RESEARCH ON A NEW NETWORK MANAGEMENT PROXY BASED ON MULTI-TECHNOLOGY NETWORK MANAGEMENT

MORTAZA MOKHTARI NAZARLU

Computer group, Islamic Azad University, Maku Branch, Maku, Iran
mortezamokhtari@ymail.com

ABSTRACT

The main protocol that is currently used for managing computer networks is known as SNMP. The main advantages of applying this protocol in computer equipments and networks are its simplicity and widespread usage. Nevertheless, despite these advantages, using this protocol will be faced with serious challenges, especially in networks with a wide range network devices and high traffic rate. There have been provided several techniques in order to overcome problems of the protocol, which one of the best available techniques is a standard under name MTNM that it has been proposed as a solution suite and it has been formed according to distributed architecture, COBRA. This article aim is to provide designing and implementing a proxy based on such a standard. The main task of the proxy is to exploit data by using SNMP commands, in order to locate at available data structures in MTNM solution suite. The results analysis will show the better performance of the proxy than SNMP protocol, based on volume of traffic produced and run time.

KEYWORDS

Network Management, SNMP protocol, CORBA, MTNM Solution Suite v3.5, Distributed programming

1. INTRODUCTION

In recent years, structure and application of computerized networks have been considerably changed, as which it has been possible to support wider range of technologies in a network only. Technologies such as TVIP and VOIP are examples from this type. Generally, networks which they are not limited to a special technology and include wider range of different technologies are called next generation networks (NGNs). Providing the above mentioned new technologies in a unit network (next generation networks) due to decrease manufacturing and maintaining costs of different private networks for different technologies, but it results emerging new dimensions of complexity.

And the networks' management and their accurate performance managing are very important because emerging these complexities. Management concept is based on SNMP protocol in one of the main loops in next generation networks, i.e. network based on TCP/IP stack protocol.
This protocol is located at the application layer and it uses UDP protocol for data transmission. This protocol is widely used in network equipments because of high-speed implementation, low memory consumption and ease of use. Despite enjoying these advantages, the following can be cited as problems in this protocol: need to exchange many messages to transmit huge volume of management data, weak encryption method, long prefix in OIDs naming schema, weak security

DOI : 10.5121/ijmnct.2012.2601

mechanisms, lack of a mechanism to overcome increasingly managerial data, monitoring is not notification driven and centralized management method [1][2].

In fact, the protocol problems are as which its usage in next generation networks result serious challenges, by considering to high volume produced traffic in such networks. A main approach for managing network based on TCP/IP stack protocol, as one of infrastructures of next generation networks and solving SNMP protocol problems, is to use standard interface technique. Standard interfaces are key identities in heterogeneous networks management, because they decrease costs of adding infrastructures and they facilitate operations. In addition, they solve no scalability problems and provide framework independence. COBRA is one of the best middle wares, which it has been formed, based on clear interfaces. MTNM solution suite is one of the best standards, which it has been formed based on COBRA architecture, which it has been provided for managing next generation (heterogeneous) networks.

Finally, this standard is a set of IDL files, which they have been defined by CORBA architecture [3]. The considered solution in this paper is also based on this standard, which it includes designing a proxy for extracting data by SNMP commands, in order to locate in available data structures in MTNM solution suite. In fact, the proxy is an interface between the implemented SNMP protocol on network equipments and management systems.
This means that the proxy is an effort to implement some of defined interfaces in the MTNM standard, by using SNMP commands.

In the second part of this paper, we will introduce the proxy structure, and we will deal with how to cover SNMP protocol problems by the proxy, benefit from advantages of using CORBA middleware and it's based on standard i.e. MTNM solution suite, as well as how to cover requirements of next generation networks.

The third section presents the results of the proxy testing, and we will refer to its strengths. In the fourth section, we present conclusions and we will introduce useful cases, which they can be used as applicable issues in other studied papers.

2. THE PROXY ARCHITECTURE

The considered proxy has been designed and implemented based on MTNM standard and CORBA middleware.

Obviously, the designed proxy has a distributed nature due to distribution nature of CORBA middleware. In other words, in conducted relation between the agent and the manager in higher layer, the designed proxy can whether be located on the agent side (on the agent computer) or it can be located on the manager side. Of course, any both states are not necessary and the proxy can be located between the manager and the agent, with any way and distance, although for maximum exploiting from the proxy advantages, locating it in the agent side (or minimum distance from the agent) will provide better results.

In Fig.1 overview of how the proxy is located on the agent machine is shown.

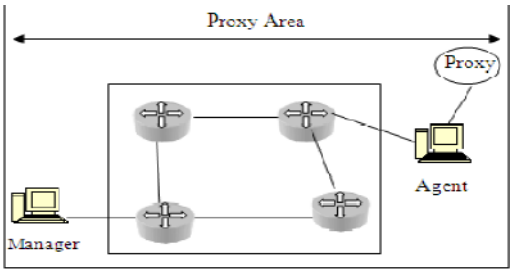

Figure 1. Relation scheme and location of the proxy

The main purpose of this proxy is to enjoy abilities of existing managerial tools and protocols as well as to overcome their constraints. Overall, it can be achieved three groups of benefits in implementation of the proxy that they will be studied in the following.

The first group of advantages of the proxy implementation is about solving problems of SNMP protocol. Some of SNMP protocol problems are solved by using the proxy because of locality characteristic. Here, locality means implementing the proxy on a system that it is appeared in the agent role and supports SNMP protocol, or it is implemented on a system which it is connected to the considered system through a broadband and secure network. In other words, as the proxy can be implemented on any system with any distance, but it is necessary to run it locally for covering SNMP problems. Problems' list and their solutions by locality characteristic are as the following.

2.1. Exchange large number of messages problem to send data

Use of SNMP protocol BULK transfer commands for transmission of a table in certain circumstances need to exchange large number of control messages between the manager and the agent that it reduces efficiency and waste network resources [4].

In the other word, sometimes a manager uses try and error method for identifying right size of a table row, which carrying out the try and error method provides a heavy burden for the manager, network and the agent, and in addition, it results exchanging a large number of SNMP protocol messages. Local implementing the proxy solve the problem partly because exchanged messages between the agent and the proxy have shorter distance, and as a result, lower costs are paid for transmitting messages. Next step is to send information to the manager by the proxy. In this section, received data by the proxy do not have a particular problem for sending to the managers because the method of sending data is TCP protocol. One of the main features of this protocol is to send information packets, as a string of continuous bytes.

In other words, there is no limitation on packet size in this protocol because if it is necessary, the protocol converts packages into smaller pieces and then convert the packages to initial state in destination. In addition, if needed, it can integrate information packages for making larger ones.

Generally, it can be said that the manager and the agent do not have any worry regarding size and accuracy of packages in CORBA architecture because TCP protocol carry out it automatically.

2.2. Poor data encoding problem

SNMP protocol uses method is known as the BER for data encoding. The most obvious features of this method include shorter code, algorithm simplicity and low memory consumption.

Nevertheless, unfortunately this method has important problems. Main problem of the method on the agents and the managers is to impose high overload and increasingly memory consumption during encoding and decoding data.

Another problem is to increase administrative data (identifier and length) in compared with payload(content), which leads to efficiency reduction and increasing data transmission delay [5][6].

Like the previous section, solving encoding problem has two aspects. One aspect is to receive data from the agent by the proxy; this problem through local property can generally be resolved or reduced. In fact, Locality property causes lesser cost paid for transmitting administrative data, because this data will traverse shorter distances.

The second aspect is to send data by the proxy to the manager. The proxy uses CDR encoding for sending data to the manager. By using this encoding method, without copying data for marshaling/unmarshaling, we can access directly to the binary representation of data in memory. By doing so, marshaling / unmarshaling process could be run faster and overload of copying data will be avoided. Data length and data type will not transmitted with content and this is one more reason that CDR to be superior to BER, because this causes to save more bandwidth for user data.

2.3. Using long prefix for OID naming schema

Part of this problem depends on SNMP protocol to communicate with the proxy that could be resolved through local property or closing the gap between the proxy and SNMP protocol. However, like the previous problems, the relationship between the proxy and SNMP protocol is only half the work.

The other part is to work with the proxy and the managers' connection.

This part of the problem is solved primarily because the connection between the managers and the proxy is not based on tree structure, so we can easily remove object identifiers (OID) and don't send them to the manager.

2.4. Unreliable transfer protocol

There are two methods to solve this problem in communication of SNMP protocol and the proxy. In the first method, the proxy can be executed locally on the agent to fully eliminate problems about sending data by using unreliable UDP protocol.

In the second method, the proxy can be connected to the agent through bed of a high speed and secure network. But it cannot be solved problem entirely by this method because the messages must go a part of network by UDP protocol, depending on the proxy and the agent distance.
In fact, the smaller distance between the proxy and SNMP protocol, the lower possibility lacking packages.

2.5. Weak security mechanisms

It must be used from TCP protocol instead UDP protocol for solving security problem. In other words, there must be implemented the proxy on the agent locally and information are send to the managers by TCP protocol. One reason is TCP to be superior than UDP from the security aspect is related to firewalls configuration and recognizing the authorized sender from the forge sender.

TCP is statefull and because of this property is safer than UDP.

This property is achieved by sequence numbers in PDUs. Actually, by using sequence numbers, firewalls could recognize authorized senders from the forge senders. Additionally, set the SYN field and clean the ACK field in TCP protocol PDU causes external managers could not start to establish a connection with the agents behind the firewalls.

In addition to the security mechanisms that devised in TCP, some security benefits could be achieved from the CORBA middleware and MTNM solution suite. For example SSL as one of the underlying security protocols of CORBA could be used for encryption/decryption and some methods in IDL files of MTNM could be used for authentication [8] [9].

The second group of the proxy advantages is rooted in its infrastructure architecture i.e. CORBA middleware. Benefits of the middleware that is available in MTNM standard include: modularity, separating interface from implementation, using reliable TCP protocol, interaction ability between written programs in different languages, rapid and low cost development of programs, enjoying advantages of distributed systems and overcome to problem of nonscalability and increase transparency and simplify for finding problems [8].The third group of advantages of designing the proxy rooted in the TeleManagement Forum, especially MTNM standard.

To summarize, the main characteristics of the standard include: standard importance and its following, wide support for all activities necessary for network management, high chance using by service providers, full compliance of managerial data of equipments network with TMF814 modules [1][9].

3. THE RESULTS ANALYSIS

In this section, we are going to compare the designed proxy with SNMP protocol from amount of network bandwidth consumption and generated traffic point of view. There can be obtained useful matters from the comparison that will led to emergence of positive aspects of the proxy.
There has been used from a command under name SNMPWALK to compare both. Our test methodology is as the following: first, we will run the SNMPWALK instruction directly by the SNMP protocol for a specific amount of data and then, we will run this instruction (SNMPWALK) by using the proxy for the same amount of data.

Actually at first, this instruction will run directly on the agent by the SNMP protocol and then it will run indirectly by the proxy. By repeating this process several times for different amounts of data, we will collect enough information in order of comparing the results.

In the first step for collecting results, a typical computer has been used for testing. Here is a typical computer means a system with specified size and relatively low volume of managerial data. This low volume is approximately equal with 4000 OIDs that they are exchanged as 4000 messages by SNMP protocol.

Result of implementing the volume of managerial is represented the first row of tables.1 and 2 by using SNMPWALK command (direct method) as well as based on proxy (indirect method).
Protocol hierarchical structure for 4000 OIDs as based on direct method is represented in table.3, and protocol hierarchical structure for 4000 OIDs as based on proxy method is represented in table.4.

By considering to the first row in tables.1 and 2, as well as by considering to structure of available protocols in tables.3 and 4, it can be resulted that the generated traffic volume is more in

based on proxy method, despite to the matter that number of the exchanged packages in indirect method is lower than direct method.

Actually, the TCP protocol can transfer more amount of data in just one packet than UDP so we can see the number of packets is decreased in first row in table.2, however because of its' control mechanisms and bigger size of packets, it produces more data than UDP.

Taking into account table.4, we can see About 22 percentages of produced traffic of TCP protocol are belonged to one of its underlying protocols that known as GIOP.GIOP is used as the infrastructure protocol of CORBA programs and establishes the connections between the parties. The produced traffic for 4000 OIDs in based on proxy method is more than SNMP-based; even though close our eyes on the produced traffic by GIOP protocol.
We repeat the experiment in another case for 8000 OIDs. Results of the case are shown in second row of tables.1 and 2, with direct method by using SNMPWALK, as well as indirect method by using the proxy.

It is clear that the generated traffic volume by the proxy is more than direct method, but by comparison, the first and second rows, we can see that distance of the generated traffic volume in direct method and based on proxy has been decreased and their amount are closed together. Because difference the generated traffic volume between direct and based on the proxy for 4000 OIDs is approximately 664940 bytes, while the difference for the 8000 OIDs is about 414415, which it represents decreasing difference between both.

Table 1. Overall evaluation of direct and based on proxy methods according to the traffic and run time

OIDs	Direct Method Traffic (Byte)	Direct Method Run Time (Second)	based on proxy Method Traffic (Byte)	based on proxy Method Run Time (Second)
4000	768101	5.741	1433041	9.102
8000	1459012	11.840	1873427	10.389
12000	2176259	16.158	2092119	14.073
16000	3020741	21.369	2252261	17.896
20000	3713570	27.059	2412154	21.444
24000	451051	34.554	2654032	27.883
28000	5194785	40.375	2843591	33.956
32000	6013756	46.475	3183589	45.410
36000	6675602	52.589	3271064	49.005
40000	7326113	59.999	3467667	49.009
44000	8217889	64.649	3744994	52.250
48000	8919880	68.111	4107998	59.750

Table 2. Overall evaluation of direct and based on proxy method according to number of packets

OIDs	Direct Method	based on Proxy method
4000	8161	1767
8000	15529	2220
12000	23167	2558

Table 3. Protocol hierarchical of direct method for 4000 OIDs

Protocol	Percentage
-Frame	100
-Ethernet	100
-IP	100
-UDP	99.99
-SNMP	99.96

Table 4. Protocol hierarchical of based on proxy method for 4000 OIDs

Protocol	Percentage
-Frame	100
-Ethernet	100
-IP	100
-TCP	100
-GIOP	21.51

Now if number of OIDs is increased to 12000 and again we repeat the test by previous methods, results are very interesting. Results of this experiment are shown in Tables.1 and 2 in the third row. As shown, the generated traffic by method based on the proxy has been reduced 84140 bytes in comparison with the direct method. In addition, the required time to perform the desired operation has been significantly improved.

Now if we perform the test for greater volume of data, then advantages of based on proxy method on direct method will be gradually revealed. In the rows after fourth row of Table.1, it has been presented results of this experiment for a wide range of data. Fig.2 shows the relevant diagrams for both direct and based on proxy methods, which it verifies our claim.

As shown in Fig. 2, the generated traffic for high volumes of data are increased linearly in based on proxy method, while this claim is not available for direct method, because direct method diagram is increased exponentially by increasing the exchanged data, while the based on proxy diagram in high volumes is increased with a fixes coefficient and it is approximately linear. The main reason that causes SNMP based method has better performance than based on proxy method for low volumes of data is related to its start up time.

In other words, in based on proxy method, some of the generated traffic is considered for setting up the session between the manager and the agent as well as implementing the considered services, but the direct method does not generate these additional data.

Fig.3 shows the required time for execution, in direct and based on proxy methods. About this Fig. it can be said that in high volumes executions, based on proxy method has better performance in compare with direct method, because number of the exchanged packages in this method is lower than the other one, which it lead to reduce execution time.

Of course, in Fig.3, time chart of both is very close together, but it is because that distance between a system with implemented manager and the proxy was only one node. Now if we increase this distance as well as number of mid nodes, better performance of the proxy will be seen in time point of view. Of course, in the state, the proxy and the agent are located on one machine, which it leads to improve performance in time point of view.

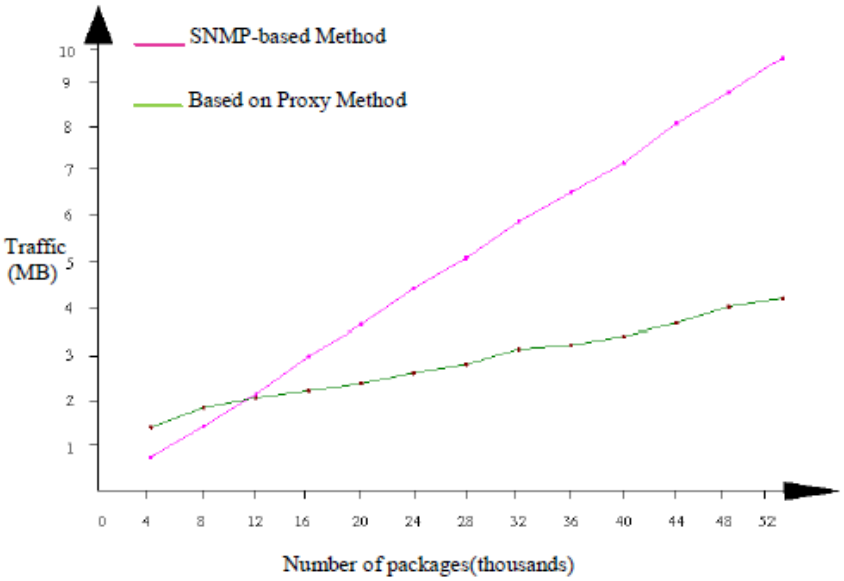

Figure 2. Evaluation diagram of the generated traffic in direct and based on proxy methods

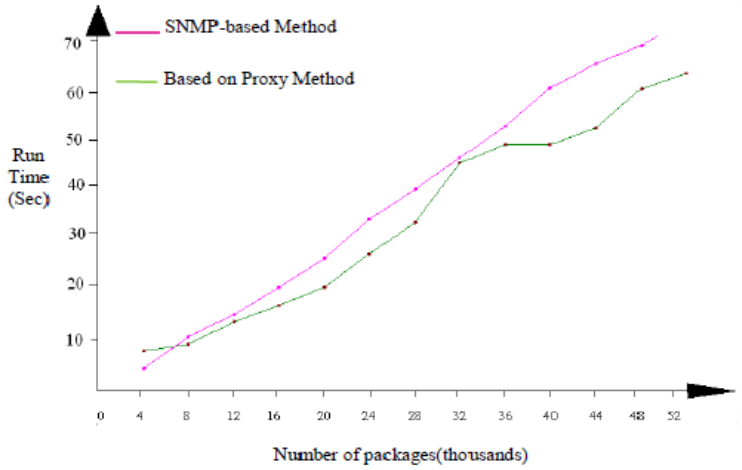

Figure 3. Evaluation diagram of run time in direct and based on proxy methods

4. CONCLUSIONS

As it was observed, local property of the proxy can solve problems in SNMP protocol. In addition, one of main problems of the SNMP protocol, namely no scalability problem that is important in next generation networks is covered and solved by CORBA distributed feature, which it is available in the proxy too.

Evaluation results showed that in low volume generated data, using directly SNMP protocol had better performance and less traffic than the proxy did. Nevertheless, if volume of exchanged data is increased, the proxy advantages over direct implementation will be revealed, a matter that surely will occur in the next generation networks.

In other hand, by upgrading the proxy from the agent level to the network level, volume of sent data will be considerably increased, and using direct method lose its efficiency, which it leads to many problems such as no scalability. In these conditions, using method based on proxy who it is a scalable and suitable solution for high volumes of data can overcome these problems well. Finally, the following matters can be pointed out for increasing quality level of the designed proxy: upgrading the proxy from agent mode to network mode, increasing security level, more benefit from distributed advantages in the proxy design, increasing implemented methods, further reforms on data structure.

REFERENCES

[1] Laxman.D, (2006) "Efficient Network Management Using SNMP", Journal of Network and Systems Management, Vol. 14, No. 2, pp189-194.
[2] Martin-Flatin J.P, (2004) "Distributed Event Correlation and Self-Managed Systems", 1st International Workshop on Self- Properties in Complex Information Systems (Self-Star), pp 61-64.
[3] TM Forum (2008), MTNM Solution Suite v3.5, teleManagement standard.
[4] Martin-Flatin J.P, (2001) "Web-Based Management", Journal of Network and Systems Management, Vol. 9, No. 1, pp. 11-13.
[5] Martin-Flatin J.P, Znaty.S, Hubaux.J, (1999) "A Survey of Distributed Enterprise Network and Systems Management Paradigms", Journal of Network and Systems Management, Vol .7, No 1, pp21-28.
[6] Martin-Flatin J.P, (2002) Web-Based Management of IP Networks and Systems, New York: Wiley, pp.15-34.
[7] Mauro.D, (2000) Essential SNMP, New York: O'Reilly, pp11-25.
[8] Aleksy.M, (2005) Implementing Distributed Systems With CORBA and JAVA, New York: Springer, pp13-45.
[9] Luciani.L, Riedel.M, (2010) "TMF814 Network Simulator", Ph.D. dissertation, Chalmers University of Technology.