International Journal of Security and Its Applications
Vol. 10, No. 1 (2016), pp.449-460
http://dx.doi.org/10.14257/ijsia.2016.10.1.39

A Security Architecture Model of Oil and Gas SCADA Network Based on Multi-Agent

Jian Zhang, Li Yang* and Haode Liao

School of Computer Science, Southwest Petroleum University, Chengdu, China
School of Computer Science, Southwest Petroleum University, Chengdu, China
xdscyl@126.com

Abstract

Modern industrial automation control network SCADA system is facing more and more serious security threat. In order to meet the demand for oil and gas SCADA system security defense, by analyzing the security risk in oil and gas SCADA system and advantage of multi-agent technology, formalization description security defense architecture based on multi-agent is presented and the roles and tasks in the architecture are described and SCADA security defense framework based on multi-agent is designed, finally, simulation model based on agent security attack and defense is given. With the experimental simulation using neural network recognition algorithm, the reliability and validity of the model are verified by comparing detection rate and false rate. Compared with the traditional security and defense, this system makes full use of many advantages of the multi-Agent architecture, and has the advantages of accurate detection, high detection efficiency and timely response.

Keywords: *SCADA; multi-agent; security defense; formal description*

1. Introduction

SCADA (supervisory control and data acquisition), is widely used in large-scale pipeline network. As industrial control network system, general computer software and hardware are installed in SCADA, thus, there are many loopholes in SCADA. Due to ensuring the safety of production and operation, SCADA network system is usually not updated, which makes the system vulnerabilities not be solved, therefore there is a serious security risk in SCADA. Also more and more oil and gas SCADA systems achieve data exchange with other enterprise network, other networks which connect to the Internet [1-2]. Most SCADA systems have been completely exposed in external network, so SCADA has a great security risk. In addition, as a large oil and gas infrastructure, if SCADA is attacked and not to be solved timely, SCADA must suffer to serious destroy, and result in a lot of damage. In recent years there have been many intrusion events for industrial control system: in 2007 attackers intruded a water control system in Canada, to destroy water dispatching control computer; in 2008 attackers intruded a Polish city subway system to change the orbit switchman by the TV remote control, resulting in four carriages; in 2010 Stuxnet invaded ICS system of Bushehr nuclear power plant, seriously threatening safe operation of nuclear reactors; in 2011 hacks attacked Illinois Urban water supply system, which destroyed water supply pump. Therefore, it is very important for SCADA to research on large scale SCADA network security defense theory and construct SCADA security defense system, which has the important strategic significance [3-4].

This paper is organized as follows: Section 2 reviews the SCADA network security related work; In section 3 SCADA network security system structure based on agent are described, description of the role and task is discussed in details; In section 4 ,attack and

* Corresponding Author

ISSN: 1738-9976 IJSIA

defense simulation model based on agent is established; Section 5 verifies the feasibility and effectiveness of the model by experiment; finally section 6 draws conclusions.

2. Related Works

At present, at home and abroad, people have attached more and more attention to industrial control system security, which includes SCADA system security and defense technology research and development of related system standard, and has also been the focus of major infrastructure protection in many countries.

In the United States, in 2002 the United States issued <<the national strategy for homeland security>>, announced that main work will be to protect industrial control system security in the important areas. In 2003, <<national security strategy for cyberspace>> was released, which emphasized the protection of industrial control system in key areas will be included in the project plan. In 2006 the national infrastructure protection plan was carried out, which put forward the industrial control system, computer system and Internet, were important parts of the network space infrastructure, a set of R & D projects were established and universal SCADA password standard was introduced, and shooting range in industrial control system was built. In 2009, the United States released the strategy for the protection of industrial control systems, focusing on the 14 key areas of industrial control system, including power, energy, transportation and *etc*.. In 2010 the United States promulgated the "national network space incident emergency response plan", specifically set up the "industrial control system network Emergency Response Team (ICS-CERT).In 2011, <<800-82 SCADA SP industrial control system security guide>> was officially released, so far the United States has formed a complete set of industrial control system security standards[5-6].

Comparing to the industrial control system security defense research in the United States, European countries started the research late, but since 2004,they has also released a series of reports on protection of industrial control system, summarizes threats and challenges that the industrial control information system was facing with, and promulgated a series of laws and regulations, grade standard and industry norms.

People have begun to carry out the research work on SCADA system security defense technology. In literature [7], Yu Yong, Lin Weimin established SCADA system security technology architecture, safety management architecture, system security service and security infrastructure architecture to ensure that the SCADA system works with stability, safety and good quality. Literature [8], described Internet brought SCADA network into a new field, at the same time also introduced new security vulnerabilities. Zhang Lina[9] from the SCADA system structure, analyzed security vulnerability of each composition unit of SCADA, pointed out a potential attacker, and put forward the solution from different aspects of laws and regulations, system structure and personnel management. In literature [10] Wu Yafeng summarized main risk of information security in the present SCADA system, proposed the information security hierarchical protection idea in SCADA system, and focused on SCADA internal information security protection technology.

3. SCADA Network Security Defense Architecture based on Multi-Agent

3.1. Security Defense Formal Description based on Multi-Agent

Definition 1: Agent is defined as a tuple Agent=<Be, Kn, Ca, Le>

Where

(1) Be (belief) is the belief of Agent which represents the agent's perception state for environment.

(2) Kn (knowledge) stands for knowledge of agent. Agent has two kinds of knowledge, one is experience base on CBR, the other is rule base on RBR; Agent also has two kinds of function, one is to provide analytical ability, the other is decision-making ability. Knowledge can be used to help Agent evaluate the real state of the environment and to select the optimal action.
(3) Ca (capability) represents capability of agent. For attackers, it includes all the executable ability such as tool sets, exploitation and action set, for defenders, it includes permissions operation (modifying the firewall), bug fixes and action set and *etc*. ,every executable capability.
(4) Le (level) is a function based on the mood and fatigue of agent which can affect the execution effect of Agent.
(5) The intrinsic properties of Agent describe the abilities of agent's perceiving environment and changing the environment. Belief is one of the factors for knowledge to select the optimal action, and the feedback of the action is also the consideration factor of renewing the belief. Le is the property which can be reflected when agent simulates human.

Define 2: Role is defined as a tuple

$$R =< name, A, R, scr, res, CR, \theta >$$

Where

(1) Name is a role name, which provides both an identity, and a job type that is also reflected in the script. Such as the role of Detector, in general is responsible for the detection of work.
(2) A is a role management type (type). There are two types: manager agent (MA) and basic agent (BA). Generally speaking, the main responsibility of the BA script is to perform the work, and the MA script is responsible for the coordination of the work.
(3) R represents the relationship between roles (Relation), which is a three-dimensional vector, (superiors, colleagues and subordinates). BA has colleagues and superiors, MA have colleagues and subordinates, may have superiors.
(4) SCR stands for the script (script), including two parts of the execution step and script object. The execution step is a subset of the script in the task. The script object is optional, if there exits a script object, the role periodically checks whether the script is completed, and if it is completed, the script is not longer executed.
(5) res represents resource, is information which can be used to complete the attack by agent, including the target host vulnerability, account password, *etc*.. The initial resource is given by the script, and the resources are changed with the execution of the task.
(6) CR (Capability Required) represents the capacity of the Agent to act as the role.
(7) θ is let to be constraints, which is consideration factor when agent does a specific action.

For example, hidden constraint is the highest, some easily exposed action will not be considered. When the time constraint is high, some efficient action is preferred.

Definition 3: Task $T =< \phi, P, L >$ is defined as the following parts:

(1) ϕ is the goal of the task, is also a logical expression, when the logical expression is true , the mission objectives is completed.
(2) P represents the task script.
(3) L is assignment table of a task role.

Definition 4:Task script P is defined as the following syntax:

$$P ::= act \mid P \wedge P \mid P \vee P \mid P \circ P \mid When(\exp) : P >$$

Both offensive and defensive may have different action sets

$P1 \wedge P2$ is AND relationship between task P1 and P2, representing that the two tasks must be completed simultaneously.

$P1 \vee P2$ is OR relationships between task P1 and P2, representing that at least one of the two tasks can be completed.

$P1 \circ P2$ is the order relationship between task P1 and P2, representing that complete P2 after P1,

When (EXP) :P represents that when exp is true, P is repeatedly executed.

The role assignment table is a complete division of task script P . Role script is a subset of the task script, and the dependence of the steps in the role script should be consistent with the description in the script.

3.2. Logic Model of SCADA Security Overall Framework

(1) Structure model

Analyzing the operating characteristics of oil and gas SCADA system and the advantage of the structure of multi-agent, multi-agent technology is applied to the SCADA security system and oil and gas SCADA security defense architecture model based on multi-agent is proposed in the paper. Using hierarchical processing method in distributed system, overall architecture in the model is divided into monitoring layer, decision layer, control layer, the three layers respectively contain different types of agent to achieve specific functions. In accordance with the above structure, complex function can be decoupled effectively and the correlation degree of each part of the system can be reduced effectively, but also the separation of defense strategy and defense methods can be achieved, the flexibility of the system configuration can be increased, and the reliability of the system can be enhanced.

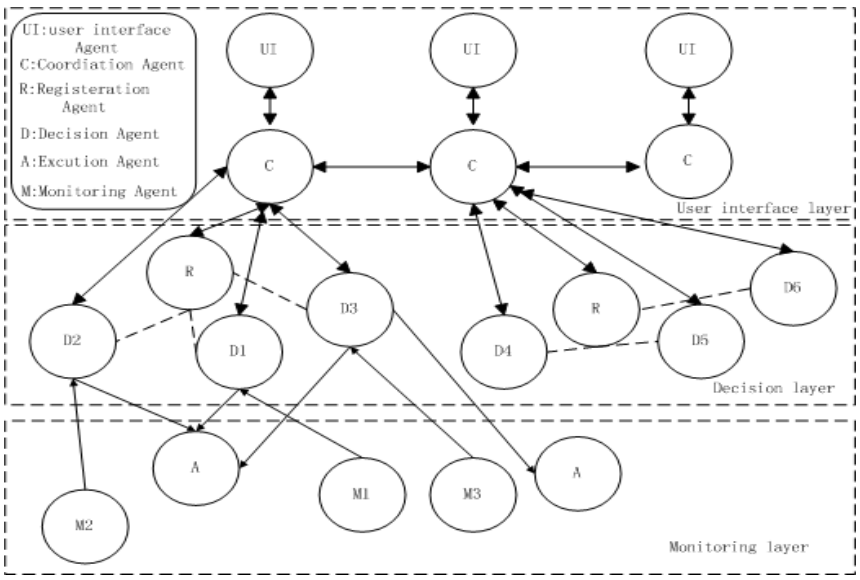

Figure 1. Logical Structure of the Model

Monitoring layer: The layer Includes monitoring agent and execution agent, this layer contains the following functions: raw data acquisition, processing relevant actions ,to monitor and control SCADA system.

Decision-making layer: The layer is the core layer in the defense model, including registration Agent and decision Agent, mainly to make the decision results by analyzing

and judging detection data from monitoring layer. Coordination agent in control layer can coordinate multiple decision agents to make decision cooperatively, and ultimately decision results will be transmitted to execution agent in monitoring layer.

User interface layer: The layer includes user interface Agent, coordination Agent, which is responsible for configuring all Agent, setup and scheduling in the model. According to the need, manager can increase or decrease the number of Agent in the model, update the knowledge base built in Agent in the model, and coordinate multiple decision Agent for cooperative decision when it needs.

Functions of the agents in each layer are described as follows:

A. Monitor agent

Monitor agent is responsible for monitoring data packets from the target host or network equipment, and has two functions of data acquisition, feature extraction. It can be located in any host in the network; the same or different types of agents can be deployed in the same host. The collected data include the audit record from the host, application log, application call sequence and network traffic. In order to reduce network traffic, the occupation of network bandwidth, and the burden of decision agent, monitoring agent must reprocess original data, including data filtering, formatting, extraction and analysis. After the completion of the pre processing monitoring Agent send data to one or more decision Agent.

B. Execution Agent

Execution agent is responsible for dealing with the threats to the SCADA system and uses parameters from decision-making to take effective measures to stop the operation of the violation security.

C. Decision agent

Decision agent uses the feature parameters from monitoring agent and embedded knowledge base to complete, information processing, make decision, and pass the results to the execution agent. Each decision Agent independently assumes a certain detection task including detecting the security of the system or network. According to the different detection tasks and environment, decision agent uses different detection techniques and methods to detect the abnormal or suspicious user behavior. In the model, different types of decision agent can have the same data source, to achieve the complementary of detection method, and to improve the detection rate.

D. Registration Agent

It is responsible for the registration and cancellation when agents migrate. When the new Agent is running in the system, it is required to register the Agent itself, so that the Agent can transmit data and migrate itself in the system. If an agent needs to migrate, the agent first need to apply to source registration agent for the cancellation, and to apply to target registration agent for registration, when permitted, they can migrate and send themselves to the destination.

E. Coordination agent

Coordination agent is responsible for coordination of the data communication between various agents, and for coordination of agent collaboration in the system.

F. User interface Agent

When the data in the model or the agent and knowledge system need to be updated and need manual intervention, user interface agent can provide a user friendly interface for operators.

(2) Response method for multi-agent defense model

When monitoring agent detects the abnormal attack, the detection information is transmitted to the decision Agent, and the decision Agent uses the information to carry

out the reasoning. If the decision agent needs to make decision cooperatively, then the coordination agent notifies other decision agents to participate in the decision activity, and obtains the decision result. The final decision results are transmitted to the corresponding execution agent, and the execution agent solves the abnormal behaviors in oil and gas SCADA system. Specific steps are illustrated as follows:

1) Monitoring Agent uses its own built-in knowledge base and processing logic to analyze the raw data. If the result is abnormal, the information is transmitted to the decision agent;
2) After receiving the information from monitoring agent, decision Agent makes a decision by using its knowledge base, and gets the exception processing method. If a single decision agent cannot make decisions, the decision agent need to ask other decision agent for help it, eventually decision information will be passed to the corresponding execution agent. if execution agent is not in target workstation, the execution agent must be migrated to the target workstation.
3) According to the information from decision agent, execute agent takes the action required by the decision, such as isolating file, blocking operations, *etc*., to deal with the abnormal behaviors of the system.
4) According to the monitor agent's report, the system registers the attacked records of SCADA system which classified by category, and determines security level of the region, reminds system users to take corresponding measures. At the same time, each cooperative decision agent will update their-own knowledge base, and complete to solve the abnormal behavior.

4. SCADA Network Security Attack and Defense Simulation based on Multi Agent

The above attack and defense model has certain universality, if the new type of attack and defense needs to be added to the model, only new task can be added to the model, the model has good scalability. The following DDoS example demonstrates the initialization and operation of two sides of attack and defense in the model:

4.1. Attack Simulation

DDoS Offensive Alliance

(1) DDoS attack

DDoS (Distribution Denial of Service) can cause a large number of abnormal network traffic in a short time and affect normal service. Taking an example of a simple ICMP/ping type of DDoS attack is to illustrate the simulation model how to describe and achieve the task. The task is that an initiator controller control three "meat chicken" machine, the attacker launched ICMP/ping type of DDoS attacks to target address. For simplicity, the DDoS attack task is not designed to occupy the "meat chicken" machine, to create the back door and to clear the log and so on. The specific description of the task T1 is as follows:

$$T_1 =< \phi_1, P_1, L_1 >, \phi_1 = !achievable(172.23.253.65 >$$

$$P_1 = when(achievable(172.23.253.65) \text{ ^}(ping(172.23.253.65))$$

$$r_1 = \{controller, MA, \{\{\}, \{\}, \{r_2, r_3, r_4\}\},$$

$$script_{controller}, CR_{controller}, \theta_{controller}\}$$

$$r_2 = \{attacker, BA, \{\{r_1\}, \{r_3, r_4\}, \{\}\},$$

$$script_{attack}, CR_{attack}, \theta_{attack}\}$$

$$r_3 = \{attacker, BA, \{\{r_1\}, \{r_2, r_4\}, \{\}\},$$

$$script_{attack}, CR_{attack}, \theta_{attack}\}$$

$r_4 = \{attacker, BA, \{\{r_1\}, \{r_2, r_3\}, \{\}\},$

$script_{attack}, CR_{attack}, \theta_{attack}\}$

$script_{commander} = (sent(r_2, start) \vee sent(r_3, start) \vee sent(r_3, start))$

$\gamma(when(achievable(172.23.253.65)) : wait(60000))$

$\gamma(sent(r_2, end) \vee sent(r_3, end) \vee sent(r_4, end))$

$script_{attacker} = wait(start) \circ (when(true) : ping(172.23.253.65))$

….

(2) Initialization and execution of DDoS attacks alliance

In the last part, a detailed description of the task T1 is given, and how to execute after G1 accepts the task T1 will be described in this part.

$$G_1 =< \Sigma_1, \Pi_1, r_1, \leftrightarrow_1 >$$

Where

$$\Pi_1 = \{a_1, a_2, \ldots, a_{10}\}$$

After G1 accepts task T1,let $G_1 \Sigma_1 = T_1 L_1$,then assume that assignment result of role distribution function r1 is

$perform(a_1, r_1)$, $perform(a_2, r_2)$, $perform(a_3, r_3)$, $perform(a_4, r_4)$

The union logic structure, $\leftrightarrow_1$, is shown in the following diagram:

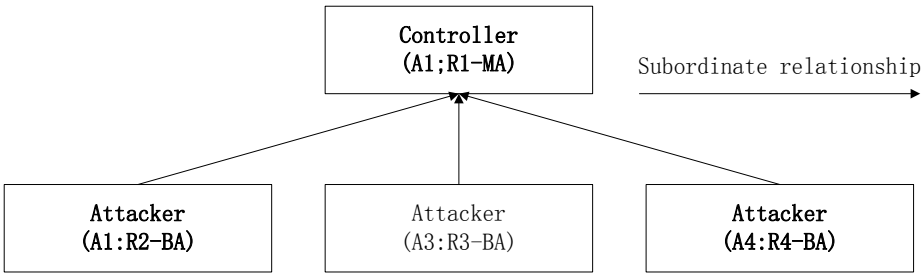

Figure 2. Logic Structure of DDoS Attack Alliance

The execution process is as follows: controller at a time sends script command, start (start) message, to the three "meat chicken" machine(attacker), the attacker receives a start message and ends wait-state, and send continuously Ping request to the target address, the part of the Ping request is as shown in Figure 3 . The initiator (controller) checks whether the target address has loss of external reaction in a period, if the target address doesn't react, it sends the script, end message, to three "meat chicken" machines to end the mission.

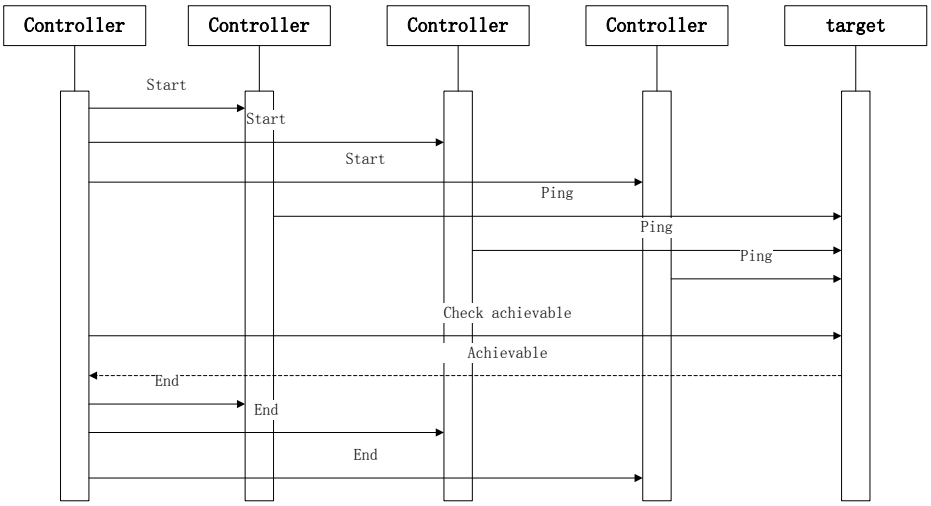

Figure 3. DDoS Attack Workflow

4.2. Defense Simulation

DDoS defensive alliance

(1) DDoS defense

The main task of the defense team is intrusion detection. Intrusion detection technology mainly has two forms: abnormal intrusion detection and misuse intrusion detection. Abnormal intrusion detection, by using a quantitative method to define the scope of the normal behavior, can detect abnormal behavior and intrusion according to the use of computer resources. Misuse intrusion detection can detect intrusion by using known vulnerabilities intrusion detection pattern. The defense task T2 uses two methods of intrusion detection. In task T2, the detector makes a direct response to some unacceptable behavior. Manager takes information statistics, and sends the abnormal IP to filter. Filter is responsible for filtering the communication of abnormal IP . Specific description about task T2 is as follows:

$$T_2 =< \phi_2, P_2, L_2 >, \phi_2 = safe$$

$$P_2 = when(true) : (detect \wedge manage \wedge filter)$$

$$role_1 = \{manager, MA, \{\{\}, \{\}, \{r_2, r_3, r_4\}\},$$

$$script_{manager}, CR_{manager}, \theta_{manager}\}$$

$$r_2 = \{detector, BA, \{\{r_1\}, \{r_3, r_4\}, \{\}\},$$

$$script_{detector}, CR_{detector}, \theta_{detector}\}$$

$$r_3 = \{detector, BA, \{\{r_1\}, \{r_2, r_4\}, \{\}\},$$

$$script_{detector}, CR_{detector}, \theta_{detector}\}$$

$$r_4 = \{filter, BA, \{\{r_1\}, \{r_2, r_3\}, \{\}\},$$

$$script_{filter}, CR_{filter}, \theta_{filter}\}$$

$$script_{manager} = when(true) : (wait(resUpdate) \circ manage \circ sent(r_4, resUpdate))$$

$$script_{detector} = (when(true) : detect \circ sent(r_1, resUpdate))$$

$$script_{filter} = when(true) : filter$$

....

(2) Workflow of DDOS defense alliance

In the last part, a detailed description of the task T2 is given, and how to execute after G2 accepts the task T2 will be described in this part.

$$G_2 =< \Sigma_2, \Pi_2, r_2, \leftrightarrow_2 >$$

Where

$$\Pi_2 = \{a_1, a_2, \ldots a_{10}\}$$

After G2 accepts task T1, let $G_2 \square \Sigma_2 = T_2 \square L_2$,then assume that assignment result of role distribution function r2 is

$$perform(a_2, role_1),\ perform(a_2, role_2), perform(a_3, role_3), perform(a_4, role_4)$$

The union logic structure, $\leftrightarrow_2$, is shown in the following diagram:

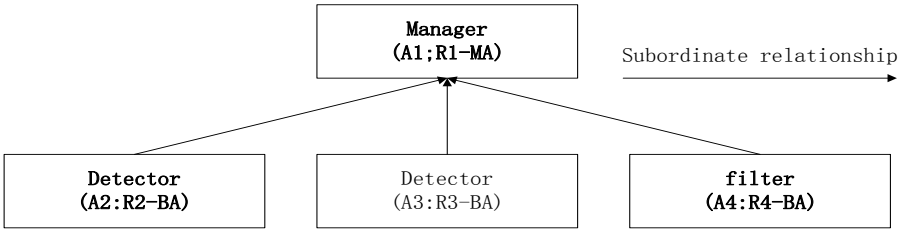

Figure 4. Logic Structure of DDoS Defense Alliance

The detailed work process of defense alliance is as follows:

Detector's work: 1) the detector matches communication behavior to intrusion patterns in its own knowledge, and makes a direct response to the intrusion behavior. 2) the detected information is transmitted to the manager in the form of update-message by the detector .

Manager's work: 1) the manager accepts the resource-updated message sent by the detector, and takes data analysis. Data analysis can have two kinds of methods: one is to extract sets of feature variables from the data, and then to detect abnormal IP with learning classifier; the other is to firstly map the communication source address to different hash table address by using hash method, then detect abnormal IP with abnormal traffic aggregation. 2) The detected abnormal IP is taken as a resource, and the resource-updated message is sent to the filter.

Filter's job: 1) the filter accepts the abnormal IP resource-updated message sent by the statistician, takes the abnormal IP as its own resources. 2) If the source address of the communication behavior is in abnormal IP list, it is filtered.

5. Experimental Simulation Results

In the model, detection agent uses BP neural network to detect abnormal behaviors. Anomaly detection data source is from the network connection data in monitored host. Due to the limitation of agent acquisition data, so in the experiment, we use KDDCUP99 data. Training data and test data in KDDCUP99 reach 7 000000 network connections data. Such a large amount of data is not convenient to be processed. In the experiment, we randomly select part of training and test data. The selected data is shown as Table 1.

Table 1. Training Data and Test Data

	Training set		Test set I		Test set II		Test set III	
	quantity	Proportion (%)	quantity	Proportion (%)	quantity	Proportion (%)	quantity	Proportion (%)
Normal	3840	100	134	22	1924	65	2032	50
Dos	0	0	254	41	932	31	693	17
Probe	0	0	187	33	78	2.6	1294	32
U2R	0	0	20	3	12	0.4	15	0.37
R2L	0	0	16	1	14	1	20	0.63

In table 1, training set contain normal network connection data without any attack; test set I is a small dataset in which the number of normal connections is far less than the attacks; test set II is a medium dataset in which the number of normal connections is far greater than the attacks; test set III is large dataset in which the number of normal connections is at the same ratio of the attacks. These three kinds of test sets represent three different network connections, which have certain universality; they can verify capability of detecting abnormal attacks. Test set I contains four kinds of network attacks, test set II contains seven kinds of network attacks, including four kinds of network attacks in test set I and some new types of attacks; test set III contains 23 kinds of network attacks, including all attack types in test set II and some new attacks. Intrusion attack types are shown in Table 1.

Experimental results of Anomaly detection agent

Anomaly detection agent adopts conjugate gradient algorithm to detect abnormal behavior. The three layers network structure is designed in the algorithm, in which the input layer has 41 neurons, 17 neurons is in hidden layer, has a output layer (output "0', represents that the network connection is normal, the output "1", represents that network connection is abnormal).

By using data in Table 1 to detect network abnormal attack, the experimental results are obtained in table 2,Figure 5-7.

Table 2. Detection Performance with Conjugate Gradient Algorithm

	Training set	Test set I	Test set II	Test set III
Sample total	3840	611	2960	4054
Normal sample total	3840	130	1956	2027
Accurate detection total	3840	121	1912	1960
False sample total	0	9	44	70
False rate(%)	0	6.923	2,24	3.45
Abnormal sample total	0	481	1004	2030
Accurate detection total	0	441	980	1532
Detection rate(%)	0	91.68	97.6	75.46

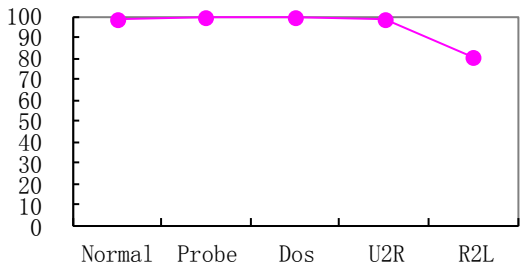

Figure 5. Detection Rate Comparison of Different Attack Types in Test I

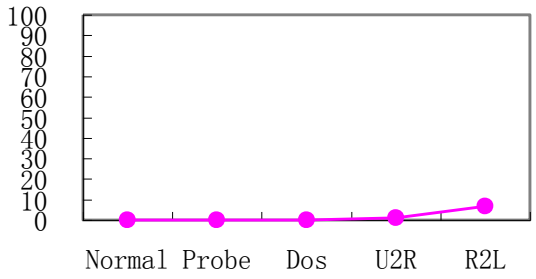

Figure 6. False Rate Comparison of Different Attack Types in Test I

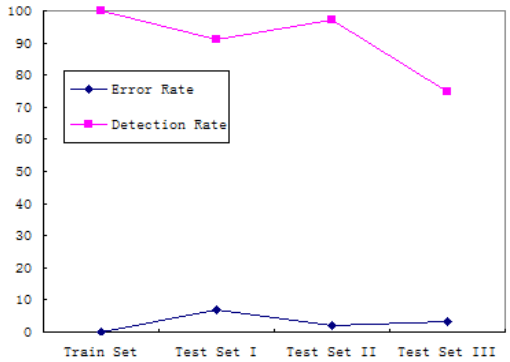

Figure 7. Detection Rate Comparison and False Rate Comparison between Different Test Sets

In the test sets, Probe and DoS, account for a large percentage, so detection rates of the two attack types are high and false rate and missing rate are relatively low, but R2L and U2R make up small proportion of test sets, so they have a low detection rate and high false rate. Generally speaking, in test tests, attack types accounted for a large percentage, detection rate is high, false rate is low.

6. Conclusions

In this paper, multi-agent technology is applied to oil and gas SCADA system, and a new SCADA security defense model based on multi-agent is proposed. In the model, the way of describing task is universal, not limited to DDoS, for the new type of attack, the model only need to add a new task. Application of multi agent technology to oil and gas SCADA system security defense, makes oil and gas SCADA system can achieve a more comprehensive defense, more accurate detection, can also cope with large-scale distributed attacks, improves the robustness and stability of the security defense; compared with the traditional security defense, multi-agent security defense model can provide a more intelligent, efficient, stable and distributed defense model. In this paper, the application of multi Agent technology has made an attempt to provide a new method for the application of multi Agent in other fields. Next research work is how agent effectively conducts autonomous learning for future detection.

Acknowledgments

This work was supported by National Natural Science Foundation Project under grants 61175122, as well as by Applied Basic Research Project of Sichuan province of China (2013JY0134) and by Key Project of Sichuan Educational Commission (No. 15ZA0049).

References

[1] M De Vivo, G O de Vivo , G Isern, "Internet security attacks at the basic levels", Operating Systems Review, vol. 32, no. 2, **(2002),** pp. 40-48.
[2] L. Teo, Y. Zheng, G. Ahn, "Intrusion detection force: an infrastructure for internet-scale intrusion detection", Proceedings of the First IEEE International Workshop on Information Assurance(IWIA'03), **(2003)**,Darmstadt, Germany.
[3] Z Liu, Y Liu, "Factor neural network theory and implementation strategy research", Beijing: Beijing Normal University Press, China**(1992).**
[4] X Cao, *et al*, "The Geological Disasters Defense Expert System of the Massive Pipeline Network SCADA System Based on FNN", Lecture Notes in Computer Science,vol. 1, no.7234, **(2012)**, pp. 19-26.
[5] P. Oman, A. Krings, D. Conte de Leon, "Analyzing the Security and Survivability of Real-time Control Systems", Proceedings of the 2004 IEEE Work shop on Information Assurance United States Military Academy, **(2004)** June 10-11,West Point, N-Y.
[6] C. Queiroz, A. Mahmood, and Z Thri, "An analytical framework for evaluating survivability of SCADA systems", IEEE computer Society ,**(2010)**, pp. 877-881.
[7] Y. yong, L. weiming, "Study on Industrial Control SCADA System's Information Security Protection System", Information network security, (5) **2012**, pp.74-77.
[8] R.Carlson, "Sandia SCADA program: High-security SCADA LDRD final report", Sandia National Laboratories,Tech.Rep, **(2002)**.
[9] Z. lina,*etc*. "SCADA security analysis and strategy", automation & instrument,**(2005)**,3, pp. 67-69.
[10] W. yafeng, "SCADA system information security technology", Automation Panorama, **(2013)**,02:,pp. 98-100.

