ISBN 978-9943-355-85-9

INTERNATIONAL CONFERENCE ON IMPORTANCE OF INFORMATION COMMUNICATION TECHNOLOGIES IN INNOVATIVE DEVELOPMENT OF SECTORS OF ECONOMY

dedicated to the 1235th anniversary of the birth of Muhammad al-Khwarizmi

April 5-6, 2018, Tashkent, Uzbekistan

THE MINISTRY FOR DEVELOPMENT OF INFORMATION TECHNOLOGIES AND COMMUNICATIONS OF THE REPUBLIC OF UZBEKISTAN

UZMOBILE

foizi uchinchi va to‘rtinchi avlod mobil aloqasi bilan qamrab olingan, bu esa MDH davlatlari ichida eng past ko’rsatkich hisoblanadi [1]. Tahlillar shuni ko‘rsatadiki, bunday yechim abonentlarga yuqori sifatli va zamonaviy multimedia xizmatlarini taqdim etish imkonini beradi. Abonentlar terminallari bu xizmatlarni qo’llab-quvvatlash masalasi ham aloxida masalani keltirib chiqaradi.

Respublikada mobil aloqani rivojlanishi o‘z o‘rinda mobil operatorlar oldiga multimedia kontentlarni rivojlantirish, aholini mobil aloqa xizmatlariga talabini qondirishga katta ahamiyatga egadir. Belgilangan vazifalarni amalga oshirishda IMS texnologiyasini qo’llash juda muhimdir.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi Prezidenti Sh.M. Mirziyoyev huzurida Respublikada axborot-kommunikatsiyalar tizimi va texnologiyalarini yanada rivojlantirish ishlarining ahvoli va bu boradagi ishlarni keskin jadallashtirish yuzasidan Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi rahbarlari hisoboti. 9 yanvar 2018 yil.
2. Дмитриев В. Н. Алгоритм оптимизации гетерогенной беспроводной сети по критерию равномерности загрузки оборудования провайдера/В. Н. Дмитриев, А. В. Чередниченко// Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2011. № 2. С. 120-125.
3. Тихвинский В. О. Мобильное цифровое телевизионное вещание: анализ технологий и бизнес-моделей / В. О. Тихвинский, С. В. Терентьев // Информационные телекоммуникационные сети. 2008. № 7. С. 16-22.
4. Sanjoy P. Digital video distribution in broadband, television, mobile, and converged networks: trends, challenges, and solutions / P. Sanjoy. New Delhi, India: John Wiley & Sons Ltd., 2011. P. 326-327.
5. Перекрестов И. С. Организация мобильного доступа к мультимедийным данным/И. С. Перекрестов, О. А. Решетняк, Э. Г. Тихий // Цифров технологи. 2008. № 4. С. 86-92.
6. Мобильное телевидение DVB-H. 2010 [Электронный ресурс]: http://www.thg.ru/mobile/mobtv_yota_beeline/.
7. Гергес М. С. Улучшение качества передачи IPTV-услуги видео по запросу через широкополосную сеть доступа / М. С. Гергес // Проблемы информатики. 2011. № 3. С. 79-88.
8. Yota перешла с WiMAX на LTE. 2012 [Электронный ресурс]: http ://www.rbcdaily.ru/media/562949982868803.
9. Гельгор А. Л. Технология LTE мобильной передачи данных/А. Л. Гельгор, Е. А. Попов: учеб. пособие. СПб.: Изд-во Политехн. ун-та, 2011. 204 с.

DEEP PACKET INSPECTION WITH APPLICATION SIGNATURES

Teshaboev Kh.N.
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, master degree student

The paper presents Deep Packet Inspection Engine implemented with Application Signatures for packet classification and filtering on the next generation IP networks. The proposed architecture is used for controlling IP packets based on the hardware and software systems by implementing hardware accelerators, shared common CAM memory and software based application signature databases. Hardware implementation reduces the searching and matching time of packet header and software implementation part of architecture compares application signatures, identifies next action.

An increasing of Internet access for corporate productivity has created an expectation of high performance and ubiquitous connectivity in the enterprise and company environment. In parallel, bring your own device (BYOD) and cloud computing trends have led to a rapid proliferation in the number of user devices and applications used in enterprise networks. These factors can strain traditional networks and create issues such as bottlenecks in network performance. It is often considered very important to support high performance and application optimization within the context of restricted costs, finite bandwidth capacity, and an expectation to deliver a minimum quality of service (QoS) for critical applications.

Two factors are critical for addressing these challenges: clear, concise insight into network performance, and an ability to enforce network policies that optimize the network's performance.

Nowadays, many enterprise and provider networks are using new technology based systems called Deep Packet Inspection or L7 packet analyzing. Deep Packet Inspection approach consists in analysis of packet full contents by using content and behavior analyzing methods, brings good results for general. The methods of payload analysis are very demanding for network performance and cannot be used in encrypted traffic while the ratio of encrypted traffic is increasing. An alternative approach is a Behavior Analysis which uses information from the L3/L4/L7 layer (i.e. characteristics of data flows in IP networks) and does not work with the content of packets at all. A combination of both methods ensures a higher ability of system to react on a wider scope of threads and therefore increases security and performance of a network in general. Because of these features, DPI technology is being popular in networking domain.

The Deep Packet Inspection (DPI) system is intended for use in mobile and fixed broadband networks. In terms of data network architecture, the DPI is a standalone system. The system can provide the following functions:

- analysis of traffic in operator's network to be aware of a particular protocol or service it belongs to;
- traffic measurement that can be provided on a per-protocol and per-service basis;
- traffic management aimed at optimum exploitation of network resources;
- providing value-added services (Anti-virus, Parental control, Anti-spam, Traffic redirect) for protecting network users and environment.

After matching a data stream to an application the DPI engine performs traffic management, packet will be discarded or forwarded to appropriate destination. In addition, traffic measurement by using DPI encompasses the accumulation of statistical information about the number of received and sent bytes, and also the actions for controlling traffic consumption by charging for traffic by means of a local billing system or by querying external systems. Statistical calculation of the amount of data that passes through the system can be done without tying to the subscriber that initiated the data transfer. Control of traffic consumption requires matching data streams with subscriber identifiers, which is done either by using the local configuration or by interacting with an external system.

Since the DPI engine knows which data stream belongs to which application, it can separately control the characteristics of the data transmission channel for each service. Knowing which subscriber initiated the data stream makes it possible to specify service policies individually for each subscriber, while the traffic measurement data allow applying the policies depending on previous consumption of the services. Thus an operator of a broadband access network can use a DPI system to flexibly control the characteristics of data transfer channel based on complete knowledge of service consumption, which allows increasing the efficiency of network infrastructure utilization [1]. Traffic management in DPI system includes control of transmission rate, prioritization of streams, blocking of packets in a stream, dynamic redistribution of bandwidth between data streams of the same subscriber or different subscribers based on the defined priorities and current network load. DPI also allows routing traffic for processing to external devices for the purposes of optimization, filtering and analysis of its content. It is also possible to transfer only

certain characteristics of the data stream to an external system, e.g. HTTP URI, SIP URI etc., for subsequent analysis of data streams.

In this paper, deep packet inspection system model is proposed for analyzing network traffic based on the application signature. The implementation of DPI system with best performance and minimized packet processing latency is advanced as an idea at the end.

In this section we discuss some of the previous work done in the area of Deep packet inspection.

Several works investigated the signature based deep packet inspection technology for traffic and bandwidth control, network security and service management in Next Generation Networks. The ITU-T Y.2770 standard series [2], [3] define requirements for Deep Packet Inspection in Next Generation Networks. Main issues of packet inspection, deep packet inspection models, DPI use cases and application scenarios are defined in this standard. Framework for deep packet inspection [4] describes a structured approach for designing, defining and implementing DPI solutions in support of service/application awareness for facilitating interoperability in the evolving networks. This Recommendation also provides DPI framework aspects from modeling and performance. Mechanisms for the network elements with support of deep packet inspection are analyzed in ITU-T Y.2772.

On the signature matching and application recognition based DPI analysis, papers [5], [6] propose utilizing algorithms from the field of bioinformatics and preprocessing methods to accelerate their system.

Using hardware for Deep packet inspection is most critical issue in today's point. Current solutions employ software filtering systems that is not practical for bandwidth beyond 100 Mbps. Therefore, implementing fast dynamic pattern search engine signature matching on field programmable gate array is proposed papers [7] and [8]. Proposed systems filters and identifies the entire 1,625 unique patterns defined in the most current version of Snort rule set and using Multi-Layer Transition Bit masking. An improved deep packet filter system designed to optimize search of dynamic patterns for high speed network traffic in [9]. The improved deep packet filter system is a hardware-based system with optimized logic area. The reduction of the logic area allows the deep packet filter system to be implemented onto a single field-programmable array chip [10].

Reviews show, proposed models don't identify stable hardware and software architecture for Deep Packet Inspection. In addition, related works don't recommend that how to partitionate hardware and software implementation of DPI system.

To address this problem, we propose hardware accelerated architecture of Deep packet inspection engine which application signature matching is implemented in software.

Deep packet inspection not only examines the packet header, but also looks through the entire payload searching for the entire user specified or application patterns based on 7 layers of OSI model (fig. 1).

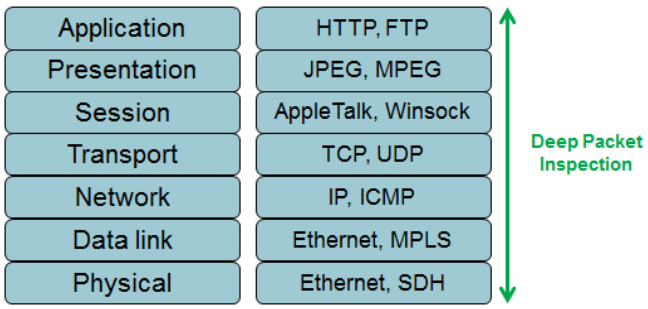

Fig.1. Deep packet inspection

DPI meets the need of network operators to gain better insight (in finer granularity) of the behavior of their users, in order to allocate the resource of the network, to enhance the quality of service or quality of experience of specific users, and to monitor the network better for security

threats. A basic building block in contemporary DPI engines is to match the packets' payload against a set of patterns (a.k.a. signatures), which, for example, indicate malicious activity [10]. Signature of payload with full packet definition is given below (fig. 2).

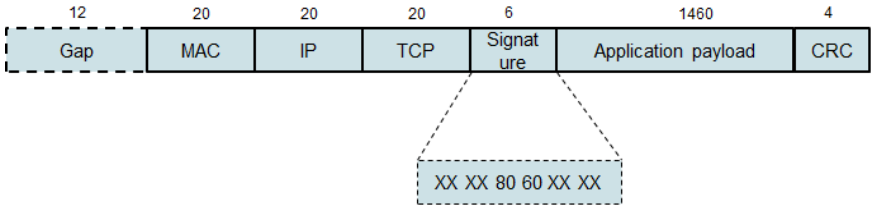

Fig.2. Ethernet packet with sample application signature

In order to provide functions of traffic analysis, measurement and control, the DPI system is installed in the operator's broadband access network inside of data communication channels. Based on the required functions, the system can be installed in different points in the network, however for traffic analysis, measurement and control procedures that needs to be applied depending on the subscriber profile the system must be incorporated into the network in such a way that the traffic processed by the system has non-translated IP addresses in order to match traffic with subscriber identifiers. The DPI engine can operate in a rupture of telecommunication link and therefore is invisible for external systems on all levels of the OSI model, in other words, it is absolutely transparent and cannot be detected by any means of network analysis.

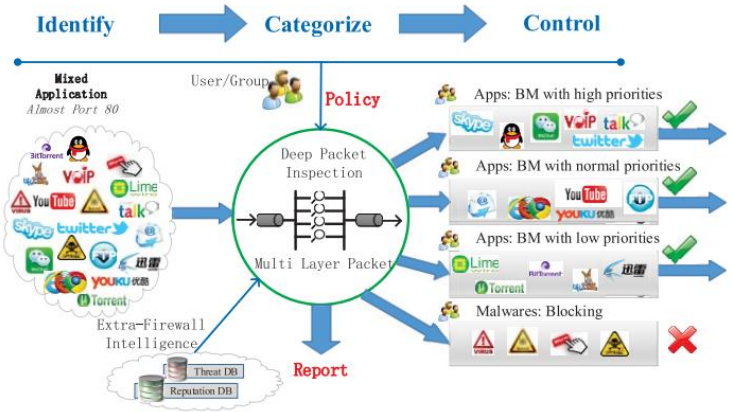

Fig.3. Procedures and typical applications of DPI, including bandwidth management and network security

We propose our system model for DPI system implementation. In this implementation, packet classification and signature analysis is used FPGA based hardware system development.

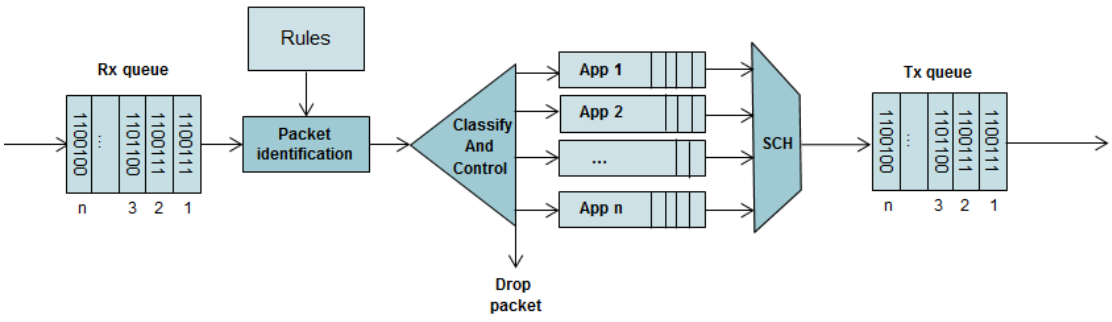

Fig.4. Proposed DPI traffic classification and management engine

In order to implement proposed DPI system certain techniques such as exact string matching algorithms, regular expressions presenting the pattern of characters and symbols and a Deterministic Finite Automata (DFA) of included signatures. The DFA and Nondeterministic Finite automata (NFA) represent the signatures corresponding to the application it has been

implemented for. Lastly the exact string matching algorithms are brought in use to match the signatures and application data fields.

Conclusion

As a purpose to our work on DPI engines, where the signatures were given as an input data, we have also presented system for zero day attack signature extraction for the DPI engine. Given main model an architecture implementation shows main idea of proposed system. Simulation model and performance analysis of system is scheduled in the next paper of DPI implementation.

References

1. Next Generation Deep Packet Inspection: An Overview of Requirements and Applications. Network Strategy Partners, LLC, 2007.
2. ITU-T Y.2770. Requirements for Deep Packet Inspection in Next Generation Networks. Telecommunications Technology Association, 2012.
3. ITU-T Y.2770 series – Supplement on DPI use cases and application scenarios. ITU, 2015.
4. ITU-T Y.2771. Framework for deep packet inspection. ITU, 2014.
5. A.F.Santos: Automatic Signature Generation, Diploma Thesis, 2009.
6. Géza Szabó, Zoltán Turányi and others. Automatic Protocol Signature Generation Framework for Deep Packet Inspection, 2012.
7. Young H. Cho and William H. Mangione-Smith. Programmable Hardware for Deep Packet Filtering on a Large Signature Set, 2004.
8. Subramanian Shiva Shankar, Lin PinXing, Andreas Herkersdorf, Thomas Wild. Hardware Acceleration of Signature Matching through Multi-Layer Transition Bit masking. 26th International Telecommunication Networks and Applications Conference, 2016
9. Young H. Cho, William H. Mangione-Smith. Programmable hardware for deep packet filtering. US7519995 B2, 2009.
10. Nitesh B. Guinde & Sotirios G. Ziavras. Novel FPGA-Based Signature Matching for Deep Packet Inspection. 4th IFIP WG 11.2 International Workshop on Information Security Theory and Practices, April 2010.

FUTURE NETWORKS: VISION, CONCEPT, AND REQUIREMENTS

[1]Usmanova N.B.,[2]Gayratov Z.K.

[1]Tashkent university of information technologies named after Muhammad al-Khwarizmi, Department of DTS & N, Associate professor

[2]Tashkent university of information technologies named after Muhammad al-Khwarizmi, master degree student.

Abstract. The Future Network should provide much better support for a broad range of applications, services, and network architectures. In the Future Network, multiple isolated logical networks each with different applications, services, and architectures should share the physical infrastructure and resources. Considering some conceptual features of Future networking, the paper states possible application issues for e-healthcare system in the terms of Uzbekistan.

Taking into account the dynamic development of technologies and tasks set by the government, the ICT sector stakeholders of Uzbekistan (operators, providers, regulators, etc.) are facing complex tasks to improve infocommunication networks and systems based on new technologies and solutions, with the possibilities of expanding the infrastructure in supporting applications and services of the information society.

In these terms, the development of the Internet and related technologies requires the study of operational and technological requirements for the next generation communication infrastructure, research on the practical use and analysis of new technologies, analytical knowledge in emerging approaches and technical solutions with a focus on the Future Networks, resource