An Active Approach to Multimedia Network Management

ZHONGWEI ZHANG & DAVID LAI
Department of Mathematics and Computing,
University of Southern Queensland,
Toowoomba, QLD 4350,
AUSTRALIA
{zhongwei,lai}@usq.edu.au

Abstract: - Most of network management systems adhere to the centralized and passive approach. For large and heterogeneous multimedia networks, the centralized approach are increasingly incapable of providing required and efficient management and of measuring up to requirements of some emerging services. What come after that is the distributed approach which require the individual network elements be responsible for their own simple management chores such as performance monitoring, or fault detection. Current distributed approach are inadequate in managing of the multimedia networks where the applications are contentious to the bandwidth and sensitive to the transmission delay.

In this paper, we study a new approach to multimedia network management. The new approach, which relies on the active networking technology and thereof called active approach, enables the network elements executing functions or programs. In contrast to the traditional network management strategies which resort to the centralized approach, following this approach yields a decentralized framework, which accedes the network components or elements be responsible for their own administrative chores. The administrative activities are implemented by a group of management functions embedded in the network elements. After analyzing several functions of such kind, we realize that the communication between the managed elements or stations is of serious security concern. To tackle this problem, we also present a set of protocols for network elements to transmit and authenticate the functions or executable programs among the network stations. The protocol guarantee the efficient communication and secure execution of the transmitted functions.

Key-Words: - Network management, Simple Network Management Protocol(SNMP), active networking, distribute network management, multimedia networking

1 Introduction

Network management is the art and science of keeping a network healthy. Network management of TCP/IP networks is a challenging task [2, 5, 7]. It is right to say the discipline of network management has been born due to the needs of administrating a rapid growing heterogeneous network. In addition to that, ever since the advent of network management, security management of network is a major part of network management discipline. The security management has significantly complicated the overall network management.

Despite the growing diversity of the network in architecture, protocol and application, the activities of network management includes nothing more than the deployment, integration, and coordination of the hardware, software, and human users to monitor, test, poll, configure, analyze, evaluate, and control the network and network element resources to meet the real-time, operational performance, and quality of service requirements at a reasonable cost. All these activities require human intervention or a central managing station to perform on behalf of human operators [2, 7]. Multimedia applications put some additional requirement to the underlying networks. For instance, the multimedia applications often are bandwidth contentious and very sensitive to the overall transmission delay. Management of the multimedia networks becomes even more difficult.

For many years, researchers have devoted themselves to explore efficient strategies to the network management. There are two categories of approach to network management (NM). Centralized network

management approaches increasingly become incompetent to satisfy the requirements of large and heterogeneous computer network [2], while distributed network management such as SNMPv2 and mobile agent network (MAN) management framework have demonstrated a clear inadequacy for efficient management of multimedia computer networks [9], which put more demands on network performance and reliability, service differentiation and service customizability.

In this paper, we propose a new approach to the multimedia network management, which is not only distributed, but also active. The active approach is based on the active networking technology which makes the internal element or nodes of the network active. The remaining of this paper is organized as follows. In Section 2, we review a popular model which has been used for many years. Following in Section 3 is an introduction of active networking technology, while in Section 4, we present our proposed approach to the multimedia network management. Based on this approach, a framework of managing multimedia network is constructed as multiple layers, the details of this framework are given in Section 5. We conclude our paper in Section 6 by presenting a list of possible research directions.

2 NM model and framework

The International Organization for Standardization (ISO) has created a network management model. This model has identified five areas of network management. (1) Performance management, (2) Faulty management, (3) Configuration management, (4) Accounting management, (5) Security management.

Traditional NM activities require that many different types of data be gathered and analyzed and the different decisions be made that depend on the activities involved [7]. Traditional network management framework consists of four parts:

- *Network management objects(MIB)*: A MIB object might be a counter, such as the number of IP datagrams discarded at a router due to errors in an IP datagram header, or the number of carrier sense errors in the Ethernet interface card; descriptive information such as the version of the software running on a DNS server; status information such as whether a particular device is functioning correctly.
- *Data definition language*: It defines the data types, an object model, and rules for writing and revising management information.
- *Protocol*: Protocol is needed for conveying information and commands between a managing entity and an agent executing on behalf of that entity within managed network device.
- *Security and administration capabilities*: These are the vulnerable part of conventional network management, and limited development have been done.

Conventional NM frameworks are centralized and require human operators to make real-time decisions and perform problem resolution. For example, the SNMP architectural model consists of NM stations that execute management applications that monitor and control network elements, where network elements such as hosts, gateway and servers have management "agents"[1] that perform the NM functions. Network management is achieved by having management stations routinely poll the managed devices for data, looking for anomalies. This technique has served us well in the past. However, due to the increase in the number and complexity of nodes in the network, now it has become problematic. For instance, management centers becomes points of implosion, inundated with large amount of information. Also the round-trip delay that is needed for the information to reach the management center and the reply to return back to the affected part of the network, is sometimes significant and the action undertaken is not up to date any more.

In recent years, network infrastructure is shifting toward service-centric networks. This trend has drastically changed the way network management is done. Distributed NM approaches such as Mobile agent (aka M-agent) based or Intelligent agent (aka I-agent) based have mitigated the difficulty the conventional NM approaches suffer, but distributed NM raise some new challenges [6]. For instance, the structure of the mobile agent and intelligent are too complicated and it requires the network elements to have a complete workable environment to be able to run M-agent or I-agent [3, 8]. We argue that it is essential that network management employs techniques with more immediate access and better ability to scale.

[1] Not to be confused with intelligent agents or mobile agents.

3 Active networking technology

Active networking technology (ANT) provides a new approach of building networks. With ANT, the packets transmitted from the source endpoint through a number of intermediate IP routers to the receiving endpoint will be replaced by `capusos` which is a code segment or a program. On the other hand, the IP router is no longer a device of routing and forwarding packets to the right hops, the routers can carry out the higher level operations which could be up to the application layer operations.

Active networks visualize the network as a collection of active nodes that can perform any computations, together with a collection of active packets that carry code and are indeed programs. Under that viewpoint, a mobile agent may be regarded as a specific type of an active packet, and a "mobile-agent-compatible" node of traditional networks could be regarded as a specific type of an active packet since the latter is secure and allows any kind of computation.

In an active network, active packets may misuse active nodes, network resources, and other active packets packets in various ways. Also, active nodes may misuse active packets. The security issue involves four aspects:

- *Damage*: An active packet can destroy or change the resources or service of a node by reconfiguring, modifying, or erasing them from memory. A node may erase an active packet before the completion of its job in the node.

- *Denial of Service(DoS) attack*: An active packet may overload a resource or services due to constantly consuming network connections or using a great portion of the CPU cycles available. The node cannot function properly under these circumstances and another active packet cannot be executed or forwarded.

- *Information stealing*: An active packet may access and steal private information from a node. On the other hand, an active packet is vulnerable toward the node at any point when visiting it. Even if it is encrypted, it is not totally safe because it usually has to be decrypted in order to execute.

- *Compound attack*: The biggest actual threat for an active node is a compound attack aimed toward a goal. For example, a malicious user may send many active packets toward a central router and try to bring it down by consuming all its bandwidth capacity.

Nevertheless, the essence of ANT is to make the internal nodes of the network active, hence to move the management centers right in the "heart" of the network. By this way, the network reduces both delays from responses and bandwidth utilization for management purposes.

To sum up, by using active networking for network management, we have the following benefits:

- Problems are tracked quickly or are reported automatically without the need of polling;

- Management centers can be in the "heart" of the network, thus delays from responses and bandwidth utilization for management purposes are reduced;

- "Patrol" and "first aid" active packets can respectively track a problem and deal with it at once;

- Information content returned to the management centers can be tailored to the current interests of the center so that back traffic and processing time are reduced;

- Management policies can be altered easily as administrative requirements change.

4 Proposed active approach

In this section, we propose a new approach to the multimedia network management, which is called *active approach*. The active approach has two objectives: efficient communication and effective security.

4.1 Network element model

The idea behind the active approach is to allow each network element(NE) (routers, gateway, switch, and hosts) in the network be responsible for their own management, and each NE is equipped with a set of functions for the purpose of management.

Those network nodes become active in the sense they are able to look after themselves to a certain

level. The model on which the NEs are based lies in between a full-fledged application and a passive router. The new model for the NE is shown in Figure 1. The NE model is very much similar to the

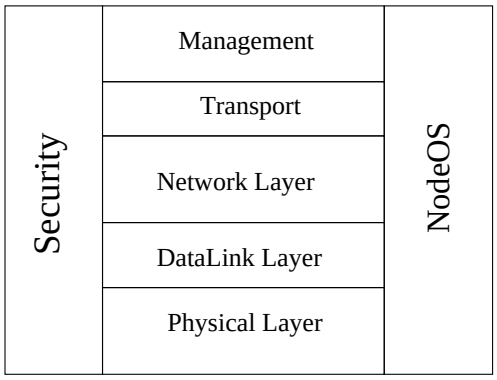

Figure 1: Network node mode

TCP/IP model. The difference is that each network node is more powerful than the traditional network nodes such as routers and/or gateways. Each active node has a set of functions designed for the node management and a set of functions to guarantee the node packet routing and scheduling. The security, which abide into all layers, is ensured by a combined effort of all layers.

Active network node is vulnerable to virus attacks from malicious nodes (users) or DoS attacks from too many peer nodes (users). The techniques that may be used to protect the active nodes include: Authentication of active packets, Monitoring and control, Limitation techniques, and Proof carrying code (PCC).

This approach is that management processing functions can be delegated dynamically to the network elements and executed locally rather than centrally. Instead of moving data from the managed elements to the management center, one can move management code or function at the network elements where the data resides.

4.2 Communication protocol among NEs

The protocol used in this approach is responsible for dynamically dispatch delegated agents to an executing elastic server at a remote system, for controlling their execution and the dispatchment is acting upon the query. The security mechanism is scattered into all layers of network node. Any security inciters will be detected by lower layers and fixed straightaway at that layer. It is important to mention that every element owns a public/private key pair; these keys are used to authenticate and authorize the delegated agents.

This approach is situated in the middle of the traditional approach and the I/M-agent based distributed approaches. The difference lie in the agents in the conventional approach are too simple but the agent in with some distributed NM approaches are mobile-agent or intelligent-agent, which are usually too heavy. As a result, the communication between network elements is transmission of functions or programs, rather than the mobile or intelligent agents as in the distributed NM frameworks [3, 4, 5]. Another difference is that this approach has transfered its security checking to all the layers where the security problem can be addressed in time, the I/M-agent based distributed address all the security issue in the highest layer of the protocol using some complicate authentication strategy. The way of addressing security which heavy distributed NM approach adopted, is not effective.

5 An active NM framework

This approach provides a powerful computational framework for scalable, decentralized, and automated management. Figure 2 represents that agents have the capability to autonomously travel (execution state and code) among different NEs to complete its task. Beside it makes the network elements (NE) active

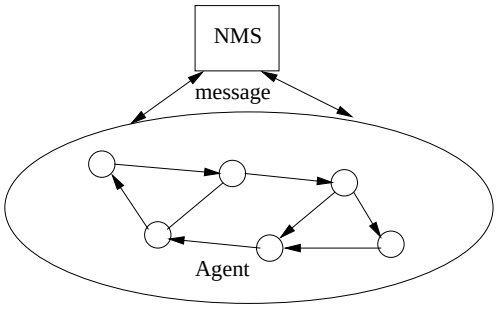

Figure 2: Active NM framework

rather than passive in the management, the network management framework based on this active approach also offers several advantages: (1) network traffic and

processing load in the Network Management Station (NMS) can be considerably reduced by performing data processing closer to the NEs; (2) scalability to large networks is improved (3) searches can be performed closer to the data, improving speed and efficiency; (4) and is inherently more robust without depending on continuous communications between NMS and NEs.

5.1 Communication protocols

In some situation, NEs need to send some management code or program each other. We refer this as agent communication. There are some issues such as authentication. The protocol used for this purpose is very much like DNS protocol, and described as follows.

- If one NE agent needs a management function, it checks its own management function base (MFB).
- If the requested function is available then the NE will invoke the function. Otherwise, it sends a request to the NMS, the NMS will find which NE has the function, then NMS will forward the request to those NEs which has the requested function.
- When the NE being of the requested function receives the request, then NE will send the required function to the requester NE.
- If the NMS can not find one NE who has the requested function, then it will return the NE with an error message.

5.2 Security issues

In [1], an architecture of a secure active network environment (SANE) has been described. Our framework is similar to SANE. A NE has no problem if the function comes from its own MFB. but if a function is sent by another NE, whether the function is coming from a trusted NE is a serious problem. Another problem is how the requesting NE is so trustful that the function would not do any damage for itself while the function is executing on it. To address this problem, each NE needs to authenticate the functions to make sure the function came from a trustful NE or from the network managing station(NMS). An authentication protocol is presented in section 5.3.

Each NE has a security policy and it will check the arriving functions' header against the policy. If a function has a disparity to the policy, then the NE will query the NMS to verify the function's authorization.

5.3 Function authenticate protocol

A NE needs requests a trusted function. The NMS will instruct the NE who has the requested function to the requester NE. The requester NE have to authenticate the function when the function arrives. This process is referred to as the function authentication, as shown in Figure 3. In Figure 3, there are many NEs

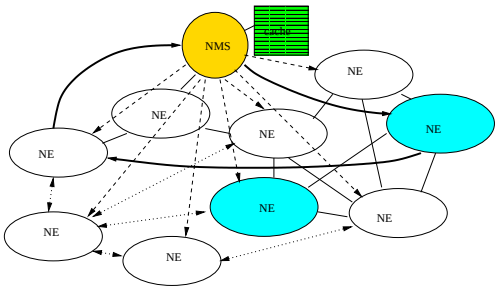

Figure 3: Authenticate protocol

and one NMS which is in yellow color with a cache in green color. Suppose one NE on the left side wants to get a function from its peers. Two NEs in light blue have the desired function. The steps are listed as follows.

- A NE checks its own function base.
- If it has no requested function, it sends a request to NMS, NMS receives the message, then it authenticates the owner's identity first.
- Then NMS looks through all cached entries in its cache if it has an entry to know who has the requested function,
- If NMS has one, the NMS will send a request to the NE who has the requested function, otherwise, NMS will broadcast a message to query who has to reply, then NMS will store this information into its cache.

- If there are more NEs having the requested function, the NMS will choose the one it has found first.
- When the NE has received the request from NMS, the NE will authenticate the request to make sure the request is coming from the trusted NMS.
- Within the request message, the NMS also issue a ticket, the ticket will be used when the NE will transmit the function to the original NE.

6 Conclusions

Neither the traditional centralized approach nor the distributed network management approach are able to meet the requirements of the current heterogeneous multimedia computer networks, which is shifting toward service-centric. In this paper, a new approach to the multimedia network management has been proposed, which is based on the active networking technology. The new approach looks into the network management from a perspective that the network elements are able to execute some network management activities and to maintain its own security. The approach is active rather than passive to self management; while the network elements are secured from the bottom layer up to the higher layers. This approach is a decentralized management scheme, which uses function query, unlike the traditional ones using polling.

The new approach has made the network management more efficient, but the active networking technology has heightened the complexity of the network management particular in security. The proposed framework can be used as a blueprint for the development of multimedia network management tools.

In the time to come, we will develop a set of management functions and implement the framework on a multimedia network. Using the proposed framework to develop a real network management system will be our direction of future research.

References:

[1] S. Alexander, W. Arbaugh, and A. D. Keromytis and J. M. Smith, A Secure Active Network Environment Architecture, *IEEE Network Special Issue on Active Networks*, pp.29-36. May/June 1998.

[2] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach Featuring the Internet*, Addison-Wesley Computing, ISBN 0-321-17644-8.

[3] D. Gavalas, D. Greenwood, M. Ghanbari and M. O'Mahony, Advanced Network Monitoring Applications Based on Mobile/Intelligent Agent Technology, *Computer Communications Journal*, Vol. 23, No 8, pp. 720-730, April 2000.

[4] T. M. Chen and S. S. Liu, A Model and Evaluation of Distributed Network Management Approaches, *IEEE Journal on Selected Areas in Communications*, Vol. 20 No.4 May 2002. pp.850-857.

[5] M. Kahani and H. Beadle, Decentralized approaches for network management, *IEEE Communication. Magazine*, Vol. 36 pp.66-70, March 1998.

[6] F. L. Koch and C. B. Wetphall, Decentralized Network Management Using Distributed Artificial Intelligence, *Journal of Network Systems Management*, Vol. 9, No. 4, 2001.

[7] S. Krause and T. Magedanz. A Survey of Distributed Network and Systems Management Paradigms, *ACM Computer Communication Review*, 27(3):pp36-47, 1997.

[8] D. Gurer, V. Lakshminarayan and A. Sastry, An Intelligent-Agent-Based Architecture for the Management of Heterogeneous Networks, *Proceedings of Ninth IFIP/IEEE International Workshop on Distributed Systems: Operations & Management(DSOM'98)*, Delaware, Oct.26-28, 1998.

[9] D. Raz and Y. Shavitt, Toward Efficient Distributed Network Management, *Journal of Network and Systems Management*, Vol. 9 No. 3. pp.347-361. September 2001.