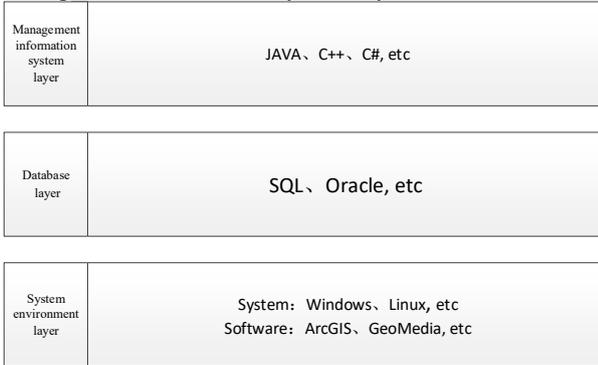


Fig. 4 The heterogeneous execution bodies pool of M-GIS

3.3 Safety Analysis

M-GIS has the characteristics of dynamic, heterogeneous redundancy, diversity and randomness. And the dynamic heterogeneous redundancy execution bodies not only increase the cost of attackers, but also make the system have the ability of intrusion tolerance. Moreover, the multi-mode decision mechanism can identify and shield unknown security threats. The combination of the above ways improves the security of M-GIS.

4 Simulation experiment

This section will simulate the security performance of the M-GIS.

4.1 The simulation platform

- (1) CPU: Intel(R) Core(TM) i7-4790 CPU @3.40GHz.
- (2) RAM: 8.0G RAM.
- (3) OS: Windows 7.
- (4) MATLAB R2014a.

4.2 The simulation of Anti-attack ability

Referring to the performance evaluation of DHR structure [10], this paper also assumes that the attacker's attack ability increases with time. The relationship between the probability of success of traditional model without mimic defense and time can be expressed as follows:

$$P(t) = \int_t \lambda e^{-\lambda t} \quad (1)$$

Within each cycle, the probability of successful attack of M-GIS at time t is expressed as:

$$P(t) = \frac{m}{M} \sum_{u=(m+1)/2}^m C_m^u P_i^u (1 - P_i)^{m-u} \quad (2)$$

Where, $\frac{m}{M}$ indicates the probability of selecting m execution bodies from M heterogeneous execution bodies pool.

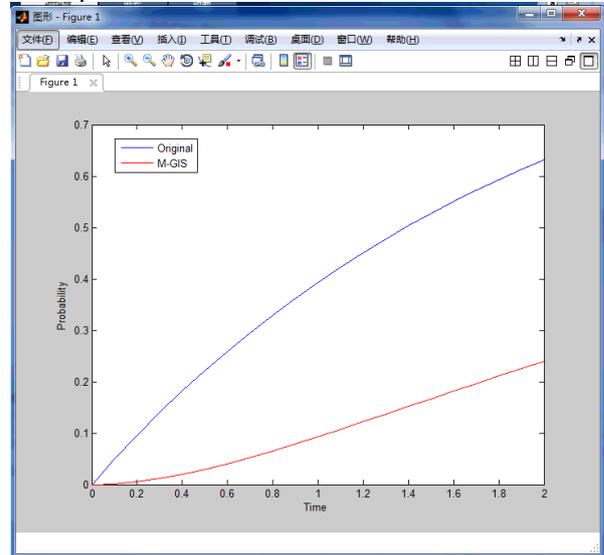


Fig. 5 The comparison of M-GIS and GIS

As shown in Fig. 5, we assume that the three the online executives are selected from five heterogeneous execution pools during the period of time without dynamic scheduling. The security of M-GIS is higher than traditional GIS because of its multi-mode decision and dynamic scheduling mechanism.

4.3 Discussion

Although M-GIS can improve the security of the system, it also brings some time and economic costs. Therefore, in the face of higher security applications, M-GIS can be used. When time performance is required, a degraded M-GIS can be used, that is, there is only one on-line execution body and the multi-mode mechanism should be removed.

5 Conclusion

In view of the potential security hazards of GIS and the shortcomings of existing protection methods, this paper proposes a dynamic and variable N-GIS with intrusion tolerance and threat shielding. This is the main contribution of this paper. The simulation experiment shows that the security of M-GIS is higher than traditional GIS. From the existing literature, this is the first time to apply the idea of mimic defense to the GIS.

Of course, the deployment of M-GIS will also bring some economic and time cost. Therefore, in the future research, we will study the time and cost optimization of M-GIS.

This work has been supported by the National Key Research and Development Program of China

(No.2016YFB0800101), the National Natural Science Foundation of China (No.U1204608, No. 61572444).

Industry Control System. *Journal of Cyber Security*, **2(1)**:54-73 (2017)

References

1. YANG Hua-xian, HONG Liang, WEI Zhong, et al. A Safety Design Method of GIS. *GEOSPATIAL INFORMATION*, **4**:8-11 (2006)
2. Kotenko I, Polubelova O, Saenko I. Logical Inference Framework for Security Management in Geographical Information Systems// Information Fusion and Geographic Information Systems (IF AND GIS 2013). Springer Berlin Heidelberg, **2014**:203-218 (2013)
3. Chun-Xia W U, Jian-Qiang L I, Xia L U. The three-dimensional authorization mechanism of Grid-GIS geological resource. *China Mining Magazine* (2011)
4. TIAN Bin SUN Jing-jie YANG Jun. A DIGITAL GIS SECURITY SOLUTION BASE ON WEB. *SURVEYING AND MAPPING OF SICHUAN*, **30(03)**:46-49 (2007)
5. GONG Jian-Ya. Geographic information system foundation. *Science Press* (2001)
6. Pandey J. geographic information system. *Springer US* (2001)
7. WU Jiangxing. Research on Cyber Mimic Defense. *Journal of Cyber Security*, **1(4)**: 1-10 (2016)
8. WU Jiangxing. Meaning and Vision of Mimic Computing and Mimic Security Defense. *Telecommunications Science*, **30 (7)**: 1-7 (2014)
9. WU Jiangxing. Introduction to Cyberspace Mimic Defense. *Beijing:Science Press* (2017)
10. Hu Hongchao, Chen Fucai, Wang Zhenpeng. Performance Evaluations on DHR for Cyberspace Mimic Defense. *Journal of Cyber Security*, **1 (4)** :40-51 (2016)
11. Tong Qing, Zhang Zheng, Zhang Weihua, et al. Design and Implementation of Mimic Defense Web Server. *Journal of Software*, **28 (4)** :883-897 (2017)
12. Ma Hailong, Yi Peng, Jiang Yiming, et al. Dynamic Heterogeneous Redundancy Based Router Architecture with Mimic Defenses. *Journal of Cyber Security*, **2 (1)**: 29-42 (2017)
13. Wang Zhenpeng, Hu Hongchao, Cheng Guozhen. Design and Implementation of Mimic Network Operating System. *Journal of Computer Research and Development*, **54(10)**: 2321-2333 (2017)
14. Wang Zhenpeng, Hu Hongchao, Cheng Guozhen. A DNS Architecture Based on Mimic Security Defense. *Acta Electronica Sinica* (**11**) :2705-2714 (2017)
15. Li B, Zhou Q, Si X. Mimic computing for password recovery. *Future Generation Computer Systems*, (2018)
16. WEI Shuai, YU Hong, GU Zeyu, ZHANG Xingming. Architecture of Mimic Security Processor for