Internetworking between OSI and TCP/IP Network Managements with Security Features

Taeyeon Kim, Bongnam Noh
Dept. of Computer Science, Chonnam National University, KOREA
E-mail : bongnam@chonnam.chonnam.ac.kr

Abstract

To integrate both the OSI network and the TCP/IP internet the application gateway with powerful and flexible paradigms has been used, but micro-managements of the gateway produces high communication costs and long delays in responding to critical situations. The mechanism that maps the access control policy is needed between two domains using the different security policy. These problems are caused by managing each domain with different standards.

In this paper, we proposed an application gateway that delegates powerful and complex services of the CMIP as well as management functions sent to an agent by a manager in order to reduce network management costs and delays. We also suggested the security mechanism converting the security policy in order to guarantee the safe communication between two domains.

1. Introduction

If good qualitative services are not supported in the complex high speed networks for time constrained applications, serious problems can occur. Because the managed services are sensitive to time, management applications which manage these services must be processed in real time. Currently, application protocols are widely used, which are based on the CMIP for the management of the OSI and on the SNMP for the management of the TCP/IP network.

The SNMP internet protocol includes SET, GET, GET-NEXT and TRAP services and the CMIP provides M-GET, M-CANCEL, M-SET, M-CREATE, M-DELETE and M-EVENT-REPORT services in the OSI network[ISO90]. Also, CMIP services provide powerful functions such as scoping, filtering and synchronization for a manager to select one or more managed objects.

The agents of the OSI network and the TCP/IP internet should control the management information base(MIB). However, structures of the MIBs of these models are different. That is, the MIB of the TCP/IP internet is maintained in the form of tables, but the MIB of the OSI network uses the object-oriented paradigm.

Today, network managements have broadly employed the SNMP, which has many advantages such that the SNMP has inexpensive costs of the use of network devices and leaves hardware which has been used in the TCP/IP internet as it is.

On the other hand, the CMIP has

0-8186-7216-1/95 $04.00 © 1995 IEEE

shortcomings such that modifications of the design of existing software and the implementation of the MIB are very difficult to maintain the consistency in the OSI management model because the network management model of the OSI adopts the object-oriented paradigm. Although the SNMP is widely used at the present day, more powerful paradigms for the network management will be needed in the future because the SNMP only supports the limited domains of the management.

Consequently, to interconnect the OSI network and the TCP/IP internet, three kinds of methodologies were proposed[Kal93]. One is that only one site of those networks manages all networks, and the other is the use of duplicated dual MIB which can be accessed by applications in both domains. The third is the application gateway for the network management which transforms one protocol into another protocol between both domains, for example, from the CMIP to the SNMP.

In this paper, we design the application gateway which has the additional function, that is, the delegation function for efficient managements of networks. In other words, we propose the application gateway that delegates powerful and complex services of the CMIP as well as management functions being sent by a manager to an agent for the purpose of reduction of network management costs and delays.

Because the authentication between two domains has been plentifully studied, this paper didn't explain the problem. But for the purpose of supporting the safe communication, we suggest the security mechanism that converts the security policy.

This paper is organized as follows. In chapters 2 and 3, we describe related works, and introduce the structures of the proposed gateway with an access control policy. Also, we explain both the mapping of services and that of delegation functions and access control policies in chapter 4. Lastly, conclusion and future researches are presented in chapter 5.

2. Related works

2.1 Interconnection of the OSI network and the TCP/IP internet.

For the strategies, techniques, and problems about integrating the SNMP and the CMIP, Rose proposed a method about the transition and coexistence in order to manage both the TCP/IP internets and the OSI networks[Rose90]. Transitions of protocols from the TCP/IP internet to the OSI network or vice versa, and coexistences of different protocols are described in the view of the protocol-based approach and the service-based approach independently.

Kalyanasundaram and Sethi presented three kinds of paradigms for the management of the OSI and the internet, and proposed the mapping of names, instances, and the function of the application gateway[Kal93].

Abeck, Clerm and Hollberg proposed an approach that integrates the SNMP to the CMIP using the gateway with the role of application gateway[Abe93]. Park, Jung and Sunwoo also proposed an integration method of the OSI network and the TCP/IP internet management, and presented structures of software and an algorithm[Par93].

In the above mentioned works, the paradigm of the application gateway was proposed to interconnect heterogeneous systems. However, these studies considered mappings of primary services and functions, not communication costs and delays problem of the gateway. Thus, we propose a mechanism which reduces communication costs and delays for network managements efficiently.

2.2 Delegation function

If a manager requests a managed operation, the manager must wait until the notifications

arrive. Also, it controls all the management behaviors. These non-trivial management tasks reqire that managers micro-manage agents through primitive steps and resulting the traffic overheads. To minimize these overheads a lot of studies have been done and one of them was the delegation model which was proposed by Yemini et al[Yem91]. The delegation model reduces traffics between a manager and an agent by delegating executions of scripts to an agent and allows a manager to write out the management scripts.

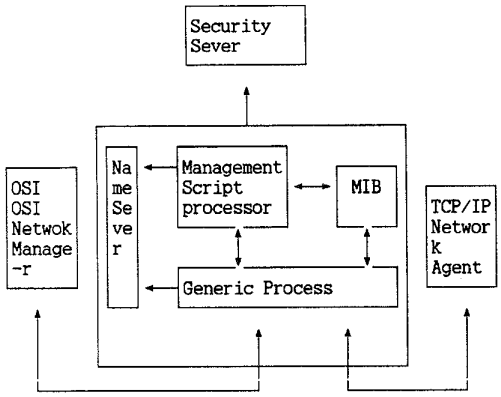
The function of the script management can dynamically create the management script whenever a manger needs. And it can delegate executions of the management script to an agent system when a manager shouldn't execute specific management functions or a manager would reduce the burden of the system with excessive management traffics.

3. Application gateway

3.1 Application gateway layout

The integrated management is required in order to manage the network efficiently among domains. In the super manager there is the relationship between the managers and the super manager which manages them as well as the relationship between the manager and the agents. In this paper, we suggest the application gateway which interconnects among domains by using the delegation and the security property under these circumstances.

There are a variety of paradigms which manage the networks without structure modifications of the existing network managements in the heterogeneous systems. One of them is the application gateway which interconnects the ISO network and the TCP/IP internet efficiently and transparently. The application gateway has the structure as shown in the figure 1.



<Figure. 1> The application gateway layout

The application gateway has the role of an agent to a manager, and vice versa. Consequently, the application gateway which serves for the transmitter performs a role of the transformation because the protocols used by a manager and an agent are different.

The application gateway consists of the generic process, the processor of the management script, the name server, the table of the management script and the MIB. The generic process is composed of the two phase commit relation between the name server and the processor of the management scripts, and takes charge of the translation of both primary protocol services and the management scripts. Also, it requests the management script from the processor of the management script when the delegation function is needed. The generic process takes the instance address of an actual managed object through the name server. The management script which is transmitted by a manager should be transformed in the form understood in an agent, and then only waits the responses. The management script which is created by the processor of the management script searches the script table, and if the table doesn't exist, the script must be stored in the table, but if exists, the script is transmitted to an agent without the process of the transformation and then waits the responses.

The name server maintains the constraints of the name of the managed object and attribute, and calls the directory services in order to find the instances of the managed objects. The directory is the repository of all the managed objects and the directory service creates the addresses of the actual instances and transmits them to the name server.

The processor of the management script creates the script sent by generic process corresponding to the management function of the OSI and stores the script to the table of the script. Also, the processor of the script transmits the script to the generic process.

The application gateway performs the transformation of the names, addresses and services between the CMIP and the SNMP. The actual mapping becomes the one-to-one mapping on the objects, or a lot of mapping in accordance with characteristics of the MIB can exist.

This paradigm can easily manage nodes of the TCP/IP internet irrespective of the structure of the protocol for the internet agent and of the protocol for the manager of the OSI domain. One side of the application gateway is connected to the OSI domain and the other side to the internet domain. If the gateway receives the CMIP request, its output becomes the SNMP request. Also, when the gateway receives the response/trap from the SNMP it sends the response of the CMIP to the OSI.

Although this paradigm provides lots of flexibility and effectiveness, the complexity of the gateway is the major problem. The SNMP limits the size of the packet but the CMIP doesn't. That is, because the SNMP uses the UDP so as to execute the services, the size of the packet is restricted. Thus, a request of the OSI domain must be transformed into multiple requests of the TCP/IP internet domain. In this case, the gateway has a lot of responsibilities because it maintains each state of requests in the OSI, collects several responses from the internet domain and then transforms them into a response of the CMIP.

To resolve these problems, we propose a method which transforms complex function into management scripts and then delegate these scripts into an agent in this paper. By means of this approach, the overheads of the gateway are reduced and thus the performance of the network management is apparently increased.

3.2 Security server properties

(1) write security property

If subject(S: super manager) is object(O: submanager)'s predecessor and one of the following conditions is satisfied, then SET, ACTION, CREATE, CANCEL, DELETE service is allowed in the write security property. First, the security label of subject is more than or equal to that of object. Second, there is the subject's access to object in the access control list(ACL). third, the subject's role is valid to object[Pfl,Pei93].

It is the security property that is applied only between the manager and the agent in the same domain.

$$R1(S,O,R,ACL,m) = \begin{cases} \text{true} & \text{if } m=\{wr, ac, ca, cr, de\} \text{ .and.} \\ & \langle C(S) \geq C(O) \text{ or } (S,m) \in ACL(O) \text{ or} \\ & \{S \in R \text{ .and. } (R,m) \in ACL(O)\} \rangle \\ & \text{.and. } pred(S,O) \\ \text{false} & \text{otherwise} \end{cases}$$

(2) read security property

If one of the following conditions is satisfied, then GET service is permitted. First, the security label of subject is more than or equal to that of object. Second, there is the subject's access to object in the access control list(ACL). third, the subject's role is valid to object. This security property is one that allows the read access if the access security property is satisfied between the requester and the responder in the different domains[Pfl,Pei93].

$$R2(S,O,R,ACL,m) = \begin{cases} \text{true} & \text{if } m=r \text{ .and.} \\ & \langle C(S) \geq C(O) \text{ or } (S,m) \in ACL(O) \text{ or} \\ & \{S \in R \text{ .and. } (R,m) \in ACL(O)\} \rangle \\ \text{false} & \text{otherwise} \end{cases}$$

(3) event report security property

If subject is object's successor and one of the following conditions is satisfied, then EVENT-REPORT or TRAP service is allowed. First, the security label of subject is less than or equal to that of object. Second, there is the subject's access to object in the access control list(ACL). third, the subject's role is valid to object. It is the security property that is applied between the manager and the agent when the event occurs in the managed object[Pfl,Pei93].

R3(S,O,R,ACL,m) =

$$\begin{cases} true \text{ if } m = e \text{ .and.} \\ \quad \langle\ C(S) \le C(O) \text{ or } (S,m) \in ACL(O) \text{ or} \\ \quad \{S \in R \text{ .and. } (R,m) \in ACL(O)\}\ \rangle \\ \quad \text{.and. } succ(S,O) \\ false \text{ otherwise} \end{cases}$$

4. Mapping of service function and delegation

In this chapter, we present the algorithm, for the management of the TCP/IP Internet, which supports the basic services, scoping, filtering and synchronization used to manage the OSI network. For the interaction among the SNMP agents, the SNMP services are based on the datagram of the unreliable UDP, and the mechanism of the time-out and request retransmission is needed to control uncommitted notifications.

4.1 Basic service mapping

The managements are performed through management primitives between a manager and an agent in the integrated management model of the OSI and the TCP/IP Internet.

(1) Attribute definition and retrieval of the managed object

To define and retrieve attributes of the managed object, the CMIP uses management services such as M-GET and M-SET, and the SNMP uses SET and GET service. When the gateway receives M-SET-indication and M-GET-indication, it generates more than one SET-requests and GET-requests for the SNMP domain. When the gateway waits the responses of the SNMP agents and then receives all the waiting responses, it maps them into service primitives of the CMIP such as M-SET-response and M-GET-response.

(2) Creation and deletion of instances of managed objects.

There are no services for creation and deletion of instances in the SNMP. Hence, the deletion function become the functions of M-DELETE service in the CMIP if the instance fields of managed objects are set to invalid using SET service. If the instance fields of objects are set to valid, then the creation functions become M-CREATE service in the CMIP.

(3) Management behavior start

To start the management behaviors of the CMIP, M-ACTIVE is used. But in the SNMP, behavior functions are achieved by designating specific values to the instance fields of the managed object.

(4) Event and notification

The CMIP and the SNMP provide different services to monitor events and notify urgent states. The CMIP uses M-GET and M-EVENT-REPORT for monitoring events but the SNMP uses the trap service.

4.2 Delegation service mapping

4.2.1 Advanced CMIP functions

To reduce the burdens of the gateway which has to maintain states of services and execute processes of the transformations, the proposed algorithm creates the management scripts and transmits them to agents. The algorithm is as follows.

[Delegation Algorithm]

Step1) The generic process requests the manag-

ement script from the processor of the management script.

Step2) The management script searches the table of scripts and if management scripts exists in the table, then sends it to the generic process, else the management script is stored in the table and sends it to the generic process.

Step3) The generic process sends the management script to an agent.

Step4) Controls the execution of the management script. That is, the manager or the application gateway cancels, restarts and halts the management script

Advanced CMIP functions such as scoping, filtering and synchronization that are not supported in the SNMP are possible in the SNMP by means of delegating these functions to the gateway.

(1) Scoping

Scoping operation can select multiple objects. This implies that a specified operation(eg., M-GET) has to be performed on all or a subset of the objects selected. Scoping can be mapped by repeating the requested operation(eg., GET)for each object selected because the scoping operation does not exist on the TCP/IP Internet. Appendix 1 is an algorithm that supports scoping.

(2) Filtering and Synchronization

Filtering and synchronization are other high quality services supported by CMIP. Filtering is a service that allows us to select managed objects that satisfy given condition. This condition is applied to the scoped managed object. In this method, the filtering mechanism can reduce traffic overhead by enforcing to receive only appropriate object values from a manager system. Because the filtering function is not compatible with SNMP, the algorithm that supports the filtering function in SNMP is as follows. The condition of managed object is determined by the scope operation and filtering, and after that, the order of managed objects is determined. This order is called the synchronization. The CMISE users can use either atomic or best effort synchronization method.

4.2.2 Management script

The script management function is used to delegate the management script to an agent when a manager cannot afford to execute specific management function or want to reduce the system overload caused by extreme management traffics. The gateway must transform the management script which can be applied to the SNMP agent, and then transfer it to the next agent because the management script which is transmitted between the CMIP and the gateway is a part of CMIP agent. The management script that transforms the management script transmitted from OSI into the management script understood in the SNMP is as Appendix 2.

Because the M-GET() and M-SET() of the received algorithm are services which monitor the event occurrence and execute the recovery of the event respectively, we compose the process which iterates as many times as the number of instances of the managed object with 'for' statement.

4.3 Access control mapping

In this chapter, we describe a mechanism by which the access control over the basic services and delegation function is guaranteed between the manager and the agents.

(1) M-GET operation

In M-GET operation, if the relationship between subject(S) and object(O) is the predecessor and the successor, subject S is continuously used without the change to map GET service. Otherwise, subject S is replaced with super manager to map GET service. For example, the manager that is not a predecessor management, to access the information in the

different domain, makes its super manager access the information and return the result to it. If the two above conditions are not satisfied the request is rejected.

```
if not (S ∈ Sset .and. O ∈ Oset .and. R2(S, O, R, ACL, m))
   then reject
   else if (pred(S) or succ(S))
          then ( S, O, GET, CLR(S))
          else  ( Super_S, O, GET, CLR(S)  )
```

(2) M-SET operation

M-SET operation is the write operation that maps SET service if the rule R1 in the section 3.2 is fulfilled.

```
if(S ∈ Sset .and. O ∈ Oset .and.(R1(S, O, R, ACL, m) or
    R3(S, O, R, ACL, m)) )
   then ( S, O, SET, CLR(S) ) )
   else reject
```

(3) M-ACTION operation

M-ACTION operation is one that the manager requests to the agent if the rule R1 in the section 3.2 is satisfied.

```
if( S ∈ Sset .and. O ∈ Oset .and. R1(S, O, R, ACL, m) )
   then ( S, O, ACTION, CLR(S) )
   else reject
```

(4) M-DELETION operation

M-DELETION operation is one that the manager requests to the agent if the rule R1 in the section 3.2 is satisfied.

```
if( S ∈ Sset .and. O ∈ Oset .and. R1(S, O, R, ACL, m) )
   then ( S, O, DELETE, CLR(S) )
   else reject
```

(5) M-EVENT operation

M-EVENT operation is one that notifys the manager of the event occurrence. It can be performed only when the rule R3 in the section 3.2 is fulfilled.

```
if( S ∈ Sset .and. O ∈ Oset .and. R3(S, O, R, ACL, m) )
   then ( S, O, EVENT, CLR(S) )
    else reject
```

(6) EVENT-RECOVERY operation

EVENT_RECOVERY operation is one used to recover the error of 5). It can be carried out only when the rule R1 in the section 3.2 is satisfied and there is a record to the event occurrence in the log file.

```
if( S ∈ Sset .and. O ∈ Oset .and. R1(S, O, R, ACL, m)
            .and.  O-event ∈ LOG  )
   then ( S, O, SET, CLR(S) )
   else reject
```

The communication traffics are decreased and the safe network management is ensured by using these constrains between the manager and the agent.

5. Conclusions

As many venders have constructed network management systems which are appropriate to their own network devices, the main issue of the network management which is studied recently is to find the method of integrated management of heterogeneous network systems.

This paper described the function of the application gateway as a paradigm of integrating the OSI network and the TCP/IP internet management. Especially, we proposed the application gateway which transforms the management script language which is capable of processing the fault monitoring of network resource, recovery and notification in a predictable way as well as the service function to perform the TCP/IP internet and OSI network management efficiently.

To efficiently interconnect the TCP/IP Internet which is widely used in commercial markets and the OSI network, we proposed an application gateway with the delegation functions and the access control function. Using the proposed application gateway, communication costs and the delays which were caused by both the transformation of protocols and the maintenance of status information could be reduce. We could ensure the safe network management by adding the access control funcitons in the gateway.

We are going to implement the delegation function in the gateway and to study the

mechanism that supports the real-time in the gateway.

Reffences

[Abe93] S. Abeck, A. Clemm, U. Hollberg, "Simply Open network Management : An Approach for the Integration of SNMP into Management concepts", Proc. 3rd International Symposium on Integrated Network Management, San Francisco., pp. 361-374, April 1993.

[Gol94] German Goldszmidt, "Distributed System Management via Elastic Servers", IEEE First International Workshop on Systems Management, April, pp. 31-35, 14-16, 1993.

[ISO90] ISO/IEC 9595, Information Processing Systems - Open Systems Interconnection - Common Management Information Service Definition.

[Kal93] P. Kalyanasundaram, A. S. Sethi, "An Application Gateway Design for OSI-Internet Management", Integrated Network Management, III (C-12), pp. 389-400, 1993.

[Park93] J. T. Park, Y. W. Choi, J. W. Jung and J. S. Sunwoo, "The Integration of OSI Network Management and TCP/IP Internet Management using SNMP", IEEE First International Workshop, pp. 145-154, April 14-16, 1993

[Pfl] Ch. P. Pfleeger, Security in Computing, Prentice Hall, Englewood Cliffs, New Jersey 07638, pp. 242-258.

[Rei93] M. Reitenspiess, "Open System Security Standards", Computers & security, pp. 341-361, 12, 1993.

[Ros90] M. T. Rose, "Transition and Coexistence Strategies for TCP/IP to OSI", IEEE JOURNAL vol.8. no. 1. pp.57-66, January 1990

[Yem91] Y. Yemini, G. Goldszmidt, S. Yemini, "NETWORK MANAGEMENT BY DELEGATION", Proc. 2nd International Symposium on Integrated Network Management, Washington DC, pp.95-107, April 1991.

[Appendix]

1) Executable scoping Script by the SNMP agent through gateway

```
main()
{
  SWITCH (scope_params)
    case n_th_level  //Get n_th_level object
         GET(n_th_level);
         while(get_object != Null)
           { GET(get_object);
             SET(get_responses);
             GET-NEXT; }
         break;
    case base to n_th_level  //Get from base
                             to n_th_level object
          while( scope_params )
          {  GET(current_level);
             while(get_object != Null)
               {  GET(get_object);
                  SET(get_responses);
                  GET-NEXT;  }  }
          break;
    case base to lowest_level //Get from base
                              to lowest_level object
          while( scope_params )
            {  GET(current_level);
               while(object != Null)
                 { GET(get_object);
                   SET(get_responses);
                   GET-NEXT;  }  }
          break;
   } }
```

2) The SNMP agent executable Script

```
main() {
  int link_congestion, flag;
  while( )      // failure monitoring
     {
    for( parameter )
       GET(get)
         .
         .
       if(link_congestion) break;     }
  for( parameter )     // failure recovery
     SET( get ) ;

EVENT-REPORT(type_GW_EventReportArgumt)
;  }        // event report to gateway
```