Introduction to Deep Packet Inspection and its Usecases

Mallikarjun A. Hadli[1*], B. K. Rajith Kumar[2]

[1]*Student, Dept. of Electronics and Communication Engineering, R. V. College of Engineering, Bengaluru, India*

[2]*Assistant Professor, Department of Electronics and Communication Engineering, R. V. College of Engineering, Bengaluru, India*

*Corresponding author: mallikarjunah.ec16@rvce.edu.in

***Abstract*: Network resource management and security is the effective management and handling of various Quality of Service (QoS) parameters and detection and interception of viruses related to the given network. This management can be carried out in several ways depending upon the type of the network and the number of subscribers to the network. Deep Packet Inspection (DPI) is one such type of method where the packets going through the network can be classified accordingly for certain use cases that the network handler would require for management and security. For example, if a new application is extremely popular and is taking up all the bandwidth of an ISP then accurately classifying this application would help the ISP to manage their resources effectively to improve the Quality of Experience (QoE) for the consumers. Deep packet inspection (DPI) is an advanced method of managing and examining network traffic. It is a form of packet filtering that locates, identifies, classifies, reroutes or blocks packets with specific data or code payloads that standard packet filtering, which examines packet headers only, cannot detect. Deep Packet Inspection works at the application layer of the Open Systems Interconnection (OSI) reference model.**

***Keywords*: Deep packet inspection, Internet service provider, Open systems interconnection.**

1. Introduction

Network security is very important in the online world. Deep packet inspection is vital in preventing worms, spyware, and viruses from getting into the corporate network. Furthermore, using deep packet inspection based on rules and policies allows the network to detect if there are prohibited uses of approved applications. Deep packet inspection is also used by network managers to help ease the flow of network traffic. It is also used to enhance the capabilities of ISPs to prevent the exploitation of IoT devices in DDOS attacks by blocking malicious requests from devices.

For ISPs a certain group of applications take most of their bandwidth and network traffic so providing better connections and management allows consumers to choose the best service provider. For this ISPs require a detailed analysis of the applications used and the number of subscribers using them to efficiently balance the load. Therefore, there is a need for low latency and high speed network management techniques. With this Mobile service operators and other similar service providers use deep packet inspection to tailor-fit their offerings to individual subscribers allowing them to differentiate data usage as “all you can use”. For example, Record labels and other copyright holders can also request ISPs to block their content from being downloaded illegally.

Deep Packet Inspection (DPI) has numerous advantages over other methods like shallow packet inspection and packet filtering. It’s highly accurate in recognising fraudulent and malicious packets. It allows the ISP to monitor the network without any performance degradation. Additionally, it provides the ISP with control over the user’s bandwidth as they can block or improve the usage of certain services and applications.

2. Motivation

- SPI does not provide the complete information about the packet.
- Full security cannot be provided.
- DPI prevents network intrusion attempts and filters unauthorized and harmful content such as viruses and spam.
- Allows a network operator to monitor the individual packets of data to examine the contents for resource management.

3. Shallow Packet Inspection

Shallow Packet Inspection (SPI) examines the packet headers (i.e. the data placed at the beginning of a packet, such as the IP addresses of the sender and receiver), as against the packet's body or "payload." This type of packet examination allows communications to remain' virtually anonymous' as the packet content is not determined, and the data in the header is also used solely for routing the packet.

SPI cannot read beyond the information in a header and focuses on the OSI model's second and third layers. SPI examines the IP address of the sender and receiver, the number of packets that a message is broken into, the amount of hops that a packet can make before routers stop transmitting it, and the synchronization data that allows the packets to be reassembled into a format that the receiving application will perceive. SPI can't read a packet's session, presentation, or application layers; it can't look at the contents of the packet within the payload of a packet.

4. Medium Packet Inspection

Medium Packet inspection (MPI) is sometimes wont to refer to' application proxies' or devices situated between ISP / web gateways and end-user computers. These proxies can examine info regarding the packet header against their loaded take apart list. once a packet enters the proxy, the system directors will simply update it against a parse-list. A take apart list permits to permit or interdict specific packet varieties on the web supported their format varieties and associated location instead of their information science address alone.

MPI devices scan the packet's payload presentation layer and confirm the appliance layer aspects. directors will use MPI devices to prevent shopper computers from receiving YouTube flash files or image files from social networking sites. By examining the appliance commands gift within the application layer and also the file formats inside the presentation layer, MPI technologies can place some packets over others.

5. Deep Packet Inspection

Deep Packet inspection (DPI) technologies square measure usually found in costly routing devices that square measure put in in major networking hubs. These devices square measure supposed to permit network operators exactly to spot the origin and content of every packet of information that passes through these hubs. Arbor/Ellacoya note that their e100 devices use, "DPI technology to watch and classify information directly from your network traffic flow.

Inspecting information packets at Layers 3-7 permits the e100 to produce crucial data to your operations and business support systems, while not compromising different services" (Arbor/Ellacoya Networks 2008). whereas MPI devices have terribly restricted application awareness, DPI devices have the potential to "look from a particular IP address within all traffic, devour communications protocol traffic, then drill any right down to capture traffic heading to and from Gmail, and so tack emails as user types" (Anderson 2007). whereas MPI devices have scaling issues to fulfill multiple application protocols, DPI devices square measure designed to see that programs generate packets for many thousands of transactions each second in real time. In giant networking environments, they're designed to scale.

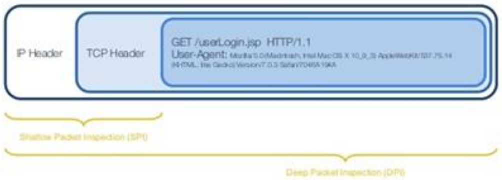
IP Header
TCP Header
GET /userLogin.jsp HTTP/1.1
User-Agent:
Shallow Packet Inspection (SPI)
Deep Packet Inspection (DPI)

Fig. 1. DPI v/s SPI

6. Why DPI

By examining packet flows at such an in depth level, DPI technologies is wont to improve network security, implement access needs, guarantee quality of service, and tailor service for specific applications. Network security is improved as a result of system directors will higher examine knowledge streams to work out if, for instance, packets' payloads carry infectious agent payloads or components of spam email messages. If either reasonably payload is suspected, directors will establish rulesets to stop the packets from being carried to their destination, and if the purpose of origin is inside the ISP's network then the pc causation the illicit payloads is quickly prevented from causation any longer packets till they stop causation the packets in question.

Quality of service, because it pertains to DPI, focuses on the flexibility to limit the transmission of packets that may degrade overall network performance by streaming massive amounts of information. to enhance quality of service, DPI devices target 'problem' applications and packet-types by either reducing their priority level or preventing them from being transmitted or received.

This notion of rising network security through knowledge traffic police work is accompanied with a drive to typically limit access to the network itself. as a result of DPI will examine all layers of packet transmissions, it will correlate packets with separate users UN agency have documented to the network; if a packet cannot be correlative with a noted documented user, the packet is prevented from escaping the ISP's network perimeter, and network directors will investigate UN agency is making an attempt to use their network while not initial authenticating.

7. Impact of Encryption on DPI

Consumers have an ambivalent relation to encryption and privacy. Widespread Internet security issues have a tendency to make it into mainstream news. One report suggests that nine out of ten respondents have heard about governmental surveillance programs outlined by Edward Snowden two years after the fact. However, user behaviour doesn't reflect this. Consumers are still disinclined to adopt security measures that require a change in behaviour. A study done after Snowden showed an increase in encryption usage by consumers. Two initiatives in particular have made it easier than ever before for a content provider to enable encryption for their content: CloudFlare's Universal SSL and ISRG's Let's Encrypt.

TLS 1.3 encrypts the handshake to a great extent. Specifically, the server certificate is transferred in an encrypted format rather than in plain text. It will be impossible for a DPI device to verify the authenticity of the server based on the certificate chain and the known trusted Certificate Authority roots. The Server Name Indication (SNI) extension required for TLS/HTTPS virtual hosting is mandated and still transferred in the clear for a full handshake.

While encrypted SNI has been a topic of discussion, there is no known technical means of encrypting SNI without sacrificing performance. All encrypted packets are to be sent with the record type of Application Data, where the record type used to be a function of whether the data being transferred was control or application data. This makes content analysis harder.

The specification also defines content padding, allowing blank data to be appended to the payload before encryption. This does expand the size of the payload, expending additional bandwidth, but yields the benefit of making content analysis harder. To what extent content padding will be used in actual implementations remains to be seen.

However, this does not mean the end of visibility into user traffic. It is still possible to see behaviour, visited destinations and similar data even when web encryption is widespread. Granularity and accuracy will suffer, requiring DPI equipment vendors to adopt to this reality and focus on QoE-enhancing use cases. Network operators that have a good understanding of how their subscribers consume bandwidth and how their network is delivering QoE will have a competitive advantage.

8. DPI usecases

A. Network security

DPI was originally developed to secure local area networks (LANs), that square measure accustomed cowl tiny geographical areas like a corporation or university, so as to confirm there's no unwanted traffic coming back in from outside the network. This task accustomed be accomplished by firewalls, however thanks to developments in net applications the bounds between the interior LAN and also the external net isn't thus well-defined, so network directors should currently absolutely examine the information coming back in and out of the LAN to attain this. DPI instrumentation permits network operators to find and intercepst recognized sorts of mal-ware (viruses, Trojans, worms, and alternative dangerous code) before it reached their customers or workers.

B. Network management

DPI are often used for the aim of network management, that involves numerous functions like guaranteeing a basic quality of service (QoS) for the end-users, preventing congestion on the network, and facilitating the creation of various packages of net access for customers. It allows ISPs to discriminate among differing kinds of traffic streams to undertake to take care of quality of service standards, or to throttle down “excessive” traffic, like peer-to-peer file-sharing or voice scientific discipline calls on mobile networks.

C. Content optimization

DPI are often used for optimisation of contents by approach of acting as proxy and modifying contents like by reducing still and video image quality, reformatting websites for mobile devices, and alternative techniques as per the information measure out there and device constraints in order that users will get pleasure from content with acceptable performance than otherwise.

D. Billing and Metering applications

DPI are often accustomed count the volumes or rates of traffic, however with additional complicated schemes to account for a combination of free, partner, and paid traffic to support schemes wherever a subscriber’s traffic is also capped to an exact volume by the bytes or others (such as payments between a service supplier and content supplier sure as shooting kinds of traffic and/or application usage).

E. Network and subscriber analysis

DPI based mostly applications will facilitate operators in gauging the health of the network by pinpointing performance and capability furthermore as offer the service supplier with a bigger understanding of their subscriber’s behaviour that will be accustomed enhance selling revenues.

F. Targeted advertising

DPI will alter ISPs to inject advertisements into websites that match the assumed interests of the users. information on what user’s square measure gazing on the web is gathered by ISPs, that is analysed and accustomed show personal advertisements that follow users across the web and directly pertain to his or her incontestable interests. ISPs square measure notably well-placed to facilitate this sort of advertising as they need access to any or all their subscribers’ net surfriding information being transported by their network.

G. Copyright enforcement

A number of massive players within the content business square measure pushing for obligatory filtering of proprietary material that's shared on peer-to-peer platforms. ISPs will use DPI filtering instrumentation that may mechanically find and block unauthorized sharing of music or video files.

H. Content regulation

DPI are often accustomed acknowledge and block access to content deemed nonlegal or harmful. e.g., filtering child-abuse websites, censoring something that's thought-about a threat to the govt. and public stability.

9. Conclusion

This paper presented on overview on deep packet inspection and its usecases.

References

[1] Jakub Svoboda, “Network Traffic Analysis with Deep Packet Inspection Method”, *MUNI University Press*, 2014.
[2] Chengcheng Xu, Shuhui Chen, Jinshu Su, S M Yiu, Lucas C K Hui, “A Survey on Regular Expression Matching for Deep Packet Inspection: Applications, Algorithms, and Hardware Platforms”, *IEEE Communications and Surveys*, May 2016.
[3] Gabriel Arquelau Pimenta Rodrigues, Robson de Oliveira Albuquerque, “Cyber security and Network Forensics: Analysis of Malicious Traffic towards a Honeynet with Deep Packet Inspection”, *Applied Sciences MDPI*, October 2017.

[4] Bendrath R. “Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection” in *Proceedings of the International Studies Annual Convention*, February 2009; Volume 15.

[5] Fuchs, “Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society”, *the Privacy & Security Research Paper,* Series 1, PACT: Uppsala, Sweden, 2012.

[6] Ashraf, M.A.; Jamal, H.; Khan, S.A.; Ahmed, Z, “A Heterogeneous Service-Oriented Deep Packet Inspection and Analysis Framework for Traffic-Aware Network Management and Security Systems”, *IEEE Access*, 2016, 4, 5918–5936.

[7] Sherry, J.; Lan, C.; Popa, R.A.; Ratnasamy, S. “Blindbox: Deep packet inspection over encrypted traffic” in *Proceedings of the ACM SIGCOMM Computer Communication Review*, New York, NY, USA, 22 April 2015; Volume 45, pp. 213–226.

[8] Yoonjae. Lee, Junseok. Oh, Joon Kyung. Lee, Dongwon. Kang, and Bong Gyou. 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).

[9] Tomasz Bujlow, Valentín Carela-Español, and Pere Barlet-Ros, “Independent Comparison of Popular DPI Tools for Traffic Classification”, *Computer Networks, ISSN 1389-1286*, vol. 76, no. 0, pp. 75 – 89, 2015.