Knowledge-based Support of Network Management Tasks using Active Information Resource

Susumu Konno†, Abar Sameera†, Yukio Iwaya‡, Toru Abe†, and Tetsuo Kinoshita†
† Information Synergy Center / Graduate School of Information Sciences, Tohoku University
‡ Research Institute of Electrical Communication, Tohoku University
Email: {skonno@isc, sameera@ka.riec, iwaya@fir.riec, beto@isc, kino@riec}.tohoku.ac.jp

Abstract

A network system is a kind of large and complex systems and the network administrators are required exhaustive work to maintain the quality and functions of the network system. To reduce the load of administrators, systematic and intelligent facilities for the network management tasks should be realized and provided for administrators. In this paper, we propose a knowledge-based support method of the network management tasks using the active information resource (AIR) which has knowledges and functions for its information resource. Furthermore, a novel network management support system based on this method, called AIR-NMS, is also proposed by using the agent-based computing technologies. In the AIR-NMS, a lot of AIRs are defined and utilized in order to monitor and collect the status information of the network automatically. The AIRs are collaborated each other and inspect the behavior of the network. The network administrator can obtain useful supports for management in responses of AIR-NMS. Moreover, a prototype system is implemented to demonstrate and evaluate the essential functions of the AIR-NMS.

1. Introduction

The network systems are becoming complicated and larger in scale, and the network administrators are required various knowledge and great effort to maintain the quality and functions of the network systems. Recently, the network management systems had been developed and utilized [9, 1, 11, 10, 2, 6, 12, 3]. A network management system can collect and measure the status information of network as a part of work of the management tasks and the administrator should deal with the rest of work by using output of the network management system such as analysis of the detailed situation, selection and execution of the suitable operations, and so on. Since the administrators uses various expertise and heuristics in these works, it's difficult to realize the support facilities to reduce the load of administrators.

To deal with this problem, the authors have proposed a knowledge-based support method for network management tasks by using the active information resource (AIR). The AIR is a generic scheme to represent, manage and utilize various information resources together with the meta-knowledge of the information resource. We have applied the scheme of the AIR to the network management tasks, and proposed a novel network management support system based on the proposed method, called AIR-NMS [7].

In the AIR-NMS, many AIRs are designed, implemented and allocated to the functional modules of a network to monitor and collect the status information of the network automatically. Using such information and knowledge accumulated in the AIR, the AIR-NMS can inspect the behavior of the network and provide the useful support such as a recommendation of trouble shooting, an executive sequence of management operations and so on. In the following sections, firstly, we explain a design concept of the AIR-NMS and propose an agent-based architecture of the AIR-NMS. Next, we define two kinds of AIR, i.e., information AIR (I-AIR) and knowledge AIR (K-AIR) of the AIR-NMS and design these AIR which are realized as the software agents. Finally, a prototype system of the AIR-NMS is designed and implemented to demonstrate the behavior of the realized system and evaluate the essential functions of the AIR-NMS.

2. Concept of Active Information Resource based Network Management

2.1. Concept of AIR

The idea of Active Information Resource (AIR) provides a scheme to enhance and extend the usability and accessibility of the distributed information resources. An AIR

Proceedings of the IEEE/WIC/ACM International
Conference on Intelligent Agent Technology (IAT'06)
0-7695-2748-5/06 $20.00 © 2006 IEEE

manages its own information resource together with meta-knowledge with respect to the use/reuse the information resource, in order to make its information resource possible to act as an active and flexible entity [8].

An AIR holds not only its own information resource, but also Knowledge for Utilization Supporting (KUS) and Functions for Utilization Supporting (FUS). An AIR activated in the AIR workplace, can receive and process a request from users or other AIRs. And manipulate the information resource by using its KUS and FUS. The AIRs communicate and cooperate with each other to deal with the problem solving tasks in the AIR workplace.

2.2. Network Management Support by Active Information Resource

When an administrator deals with the management tasks, various types of information are needed such as the topology of the network, the status information of network devices (server, router, etc.), the log data of applications, and so on. Furthermore, the administrator also needs his/her own expertise and heuristics on network management tasks.

For example, consider a failure between a client in subnet$_A$ and a server in the subnet$_B$ (Figure 1(a)). Then, an administrator has to perform the following tasks.

1. Collection of status information, such as a client in the subnet$_A$, a server in the subnet$_B$, a gateway of each subnet, a router between both subnets, and a backbone network.
2. Integration and analysis of collected information.
3. Exploitation of the cause of failure.
4. Decision about appropriate recovery method to the failure.
5. Execution of recovery method which has been decided at Task 4.

For a large scale complicated network system, the workload of network administrator increases to a great extent, because the administrator has to have both the expertise of management tasks and the technical information of target network such as configuration and specification of the subnet.

It's possible to design and implement a set of AIRs as shown in Figure 1(b) (In Figure 1, AIR-ized means its information resource is activated as an AIR). In this figure, two types of resource are used such as a knowledge and information. The former is acquired from the human administrators and the latter is collected from the network devices. Using these AIRs, the management tasks are formalized as the problem solving tasks which done by the cooperation of

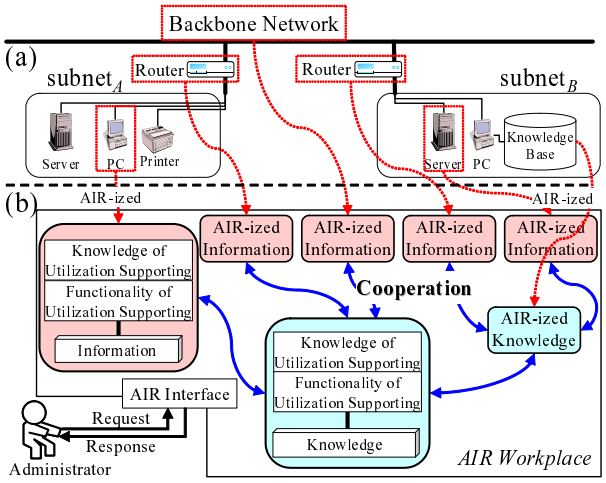

Figure 1. Network Systems and AIR-NMS

these AIRs in an automatic way, in order to reduce the load of the network administrator.

3. An Architecture of AIR based Network Management System

In this chapter, we described details of a network management support system using the concept mentioned above, named as AIR-NMS (AIR based network management system).

3.1. Components of AIR-NMS

The AIR-NMS consists of two types of AIRs, i.e., I-AIR (AIR with status information of network) and K-AIR (AIR with expertise of network management task).

I-AIR is further classified into two types. The one is I$_s$-AIR (Static Status Information AIR) which contains fixed information in the network such as subnet name, administrator name, administrator e-mail address, various server names and their corresponding IP addresses, and so on (Figure 2(a)). The other is I$_d$-AIR (Dynamic Status Information AIR) which has information which change from time to time such as information get from MIB, server-log of mail processes, and so on (Figure 2(b)).

On the other hand, K-AIR manages various heuristics and expertise of expert administrators which can utilized as the generic knowledge of network management task. The K-AIRs and I-AIRs interact with each other to solve the given problem cooperatively. For instance, a K-AIR depicted in Figure 2(c) holds knowledge to generate a concrete description of the verification operation for a specific network by using a server-log stored in an SMTP server$_X$. For instance, the K-AIR get an IP address of a SMTP server$_X$

Proceedings of the IEEE/WIC/ACM International
Conference on Intelligent Agent Technology (IAT'06)
0-7695-2748-5/06 $20.00 © 2006 IEEE

(a) I_s-AIR

```
<? Xml version="1.0"encoding="Shift_JIS"?>
  <subnet>
    <subnetName>Subnet_A</subnetName>          <domain>example.jp</domain>
    <addrspace>172.20.2.0/24</addrspace>       <gateway>172.20.2.1</gateway>
    <firewall>active</firewall>                <adminName>Mr. Noname</adminName>
    <adminMail>noname@example.jp</adminMail>
      <server>
        <service>SMTP</service>                <ipaddress>172.20.0.2</ipaddress>
        <name>smtp.a_lab.example.jp</name>     <process>Postfix2.1</process>
      </server>
  </subnet>
```

(b) I_d-AIR

```
Apr 1 01:38:48 mail sendmail[1892]:: ruleset = check_rcpt, arg1 =
  <noname@example.jp>, relay = nohost.example.jp[192.168.0.1], reject=550 5.7.1
  <noname2@example.jp> ... Relaying denied
Apr 3 16:17:23 mail sendmail[1925]:: ruleset = check_rcpt, arg1 =
  <noname@example.jp>, relay = [192.168.0.2], reject=550 5.7.1 noname3@example.jp
  ... Relaying denied. IP name lookup failed [192.168.0.2]
```

(c) K-AIR

```
A) Can't send e-mail in a subnet.
   1) The IP address of the SMTP server is acquired from I-AIR which has configuration
      information of subnet____. → Goto B)
B) Procedures for determining the obstacle of the subnet____'s SMTP server are carried out.
   1) The log of SMTP server____is verified. → Goto C)
   2) The status of SMTP server____is verified. → Goto W)
   3) The setting of e-mail client software____. → Goto X)
   4) The setting of network interface at client PC____is verified. → Goto Y)
   5) The status of network route____is verified. → Goto Z)
C) Verifying the log of SMTP server.
   1) Id-AIR with the log of SMTP server____is called. → Goto D)
D) Inspection of the log of SMTP server____.
   1) There is an error. → K-AIR with the knowledge which solves an error____.
   2) There is no error. → finish.
```

Figure 2. Example of Information Resources for I_s-AIR, I_d-AIR and K-AIR

from the I_s-AIR. Using this information, the request for verifying the log information can be forwarded to I_d-AIR which contains a server-log of the SMTP server$_X$. As explained above, the K-AIR has FUS functions which rewrite a generic description of management knowledge of K-AIR and generate a specific description based on the specific information sent from I_s-AIR and I_d-AIR, cooperatively. The FUS mechanism of K-AIR is an essential function to make it possible that the generic knowledge of management tasks can be applied to the specific network management tasks in a systematic way.

3.2. Behavior of AIR-NMS

The AIR-NMS has two kinds of the behavior control modes, i.e., "Request-based driven mode" (Figure 3(a)) and "Alert-based driven mode" (Figure 3(b)).

[Request-based driven mode]

For example, when a failure "can't send e-mail from the subnet$_A$" occurs in a network, an administrator submits a support request to the AIR-NMS depicted as the "Failure Information" in Figure 3(a). The request should holds information of "failure" and "detailed situation". In this case, the failure is "subnet$_A$" and the detailed situation is "can't send e-mail", respectively.

A K-AIR$_i$ which receives a support request through the AIR interface, foremost activates the management knowledge (A) of Figure 2(c). Then, the K-AIR$_i$ cooperates with an I_s-AIR which contains information of the constitution of the subnet$_A$, in order to specify an IP address of a SMTP server. Through this process, the K-AIR$_i$ creates detailed failure information such as "IP address of SMTP server inside the subnet$_A$ is 192.168.255.3". Then, this information is forwarded to the next K-AIR$_j$ and the K-AIR$_j$ executes the management knowledge (B) of Figure 2(c).

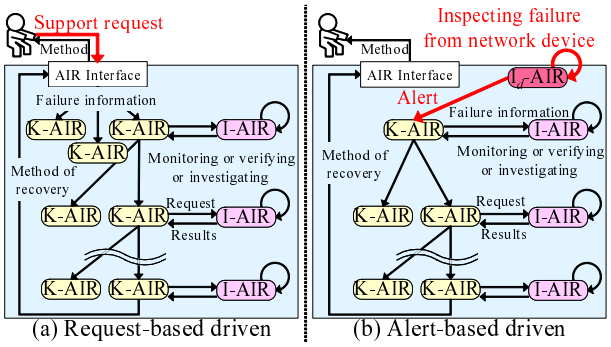

Figure 3. Operation of AIR-NMS (Request-based driven / Alert-based driven)

On the other hand, various state information is collected from the I-AIRs, in order to make a specific description for the e-mail forwarding failure. For instance, an I_d-AIR sends the server-log information of a SMTP server to the K-AIR$_j$. Using this information, the K-AIR$_j$ generates a specific error description and adds it to the failure information, and then, the failure information is forwarded to the next K-AIR$_k$. In the K-AIR$_k$, if the detailed failure information can generated, a request is forwarded to a K-AIR$_l$ which has knowledge of the failure recovery. Then, the K-AIR$_l$ presents a method of the failure recovery for the administrator via the AIR interface as shown in Figure 3(a).

[Alert-based driven mode]

An I_d-AIR can monitor the status information of the network devices continuously, and detect a failure of a network device autonomously by using its own KUS knowledge. When an I_d-AIR detects a failure, a failure information is sent to a K-AIR, and the problem solving of failure recovery will done as same as the administrator driven mode. And finally, a method of the failure recovery is presented to the administrator (Figure 3(b)).

3.3. KUS and FUS of AIR

AIR has KUS and FUS. And manipulate the information resource by using its KUS and FUS. In this section, we describe KUS of K-AIR. KUS of K-AIR is defined by using the BNF notation as shown in Figure 4, and composed of the following four knowledge.

```
K-AIR ::= <ID> <IR> <CM> <CP>
  ID ::= <air id> <workplace id> <task id> <failure info>+ <detail info>*
    air id = Identification of an AIR
    workplace id = Identification of an AIR workplace
    task id = Identification of an AIR tasks
    failure info ::= <failure list>* <precheck list>* <info list>*
      failure list = List of trouble that can be dealt
      precheck list = List of necessary prior information
      info list = List of information that should detail
    detail info = Detailed information

  IR ::= <meta info> <knowledge info> <time>
    meta info = Meta information on management knowledge
    knowledge info = Management knowledge
    time = Last updated time

  CM ::= <method> <argument>* <returned value>*
    method = Method name of FUS
    argument = Argument of FUS
    returned value = Returned Value of FUS

  CP ::= <protocol>+
    protocol = Cooperation protocol
```

Figure 4. The knowledge representation scheme of K-AIR in BNF

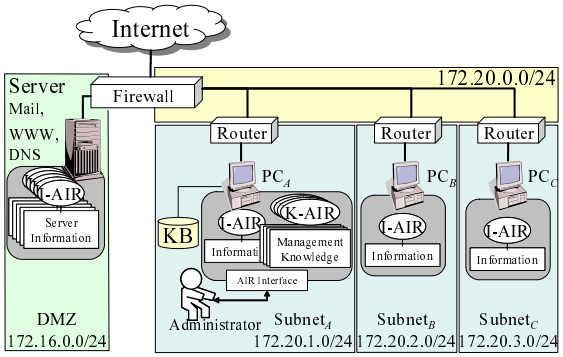

Figure 5. Construction of Network Systems and AIR-NMS

- ID: AIR Identification Knowledge.
  ⟨air id⟩ represents the identification knowledge of an AIR. ⟨workplace id⟩ is the identifier for the environment where the K-AIRs are instantiated and cooperate actively. In addition, information on the failure that K-AIR can correspond is described as ⟨failure info⟩. K-AIR becomes possible by this identification knowledge the selection of possible AIR for cooperation.
- IR: Knowledge about Information Resource.
  ⟨IR⟩ characterizes the knowledge about the network management knowledge. Meta information on the network management knowledge of K-AIR is described as ⟨meta info⟩. K-AIR offers the administorator appropriate network management knowledge by detailing this ⟨IR⟩.
- CM: Knowledge about Control Method.
  Knowledge concerning the method for the request of processing to FUS is described. Operating the information resource by using this method becomes possible.
- CP: Knowledge about Cooperation Protocol.
  CP represents the knowledge regarding the interaction/cooperation protocol amongst various AIR.

4. Implementation of AIR-NMS

4.1. Agent Framework for AIR-NMS

Each AIR in AIR-NMS is realized as a program which works autonomously based on the rule type knowledge. As an actualization method of this kind of AIR, a notion of multi-agent based AIR is proposed [8].

In this paper, ADIPS/DASH framework is utilized in which multi-agents are actualized with respect to distributed environment [5, 4]. In an ADIPS/DASH framework, the agent knowledge is described by the rule type knowledge, and autonomous control of a java program based on agent knowledge can be executed.

By using ADIPS/DASH framework, AIR-NMS operates FUS based on KUS, and executes information resources (experiential knowledge of network management/status information of networking device) thereby modifying and cooperating with other AIRs.

4.2. Experimental Prototype System and its Result

To evaluate the operation of AIR-NMS, the network and AIR-NMS shown in Figure 5 were constructed. In this experiment, it thought about the failure "The error occurred when the HTTP connection was tried from PC$_C$ of Subnet$_C$ to WWW Server of DMZ", and it thought about the case where the user of PC$_C$ reported on the failure to the network administrator. In general, there are the following five patterns as a cause thought about when such an error occurs.

- WWW Server is a down or in the state of the overload.
- Contents do not exist on WWW Server.
- The access limitation is done by WWW Server and the firewall.
- The equipment in the route between PC$_C$ and WWW Server has been downed.
- The setting of PC$_C$ has made a mistake.

In a usual network management technique, the network administrator one by one verifies to each case and specifies the cause. After that, it was necessary to devise the method (e.g., method of reactivating the process of the server) for the cancellation of the cause and to execute it.

In this experiment, these hard work is supported by AIR-NMS. So, the series of operations can be played in parallel in AIR-NMS. As a result, the manager's load is reduced. Then, the empirical knowledge of the following administrators was stored in the knowledge base.

- Method of error concerning WWW Server
- Method of confirming operation status of WWW Server
- Method of judging status from log of WWW Server
- Method of confirming setting of firewall
- Method of confirming status of network equipment
- Method that recovers from error of WWW Server
- Method of restarting WWW Server
- Method of changing setting of WWW Server
- Method of changing setting of firewall
- Method of reactivating network equipment

And, each knowledge was developed on PC_A as ten independent K-AIR. Moreover, to obtain the situation of the server and the firewall, nine following I-AIR was developed in this experiment.

- Information on equipment composition of each subnet (I-AIR$_A$, I-AIR$_B$, I-AIR$_C$, I-AIR$_{DMZ}$)
- Set up information of WWW Server (I-AIR$_{W1}$)
- Log information on WWW Server (I-AIR$_{W2}$)
- Set up information of firewall (I-AIR$_{F1}$)
- Log information on firewall (I-AIR$_{F2}$)
- Status information on network devices (I-AIR$_N$)

In this experiment, it thought about the failure "The error occurred when the HTTP connection was tried from PC_C of Subnet$_C$ to WWW Server of DMZ". And, the cause was assumed to be "WWW Server has been downed". In this case, the administrator inputs to the AIR interface, "Failure object: WWW Server and PC_C" and "Failure situation: WWW Server Access deny".

The AIR interface that receives this request transmits to K-AIR by converting the request into ACL and using the request protocol. K-AIR that receives the request judges whether to deal by using own knowledge. Each K-AIR cooperates with each I-AIR when it is possible to deal.

In this experiment, K-AIR with the knowledge of "Knowledge concerning method of error concerning WWW Server" and "Knowledge concerning method of restarting WWW Server" shows the manager "Method of restarting WWW Server".

These a series of work is processed parallel on each environment. Moreover, the work that the administrator should do is only "The request is input to the AIR interface" and "The action method is executed". So, it is thought that the administrator's load has been reduced.

5. Conclusions

In this paper, we propose a knowledge-based support method of the network management task and also propose a support system using active information resource (AIR-NMS).

In the proposed AIR-NMS, various AIR hold information and knowledge of management tasks of the target network system, and provide useful support for the administrators based on the cooperative processing of AIR. To demonstrate the properties and functions of the proposed AIR-NMS, we design and implement a prototype system of the AIR-NMS by using the multi-agent development tool, ADIPS/DASH framework. Through the experiment using the prototype system, we confirm that the AIR-NMS can provide the systematic support of management tasks for human administrators based on both the status information and the heuristics of management tasks that accumulated and utilized by the AIR allocated in the network.

References

[1] S. M. Baker and B. Moon. Scalable web server design for distributed data management. In *15th International Conference on Data Engineering*, page 98, 1999.

[2] Z. Constantinescu. Towards an autonomic distributed computing system. In *14th International Workshop on Database and Expert Systems Aplications*, pages 1–5, 2003.

[3] N. Damianou, N. Dulay, E. Lupu, M. Sloman, and T. Tonouchi. Tools for domain-based policy management of distributed systems. In *IEEE/IFIP Network Operations and Management Symposium*, pages 203–218, 2002.

[4] DASH GROUP. *DASH – Distributed Agent System based on Hybrid architecture*. [Online].Available: http://www.agent-town.com/dash/.

[5] S. Fujita, H. Hara, K. Sugawara, T. Kinoshita, and N. Shiratori. Agent-based design model of adaptive distributed systems. *Journal of Applied Intelligence*, 9(1):57–70, 1998.

[6] M. Hasan, B. Sugla, and R. Viswanathan. A conceptual framework for network management event correlation and filtering systems. In *IEEE/IFIP 6th International Symposium on Integrated Network Management*, pages 233–246, 1999.

[7] S. Konno, Y. Iwaya, T. Abe, and T. Kinoshita. Design of network management support system based on active information resource. In *The 18th International Conference on Advanced Information Networking and Applications*, pages 102–106, 2004.

[8] B. Li, T. Abe, and T. Kinoshita. Design of agent-based active information resource. In *The 1st International Conference on Agent-Based Technologies and Systems*, pages 233–244, 2003.

[9] J.-P. Martin-Flatin, S. Znaty, and J.-P. Hubaux. A survey of distributed enterprise network and systems management paradigms. *Network and Systems Management*, 7(1):9–26, 1999.

[10] I. Satoh. Building reusable mobile agents for network management. *IEEE Transactions on Systems, Man and Cybernetics*, 33(3):350–357, 2003.

[11] R. Stephan, P. Ray, and N. Paramesh. Network management platform based on mobile agent. *International Journal of Network Management*, 14:59–73, 2003.

[12] A. Virmani, J. Lobo, and M. Kohli. Netmon: Network management for the saras softswitch. In *IEEE/IFIP Network Operations and Management Symposium*, pages 803–816, 2000.