The Design of Huge Amounts of Information Network Forensics System in View of the Network Crime Prevention

Baozhong Liu*

Chongqing College of Electronic Engineering, Shapingba, Chongqing, China

Abstract: The advent of the information age has brought great convenience to people's life, at the same time all kinds of cyber-crimes have become increasingly rampant, causing great damage to people's life. To build a network forensics data which is based on multi Agent system model, which is further based on multi Agent technology, by means of an agent, in a distributed implementation method of network data packet capture, and division of labour and allocation of Agents, which realizes the communication and collaboration between Agents, solve the bottleneck problem of massive data processing that has characteristics of dynamic network in data acquisition, and improve the efficiency of the network data collection. At the end of the system database and the data sheet for the design. Realizing the functions of the system, the network forensics relates to the collected data, the work provides a rich source of data for the subsequent forensic analysis, the application effect is good.

Keywords: Data acquisition, multi agent, network forensics, network packets.

1. INTRODUCTION

The rapid development of the computer network greatly promotes the process of human civilization, which provides great convenience for our life. At the same time, computer crime is becoming rampant. Computer crime is a newer crime which appears with the increasing popularity of the Internet, it began in the 60's to the 80's, and especially since the 90's there has been a rise in cyber-crimes; domestically and abroad. Computer crime is destructive to people's lives and has brought huge losses, which in the year 2000 began to spread the love bug virus. So far the fastest and the most widespread computer virus , infected the world and millions of computers causing damage and economic losses of up to tens of billions of dollars. Results of the Norton survey in 2013 show that about 84% of the Chinese people have been invaded by perpetrators of cybercrime, with the annual economic losses of up to 1126 yuan. And this data in the global scope, from $197 last year increased to $298 [1]. From the above data, we can see that, the computer crime is an increasing trend, so to prevent and combat computer crime has become imperative. Network forensics is a branch of computer forensics, and it is to protect users and resources through the extraction and analysis of network flow, prevent network attacks and other cybercrime series [2]. The primary work of network forensics is data acquisition. Network data collection is the basis of network forensics, it can effectively obtain the foundation of network security data by simulating the attack and other methods, to understand the current state of the network, to forecast the trend of its development, and to make the necessary preparations for network forensics. However, the network data is massive. Collection for network forensics and the type of data, is a big problem that this system is facing, and in order to reduce the human and material resources in the process of data collection and to reduce human error in the collection process, the use of Agent technology. Multi Agent technology is developed with the Agent technology. It is a complex and large-scale problem which provides a solution to the problem of decomposition. If the multi-Agent system is decomposed into a single Agent, with each Agent to solve a specific problem, and through the communication and collaboration between the Agents, the large-scale problems will eventually be complicated by a distributed solution [3-7]. The appearance of Agent technology provides a new method for the design and analysis of distributed open system, which is a major breakthrough in the development of software. Theory and technology of Agent is derived from DAI (Distributed Artificial Intelligence), but in the late 80's, research on the theory and technology of Agent began to expand from the DAI field, and many other fields of reference and integration technology, in information management, database, data mining, intelligent network management and e-commerce and other fields [8-10], are compatible with Agent technology and there has been wide application of them. The databases of Dartmouth College and University of Minnesota have made a special study of how to use Agents for distributed data query, test the development of D 'agent and Ajanta mobile Agent platform [11-12]. Oracle Corp has launched a mobile agent in the mobile Agent platform Oracle Lite, mobile users to access the data source can make the center of mobile devices without connecting to the server at any time by "client/agent/server" service mode, greatly reduces the communication time. The Carleton University in Canada has often used mobile Agent network management. Pinheiro *et al*. [13] described a conceptual model, the network changing data collected by mobile Agent and calculated according to the data of network state.

*Address correspondence to this author at the Chongqing College of Electronic Engineering, Shapingba, Chongqing, China;
E-mail: jianqiu27@163.com

2. THE AGENT AND ITS CHARACTERISTICS

Agent is an emerging field of artificial intelligence technology, are widely used in software engineering, network management at present. Agent can be simply understood as the specific target, according to the external environment can play a role to achieve the goal of autonomous software entities.

Generally speaking, Agent has the following characteristics:

(1) Independence

Each Agent has its own resources and the behavior of their own control, it can't control through its own perception of the outside world, the surrounding environment to decide and control their own behavior, in order to complete its intention or goal, the autonomy of the Agent determines that the Agent is an intelligent individual.

(2) Interaction

Between Agent and Agent and can communicate through a particular language, Agent interaction is the base of Agent to realize the communication and cooperation, is the most basic characteristic of multi Agent system.

(3) The active reaction

Agent can not only make the passive response to the external environment and the changes of the other Agent, but also according to their own goals or willingness to take positive action reaction.

In addition to the above characteristics, the Agent should also have the reasoning, learning, mobility, adaptability, planning of human characteristics. On the whole, Agent is flexible, autonomous, intelligent, portable software entities, the technical characteristics of Agent is shown in Fig. (**1**).

2.1. Multi Agent System

Multi Agent system (Multi Agent System) referred to as MAS, is composed of a plurality of Agent, is used to solve the complex problems of large scale. For large and complex problems, a single Agent is usually unable to solve or it is very difficult to solve the problem, have the ability of multi Agent system not only more than any single Agent is greater than Agent, and the ability to make up for the lack of and, single Agent capabilities, able to complete a specific task, is widely used in solving large-scale complex problems hand. This is the most direct cause of MAS [13].

The advantage of multi Agent system:

(1) the same task is especially complicated tasks were handed over to a single Agent system and the MAS, in order to make the system can handle the problem better, single Agent system needs to have the internal structure is very complex. In order to meet the requirements to deal with the problem, in MAS, only the problem decomposition, each Agent only a small part of the problem can be completed in.

(2) the multi Agent system through the Agent communication, collaboration makes it compared with the internal Agent and greater ability, solve the single Agent capability and limited in scope of application, the application scope has been expanded. The multi Agent system's advantages make it has been widely used in various fields.

2.2. The Collaboration between the Agent

Agent cooperation is the main way to solve the conflict between the Agent can't avoid. Each Agent to accomplish a common task by cooperation way, adjust their own behavior, to improve the system performance, the group to maximize, and enhance their ability to solve problems, is an important characteristic of unique MAS [14].

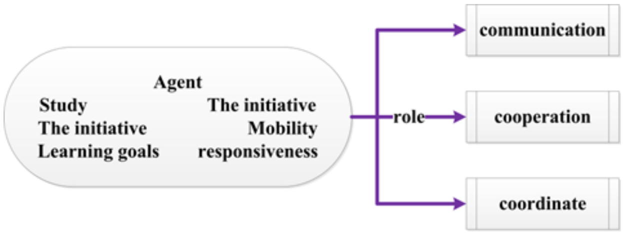

Fig. (1). Agent technology features.

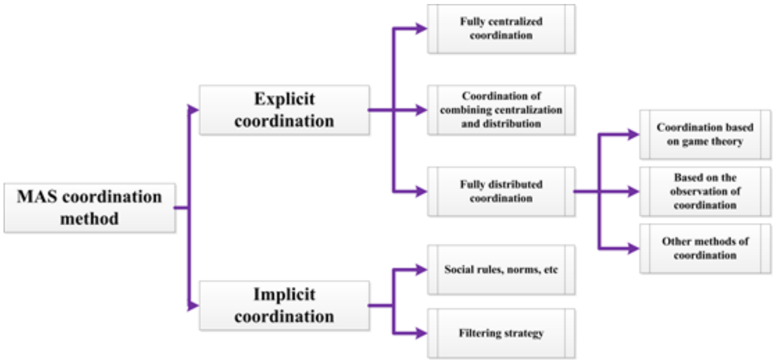
MAS coordination method
Explicit coordination
Implicit coordination
Fully centralized coordination
Coordination of combining centralization and distribution
Fully distributed coordination
Social rules, norms, etc
Filtering strategy
Coordination based on game theory
Based on the observation of coordination
Other methods of coordination

Fig. (2). MAS coordination classification method.

Under normal circumstances, we will coordinate of Agent is divided into explicit and implicit coordination two. Explicit coordination can be divided into several kinds according to the concentration and distribution in different ways, but the implicit coordination in Agent by following certain social rules, strategies to coordinate actions. The classification of MAS coordination method is Fig. (**2**).

3. SYSTEM REQUIREMENTS AND SYSTEM DEVELOPMENT ENVIRONMENT

3.1. System Requirements

In this paper, at the beginning of design thoroughly investigated the system requirements, types of network data acquisition system to the have a rough idea, is ready to take the following five types of data, respectively is: basic information, static network dynamic network data packet, the firewall log browser information, and through the implementation of some of the network data monitoring.

Specifically, the basic information of static network we want to collect the card information, installed network protocol and network connection status; dynamic network packets to capture network packets, the ability of each packet analysis, analysis of network data and to the data stream; and the browser information to the browser after leaving the Cookies, the use of temporary files as well as favorites for forensic personnel information, understanding of the offender; finally, we hope that the system can get the memory, screen, keyboard and mouse usage information through the assistant means of monitoring.

3.2. System Development Environment

The system development environment is Visual Studio 2010,.NET Framework 4 it is the Microsoft Corp for the development of:

An important tool send personnel to perform basic development tasks. Support for Windows 7, Windows 8 and other commonly used system.

Visual Studio 2010 compared to version has the following several aspects of innovation:

(1) The VS2010 keyword search code and function more humane and efficient.

(2) VS 2010 in the Web configuration file. In the use of VS2008 to create a Silverlight Application, feel to see things in a blur, because the code in the Web.Config file can be up to 107. In the latest release of S2010 is simple, to create the same Web.Config project file can be only 11 lines of code.

(3) Easy and convenient reference dialog. Developers in VS2008 if you use the add reference function, you will find the loading speed is very slow, computer hardware configuration is slightly lower or even downtime, feign death etc.. In view of this situation, Microsoft in VS2010 to Add Reference dialog box is improved. The Microsoft Visual Studio 2010 supports C#, C++, VB and other languages.

4. THE SYSTEM DESIGN

Based on system requirements analysis, system design is completed the design of the system design, including the overall system design, detailed design and database. The overall design for the construction of an overall framework of the system, and provides a way for the detailed design, the detailed design of each module according to the system functional requirements to complete the database design, and can improve the efficiency of the system, further improve the system. Simply put, the part of system design is how to define "software system". The design of the system in strict accordance with the system requirement analysis has been done to the system, so as to guarantee the maximum eventually developed to meet the needs of users.

4.1. Network Forensics Data Acquisition System Based on Multiple Agent Profile

Network forensics data acquisition system based on the Agent is the basis of network forensics work, effective access to network security data by simulating the attack and other methods, to understand the current state of the network, to forecast the trend of its development, so as to further determine the network suffered what type of attack, and then targeted to network attack prevention, ultimately blow the purpose of the network crime.

Based on the multi Agent network forensics data acquisition system is mainly to design a data acquisition model based on Agent, to coordinate between the various Agent collected by the communication between Agent, achieve a variety of types used in network forensics data according to different methods of data collection, and the collected data are preprocessed after preliminary norms in the database, so as to prepare for the next forensics. Synergistic effect and system using multi Agent technology, realize the diversity of data acquisition, the original and real time. It is Based on the framework of dynamic computer forensics system Agent as shown in Fig. (**3**).

In conclusion, this system is a data type collected by multi Agent technology the richness, diversity, and the image data is realized through the collaboration between Agent, the protection of data, and then improve the reliability, stability and efficiency of the whole data acquisition system, make the foundation for the subsequent network forensics the work.

4.2. The Technical Architecture Design

This system uses C# as the development language, using the three layer architecture, we usually three layer architecture is divided into: the presentation layer, business logic layer, data access layer, layer division increased the "high cohesion, low coupling" thought. The three layer architecture is shown in Fig. (**4**).

The presentation layer is mainly the system with a friendly operation interface presented to the user, users only need to click the function button to select the corresponding operation, the part of the function is realized by the method invocation of business logic layer. The business logic layer is the core module of the realization of system functions, the layer according to the specific problem, to realize the functions by calling methods of the data access layer. The data access layer contains the operation method of the database, such as data write, delete, change and search.

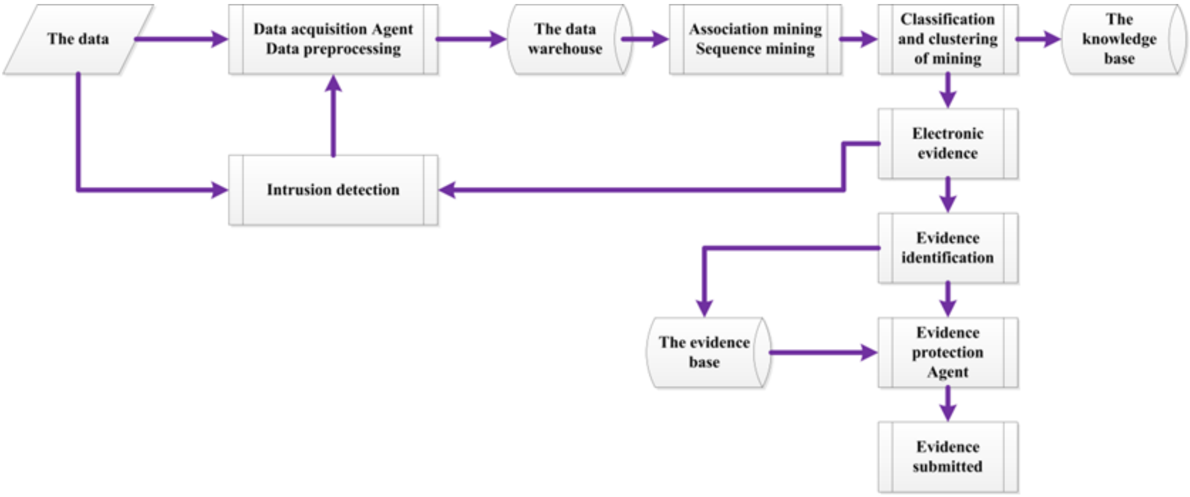

Fig. (3). The computer dynamic forensics system framework based on agent.

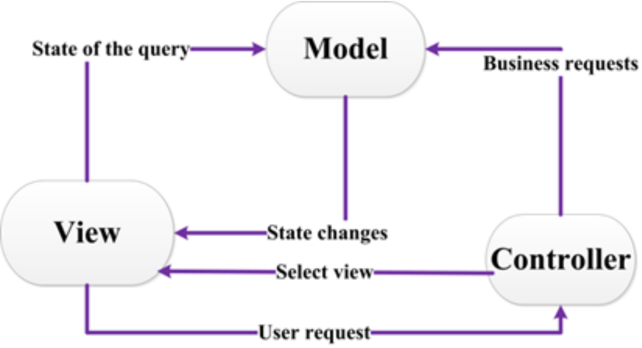

Fig. (4). The working principle of the MVC Figure.

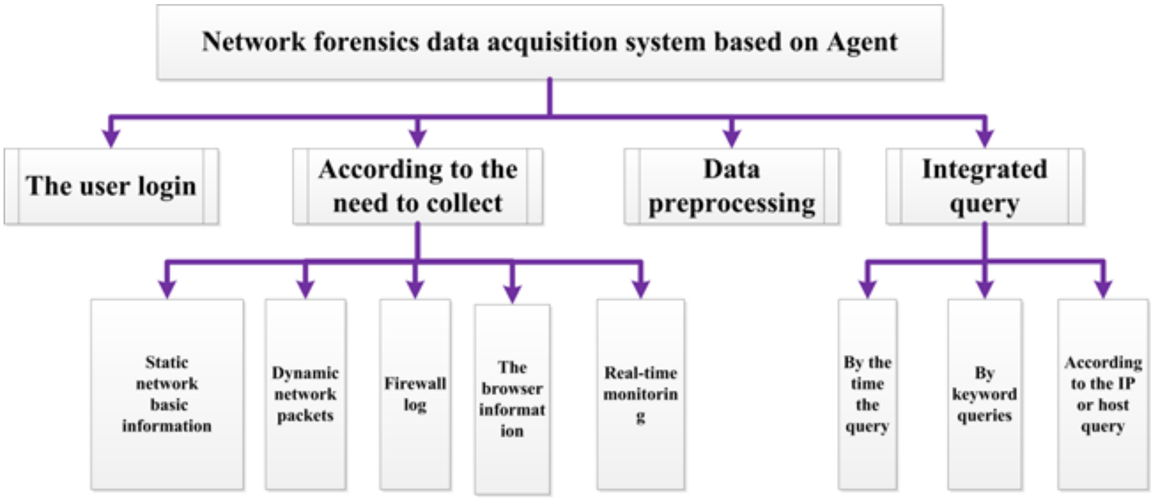

Fig. (5). The system function structure diagram.

4.3. Functional Architecture Design

A complete forensics system including data collection, data preprocessing, evidence analysis, function module etc. the main evidence report, to obtain the necessary to add some auxiliary tools to assist data. Of course, in order to make the system more perfect, we can also add the user login module, user manual and other users to use more handy. According to the above evidence collection process, in accordance with the transfer of data in the system, using a combination of multi Agent technology, we design the logical framework of Network Forensics System Based on multi Agent. The organizational structure is shown in Fig. (**5**).

The on-demand acquisition module is the core of the system function module, the module of each part and contain a

Table 1. System function relation table in detail.

Functional expression	The specific function operation
Static network basic information	The network adapter information; Installed in the network protocol; The network connection status;
Dynamic network packets	Network packet capture; Analysis of data packets; Data flow analysis;
Firewall log	Firewall Settings; Firewall log collection; Many conditions query log (time, source address, destination address, source port, destination port, behavior, protocol)
The browser information	The browser monitoring; Favorites; Cookies information; The temporary file information;
Real-time monitoring	Memory monitoring; Screen real-time monitoring; Keyboard mouse real-time monitoring;

Table 2. Network packet function module of system test case table.

The test title	Network packet module test		
Test purposes	**The availability of network packet module function**		
The test object	**Network packet capture module**		
Test options	**The test content**	**Test steps**	**The test results**
1	Network packet capture	After the user automatically obtain the IP address of the native, click start, empty, save and exit.	Users can access to the machine IP automatically, click start after packets will be able to show, in the form of a list of packets disappear after emptying, saved packets can continue to see in the database.
2	Network packet analysis	Double-click the network packets	Displays detailed information about the packet, including start time, the source and destination port, protocol type, version information, survival time, and the size of the header, packet length, priority, delay, throughput, reliability, etc., and display specific hexadecimal data packets.
3	Data flow analysis	Users according to their own need to choose a time period, click the generate analysis report and analysis report.	Analysis includes the host information, basic information and data network access to information, can also remains in the folder to get analysis report under the specified path.

series of functions, each function module contains the sub module as shown in Table **1** for details. The function of the system is introduced in detail, for the detailed design has been clear about the direction of the next, made adequate preparations.

5. THE SYSTEM TEST

In the process of software development, system testing is an essential part of the system, the purpose of the test is to compare the system which has been developed with the needs of the user, the contradiction between the local character and system have been developed with the demand of the. General test system was completed by the system developers, but in order to achieve better results, but also allows users to participate in, and puts forward some pertinent advice, to help developers to better accomplish the testing work.

Testing of the system can be divided into functional, nonfunctional testing test. Functional test design test cases corresponding to, is to ensure that the system functions correctly; the system functions such as system stability, reliability, portability is required by the nonfunctional testing to ensure correct. The system software after repeated modification and improvement, no matter from the operation and stability are better able to meet the requirements of the user. This paper selects two module analysis test, Table **2** the following is the case analysis:

In the system requirements analysis, overall design, system detailed design, database design and other related work on the use of C# as a programming language, through the implementation of the various modules of the system function, and the key code, visual display interface to achieve the process for a detailed description of. On this basis, in order to make the data acquisition system to be more perfect, to meet the needs of users, and has carried on the system testing has been completed, and further modified according to the test results, improve the system has been develop Table **3**.

CONCLUSION

In this paper the design and implementation of network forensics data acquisition system based on the Agent, this paper expounds the main problems of network forensics data acquisition system development background and significance, current, analyzes the related theory and technology of multi Agent system, then the system function and database structure of the overall and detailed design, the last 2010

Table 3. Network packet function module of system test case table.

The test title	**Real-time monitoring of the test**		
Test purposes	**The availability of real-time monitoring function**		
The test object	**Real-time monitoring module**		
Test options	**The test content**	**Test steps**	**The test results**
1	Memory monitoring	Click on the memory monitor button	Real-time display CPU and memory information, when the CPU or memory utilization rate more than 70% will alarm warnings.
2	Screen monitor	Click on the monitor screen button	System users to click on the button will be the moment of screen capture, and deposited in the database, can automatically every second will screen in the database.
3	Keyboard mouse monitoring	Click on the keyboard mouse control button	The coordinates of the mouse, operation type, key activities, press the location, types, characters, keyboard keys shift, CTRL and Alt keys usage will be recorded in real time.

code to implement a network forensics data acquisition system based on the Agent using Visual Studio.

The main features of the network forensics data acquisition system: (1) system using multi Agent technology to solve the problem of low efficiency of the traditional data acquisition system of mass (2), the data is involved in the network data network forensics, and network data of different types in different ways for the efficient acquisition provides a rich source of evidence, the evidence for later analysis, the application effect is good.

The development of network forensics data acquisition system based on Agent, network forensics analysis, for the next report evidence links to the basic work, and to prevent, combat network crime purpose. The system uses the Agent technology in the process of data collection, reducing the waste of manpower, greatly improving the efficiency and stability of the system. To combat Internet crime, reduce the low efficiency and high cost of manual collection. However, in practical applications, due to the diversity of network crime and unpredictability, the system also need to continue to improve, increase of new types of data collection, in order to adapt to the changes of network crime, so as to provide better help for network forensics. With increasing of network crime type, the request and the challenge for our next work, how to make the system capable of acquiring new cyber crime and efficient data will be the focus of our next work.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] L. Ding, "The research status of computer forensics analysis of", *Information Network Security*, no. 011, pp. 9-11, 2010.

[2] X. Hu, "Computer forensics in the law of the important position of", *Information And Communication Security*, no. 7, pp. 7-9, 2010.

[3] Y. Zhang, Q. Ceng, and J. Wang, "Calculation of", *Computer Network Forensics Research Collaboration*, vol. 3, no. 33, pp. 504-513, 2010.

[4] L. Zhang, Y. Xu, and F. Liu, "Research on technology of, and the development of computer technology", *The Multi Agent System*, vol. 18, no. 8, pp. 80~83, 2008.

[5] Y. Y. Huang, "Research on distributed network management system for mobile agent based on", *Micro Computer Information*, vol. 22, no. 11, pp. 154-156, 2006.

[6] M. Zhou, and A. Kung, "Distributed computer forensics model of", *Microelectronics and Computer*, vol. 29, no. 02, pp. 40-43, 2012.

[7] Z. Geng, and P. Shao, "Based network management framework based on mobile agent in Computer Engineering", vol. 28, no. 3, pp. 286-288, 2002.

[8] X. Yongqing, "An adaptive distributed network management architecture", *Computer Applications*, vol. 3, no. 12, pp. 30-32, 2002.

[9] R. J. Kuo, J.L. Liao, and C. Tu, "Integration of ART2 neural network and genetic k-means algorithm for analyzing web browsing paths in electronic commerce", *Decision Support Systems*, vol. 40, pp. 3 55-374, 2005.

[10] M. Hahsler, "A model-based frequency constraint for mining associations from transaction data", *Data Mining And Knowledge Discovery*, vol. 13, pp. 137-166, 2006.

[11] J. Li, and Z. Guo, "Study on improving the Mini micro systems the performance of network management based on mobile agent", vol. 27, no. 3, pp. 412-413, 2006.

[12] D. Liu, "Current situation and development trend of Chen Jianzhong. Agent research", *Journal of Software*, vol. 11, no. 3, pp. 315-321, 2000.

[13] W. Li, and F. Zhang, "Research and application of multi Agent technology", *Micro Computer Information,* vol. 22, no. 8, pp. 293-295, 2006.

[14] M. Cao, "Principle and application of intelligent agent", *Journal of Hunan Industry Polytechnic*, vol. 10, no. 2, pp. 23-25, 2010.

Received: May 26, 2015 Revised: July 14, 2015 Accepted: August 10, 2015