Journal of Engineering Education Transformations,
Volume 30, No. 3, January 2017, ISSN 2349-2473, eISSN 2394-1707

Encourage research thinking in network domain using traffic analysis tool

Padmashree Desai[1], Vijayalakshmi M[2]., Meenaxi M.Raikar[3]
[1,2,3]Department of Computer Science and Engineering B.V.B.College of Engineering and Technology
[1]padmashri@bvb.edu,[2]viju11@bvb.edu,[3]mmraikar@bvb.edu

Abstract: Explosive growth of Computer network technologies and use of these technologies have led a new thinking for researcher. In recent days the research focus in network domain is on areas like, Performance measurement of broadband and mobile access networks, Censorship measurement and circumvention, Software-defined networking (SDN), Internet of Things (IoT) security. This has created a challenge to the academicians to make students think towards these research fields and to adopt activity based teaching learning techniques to deliver the basics as well as the advanced concepts of computer network. As most of the students are visual learner teaching computer networking principles can be enhanced using simulation through the use of interactive simulation. With networking simulation tools, students can construct, tune, and analyze network performance while reinforcing their understanding of networking theory.

The course expects the students should have an ability to understand the concepts, design and analyze the performance of the network. Experience of authors says that have an ability to understand the network concepts but they lack in analysis. So authors have put effort to address the lacunae. The activity has been designed by integrating theory and laboratory course on computer network which focuses on network traffic analysis by applying the concepts learnt. WireShark traffic analysis tool is used by students to capture the real time data and analyze the data for the selected network protocol. The paper discusses the design, conduction of activity, in computer network course focusing on analysis on network traffic which in turn created a space to think on research related to the network domain. Through this activity we could attain course outcome 3 and Program outcome (PO) 4 and 5 which is more than 80%.

Keywords: Traffic Analysis; WireShark; Research; Network.

1. Introduction

Network traffic analysis plays a very important role in the industry as well as in research field. The traffic analysis is basically used for optimization and event detection, finding patterns from which we can decide the resource utilization or performance improvement like packet loss, bandwidth management in computer networks, diverting the traffic on to different routes to handle the congestion

Padmashree Desai
Department of Computer Science and Engineering
B.V.B.College of Engineering and Technology
padmashri@bvb.edu

on streets. In its most general case, traffic analysis is intelligence gathering done by looking at the metadata of a conversation, rather than the actual content and making deductions and inferences based upon that metadata.

Network analysis also gives the insight into wide area and local area network and does the analysis pertaining to network traffic flows, individual data packets, bandwidth utilization and even protocols which can allow the IT organization to have better operating performance. The information which network analyses provide can be used to resolve the issues by degradation of the network performance and can improve network availability, track quality of service metrics, and minimize the mean time to repair problems when they arise through rapid detection and accurate isolation.

Network Analysis is also important in online social media, as online social media has become an integral part our daily life, as we are connected to people, information, places and events. In technical way if we think sense of connection makes to analyse the structure, evolution and traffic by connecting different disciplines like mathematics, sociology, computer science, economics etc[1].

1) Research directions in network domain.

Following sections discuss some of current focus areas of research in network traffic analysis.

a) Performance measurement of broadband and mobile access networks.

As broadband Internet access has became insidious, so understanding the performance of the user receive data and how they use the available resources is important than earlier. Research includes to:

- Understand the performance of Mobile data usage and performance.
- Investigating the locations of congestion.
- Troubleshoot performance of Home network.
- Measure the performance and characterization of emerging technologies.

b) Censorship measurement and circumvention.

Internet censorship has been implemented by more than 60 countries in the world. In this the possible research questions are

- To collect and analyse the measurement of internet censorship.
- To have the improved understanding of the limitations and capabilities of circumvention tools existing.
- To design the novel approaches for circumvention.

c) Software-defined networking (SDN).

SDN makes it potential to control the behaviour of the network from a single high-level program. This standard opens up many new possibilities, since controlling the network becomes a software development problem, rather than one that is constrained by low-level, vendor-specific, proprietary interfaces. This research space includes:

- Applications of SDN to Wide-Area Networking.
- Fast, scalable and accurate inference algorithms that can provide input to network control systems.

d) Internet of Things (IoT) security.

The diversity and increasing number of consumer electronics devices connected to the Internet introduces a serious security hazard, since many of these devices are "fundamentally insecure". Given that we are likely to have a large number of insecure devices connected to the network that cannot be patched, we need new capabilities in the network that ensure both the security of these devices and the privacy of their users. Main questions arise are:

- Device fingerprinting. The traffic patterns are from devices on the network and determining the types of devices which are connected to the network.
- Anomaly detection. Designing and developing algorithms to identify the abnormal behaviour of the IoT device. Incorporate these algorithms into a "network firewall" that can automatically detect and mitigate abnormal or attack traffic.

2. Need of Simulation tool in teaching learning process.

Visual learning demands the use of images, animations, simulations[2] and graphics to enable and improve the learning in computer network course. Visual learning is a proven method in which ideas,

concepts, data and other information are associated with images and animations, while the subject is represented graphically. As an example, techniques and tools such as flowchart, UML, simulator and animations are used in visual learning to enhance thinking and learning skills. Students can understand subjects much more easily if they can see, or even touch them in real. Visual learning uses methods that help students to open their minds and think graphically. Associations between images and some sort of information can help to better memorize and use the learned knowledge or information.

Chinese proverb says "Tell me and I forget. Show me and I remember. Involve me and I understand." The understanding of network protocols can be greatly improved by seeing the action of protocols, and playing around the protocols by observing the sequence of messages switch over between the two protocol entities, exploring them into the details of their operation, modifiying few parameters causing harm to protocols and then observing the actions and their consequences. These things can be done by using simulators either in real time or in simulated environment.

These things made us to think of traffic analysis tool for teaching some of the basic concepts further same tool can be used to explore other details. The benefit of using network analysis tool has the considerations like Accessibility, Aggregation, Granularity, and Visibility.

a) Why traffic analysis is to be taught at UG level?

Traffic analysis tools can be used to enhance students' understanding and develop network traffic analysis skills at Under Graduate (UG) level. The table 1 shows the opportunities of research in network domain, if we make the students to work on these analysis techniques at undergraduate it will ignite their mind to think towards the research in network domain.

Observations in Computer Network Domain	Key areas of research and development
• Networking traffic will quadruple by 2017 driven by wireless and mobile communication • 2+ billion videos watched online every day. • Mobile, tablets and sensors to join with existing internet cloud to form "network of things".	• Mobile Ad-hoc Networks • Wireless Sensor Networks • Cognitive Radio • LTE/LTE-A • Internet of Things (IoT)

Network traffic Analysis tools available.

Following are some of the network traffic monitoring tools available but not limited to these - Microsoft Network Monitor ,Nagios, OpenNMS,Advanced IP Scanner, Capsa Free Fiddler ,NetworkMiner, Pandora FMS, Zenoss Core.

b) Why WireShark?

WireShark is an open source and free network protocol analyser which runs on a variety of operating systems including, Mac, UNIX, and Windows and Linux. A basic tool which is used for observing messages which are exchanged between the protocol entities in Packet sniffer. This is an important part of protocol analyser [3].

It passively sniffs packets that are received by or sent from a designated network interface, but never sends packets itself. The copy of packets is received by or sent from the applications and protocols which are executed at the end system. It has graphical front end to display the packets which it has sniffed. Figure.1. shows the network protocol analyser structure.

According to literature, the research papers in IEEE or ACM indicate that 50% of papers use Wireshark for network traffic analysis. Also Table 1 explains the observations in network areas and key areas of research in this domain. This creates job opportunities in network domain.

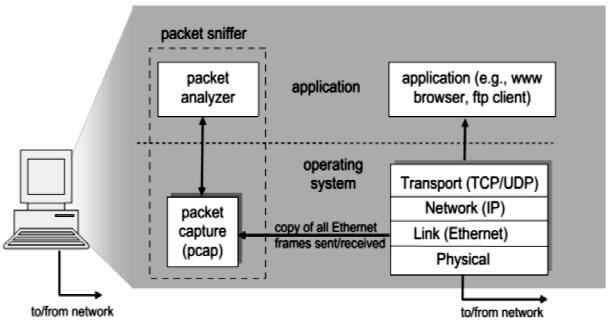

Figure 1: Network protocol analyser structure

3. Proposed methodology

1) Research problem

Implant the research thinking in undergraduate students in the network domain. In this students were made to think on the importance of network analysis.

The research was developed and conducted in computer network laboratory course and aimed to get an ability to analyse and interpret the data collected from the real time network.

2) Research tasks

1. Exploring how important the network traffic analysis in today's scenario.
2. Use of appropriate tools, techniques and procedures to collect and analyse Data.
3. Critical analysis of data for trends and correlations, stating possible errors and limitations.

The students are instructed to do the literature survey to know the importance of the network analysis and field in which this is going to be the important in future research. Explore the network analysis tools available and comparison has to be done to choose the one to implement. Get the proficiency in the tool to perform the defined task. Finally analyse and interpret the data.

3) Methodology:

Course Outcomes are written for Computer Network Laboratory course following Outcome based education (OBE).

a) Course Outcomes (COs):

At the end of the course the student should be able to:

CO1. Demonstrate the network scenario using different networking commands.

CO2. Simulate a given network topology and analyse the performance for different network parameters.

CO3. Analyse the behaviour of different network protocols using the analysis tool.

CO4. Develop client server applications using TCP/UDP for wired/wireless devices.

The Computer network theory course is integrated with computer network laboratory and accordingly designed the experiments keeping two things in the mind i.e. one is making students to have better understanding of fundamental network concepts and the second one is to bring the research thinking in network domain using network traffic analysis as analysis of network data generated is very important as discussed in previous section number.

As mentioned in the Figure 2 , the entire course focuses on two tools i.e CISCO packet tracer is used to give better understanding of fundamental network concepts [6] and another tool is WireShark which is network traffic analysis tool used to collect the data , analyse and interpret the result.

Our further discussion is to implant the research interest in students by using network traffic analysis tool- WireShark.

An activity has been designed in computer network laboratory course pertaining to the experiments designed on network traffic analysis using Wireshark to address the research problem proposed.

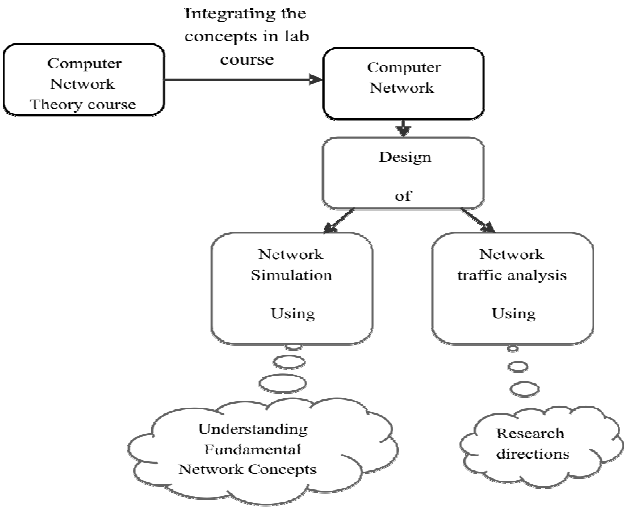

Figure 2: Activity Framework of computer Network laboratory course

b) Design of Activity:

The activity is designed to attain the course outcome 3 (CO3); Analyse the behaviour of different protocols using the analysis tool.

- Objective of the activity:

1. To investigate the usage of network resources
2. To assess the performance of network applications
3. To identify the Quality of Service (QoS) suitable for the study.
4. To create research in students.

Experiments have been designed by integrating concepts of theory in laboratory, where students observe the traffic generated in real time and analyse different aspects of network traffic.

A team of four members are assigned the activity where each team has to choose a protocol and they need to learn the tool so that they can capture the data in real time scenario required for analysis of the protocol. Set the QoS parameters for the study of the protocol. Analyse the data captured and interpret the data and finally draw the inferences. The flow of the activity is shown in figure 3.

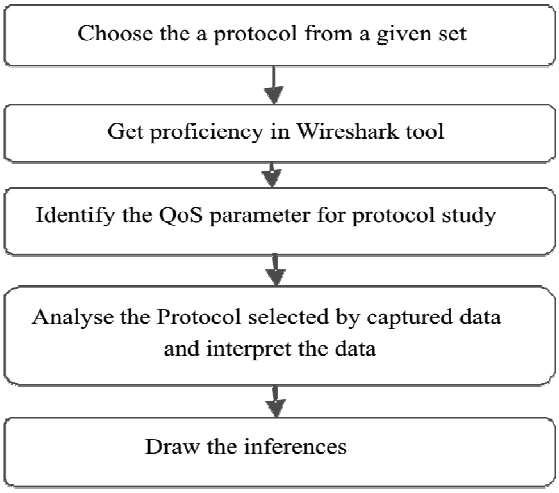

Figure 3: Flow of activity conduction

Table 2 lists the different protocols assigned for each team and observations they need to do it.

Table 2: List of Protocols

S.N.	Tasks	Observations
1	Explore several aspects of the HTTP protocol	The basic GET/response interaction, HTTP message formats, retrieving large HTML files, retrieving HTML fi les with embedded objects, and HTTP authentication and security.
2	Study TCP's use of sequence and acknowledgement numbers for providing reliable data transfer	TCP's congestion control algorithm – slowstart and congestion avoidance – in action; and TCP's receiver-advertised flow control mechanism.
3	Study working of UDP used for communication	The characteristics of UDP packet loss are investigated through simulations
4	Investigate the IP protocol, focusing on the IP datagram	Analysing a trace of IP datagram's sent and received by an execution of the trace route program
5	Investigate the Ethernet protocol and the ARP protocol	How ARP protocol is used by an IP device to determine the IP address of a remote interface whose Ethernet address is known.
6	How ICMP (Internet Control Message Protocol) is used in companion with IP that helps IP to perform its functions by handling various error and test cases.	ICMP error packets (where Time-to-live is exceeded)
7	Investigate the behaviour of the NAT protocol.	Capturing packets at both the input and output of the NAT device & study patterns

c) Assessment:

The activity is assessed by team of evaluator on the set of parameter and defined rubrics as per the Program Outcome (PO), Competency, and Performance indicators (PI) and Blooms Level (BL) are as shown in table 3. The detailed rubrics are given in table 3. The authors planned to show the attainment of program outcome 4. Which focuses on use of research based knowledge to conduct experiments, analyse and interpret the data.

Table 3 PO-CO-BL Matrix

Course Outcome 3: Analyze the behaviour of application layer protocols using the analysis tool.			
Program Outcome 4: Conduct investigations of complex problems:	Use research -based knowledge and research methods includi ng design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.		
Competency 4.3	Demonstrate an ability to critically analyze data to reach a valid conclusion		
Program Outcome 5: Modern Tool Usage:	Create, select and apply appropriate techniques, resources, and modern engineering and IT tools, including prediction and complex engineering activities, with an understanding of the limitations.		
Competency 5.3	Demonstrate an ability to apply IT too ls for the chosen engineering activity		
Performance Indicators			
Performance Indicators	Description	Parameters of Assessment Rubrics	Blooms Level
CSPI 4.3.1	Use appropriate procedures, tools and techniques to collect data and analyze	Demonstration of given protocol using wireshark tool	L3
CSPI 4.3.2	Critically analyze data for trends and correlations, stating possible errors and limitations	a. Statistical analysis of the captured packets for the given protocol using various parameters.	L4
		b. Interpretation of data and drawing the Conclusion.	L4
CSPI 5.3.1	Demonstrate proficiency in using IT tools for performing engineering activity		L3

d) Implementation Details of sample activity

The activity is conducted for class strength of 140 students which is divided into 36 teams. This section discusses the sample implementation as part of activity carried out by the students.

The students have done the analysis of TCP protocol using WireShark tool. The snapshots of the results are shown below in (figure 4-7). Using WireShark tool the students captured packets of sending E-mail (SMTP), they have done the packet analysis, calculated RTT (Round Trip Time), Throughput and understood the three way handshaking mechanism involved in E-mail transmission using packet details.

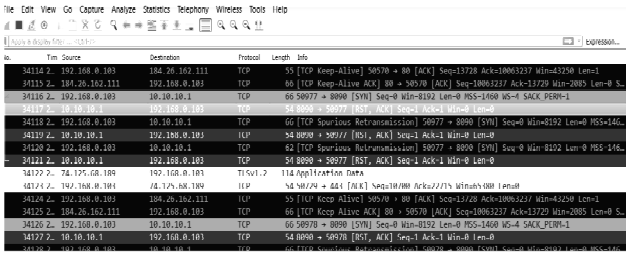

Figure 4: Packet details of Email transaction

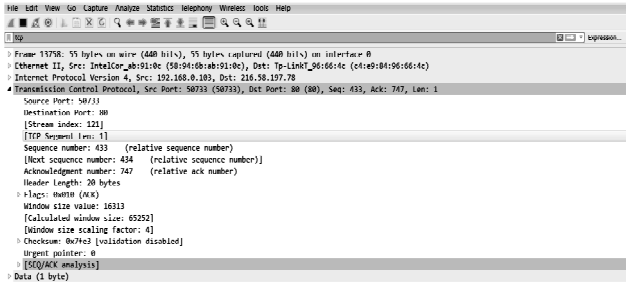

Figure 5: Packet details of Email transaction between source and destination.

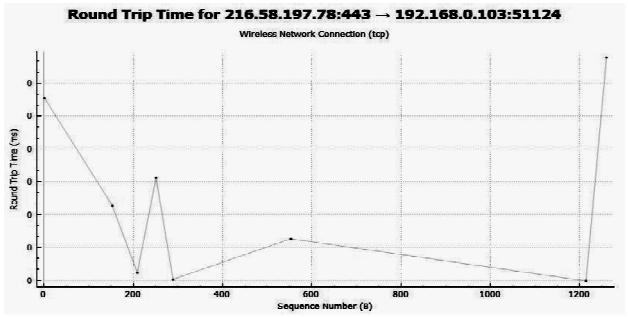

Figure 6: Round Trip Time of Email transaction between source and destination.

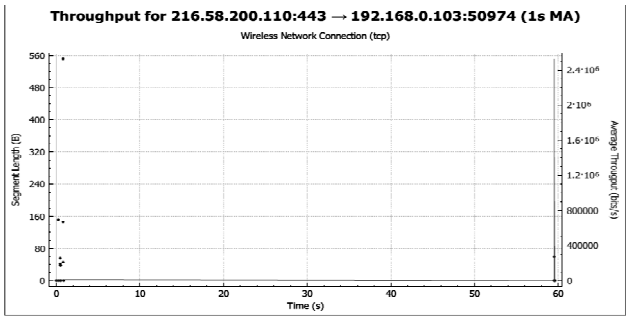

Figure 7: Through put for Email transmission from source to destination.

4. Result and Discussions

The activity is assessed through set of parameter and rubrics. The marks obtained are used to show attainment of course outcomes and analysis of these data is done by the Contineo (Student information management software). Figure 8 shows the % attainment of course outcome 3, from the graph it is observed the outcome 3 is almost equal to the target set by the course. Figure 9 shows the % attainment of Program outcome 4 and 5. The feedback taken from students (140 samples) on the set questionnaire which is shown in table 4. The feedback analysis is shown in Figure 10 and it is observed that more than 80% of the students strongly agree that the activity has helped and motivated towards research thinking in the network domain.

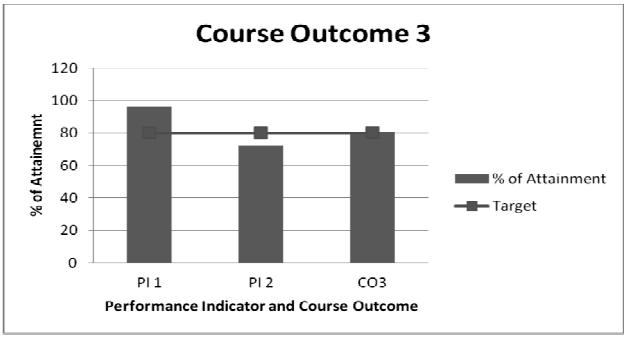

Figure 8: Attainment of Course Outcome through performance Indicators

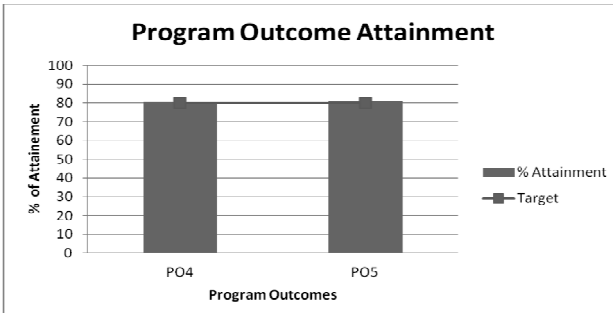

Figure 9: Attainment of Program Outcome

Table 4 Feedback Questionnaire

Sl. no.	Questions	Strongly Agree(SA)	Agree(A)	Neutral(N)	Disagree(DA	Strongly Disagree(SDA)
1	The activity helped to explore the tools available for network traffic analysis.					
2	The activity helped to understand the working of protocol.					
3	Activity has helped to understand the need of traffic analysis.					
4	Activity h as created an interest in the network domain towards research.					
5	Activity has made us to work in a team.					

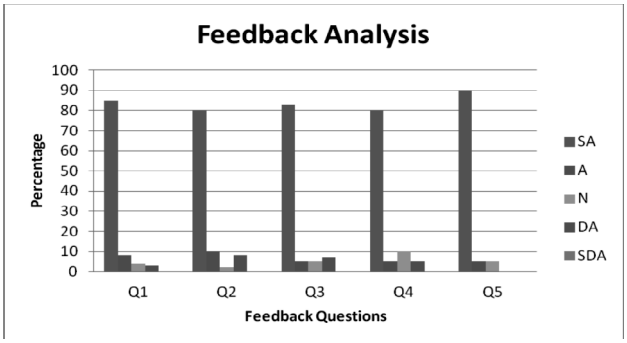

Figure 10. Feedback analysis

5. Conclusion

The traffic analysis is needed for optimization and event detection, resource utilization and performance improvement. Due to technology advancement in network domain which has created challenges for researcher and job opportunities for engineers. Introduction of WireShark for traffic analysis at UG level helped to cope with the industry needs. The outcome of the activity shows the 80% of attainment of the CO3 and PO 4 and 5.

References

[1] Thomas Allmer, "Research Design & Data Analysis, Presentation, and Interpretation: Part One The Internet & Surveillance" - Research Paper Series: 2012 (http://www.sns3.uti.at)David R. Surma, "Lab Exercises and Learning Activities for Courses in Computer Networks", 33 ASEE/IEEE Frontiers in Education Conference, November 5-8, 2003, Boulder, CO.

[2] Jesús Expósito, Valentina Trujillo, and Eric Gamess , "Using Visual Educational Tools for the Teaching and Learning of EIGRP", Proceedings of the World Congress on Engineering and Computer Science 2010 Vol I WCECS 2010, October 20-22, 2010, San Francisco, USA"

[4] Gerhard M¨unz, Georg Carle, "Real-time Analysis of Flow Data for Network Attack Detection" European research project and partly funded by the European Commission (FP6 IST-2002-002154).

[5] Network Analysis by Nigel Trodd 2005.

[6] Vijayalakshmi M., Padmashree Desai, Meenaxi M. Raikar,"Packet Tracer Simulation Tool as Pedagogy to Enhance Learning of Computer Network Concepts", IEEE MITE conference 2016.

[7] http://www.gfi.com/

[8] http://www.nyu.edu/