

Decentralized Management of Multimedia Network using Active Network Technology

ZHONGWEI ZHANG & DAVID LAI

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

Abstract: - Though being centralized, traditional approaches of network management have accomplished their overall mission that is to provide efficient management of underlying heterogeneous distributed networks. However the size of networks has been growing, and so has the number of novel applications and protocols running on the networks. These new services raise more stringent requirements, and significantly increase the complexity of network administration. Apparently the traditional approaches to network management are no longer adequate for the management of multimedia networks.

Much research has been carried out in past years which mainly deployed the decentralization technique. These decentralized approaches are at most a step toward improving the centralized approach, but still not capable of efficiently managing multimedia networks. In this paper, we study a new approach to multimedia network management. The new approach, which relies on active networking technology and therefore called active approach, enables the network elements to execute functions or programs. In contrast to traditional network management strategies which resort to the centralized approach, following this approach yields a decentralized framework, which enables the network components or elements to 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 this kind, we realized that the communication between the managed elements or stations presents a 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 protocols guarantee efficient communication and secure execution of the transmitted functions.

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

1 Introduction

The number of protocols used in computer networks and the number of applications running on the network have been growing at an unprecedented rate. The task of administrating the services networks can provide to us has become very complicated nowadays. Network management is the art and science of keeping a network healthy. Network management of TCP/IP networks is a challenging task [2, 6, 8]. It is right to say the discipline of network man-

agement has been born due to the needs of administrating a rapidly growing heterogeneous network. In addition to that, ever since the advent of network management, security management of networks is a major part of network management discipline. Security management has significantly complicated overall network management.

Despite the growing diversity of the network in architecture, protocols and applications, the activities of network management includes nothing more than the deployment, in-

tegration, 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, 8]. Multimedia applications put some additional requirement on the underlying networks. For instance, multimedia applications often are bandwidth contentious and very sensitive to overall transmission delay. Management of multimedia networks becomes even more difficult.

For many years, researchers have devoted themselves to exploring efficient strategies for network management. There are two categories of approach to network management (NM). Centralized network management approaches increasingly become inadequate to satisfy the requirements of large and heterogeneous computer networks [2], while distributed network management such as SNMPv2 and mobile agent network (MAN) management frameworks have demonstrated a clear inadequacy for efficient management of multimedia computer networks [10], which put more demands on network performance and reliability, service differentiation and service customizability.

In this paper, we propose a new approach to 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 remainder of this paper is organized as follows. We start with a general overview of the characteristics of multimedia networks and the peculiarities of multimedia network management in Section 2. In Section 3, we review a popular model which has been used for many years. Following in Section 4 is an introduction to active networking technology, while in Section 5, we present our proposed approach to 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 6. Before we conclude our paper, we show some related research which has been done in the past decade in Section 7. Finally, we conclude our paper in Section 8 by presenting a list of possible research directions.

2 Multimedia networks management

Multimedia networks are capable of providing more advanced services to users. These services include quality-of-service, real time video streaming, and on line games. These new services or networking applications and the increasing complexities of multimedia networks have placed higher demands on network management. For instance, timing considerations and tolerance of data loss are particularly important. Timing considerations are important because networked multimedia applications are highly delay-sensitive, but occasional loss is acceptable for many multimedia services. These delay-sensitive but loss-tolerant characteristics are clearly different from those of traditional applications.

Management of multimedia networks raises additional complexity and requirements. For instance, the management of multimedia networks include not only the security measurement of the traditional network such as confidentiality, authentication between users and availability and access control, but also security enforcement among the network components [3].

Management of multimedia networks is different from that of traditional networks in the following aspects:

- Performance management

With Quality of Service levels an important criteria of multimedia networks, it is highly desirable that a MN network management system have the capability to optimally tune the network.

- Accounting management

Multimedia networks provide different services to meet the requirements from different network applications. The resources of the network must be carefully utilized. Controlling resource allocation and consumption is accounting management. A few issues associated with accounting management need to be particularly considered. For instance, user-based and application-based accounting profile and statistics are worth keeping.

- Security management

The bandwidth used for transmitting multimedia components needs to be safely guarded. The main challenge resides in providing these mechanisms without unduly affecting the performance, usability and affordability of network devices including wireless devices.

In summary, multimedia networks are more complicated and more versatile to provide more desirable services. The efficient management of multimedia networks requires new approaches and creative techniques.

3 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) Fault 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 different decisions be made depending on the activities involved [8]. The 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 a managed network device.
- *Security and administration capabilities*: These are the vulnerable part of conventional network management, and limited development has 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 amounts 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 has been 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)

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

based or Intelligent agent (aka I-agent) based have mitigated the difficulty the conventional NM approaches suffer, but distributed NM raise some new challenges [7]. For instance, the structure of the mobile agent and the intelligent are too complicated and requires the network elements to have a complete workable environment to be able to run M-agent or I-agent [4, 9]. We argue that it is essential that network management employs techniques with more immediate access and better ability to scale.

4 Active networking technology

Active networking technology (ANT) provides a new approach to 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 for routing and forwarding packets to the right hops, as well 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 computations, together with a collection of active packets that carry code and are indeed programs. From that viewpoint, a mobile agent may be regarded as a specific type of active packet, and a “mobile-agent-compatible” node of traditional networks could be regarded as a specific type of 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 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 service 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 to the “heart” of the network. 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 cur-

rent interests of the center so that back traffic and processing time are reduced;

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

5 Proposed active approach

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

5.1 Network element model

The idea behind the active approach is to allow each network element(NE) (routers, gateway, switch, and hosts) in the network to 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

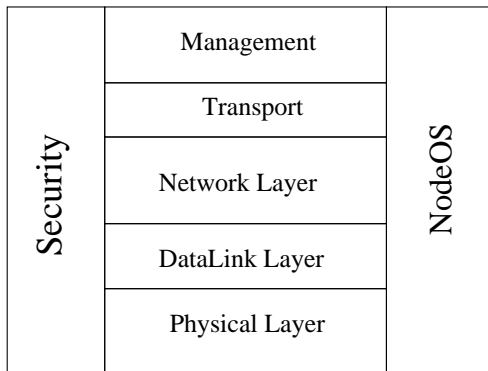


Figure 1: Network node mode

similar to the 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 node management and a

set of functions to guarantee node packet routing and scheduling. The security, which resides in all layers, is ensured by a combined effort of all layers.

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

- *Authentication of active packets* Any active packet should have authenticating credentials produced using one of a number of algorithms such as public key signature algorithms.
- *Monitoring and control* A reference monitor may be used to restrict the information, system resources and services that active packets are allowed to access and use.
- *Limitation techniques* Time limits such as the amount of time an active packet may be allowed to be executed, range limits such as the total number of nodes the packet is allowed to traverse, as well as duplication limits.
- *Proof carrying code (PCC)* For a mobile program is paired with a proof of its correctness. The active node may easily check the proof and then run the program.

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.

5.2 Communication protocol among NEs

The protocol used in this approach is responsible for dynamically dispatching delegated agents to an executing elastic server at a remote system, for controlling their execution and the

dispatchment acting upon the query. The security mechanism is scattered into all layers of the 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 somewhere between the traditional approach and the I/M-agent based distributed approaches. The difference lies in the fact that the agents in the conventional approach are too simple but the agents in some distributed NM approaches are mobile-agents or intelligent-agents, which are usually too heavy. As a result, the communication between network elements consists of transmission of functions or programs, rather than mobile or intelligent agents as in the distributed NM frameworks [4, 5, 6]. Another difference is that this approach has transferred its security checking to all the layers where the security problem can be addressed in time, whereas the I/M-agent based distributed framework addresses all the security issues in the highest layer of the protocol using some complicated authentication strategy. The way of addressing security which the heavy distributed NM approach has adopted, is not effective.

6 An active NM framework

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

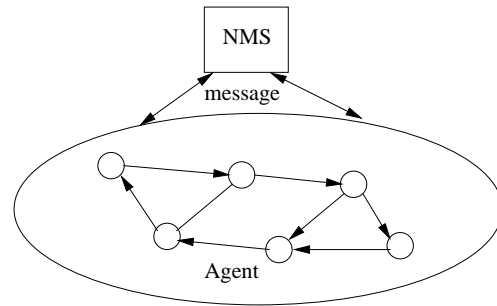


Figure 2: Active NM framework

formed closer to the data, improving speed and efficiency; (4) and it is inherently more robust without depending on continuous communications between NMS and NEs.

6.1 Communication protocols

In some situations, NEs need to send some management code or programs to each other. We refer to this as agent communication. There are some issues such as authentication.

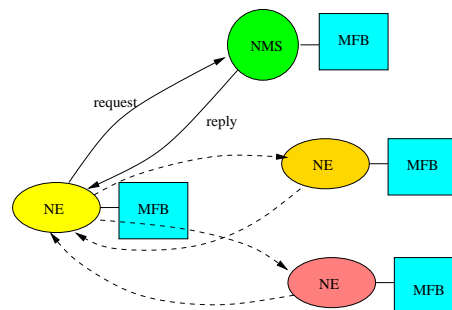


Figure 3: DNS-like protocol

The protocol used for this purpose is very much like DNS protocol which has been illustrated in Figure 3, 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 the NMS will forward the request to

those NEs which have the requested function.

- When the NE having the requested function receives the request, then the NE will send the required function to the requester NE.
- If the NMS can not find one NE which has the requested function, then it will return the NE with an error message.

6.2 Security issues

Multimedia networks are able to provide secure communication, but also timely communication. What the sender injected to the network might be significantly different than what the receiver received. For instance, a program might be sent out by a sender, the program might be run at some network components on the way to the receiver. What eventually arrives at the receiver might be the result or simple process. This has raised the complexity of security measurements.

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 to 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 6.3.

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.

6.3 Function authenticate protocol

A NE requests a trusted function. The NMS will instruct the NE which has the requested

function to the requester NE. The requester NE has to authenticate the function when the function arrives. This process is referred to as the function authentication, as shown in Figure 4. In Figure 4, there are many NEs and one NMS

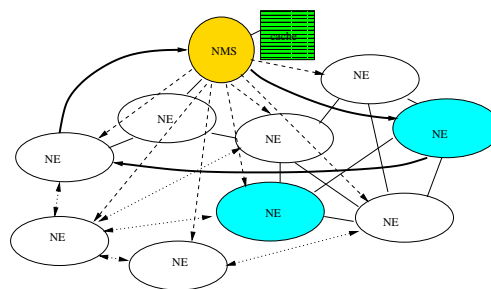


Figure 4: Authenticate protocol

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 does not have the requested function, it sends a request to the NMS, the NMS receives the message, then it authenticates the owner's identity first.
- Then the 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, the 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 the 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 issues a ticket, the ticket will be used when the NE will transmit the function to the original NE.

7 Related works

Centralized network management is based on the client/server model. This approach has pioneered network management, and there are some extensions such as the decentralized network management approaches. In this section, we will present a brief review.

In 1998, an intelligent agent-based architecture [9] was developed which integrated diverse NM processes, data analysis, and data sharing. In this approach, each agent represents a different technology, and is activated upon receiving the appropriate data or information.

Multiagent approaches to network management were proposed in 2001 [7]. The application of multiagent and artificial intelligence (AI) technologies has added some flexibility and decision making capability to NM, with many approaches focused on one aspect of NM such as fault diagnosis.

Most work on mobile agents concentrated on the application level, and thus usually neglect the need to interface with the network layer management information base (MIB).

Apparently the three research outcomes mentioned above brought the decentralisation technique into network management. They are also applicable for multimedia networks. If the features and requirements of multimedia networks are taken into consideration, however, these approaches are far from being adequate.

To date, the most closely related research in this area is HiFi [11]. HiFi is based on two models: programmable monitoring agents and event-filter-action recursive model. Using HiFi, the monitoring agents can be programmed to modify their monitoring tasks dynamically based on observed events information, and initiate the appropriate management actions accordingly.

The problem with HiFi is that the monitoring agents need to wait and see the event infor-

mation. This is basically reactive, rather than active. Our framework is that the network component is to actively activate the appropriate management functions.

8 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 multimedia network management has been proposed, which is based on active networking technology. The new approach looks at network management from the perspective that the network elements are able to execute some network management activities and to maintain their own security. The approach to self management is active rather than passive; 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 makes network management more efficient, but active networking technology has heightened the complexity of the network management, particularly in security. The proposed framework can be used as a blueprint for the development of multimedia network management tools.

In 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 Featur-*

- ing the Internet*, Addison-Wesley Computing, ISBN 0-321-17644-8.
- [3] J. A. Gutierrez and D. P. Sheridan, A Framework and Lightweight Protocol for Multimedia Network Management, *Journal of Network and System Management*, Vol. 8, No 1 March 2000.
- [4] 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.
- [5] 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.
- [6] M. Kahani and H. Beadle, Decentralized approaches for network management, *IEEE Communication Magazine*, Vol. 36 pp.66-70, March 1998.
- [7] F. L. Koch and C. B. Wetphall, Decentralized Network Management Using Distributed Artificial Intelligence, *Journal of Network Systems Management*, Vol. 9, No. 4, 2001.
- [8] S. Krause and T. Magedanz. A Survey of Distributed Network and Systems Management Paradigms, *ACM Computer Communication Review*, 27(3):pp36-47, 1997.
- [9] 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.
- [10] 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.
- [11] E. S. Al-Shaer, Active Management Framework for Distributed Multimedia Systems, *Journal of Network and System Management*, Vol. 8, No 1 March 2000.