IOP Conf. Series: Materials Science and Engineering **190** (2017) 012011 doi:10.1088/1757-899X/190/1/012011

Monitoring and Indentification Packet in Wireless With Deep Packet Inspection Method

Ahmad Fali Oklilas[1], Tasmi[2]

[1]Computer Engineering, Computer Science Department, Sriwijaya University
[2]Master of Engineering Informatics, Computer Science Department, Sriwijaya University

fali@ilkom.unsri.ac.id. faliunsri@gmail.com
tasmi@ilkom.unsri.ac.id, tasmisalim@gmail.com

Abstract. Layer 2 and Layer 3 are used to make a process of network monitoring, but with the development of applications on the network such as the p2p file sharing, VoIP, encrypted, and many applications that already use the same port, it would require a system that can classify network traffics, not only based on port number classification. This paper reports the implementation of the deep packet inspection method to analyse data packets based on the packet header and payload to be used in packet data classification. If each application can be grouped based on the application layer, then we can determine the pattern of internet users and also to perform network management of computer science department. In this study, a prototype wireless network and applications SSO were developed to detect the active user. The focus is on the ability of open DPI and nDPI in detecting the payload of an application and the results are elaborated in this paper.

1. Introduction

The various types of data traffic on the Internet often complicate the process of identification of traffic on the network monitoring system. Callado et al [1] stated that in many internet services there are applications that use the same port with used standard services.

There are many challenges in the classification of traffic. Running a network application can produce a series of packets which consists of header, payload and header information carrying layering. In the study conducted by [2], currently a mechanism of network monitoring system is desperately needed to monitor the status of infrastructure, LAN / WAN and ensure devices under normal conditions and active. The method used in the monitoring of the network in order to obtain a connection and good information is a way to process classification of traffic. In general, the methods used in the classification consist of a Port-Based, Payload-Based, or a Heuristic Behaviour Protocol Based Classification.

Based on previous research [3] systems on the network not only focus in process of identifying the data on the type of protocol and port number, but rather than identification and regulation of the signed application. Similarly for case of access restriction to certain web applications cannot be done simply by using a firewall by stopping access to the web IP address.

This paper focuses on the development of a prototype system to monitoring and identification data packets on a wireless network. This study was submitted to prove the real method of Deep Packet Inspection in the classification process data packets

2. Overview and Background Problems

Previous research [3] stated that systems in the network not only focus on the process of data identifying on the type of protocol and port number but rather than identification and regulation of the signed application. Similarly for case of restriction access to certain web applications, it cannot be done simply by using a firewall by stopping access to the web IP address.

Solutions for classifying data packets have been carried out both in the network online and offline by using machine learning, such as in [4] using the port number for the classification process data packets, as well as research conducted by [5] and [6] with combining methods of machine learning (ML) and artificial intelligent to classify IP traffic. Meanwhile, the research conducted by [7] and [8] explain that the classification of data packets on network online was by recognizing the payload. Moreover, network research conducted by [9] used Deep Packet Inspection with the signature on the payload to identify the protocol.

Deep Packet Inspection is a method used to perform thorough inspection process in the packet header of the TCP / IP and Payload. Some previous researches conducted by [10], [11] and [12] have been using the DPI as a method for packet classification process incoming and outgoing data

3. Proposed Design

In this research, a prototype of data packet monitoring system in wireless networks has been developed. Figure 1 is a schematic of experiments conducted.

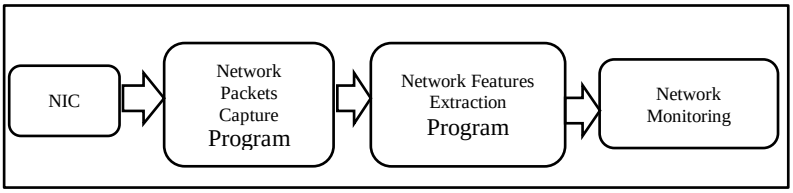

Figure 1. The procedure of monitoring data packets

At this research stage, it begins with Phase (i) to produce raw data obtained from sniffing packets of data using a sniffing application tool. IPv4 header structure is unique and has a hidden header depend on the protocol and encapsulated process that causes the raw data is difficult to read by human. Therefore, we need a new file type that can be processed and facilitate the training process. In this study, the type of files generated from the processing of raw data is .csv, where these file type easily processed and can be general received.

Phase (ii) is Feature extraction process to generate strong standards to serve as a benchmark as the archetype of the process. At this stage it made an algorithm to extract the layers to find the same patterns that mapping the characteristics possessed by a field. The third stages (iii) is the Feature Selection, as a field produces features as the unique cause difficulties in terms of identification of data packets, because not all features can be used the classification process data packets, therefore it created an algorithm to process the kind of selection data packets.

The last stage in this study (iv) is the training process (training) using Deep Packet Inspection methods and algorithms used are AC (Aho-Corasick). Aho-Corasick algorithm uses multi pattern that can solves the string matching problem relating to the timing and size of output. We uses Single-Sign-On (SSO) as the central authentication of users which are used in the Fasilkom Sriwijaya University (UNSRI)’s campus wireless network as shown in Figure 2.

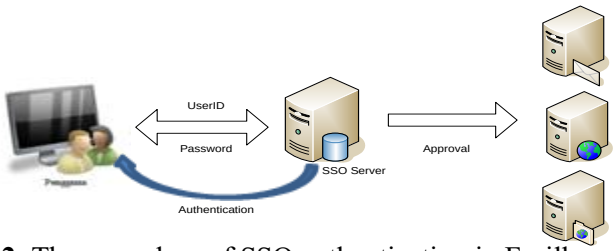

Figure 2. The procedure of SSO authentication in Fasilkom UNSRI

4. Implementation and Result

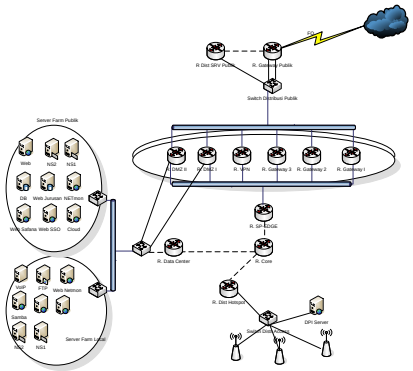

Figure 3. Topology research

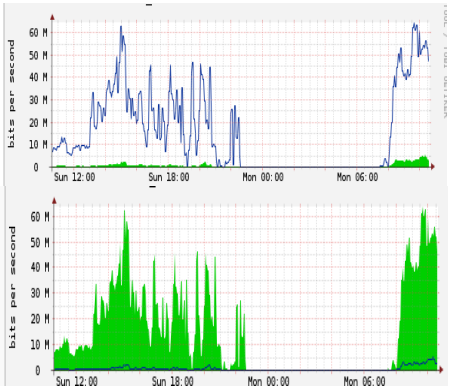

Figure 4. Traffic in the graph of router

Draft Design to create a depiction topology, router configuration, IP address allocation, configuration of multiple devices Wi-Fi, and election monitoring system is shown in Figure 3. In this case, a limited prototype was implemented in the Laboratory of Computer Science UNSRI network. The detail of works on this stage are: (i) Topology integrated into the Fasilkom Unsri campus network, (ii) selection of the device, (iii) Coding system applications and configuration monitoring and (iv) integrating the device into the application

Figure 4 shows the results of the traffic monitoring in which data obtained from users who conduct connection test. Results obtained shows heavy traffic between 40 -70 Mbps, this is because of the manual process of uploading and downloading for several applications. Figure 5 is the result of a user login which uses SSO.

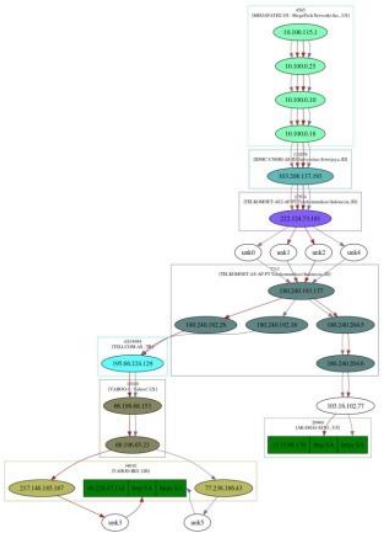

Figure 5. Routing packet data

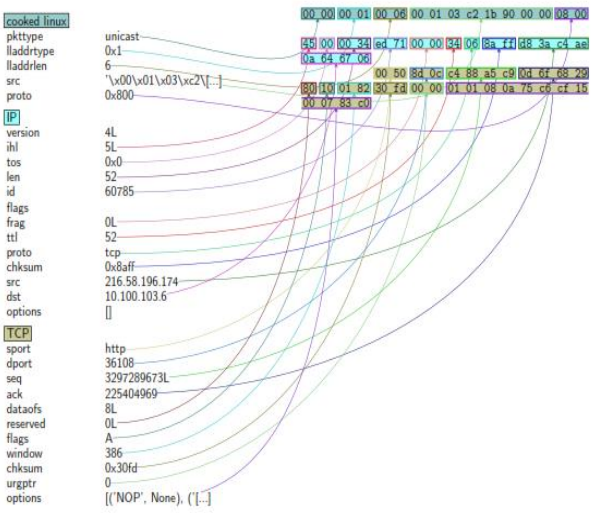

Figure 6. Result of extraction packet data

Table 1. Results of monitoring packet data

Protocol	∑ Packets	∑ bytes	∑ flows
DNS	292	64167	147
HTTP	44	8980	5
NETBIOS	48	4567	4
SSDP	51	21330	2
DHCP	4	1378	3
Unknown	**22127**	**20765840**	**97**

In the process of getting the results as shown in Table 1, first made the process sniffing packets of data in real time, then results in sniffing extracted by using a program that was built using C language, after which the process of grouping data packets. The result obtained from the protocol that is widely used by the user is a standard protocol such as HTTP, DNS and DHCP, but this result was also obtained unknown protocol

5. Conclusion

Deep Packet inspection one of methods which can be used for identification of data packets based on application signatures. By using Single-Sign-On can be used in active hotspot user identification.

From the initial results obtained there are still many protocols that cannot be monitored (unknown), protocols which produced still standard such as DNS, HTTP, many applications on the internet that use SSL such as social media applications. But the results are still difficult to monitor data packets using SSL.

But the results of this study can be developed again in terms of process monitoring applications that use SSL/TLS

Reference

[1] A. Callado, A. Callado, C. K. Member, G. Szabó, B. Péter-gerö, and J. Kelner, "A Survey on Internet Traffic Identification . A Survey on Internet Traf fi c Identi fi cation," vol. 11, no. November 2015, pp. 37–52, 2009.

[2] D. Stiawan and A. Oklilas, Fali, "Intrusion Prevention in Heterogeneous System based on Behavior Approaches," *Int. Conf. Sci. Inf. Technol. (ICSITech)*, 2015.

[3] H. Nazief, T. Sabastian, A. Presekal, and G. Guarddin, "Development of University of Indonesia Next Generation Firewall Prototype and Access Control With Deep Packet Inspection," *ICACSIS*, pp. 47–52, 2014.

[4] T. T. T. Nguyen and G. Armitage, "A Survey of Techniques for Internet Traffic Classification Using Machine Learning," *Commun. Surv. Tutorials, IEEE*, vol. 10, no. 4, pp. 56–76, 2008.

[5] R. N. Jesudasan, P. Branch, and J. But, "Generic Attributes for Skype Identification Using Machine Learning," no. August, pp. 1–7, 2010.

[6] R. Alshammari and A. N. Zincir-Heywood, "An investigation on the identification of voip traffic: Case study on Gtalk and Skype," *Proc. 2010 Int. Conf. Netw. Serv. Manag. CNSM 2010*, pp. 310–313, 2010.

[7] H. Chen, F. You, X. Zhou, and C. Wang, "Algorithm Comparison of P2P Traffic Identification Based on Deep Packet Inspection," vol. 1, pp. 3–6, 2009.

[8] M. F. Sun and J. T. Chen, "Research of the traffic characteristics for the real time online traffic classification," *J. China Univ. Posts Telecommun.*, vol. 18, no. 3, pp. 92–98, 2011.

[9] Z. Cao, G. Xiong, Y. Zhao, Z. Li, and L. Guo, "A Survey on Encrypted Traffic Classification," *Appl. Tech. Inf. Secur.*, pp. 73–81, 2014.

[10] D. Smallwood and A. Vance, "Intrusion Analysis with Deep Packet Inspection Increasing Efficiency of Packet Based Investigations," pp. 342–347, 2011.

[11] M. Najam, U. Younis, and R. ur Rasool, "Speculative parallel pattern matching using stride-k DFA for deep packet inspection," *J. Netw. Comput. Appl.*, vol. 54, pp. 78–87, 2015.

[12] Thaksen j Parvat and P. Chandra, "A Novel Approach to Deep Packet Inspection for Intrusion Detection," *Int. Conf. Adv. Comput. Tecnol. Appl.*, vol. 45, pp. 506–513, 2015.