

SERVER CONGESTION CONTROL AND REDUCTION OF SERVER POWER CONSUMPTION WITH DPI TECHNOLOGY

Shin-ichi Kuribayashi

Department of Computer and Information Science, Seikei University, Japan

ABSTRACT

Deep packet inspection (DPI) technology has conventionally been introduced for traffic monitoring, bandwidth control, access control of specific types of traffic, etc. As a new potential application of DPI technology, this paper proposes three promising approaches of network and server control with DPI technology, and presents implementation examples of two approaches. These approaches could simplify dramatically the conventional work load for system management and reduction of power consumption by servers and accelerate the control action.

First, this paper proposes an example of server congestion control method, in which the DPI equipment estimates the CPU usage of each server by constantly monitoring the number of TCP live connections established by each server, and moves some of virtual machines on the congested server to other servers through remote control timely. Next, this paper proposes an example of reducing power consumption by servers, in which the DPI equipment constantly monitors the traffic sent or received in each area with multiple servers. Finally, the feasibility of the proposed approaches is demonstrated by an evaluation system with a real DPI equipment.

KEYWORDS

Deep packet inspection, congestion control, reduction of power consumption

1.INTRODUCTION

Deep Packet Inspection (DPI) has been a very important research topic within the traffic classification field. Its concept consists of the analysis of the contents of the captured packets in order to accurately and timely discriminate the traffic generated by different Internet protocols. That is, DPI monitors the data parts (payloads) of IP packets and to determine the type of processing to be applied to packets, such as filtering, based on the content of the payloads [1],[2]. A variety of data, such as email messages and videos, are exchanged using HTTP in the internet. DPI can inspect URLs, content of messages, and packet information that is at a layer higher than that for information used for conventional packet filtering. This capability of DPI also makes it possible to take more finely tuned security measures than before, such as detection of viruses that attempt to invade using HTTP or prevention of information leakage in enterprises.

DPI technology has conventionally been introduced for traffic monitoring, bandwidth control, bandwidth allocation, control of specific types of traffic, etc [3],[4]. A lot of service providers are adopting the DPI equipment for securing the visibility of the data traffic, due to the dramatic increase of data traffic in mobile networks [5]. For example, peer-to-peer (P2P) traffic would give ISPs a great deal of trouble and DPI allows the ISP to perform traffic control and bandwidth allocation.

In recent years, there have been intense studies to use DPI to enhance charging (charging based on usage or data content, etc.) or security (identifying types of traffic and encrypting them accordingly, etc.). There have also been studies to combine DPI with different technologies in order to identify types of traffic and use this information for behavior-based targeted advertising [4], in which sites browsed, products purchased, or search key words used by Internet users are collected and analyzed.

DPI equipment installed at any arbitrary point in a network can monitor communications of many servers simply and analyze the type of processing to be applied to packets without packet capture tools and skilled engineers in every server. This could simplify dramatically the conventional work load for system management and reduction of power consumption by servers and accelerate the control action. Moreover, DPI functions can be virtualized and deployed on commodity hardware as a piece of software with Network Functions Virtualization (NFV) [5]. It enables to rapidly scale up (or down) the deployment of DPI functions economically [6], as it only requires the installation of virtual appliances on existing server equipment.

This paper explores the possibility of applying DPI technology to the server control and the reduction of power consumption. The rest of this paper is organized as follows. Section 2 explains related works. Section 3 proposes three promising approaches of network and server control with DPI technology. Section 4 proposes an example of server congestion control with DPI technology and demonstrates it by the evaluation system with a real DPI equipment. Section 5 proposes an example to apply DPI technology to the reduction of power consumption by servers and demonstrates it by the evaluation system with a real DPI equipment. Section 6 presents the conclusions. This paper is an extension of the study in Reference [18].

2.RELATED WORK

Reference [3] summarizes potential uses of DPI technology as follows:

- Network security: DPI's ability to inspect data streams at such a granular level will prevent viruses and spyware from either gaining entrance to a network or leaving it.
- Network access: DPI creates conditions where network access rules are easy to enforce due to the deep inspection of packets.
- SLA enforcement: ISPs can use DPI to ensure that their acceptable use policy is enforced. For example, DPI can locate illegal content or abnormal bandwidth usage.
- QoS: P2P traffic gives ISPs a great deal of trouble. DPI would allow the ISP to instigate traffic control and bandwidth allocation.
- Tailored service: DPI allows ISPs to create different services plans, which means users would pay for a certain amount of bandwidth and traffic priority.

- DRM enforcement: DPI has the ability to filter traffic to remove copyrighted material. There's immense pressure from the music and movie industries to make ISPs responsible for curtailing illegal distribution of copyrighted material.

Reference [6] has proposed a network management system with DPI server which supports the network management system to classify the network traffic. For example, if the DPI equipment finds that the user id of the VoIP session is in the black list, the DPI equipment informs the NMS about this SIP session. Then the NMS configures related switches to intercept that VoIP session. Reference [5] has proposed to apply DPI technology to the CDMA mobile network packet switch domain and constructed a DPI based network traffic monitoring, analysis and management system. References [7] and [8] has presented a technical survey for the implementation and evaluating of traffic classification modules under a common platform. Reference [9] has proposed a method that enables to find out a DPI engine deployment that satisfies the trade-off between the minimum number of engines and the minimum network load for a considered set of costs and operational constraints. Reference [10] has described the hardware and software components of the platform of DPI with its four utilization fields. Reference [11] has proposed a method, based on genetic algorithms, that optimizes the cost of DPI engine deployment, minimizing their number, the global network load and the number of unanalyzed flows.

Most of these studies mainly try to restrict transfer of specific types of traffic. To the best of our knowledge, applying DPI technology to server congestion control and the reduction in server power consumption has not been fully studied.

3.THREE PROMISING APPROACHES OF APPLYING DPI TECHNOLOGY TO NETWORK AND SERVER CONTROL

Today, identifying the types of application used in each server in a data center requires sophisticated processing and a considerable workload. For example, it is necessary to introduce a packet capture tool in each server and to have skilled engineers analyze packets used by different applications. DPI can simplify this, because it is possible to analyze in detail the content of data that flow in the network just by installing DPI equipment at any arbitrary point in a network. There is no need to introduce a packet capture tool and skilled engineers in every server. It is easy to identify the type of application used and the characteristics of its traffic, such as communication content and communication time. It is performed without any access to individual servers. In addition, DPI makes it possible to simultaneously monitor many servers scattered over a wide area and control the network from a network-wide perspective.

Three promising approaches of applying DPI technology to network and server control are as follows:

<Case 1> Server Congestion Control

An image of server congestion control with DPI technology is illustrated in Figure 1. The DPI equipment in the network monitors traffic related to server #1 and estimates the following values:

- CPU utilization of server #1 and VM in the server #1
- Utilization of bandwidth used for server #1

For example, if DPI equipment monitored traffic related to server#1 and estimated that server #1 is in a congested state, the following actions could be taken to maintain QoS:

- Move virtual machine on the congested server to other uncongested servers (① in Figure 1)
- Reduce the bandwidth available to virtual machine that is causing the congestion (② in Figure 1)

This approach could simplify dramatically the conventional work load for system management and accelerate the control action.

<Case 2> Reduction Of Power Consumption By Servers

Server administrators need to handle considerable workloads if they monitor traffic and instruct maintenance staff to put the server concerned to sleep mode or shut it down, upon detecting absence of traffic (except for monitoring packets) in a server for a certain period. If a DPI equipment is applied instead, the communication states of many servers can be monitored easily and timely from a single point in the network, and, based on that information, servers that are not handling traffic can be put in sleep mode or shut down automatically through remote control.

An image of reduction of power consumption by servers with DPI technology is illustrated in Figure 2. In this example, the DPI equipment installed in the network constantly monitors the volume of traffic carried in areas A, B and C. Each area has multiple servers. When the DPI equipment detects an area that carries no traffic except for monitoring packets, it either puts all servers in the area to sleep mode or shut them down. On the contrary, DPI equipment remotely turns on the server with Wake-on-LAN (WOL) [12], when it monitors the start of traffic flow to the server. This approach could reduce power consumption simply and timely, compare with the conventional method with maintenance staffs.

<Case 3> Link Congestion Control In The Network

An image of link congestion control with DPI technology is illustrated in Figure 3. The DPI equipment in the network monitors traffic flows and estimates the utilization of each link on the route. If the utilization exceeds the threshold, DPI equipment judges the risk of link congestion and makes a preparation for detouring specific flows on another non-congested route. Assuming SDN-based network [13],[14], DPI equipment requests SDN controller to set flow entries at each SDN node (switch) on the alternate route. Then, node x in this example detours specific flows to the alternate route and it could avoid link congestion. These approaches can avoid link congestion in the network simply and timely, compare with the conventional method with maintenance staffs.

Implementation examples of the above two cases, case 1 and case 2, are proposed in Section 4 and Section 5 respectively.

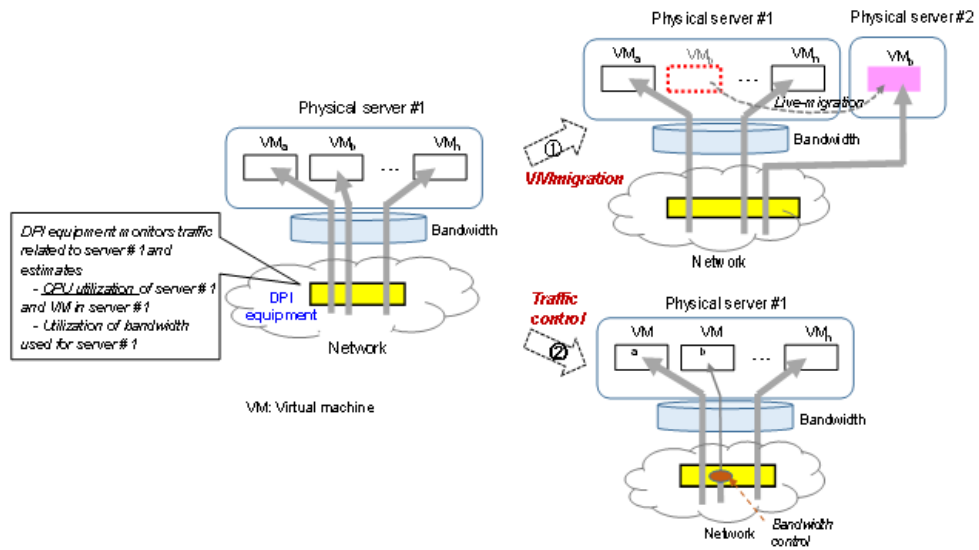


Figure 1. Image of server Congestion control with DPI technology(Case 1)

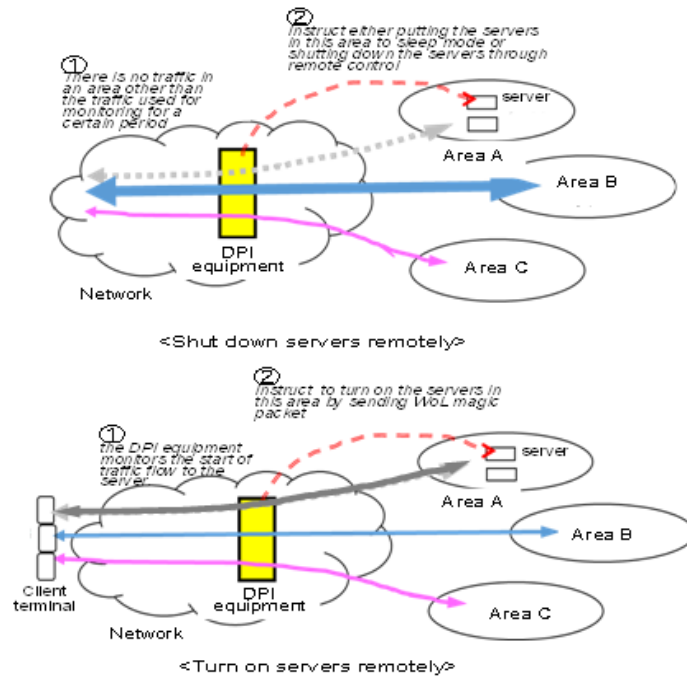


Figure 2. Reducing power consumption of server with DPI technology(case 2)

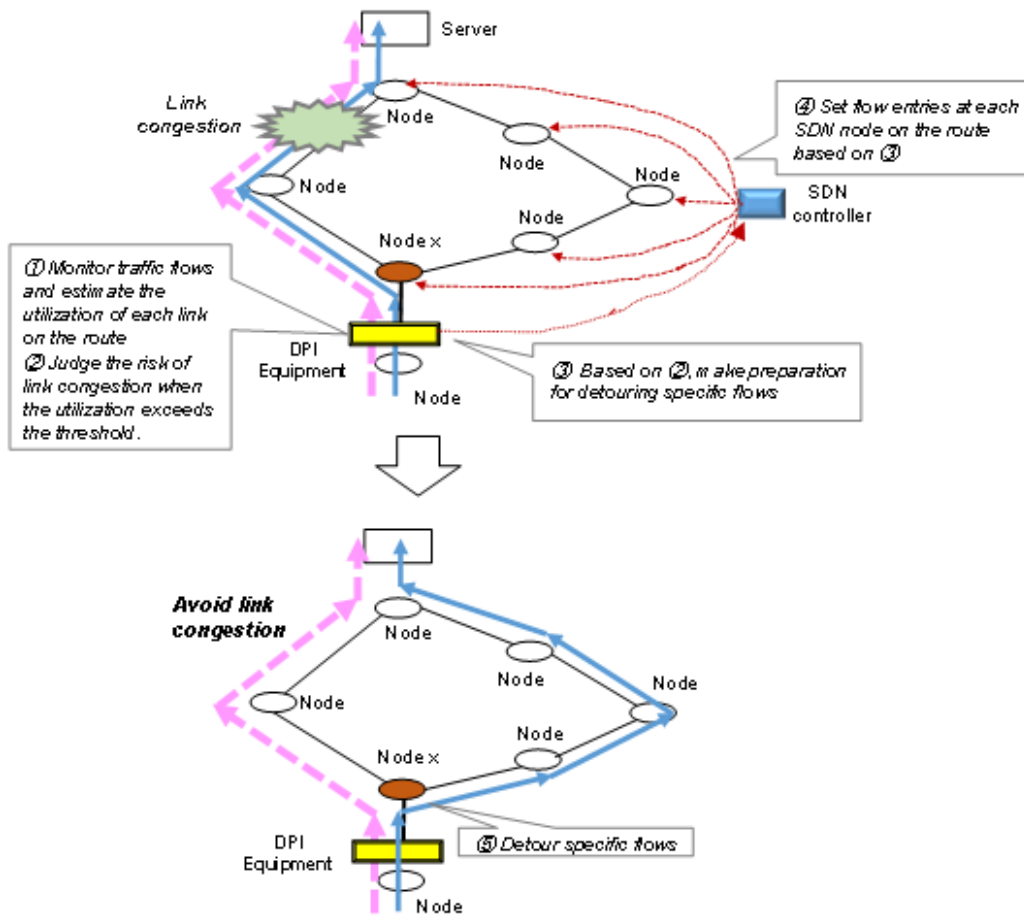


Figure 3. Image of link congestion control by detouring specific flows(Case 3)

4. SERVER CONGESTION CONTROL WITH DPI TECHNOLOGY

4.1 Example of server congestion control method (Example of Case 1)

Applications could be classified into a 'bandwidth type' (applications that use a large bandwidth) and a 'transaction type' (applications that demand high CPU usage). As for bandwidth type, DPI equipment can estimate applications and bandwidth used for each server. For example, if the amount of bandwidth for videos exceeds a certain threshold, it is possible to reduce bandwidth for the server which handles videos. The monitoring example of traffic volume of each application is illustrated in Figure 4. In this example, the traffic volume of HTTP download exceeded the threshold and it is required to reduce bandwidth to the VM (virtual machine) which processes HTTP download application.

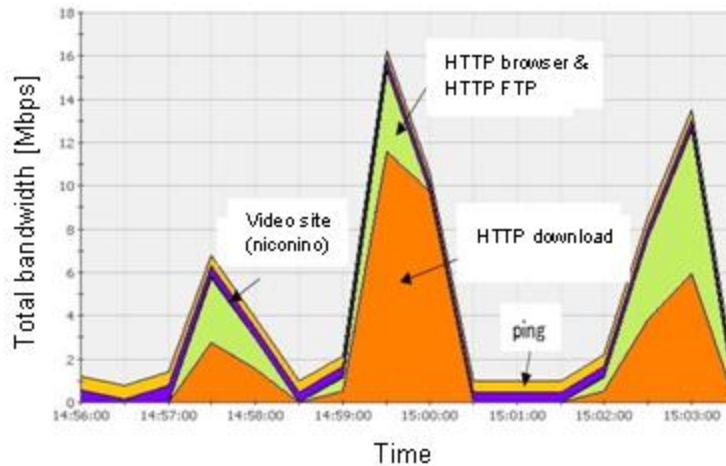


Figure 4. Total bandwidth measured by DPI equipment

As for transaction type, the following procedure is proposed, assuming the scenario in Figure 1. It is also assumed that DPI tool installed in the network monitors and controls a physical server (server #1) in which a number of virtual machines are implemented. A detailed processing flow is shown in Figure 5.

<Step 1> The DPI equipment monitors the type (video on demand (VoD), peer-to-peer (P2P), Web access, etc.) of application running on each virtual machine in server #1. It is assumed that the DPI equipment knows in advance the relationship between the number of transactions and CPU utilization in server #1.

<Step 2> The DPI equipment constantly monitors the number of transactions handled in server #1 per unit time. If the number exceeds a certain threshold (which is preset for each physical machine based on its normal usage) for more than a certain period, the tool determines that the service is in an overload state. It either moves the VM associated with the specific application (e.g., VoD, P2P) responsible for the overload to another physical server (server #2) (① in Figure 1). Alternatively, if that is not possible, the tool reduces the bandwidth used by the traffic to and from the VM (② in Figure 1). These measures can resolve congestion in server #1.

<Step 3> The DPI equipment continues to monitor the number of transactions on server #1 constantly. When the number goes down below the threshold, the tool releases the restriction imposed in Step 2 above.

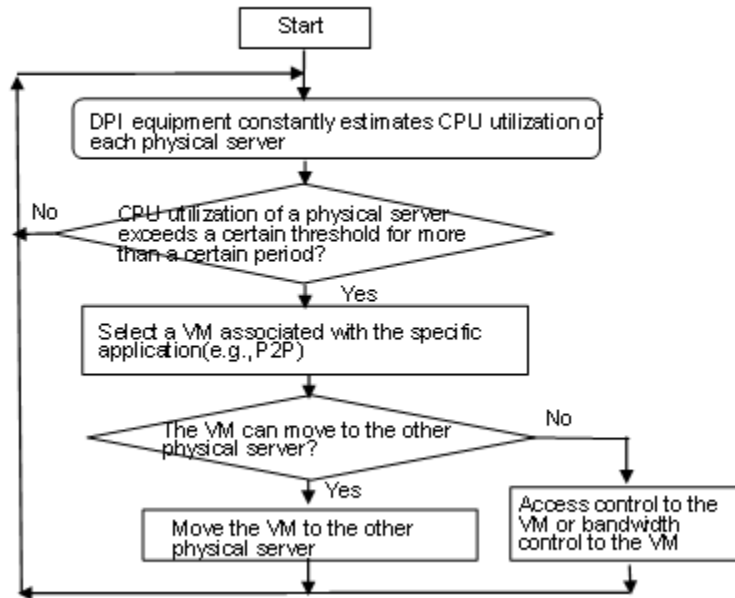


Figure 5. Processing flow of the proposed server congestion control with DPI technology

4.2 Evaluation of the proposed server congestion control method

(1) Evaluation system

To evaluate the server congestion control method proposed in Section 4.1, the evaluation system shown in Figure 6 is constructed. NetEnforcer AC-502 [15] from Allot Communications is used as the DPI equipment. A software program (NetXplorer) that monitors AC-502 is installed in an NX server. As AC-502 is not able to collect the number of transactions per unit time in each server, the number of TCP live connections per unit time is used estimate CPU usage instead. Every minute AC-502 measures the number of TCP live connections between the client terminal and the source server. This information is collected by DPI tool (software) that is installed in the NX server.

Figure 7 illustrates the actual evaluation system constructed. Dell PowerEdge T110 with Windows Server 2008 is used as NX server, and Dell Vostro3350 (Intel Core i3, CPU 2.27GHz) is used as client terminal and servers. VirtualBox [16] is used as a virtual system, and both host OS and guest OS are Windows 7.

(2) Effectiveness of using the number of TCP live connections

An example of the relationship between the number of TCP live connections (Web-based applications with TCP) and the CPU utilization in the source server is shown in Table 1. This example shows a high coefficient of correlation (around 0.9), indicating a good possibility of determining the degree of server congestion from the number of TCP live connections.

(3) Evaluation of the proposed server congestion control method

The operation of the proposed method was verified under the following conditions:

- 1) The evaluation tool monitors the number of TCP live connections every minute in source server.

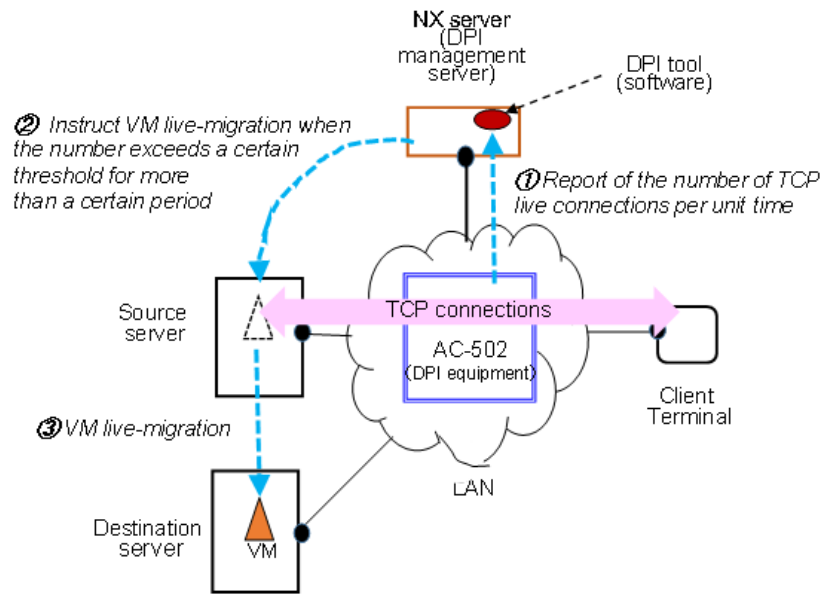


Fig 6. Configuration of evaluation system

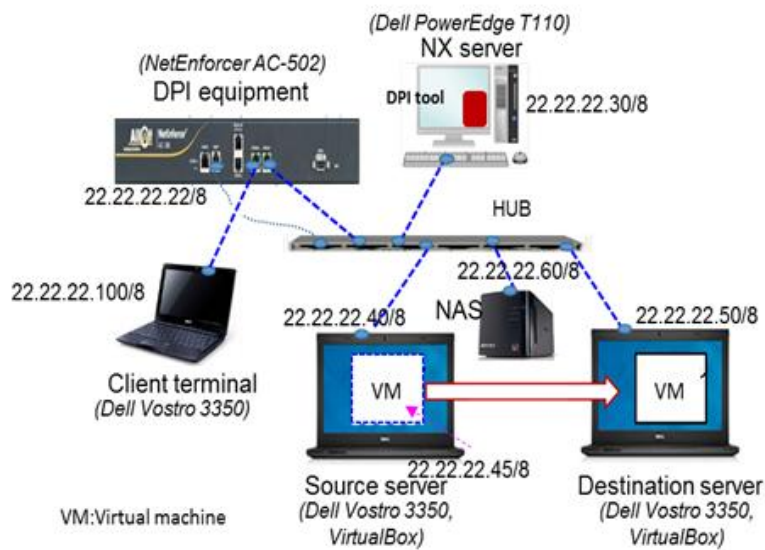


Figure 7. Overview of developed system for evaluation

Table 1.Example of measured CPU utilization

Number of TCP live connections	CPU utilization
30	55%
35	62%
42	70%
55	78%
55	82%
69	85%
75	90%

2) When the number of TCP live connections exceeded 55 (this is determined based on data in Table 1) continuously for 3 minutes on end, a VM on the source server is moved (live-migration) to destination server. The evaluation tool installed in an NX server remotely instructs both the source and the destination server to migrate virtual machines, with PsExec[17] from Microsoft.

It is confirmed that the proposed method operated as had been expected, and it means that DPI technology can allow the server congestion control without packet capture tool and skilled engineers in every server.

(4) Scalability of the proposed method

As mentioned in Section 1, DPI functions can be virtualized and deployed only at the time when needed with NFV. It enables to rapidly scale up (or down) the deployment of DPI functions in the network economically, as it only requires the installation of virtual appliances on existing server equipment.

5. USE OF DPI TECHNOLOGY FOR REDUCTION OF SERVER POWER CONSUMPTION

The proposed method of reducing power consumption by servers is explained with Figure 2. The DPI equipment installed in the network constantly monitors the volume of traffic carried in areas A, B and C. Each area has multiple servers. When the tool detects an area that carries no traffic except for monitoring packets, it either puts all servers in the area to sleep mode or shut them down. This reduces power consumption by servers in that area simply and timely, compare with the conventional method with maintenance staffs. Figure 8 illustrates a processing flow of the proposed method.

The proposed method was evaluated by reusing the evaluation system described in Section 4 under the following conditions:

- Instead of source and destination servers in Figure 7, three servers (each represents one area) are added to the evaluation system.

- The DPI equipment constantly monitors the volume of traffic carried in each area. If it detected an area where there was no traffic (except for monitoring packets) for 10 minutes or longer, it remotely shut the server down with PsExec [17] from Microsoft.

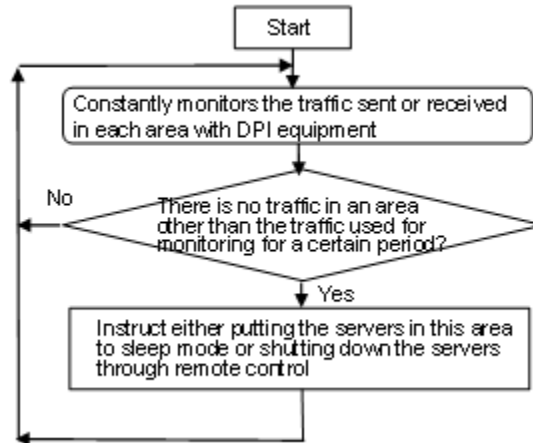


Figure 8. Processing flow for reducing power consumption of server with DPI technology

It is confirmed that power consumption is reduced as had been expected. Moreover, it is also confirmed that DPI equipment can remotely turn on the server with WOL technology.

6. CONCLUSIONS

As a new potential application of DPI technology, this paper has proposed three promising approaches of network and server control with DPI technology. The proposed approaches could simplify dramatically the conventional work load for system management and reduction of power consumption by servers and accelerate the control action.

This paper has proposed an example of server congestion control method, in which the DPI equipment at any arbitrary point in a network estimates the CPU usage of each server by constantly monitoring the number of TCP live connections established by each server, and moves some of virtual machines on the congested server to other servers through remote control timely. Next, this paper has proposed an example of reducing power consumption by servers, in which the DPI equipment constantly monitors the traffic sent or received in each area with multiple servers and put all servers in that area to shut them down remotely. The feasibility of two proposed approaches was demonstrated by an evaluation system with a real DPI equipment.

As NFV technologies enables to rapidly scale up (or down) the deployment of DPI functions in the network economically, the proposed methods have a scalability in larger network constructed with NFV technologies. However, it will be necessary to investigate the effectiveness of the proposed methods further and to study total network congestion control and reduction of power consumption by network equipment with DPI technology.

ACKNOWLEDGMENT

We would like to thank Mr. Kohei YANAGISAWA and Mr. Hirohumi KUBOTA for their help with the evaluation.

REFERENCES

- [1] M.Finsterbusch, C.Richter, E.Rocha, J.A. Muller, and K.Hanßgen, "A Survey of Payload-Based Traffic Classification Approach," IEEE Communications Surveys & Tutorials, Vol. 16, No. 2, 2014.
- [2] A. Callado, C. Kamienski, G. Szabo, B. Gero, J. Kelner, S. Fernandes, and D. Sadok, "A Survey on Internet Traffic Identification," IEEE Commun. Surveys & Tutorials, vol. 11, no. 3, pp. 37–52, 2009.
- [3] M.Kassner, "Deep Packet Inspection: What you need to know" <http://www.techrepublic.com/blog/data-center/deep-packet-inspection-what-you-need-to-know/>
- [4] G.Finnie, "ISP Traffic Management Technologies: The State of the Art," Jan. 2009.
- [5] M. Chiosi et al., "Network Functions Virtualization - An Introduction, Benefits, Enablers, Challenges and Call for Action," ETSI NFV, Oct. 2012.
- [6] M.Bouet, J.Leguay, and V.Conan, "Cost-based placement of virtualized Deep Packet Inspection functions in SDN," 2013 IEEE Military Communications Conference, pp.992-997, Nov. 2013.
- [7] C.S. Yang etc. "A Network Management System Based on DPI", 13th International Conference on Network-Based Information Systems (NBIS2010), pp.385-388.
- [8] X.Lu, "A Real Implementation of DPI in 3G Network," 2010 IEEE Global Telecommunications Conference (GLOBECOM 2010).
- [9] A.Santos, S.Fernandes, R.Antonello, P.Lopes, D.Sadok and G.Szabo, "High-performance traffic workload architecture for testing DPI systems," GLOBECOM2011, Vo.30, No.1, Dec.2011
- [10] Y.Lee, J.Oh, J.K.Lee, D.Kang and B.G.Lee, "The Development of Deep Packet Inspection Platform and Its Applications," 3rd International Conference on Intelligent Computational Systems (ICICS'2013) January 26-27, 2013 Hong Kong (China).
- [11] M.Bouet, J.Leguay and V.Conan, "Cost-based placement of virtualized deep packet inspection functions in SDN," MILCOM2013, Vol.32, No.1, Nov.2013
- [12] S.Ricciardi, etc. "Evaluating energy savings in WoL-enabled networks of PCs," 2013 IEEE International Symposium on Industrial Electronics, pp.28-31, May 2013.
- [13] ONF: "Software-Defined Networking: The New Norm for Networks", April 2013. <https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf>
- [14] H. Kim and N. Feamster, "Improving network management with software defined networking," IEEE Communications Magazine, IEEE, vol. 51, No. 2, pp. 114–119, 2013
- [15] NetEnforcer, Allot Communications <http://www.allot.com/netenforcer.html>
- [16] VirtualBox <https://www.virtualbox.org/>
- [17] Windows Sysinternals "PsExec" <https://technet.microsoft.com/ja-jp/sysinternals/bb897553.aspx>
- [18] K.Yanagisawa and S.Kuribayashi, "Use of DPI Technology for Server Congestion Control and Reduction of Power Consumption by Servers", Proceeding of 2015 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (Pacrim2015), C1-2, Aug. 2015.

Author

Shin-ichi Kuribayashi received the B.E., M.E., and D.E. degrees from Tohoku University, Japan, in 1978, 1980, and 1988 respectively. He joined NTT Electrical Communications Labs in 1980. He has been engaged in the design and development of DDX and ISDN packet switching, ATM, PHS, and IMT 2000 and IP-VPN systems. He researched distributed communication systems at Stanford University from December 1988 through December 1989. He participated in international standardization on ATM signaling and IMT2000 signaling protocols at ITU-T SG11 from 1990 through 2000. Since April 2004, he has been a Professor in the Department of Computer and Information Science, Faculty of Science and Technology, Seikei University. His research interests include optimal resource management, QoS control, traffic control for cloud computing environments and green network. He is a member of IEEE, IEICE and IPSJ.

