A Study on Traffic Identification on TCP Protocol

Saravana Kumaran B[1], Marrynal S Eastaff [2]
[1, 2] Department of IT
[1, 2] Hindusthan College of Arts and Science, Coimbatore

Abstract- *The Internet was originally conceived as an open, loosely linked computer network that would facilitate the free exchange of data. The network performance is affected due to congestion. The congestion is occurred due to overloading data over low capacity handling node. Traffic learning and prediction is the heart of the evaluation of the performance of telecommunications networks and attracts a lot of attention in wired broadband networks. A major problem with current Internet traffic monitoring and analysis concerns the large number of newly emerging network-based applications possessing more complicated communication structures and traffic patterns than traditional applications. The amount of traffic generated by these applications, such as peer-to-peer (P2P), streaming media, games, etc., is reported to be well over half of the total traffic. Our simulation is to offer a unified solution for traffic learning and prediction and significantly contribute to solve the modelling and forecasting issues.*

Keywords- TCP/IP, multicast,P2P, bandwidth,traffic congestion.

I. INTRODUCTION

TCP is a transport layer protocol, part of the TCP/IP suite which defines how to establish and maintain a connection in a network. It is a connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols which supports a variety network applications. In internet transmission control protocol is used at large scale whose efficiency depends on congestion avoiding and reliable transfer ability. Congestion control mechanism based on that packet losses due to buffer over flows. TCP is not suitable for wireless links since it cannot differentiate packet losses caused by congestion or link failure. Reduce transfer rate on observing packet losses even having no congestion and causes to lower the TCP's throughput over wireless link than actual which is not justifiable.TCP throughput prediction can provide the guest user with the TCP-friendly rate, which is useful for limiting non-TCP traffic that the guest can introduce to levels that are not disrupting for the network. This is an important application, because clearing guest traffic to be high levels is essential to the success of opportunistic networks. Basically there are two types of flows in the network traffic: unidirectional and bidirectional. The unidirectional flow shares information such as source and destination ports, IP and Transport Protocol. In bidirectional the analysis of flow between source and destination starts from the establishment of connection to end of the network connection.

II. TCP FLOW CONTROL

TCP's primary function is to properly match the transmission rate of the sender and the receiver and the network. It is important for the transmission to be at a high rate to ensure good performance, but also to protect against overpowering the network or receiving host. Flow control is defined as the amount of data a source can send before receiving an acknowledgement from receiver. The flow control protocol must not be too slow (can't let sender send1 byte and wait for acknowledgement). The flow control protocol must make sure that receiver does not get over whelmed with data (can't let sender send all of its data without worrying about acknowledgements).TCP uses a sliding window protocol to accomplish flow control.

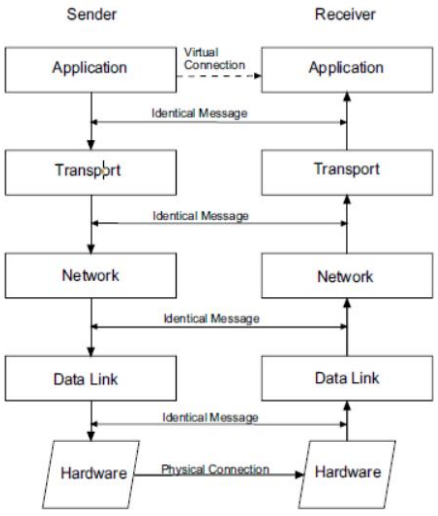

Figure 1.

III. APPLICATION LEVEL TRAFFIC IDENTIFICATION

We assume that all traffic directed to the same subnet is generated by the same application or service. This assumption is reasonable if the traffic is generated by a server-

client application. We consider two steps to determine the original application name of individual packets. The first step is to decide the important port number between source port and destination port. Most traditional Internet-based applications such as WWW, FTP, and Telnet use a well-known port that is below 1024. This shortens determining the important port for packets with a port number below 1024.The servers for a service remain assigned to IP addresses that are also assigned to an organization hence, the same application traffic is observed in a single subnet. On the other hand, most peer-to-peer (P2P) applications are used by desktop PC as both client and server. Application traffic identification methods and classifies them into the following sorts: Session-based, Content-based, and Constraint based Traffic Identification.

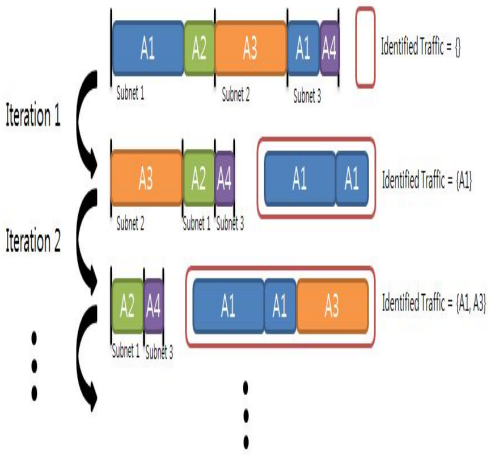

Figure 2.

IV. TRANSPORT LEVEL TRAFFIC IDENTIFICATIOIN

The Peer-to-Peer (P2P) networks have seen a rapid growth, spanning diverse application like online privacy, online payment, file sharing, etc. The success of these applications has raised concerns among ISPs and network administration. These types of traffic worsen the congestion of the network and security vulnerabilities.

Transport level multicast protocol support for distributed applications is essential due to the fact that large scale deployment of network level multicast on the Internet has still not been realized. Most of the efforts in multicast studies are focused on developing new protocols and applications. Reliable traffic estimation of P2P requires examination of packet payload, a methodological landmine from legal, privacy, technical, logistic and fiscal perspectives. Indeed access to user payload is often reduced impossible by one of these factors, inhibiting trustworthy estimation of P2P traffic growth and dynamics.

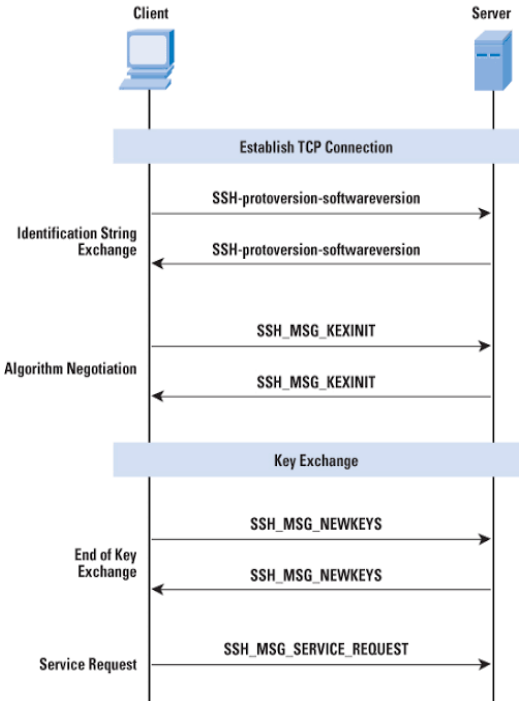

Figure 3.

V. NETWORK LEVEL TRAFFIC IDENTIFICATION

This is the network where telecommunication services are active and router activities are defined. On this layer, data in segments are divided into packages and gradually transferred to the lower layer. In network, the most economical data transfer between two stations is controlled. Owing to this layer, data is directed through routers. Messages are addressed at network phase and also reasonable addresses are changed into physical addresses. At this phase, procedures such as network traffic and directions are completed. IP protocol starts on this layer. Traffic monitoring and analysis is essential in order to more effectively troubleshoot and resolve issues when they occur, so as to not bring network services to a stand still for extended periods of time. Numerous tools are available to help administrators with the monitoring and analysis of network traffic. Router based network monitoring tools available are (SNPM, RMON and Cisco Netflow). They provide information about two newer monitoring methods that use a combination of passive and active monitoring techniques (WREN and SCNM).

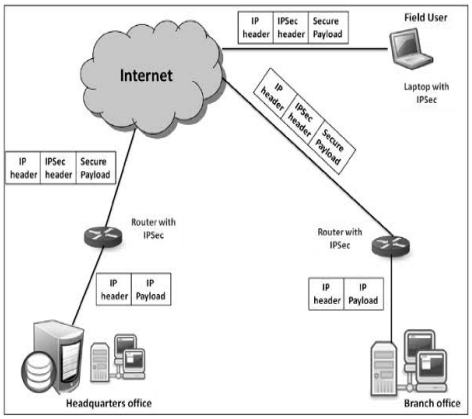

Figure 4.

VI. CONCLUSION

A major challenge in traffic modelling and performance analysis for the transmission control protocol (TCP) shoots that the incoming traffic is not independent of the congestion in the network. The essential behaviour of TCP like flow control that the packet rate of active connections can be curbed in order to avoid overall packet stream exceeds router. By providing appropriate adjustment of the connection duration, the number of packets in the connections remains unaffected. The classifier has limitations needed to be focused in future work, first it cannot identify data packet losses due to timeout expiration, second the database for supervised learning process built by simulation tool that can differ in real physical network environment but classifier is bias free since database included samples of usually maximum network conditions.

REFERENCES

[1] Nasir Jamal, M Zulqarnain, M WaqasBoota, S M Mohsin, Javed A. S "Role of Machine Learning Applications in Communication Network's TrafficClassification to Manage TCP Congestion", International Journal of Novel Research in Computer Science and Software Engineering Vol. 2, Issue 3, pp: (22-25), Month: September-December 2015.

[2] Yan Liu, Yulong Yang , "Analysis of P2P Traffic Identification Methods",Vol. 4, No. 5 May 2013 ISSN 2079-8407 Journal of Emerging Trends in Computing and Information Sciences.

[3] Suhas J Manangi, ParulChaurasia ,MahendraPratap Singh "Analysis of Security Features in 5 Layer Internet Model",International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 777-781

[4] SoniSamprati, "Next Generation of Internet Protocol for TCP/IPProtocol Suite", International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012 1 ISSN 2250-3153.

[5] Dr R Suguna, SuriyaPrakash J, "A Survey On Network Traffic Classification Techniques", International Journal of Pure and Applied MathematicsVolume 117 No. 22 2017, 107-111ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version).

[6] Murat Kayri, SmailKayri, "A Proposed "OSI Based" NetworkTroubles Identification Model", International Journal of Next-Generation Networks (IJNGN) Vol.2, No.3, September 2010.

[7] Security assessment of the Transmission Control Protocol (TCP) Technical notes archive ID: 00003 Ref: TN0309 Date: February 2009.

[8] "Secure TCP - providing security functions in TCP layer"INET'95 Paper no:144

[9] P. Gupta, P. R. Kumar, "The capacity of wireless networks," IEEE Transactions on Information Theory, vol. 46, no. 2, pp. 388–404, 2000.

[10] M. Jain and C. Dovrolis, "End-to-end Available Bandwidth: Measurement Methodology, Dynamics, and Relation to TCP Throughput,"in Proceedings of ACM SIGCOMM, Pittsburgh, PA, August. 2002.

[11] R. Li, Z. Zhao, X. Zhou, J. Palicot, and H. Zhang, "The prediction analysis of cellular radio access network traffic: From entropy theory to networking practice," IEEE Commun. Mag., vol. 52, no. 6, pp. 238–244, Jun. 2014

[12] A. Karasaridis and D. Hatzinakos, "Network heavy traffic modeling using alpha-stable self-similar processes," IEEE Trans. Commun., vol. 49, no. 7, pp. 1203–1214, Jul. 2001.