ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ

МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

ЎЗБЕКИСТОН РАДИОТЕХНИКА, ЭЛЕКТРОНИКА ВА АЛОҚА ИЛМИЙ-ТЕХНИКА ЖАМИЯТИ

ИҚТИСОДИЁТНИНГ РЕАЛ ТАРМОҚЛАРИНИ ИННОВАЦИОН РИВОЖЛАНИШИДА АХБОРОТ–КОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИНИНГ АҲАМИЯТИ

Республика илмий-техник анжуманининг

МАЪРУЗАЛАР ТЎПЛАМИ
3-ҚИСМ

СБОРНИК ДОКЛАДОВ

Республиканской научно-технический конференции

ЗНАЧЕНИЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ИННОВАЦИОННОМ РАЗВИТИИ РЕАЛЬНЫХ ОТРАСЛЕЙ Э КОНОМИКИ

ЧАСТЬ 3

6-7 апрел 2017 йил

ТОШКЕНТ – 2017

Message	Description
Controller-to-Switch	
Features	Request the capabilities of a switch. Switch responds with a features reply that specifies its capabilities.
Configuration	Set and query configuration parameters. Switch responds with parameter settings.
Modify-State	Add, delete, and modify flow/group entries and set switch port properties.
Read-State	Collect information from switch, such as current configuration, statistics, and capabilities.
Packet-out	Direct packet to a specified port on the switch.
Barrier	Barrier request/reply messages are used by the controller to ensure message dependencies have been met or to receive notifications for completed operations.
Role-Request	Set or query role of the OpenFlow channel. Useful when switch connects to multiple controllers.
Asynchronous-Configuration	Set filter on asynchronous messages or query that filter. Useful when switch connects to multiple controllers.
Asynchronous	
Packet-in	Transfer packet to controller.
Flow-Removed	Inform the controller about the removal of a flow entry from a flow table.
Port-Status	Inform the controller of a change on a port.
Error	Notify controller of error or problem condition.
Symmetric	
Hello	Exchanged between the switch and

Figure 2: OpenFlow Messages

The OpenFlow protocol describes message exchanges that take place between an OpenFlow controller and an OpenFlow switch. Typically, the protocol is implemented on top of SSL or Transport Layer Security (TLS), providing a secure OpenFlow channel.

The OpenFlow protocol enables the controller to perform add, update, and delete actions to the flow entries in the flow tables. It supports three types of messages, as shown in Figure 2.

The OpenFlow protocol enables the controller to manage the logical structure of a switch, without regard to the details of how the switch implements the OpenFlow logical architecture

DEEP PACKET INSPECTION AND ITS BENEFITS

A. A. Makhamadjonov (master of TUIT)

A number of researchers have examined DPI technology. For example, stated that DPI devices can operate on layers two through seven of the Open Systems Interconnect (OSI) model. Deep packet inspection is packet filtering that inspects the data payload of an IP packet.

DPI devices take deep looks into the data of each packet and either allows or denies passage according to some set of predetermined rules. As networks incorporate increasingly sophisticated services into their infrastructure, DPI uses application-specific data found in packet payloads to make routing decisions, to block or rate-limit unwanted traffic, to perform intrusion detection, and to provide quality of service. The DPI inspection engine parses each packet and compares the contents against its rule set. This rule set is comprised of known electronic signatures of content which allow identification of the packet's data. In the past, network packets were classified by their headers, but DPI now allows them to be classified by the actual content of their payloads.

To perform this functionality, DPI devices rely on a database of application signatures that are crosschecked against to determine the nature of the packet traversing the network. The DPI device groups the packets by protocol and security levels then processes the packets by "performing application level checks as well as stateful inspection". DPI devices look for any anomalies in the packets based on their know application signatures. If any packet is deemed out of the ordinary, it is not allowed to pass. An example would be the order in which commands are given for a certain protocol. An application will always order commands in the same sequence, where as a human attempting to hack into a system might issue the commands in some random order. By inspecting the packet for its application signature, then comparing that signature

against known parameters, DPI devices can thwart attacks that would have gotten past traditional packet inspection principles.Normally, DPI is used to monitor and shape IP traffic. ISPs can use DPI to monitor the type of traffic on their networks and give priority to the protocols they deem more important.This type of traffic shaping can slow down less important protocols, while not entirely cutting of access to the particular service.

Deep packet inspection does come with a heavy cost on the processing and bandwidth sides of the equation. To perform such a thorough look at each individual packet traversing a network, while keeping the throughput speed at normal levels, is quite a challenge. Becchi (2007) and Kumar (2006) showed that advanced algorithms are needed to enhance DPI's ability to meet the challenge. They argued the processing bottleneck is a result of the speed in which comparisons between known electronic signatures and quickly moving data occurs. As the data is moving at ever increasing speeds, it is necessary for the processing to increase at the same rate as the bandwidth. Not until recently have DPI device vendors been able to come close to real time DPI for mass market consumption. Even then, the financial costs can be prohibitive. Anderson (2007) noted that "...top-of-the-line products can set you back several hundred thousand dollars, but some of them can inspect and shape every single packet—in real time— for nearly a million simultaneous connections while handling 10-gigabit Ethernet speeds and above." The processing power needed to make DPI successful at real time speeds has been the major roadblock to widespread adaptation of the technology. Along with throughput concerns comes the fact that DPI devices depend upon software to match, categorize, interpret and finally decide which packets are allowed to pass. As with any software, there are bound to be some cases of vulnerability. According to Porter (2005), Remote Procedure Call (RPC) attacks, stack overflow attacks, buffer overflow attacks, VoIP command processing vulnerabilities and H.225 messages over TCP are all cases of known DPI vulnerabilities. Even though DPI provides a robust manner in which to monitor network communications, it is an evolving technology.

Deep packet inspection can provide many benefits for corporate and ISP environments. The addition of a DPI to a network monitoring portfolio can help to bolster the services and security provided by their respective networks. Increased service levels can be attained by utilizing content-based traffic management while increased understanding and control of their networks will help to cut operating and capital expenditures. Application aware switches can provide increased load balancing, authentication and monitoring capabilities. In addition to increased service levels and more control, DPI can help ISPs secure their networks by implementing network intrusion detection systems based on electronic signatures of well known threats.

Previous network monitoring devices only gave the network administrators an overview of bandwidth, services and the destination of network traffic. By adding DPI functionality, network monitoring takes a step up to the next level. Companies will be able to stop many network attacks in their tracks. Combining existing intrusion prevention technology with the additional filtering of DPI devices will allow for networks to identify and prevent many attacks that currently are able to bypass today's prevention measures. ISPs will be able to shape their bandwidth to better serve their customers most critical needs. DPI will allow them to throttle services at peak usage times to better accommodate the needs of their customers. While a DPI device is in use, ISPs and corporations will gain a deeper understanding of what their networks are actually being used for. This greater level of knowledge will allow them to focus on specific areas of need and not waste time or expense on areas that are performing up to par. As a result of a more controlled network, companies can focus on additional services and offerings that will help to generate additional opportunities for revenue generation. Hill (2006) wrote that "Once ISPs have networks under better control, it is time to look into how to extract additional revenue streams, and DPI can be leveraged to create additional tiers of service."