International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-4 Number-2 Issue-15 June-2014

ATM, FDDI and Network Intrusion Simulation for Packet Data Networks

Shahiruddin[1], D K Singh[2], Nidhi Verma[3], Sugandha Shukla[4]

Abstract

In this paper we describe the use of the OPNET simulation tool for analysis of packet data networks. The motivation is to provide knowledge on packet level networks: Fiber Distributed Data Interface and Network intrusion simulation. FDDI protocol is examined by varying network parameters in two network configurations. Geographic distribution of servers and workstations in different buildings by capitalizing on the long-distance capability also saves money by eliminating the necessity for moving equipment to a single location provides high utilization on the FDDI LAN, thus lowering the cost of transporting data. We discussed about OPNET process model and its performance and effect on the traffic patterns in an ATM network. In this paper we also report studies of simulation efficiency and network performance of simulated network using firewall.

Keywords

OPNET, Network simulation, Intrusion Simulation, Firewall, CBR, ABR, RT_VBR, NRT_VBR, and UBR

1. Introduction

Fiber Distributed Data Interface (FDDI) and Asynchronous Transfer Mode (ATM) are two well-known technologies used these days. FDDI specifies a 100-Mbps, token-passing, dual-ring LAN using a fiber-optic transmission medium that can extend in range upto 200km.It defines the physical layer and media-access portion of the link layer, and so is roughly similar to IEEE 802.3 and IEEE 802.5 and follows Open System Interconnection (OSI) as a reference model[1]. FDDI is quite similar to token ring, the only difference is that it is a bit faster.

Manuscript received April 27, 2014.
Shahiruddin, Electronics and Communication Engineering Department, Birla Institute of Technology, Patna, India.
D K Singh, Electronics and Communication Engineering Department, National Institute of Technology, Patna, India.
Nidhi Verma, Electronics and Communication Engineering Department, Birla Institute of Technology, Patna, India.
Sugandha Shukla, Electronics and Communication Engineering Department, Birla Institute of Technology, Patna, India.

One of its most important characteristics is that it uses optical fiber as a transmission medium which offers several advantages over traditional copper wiring, including security, reliability and speed. The protocol of the FDDI standard provides a natural means for message integrity and availability verification [2].

The high demand for fast web based applications and multimedia transmissions are the major driving force behind emergence of (Asynchronous Transfer Mode) ATM technology. ATM is a growing technology used to support the high-speed networks.It transports different types of information including voice, data, and multimedia. It was designed for a network that must handle both traditional high-throughput data traffic and real-time, low-latency content such as voice and video. The reference model for ATM approximately maps to the three lowest layers of the ISO-OSI reference model. It is a core protocol used over the SONET/ SDH backbone of the public switched telephone network (PSTN) and Integrated Services Digital Network (ISDN), but its use is declining in favour of all IP. Its different applications require different QoS and therefore different Service categories. It has five different service categories CBR, ABR, RT_VBR, NRT_VBR, and UBR. Each provides a different QoS and a different traffic management procedure. ATM also helps to minimize infrastructure costs by effective bandwidth management, and the integration of overall networks. ATM technology allows core network stability while allowing service interfaces and other equipment to evolve rapidly [3].

2. FDDI Networks

FDDI networks are token passing networks that support data rates of up to 100Mbps. A token is made to around a ring. Whenever a station wants to transmit, it waits for the token arrival. Upon receiving a token it can transmit for a fixed interval called Time Holding Time (THT) .After the transmission, the station either release token immediately or after arriving of the entire packet it transmitted.
We simulate FDDI Protocol performance in this report. Various parameters like number of stations attached to the ring load, bandwidth allocation and

target token rotations time (TTRT) can be changed. The performance of FDDI with network parameters such as throughput, delay and collision count has been evaluated. We can increase the length of queue at each server by increasing the number of packets (load) in the network. A time varying relation has been produced between the throughput and sent packets in traffic characteristics. In any case of throughput it increases with delivered load and reaches a certain value but after the attainment of maximum value any further increase in load leads to decrease in throughput. Therefore, selection of load is an critical task in order to maximize the throughput. Fact behind this is the, occurrence of more collisions due to increase in traffic leads to retransmission of frames and hence increases the overall delay factor [4].

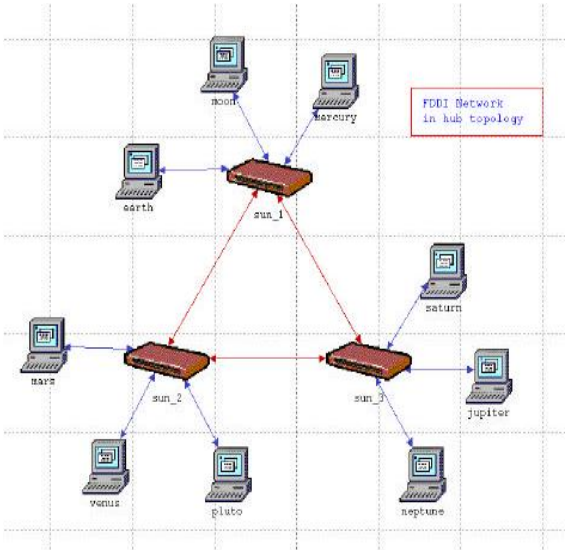

Figure 1: Network consists of 3 concentrators and 9 stations [5].

In addition to being large geographically, FDDI LAN can support thousands of users. FDDI is frequently used on the backbone for a wide area network (WAN).An FDDI network consists of two token rings. The primary ring offers up to 100 Mbps capacity and the secondary used for possible backup in case the primary ring fails. In the absence of secondary ring it can also speed up to 200 Mbps .Both single- and dual-attachment options for high-availability alternate paths also provide support for an optical bypass switch to keep the FDDI loop operating even if a station fails. Other benefits include speeding up Ethernet to 100 Mbps, thus providing faster access to important Internet and intranet Web applications. Also it helps to eliminate network bottlenecks caused by lower-bandwidth LAN links, reduces downtime caused by link outages, allows geographic distribution of servers and workstations in different buildings by capitalizing on the long-distance capability and saves money by eliminating the necessity for moving equipment to a single location, thus lowering the cost of transporting data.

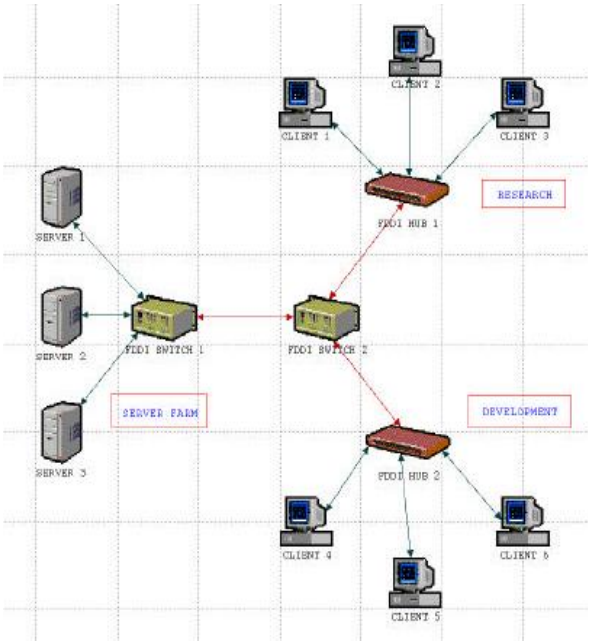

Figure 2: Clients are connected to the network via hubs. Hubs and servers at different locations are connected via two FDDI switches [5].

This network topology is suitable for applications such as FTP. In it we can see that the clients are connected to the network through FDDI hubs. Hubs and servers at different locations are connected via two FDDI switches deployed for real time applications such as voice and video, which put tight constraints on delay and delay jitter.

We now consider the second network configuration. In this network the time-average FDDI end-to-end delay is shown (Fig. 3).Our motto is to analyse the FDDI network performance for one custom application - file transfer protocol (FTP). From the plot it can be observed that as the network load increases the end to end delay decrease in the network. Also it can be seen that the delay is

levelling off with time, which indicates that it is a stable network.

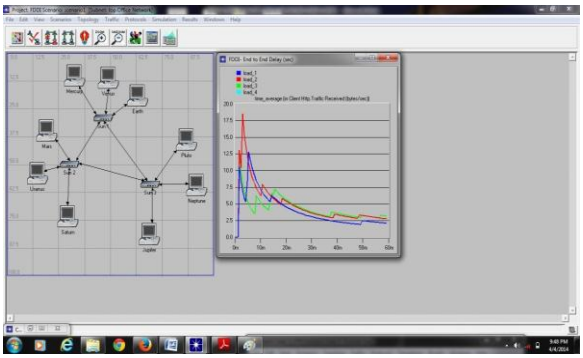

Figure 3: End-to-end delay plots with load parameter, Delay levels off with time indicating that the network is stable

Messages in the network can be classified into two classes synchronous and asynchronous. Synchronous messages are used primarily for real-time communication and suited for audio and video transmission. In synchronous communication between a client and a server, the client after sending message, waits for the server to respond to that message. So in this case if one end is down the entire communication will fail .Synchronous, or real-time, communication takes place like a conversation for example it may include chat sessions. While in case of Asynchronous communication client does not need to wait for the message from the server. An event is used to trigger a message from a server. Sending an email or file transfer are examples of asynchronous messages.

FDDI token ring network provides a guaranteed throughput for synchronous messages and a bounded medium access delay for each station. However, only this cannot effectively support many real-time applications that require the timely delivery of each critical message. Synchronous bandwidth allocation scheme calculates the synchronous bandwidth necessary for each station to satisfy its message-delivery delay requirement for supporting real-time communication.

Since real time communication requires a minimum bandwidth allocation for the synchronous messages so applying this in its strategy FDDI MAC ensures that every station in the network is guaranteed a certain average bandwidth for its synchronous traffic, with the remaining bandwidth dynamically shared by all stations for asynchronous traffic. The FDDI provides a priority mechanism in which it essentially locks outstations that cannot use synchronous bandwidth [6].

3. ATM

Asynchronous transfer mode protocol is a cell relay protocol designed by the ATM forum and adopted by ITU-T.The combination of ATM and SONET will allow for high speed interconnection of all world's network.ATM is a cell switched network which uses the cell as the basic unit of data exchange.A cell is defined as a small ,fixed size block of information. The user access devices called end points are connected through the user to network interface(UNI) to switches inside the network.The switches are connected through network to network interfaces(NNI).Connection between the two ends points is accomplished throgh transmission paths,virtual paths and virtual circuits.Transmission path is the physical connection between the end points and the switch or between two switches.Virtual path are the combination of virtual circuits that are bundled together because parts of their paths are the same.Virtual circuits logically connects two points.ATM uses switches to route the cell from source endpoint to destination endpoint using both virtual path identifiers and virtual circuit identifiers. Some form of transmission structure must be used to transport ATM cells. One option is the use of a continuous stream of cells, with no multiplex frame structure imposed at the interface. Synchronization is on a cell-by-cell basis. The second option is to place the cells in a synchronous time-division multiplex envelope. In this case, the bit stream at the interface has an external frame based on the Synchronous Digital Hierarchy (SDH).

ATM has very developed congestion control and quality of services.The ATM forum defines following five sevice classes:

- CBR-Constant bit rate is designed for the customers who need real time audio or video services.
- VBR-Variable bit rate class is divided into subclasses: real-time and non real time.VBR-RT is designed for the users who need real time services and use compression techniques to create variable bit rate.VBR-NRT is designed for those users who don't need real time services but compresssion techniques to create variable bit rate.

- ABR-Available bit rate class delivers cell at minimum rate.It is particularly suitable for applications that are bursty.
- UBR- Unspecified bit rate class is best effort delivery service that doesn't guarantee anything.
- GFR-Guaranteed frame rate is designed specifically to support IP backbone subnetworks.It provides better service than UBR for frame-based traffic,including IP and Ethernet.Its major goal is to optimize the handling offrame-based traffic that passes from a LAN through a router onto an ATM backbone network.

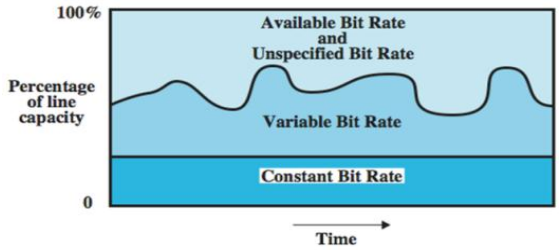

Figure 4: Relationship of service classes to total capacity of network

OPNET library contains ATM client-server network with client demanding different QoS like CBR and ABR. To observe the performances of various service categories we have total five clients. Each client having different service category, sends request packets of 1 byte to the server. The request is generated at same rate for all clients. The connections from the clients will only be admitted only if all the intermediate nodes in the network which includes clients and the switches, can support the requested bandwidth and QoS.

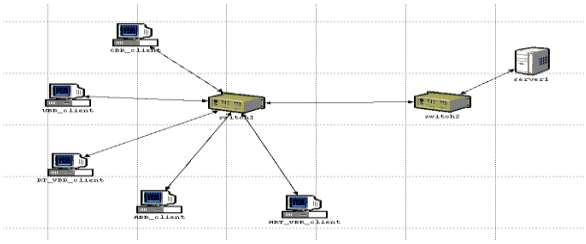

Figure 5: Network consisting of two switches, and ATM server, and five clients all requesting distinct service categories [5].

Once it checks the bandwidth and Qos is supported by nodes the call is admitted. The request is then routed through the switches to the server. The server processes the requests applied by the clients and sends them response packets of 500 bytes. Traffic patterns received by each client are shown in Fig.6. From the plot it can be observed that the traffic has a constant bit rate for the CBR client and is of a more bursty nature for the remaining clients. The Propagation delay (sec) is the smallest for the CBR source.

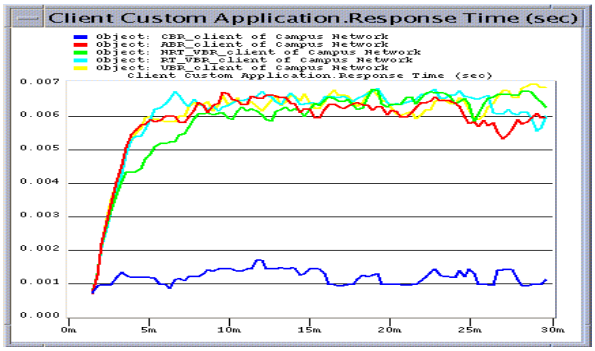

Figure 6: Among all the service categories CBR has the smallest response time, hence the best QoS [5].

Comparing and Ranking the performance of these ATM service categories is very difficult as they differ in various aspects. Each service categories has their certain features which are advantageous and desirable while certain which are undesirable. For real time application in which there are tight constraints on delay and jitter, we usually deploy CBR and RT_VBR traffic. CBR is, however, more reliable. [7].It requires the user to determine a fixed bandwidth requirement at the time of connection is setup so that the data can be sent in a steady stream. . CBR processes audio faster than VBR due to its fixed bit rate value. The downside to a fixed bit rate is that the files that are produced are not as optimized for quality vs. storage as VBR.

4. Network Intrusion Simulation

Wireless has opened a new and exciting world to many of us. However wireless networking is vulnerable in many ways like eavesdropping, illegal use, Mac spoofing, null probes, flooding. IPsecurity (IPSec) is a collection of protocols designed by Internet Engineering Task Force (IETF) to provide security for packet at the network level. It helps to

create authenticated and confidential packets. It requires logical relationship between two hosts called security association (SA).The Internet Key Exchange (IKE) is protocol designed to create security associations, both inbound and outbound. Two protocols are dominant today for providing security at transport layer: Secure socket layer (SSL) and Transport Layer Security (TLS).SSL provides security, compression, fragmentation, message integrity, confidentiality, and framing of data received from application layer. There are other security protocols like Pretty Good Privacy (PGP) for security of email system.

Even all these security measures cannot prevent eve from sending harmful message to a system. An array of techniques are applied by hackers cause disruption of normal functioning , but on the defense, the firewalls and practical intrusion detection systems (IDS) nowadays are only effective in defending known intrusions using their signatures [8].

A firewall is a device (usually a router or a computer) installed between internal network of an organization and rest of the internet. It is designed to forward some packet and filter some. Firewall is classified as a packet-filter firewall and proxy based firewall. A packet-filter firewall filters at network or transport layer. A proxy firewall filters at the application layer. Intrusion detection and prevention system (IDPS) is a security system that monitors the computer and network traffic for possible hostile attacks originating from outside organization and also for system misuse or attack originating from inside the organization ,track down the accurate location of vulnerable or threat posing device and attacker's device using smart forensic technique. Majority of intrusion detection prevention system utilizes signature based detection system. Signature detection is most popular type of IDS and they work by using database of known bad behaviors and patterns. Signature detection engines can query any portion of a network packet or look for specific series of data bytes. The defined pattern of codes are called signatures and often they are included as part of a governing rule when used within an IDS.

Our work deals with simulation of intrusion traffic by generating data packets based on real-life data that contain intrusion packets. In this OPNET simulation, we explicitly generated traffic to our research dealing with data filtering and intrusion detection strategies.

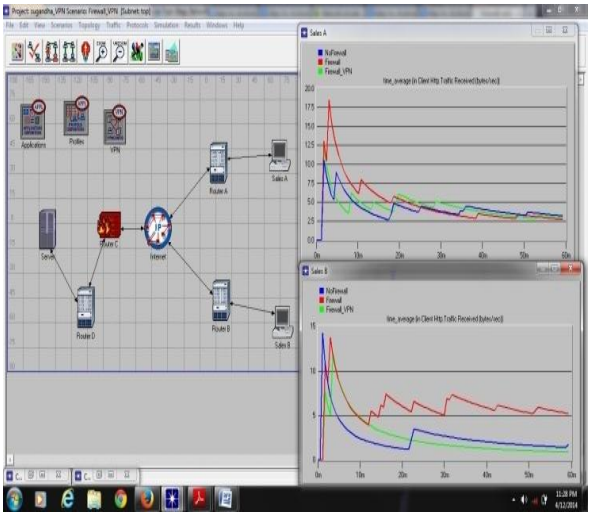

Figure 7: The overall network traffic during simulation. It has three scenarios- No Firewall, Firewall, Firewall_vpn.

5. Conclusion and Future Work

We simulated two commonly used packet data network technologies FDDI and ATM. One FDDI and one ATM network scenarios were implemented. We used simulations to compare the performance of various service categories in ATM networks. It was shown that CBR traffic delivers the least delay and delay jitter among ATM service categories. The future work is a process model for the leaky bucket policing mechanism in ATM networks. The model named 'leaky bucket' is available from the OPNET Contributed Model Depot. This model can be used to work in a source-destination network scenario. It can be used to check that data transmissions in the form of packets conform to defined limits on bandwidth and burrstones (a measure of the unevenness or variations in the traffic flow). It can also be used as a scheduling algorithm to determine the timing of transmissions that will comply with the limits set for the bandwidth and burrstones.

References

[1] Fiber distributed data interface Url: http://srohit.tripod.com/FDDI.pdf.
[2] Fiber distributed data interface, Url: http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Fiber_distributed_data_interface.html.
[3] Dr. S. S. Riaz Ahamed, "The role of ATM technologies in future data communication systems", Journal of Theoretical and Applied

Information Technology. Vol.4 No 7/10 pdf, 2005.
[4] Amarvir Singh, "Throughput Analysis of Ethernet and Fiber Distributed Data Interface using OPNET IT Guru Academic Edition 9.1", An International Journal of Engineering Sciences ISSN: 2229-6913 Issue Sept 2011, Vol 4 No 455.
[5] FDDI ATM, Url: http://www2.ensc.sfu.ca/~ljilja/NSC833/Spring01/News/Presentations/FDDI_ATM.pdf.
[6] FDDI Adapter Cards Information Library, Url**:** http://www.hp.com/products1/serverconnectivity/adapters/adapter05/infolibrary.html.
[7] Nazy Alborz, Maryam Keyvani, Milan Nikolic, and Ljiljana Trajkovic, "Simulation of Packet Data Network Using Opnet" ppt.
[8] Network Intrusion Simulation using opnet www.cs.ucf.edu/csdept/faculty/lang/pubs/opnet2002.pdf.

Nidhi Verma was born on December 23 ,1992 in Patna (Bihar).She has done her schooling from D.A.V. Public School, B.S.E.B. Patna. She is currently pursuing Electronics and Communication Engineering at Birla Institute of Technology, Extension Center Patna. Her fields of interest include networking and communication.

Sugandha Shukla was born on 26 February 1992 in Bareilly (Uttar Pradesh). She completed her schooling from Bishop Conrad Senior Secondary School. She is currently pursuing Electronics and Communication Engineering at Birla Institute of Technology, Extension Center Patna. Her fields of interest include networking and communication.