Efficiency Evaluation of Simulated Networks Using Opnet And Firewall

Kavitha Kuthumbaka *(Computer Science), Research Scholar, SunRise University, Alwar(Rajasthan)*
Dr.Pawan Kumar Pareek ,(Computer Science) Assistant Professor, SunRise University , Alwar (Rajasthan)

ABSTRACT

In this research, we present a method for analysing packet data networks using the OPNET simulation tool. The goal is to educate users about packet-level networks, such as the Fibre Distributed Data Interface and Network Intrusion Simulation. The FDDI protocol is investigated by switching between two networks with different settings. High utilisation on the FDDI LAN reduces the cost of transporting data, and geographically dispersing servers and workstations in different buildings to make use of the long-distance capability is a cost-effective strategy. The effectiveness of the OPNET process paradigm and its impact on ATM traffic patterns were discussed. In this research, we also present results from analyses of the effectiveness and performance of firewall simulations in simulated networks.

Keywords : OPNET Simulation, FDDI LAN, ATM Traffic Patterns.

INTRODUCTION

Simulated networks using OPNET and firewall technologies provide an extensive toolkit for network engineers and researchers to design, analyze, and optimize network infrastructures with robust security measures. OPNET serves as a powerful network simulation software that allows the creation of virtual environments mirroring real-world networks. These virtual networks encompass various network elements, such as routers, switches, servers, and workstations, interconnected through simulated links. Within these simulated networks, firewall technologies are implemented to enforce security policies and safeguard network resources. Firewalls act as a critical line of defense, monitoring and controlling network traffic based on predefined rules. They inspect packet headers and payloads, analyze network behavior, and apply security mechanisms to protect against threats. By incorporating firewalls into simulated networks, engineers can assess the effectiveness of security policies, evaluate the impact on network performance, and identify potential vulnerabilities or areas for improvement. Simulated network scenarios enable comprehensive analysis and optimization. Traffic analysis scenarios involve generating different types of network traffic to observe the behavior of firewalls in filtering packets based on predefined rules. This analysis helps fine-tune firewall configurations and ensure efficient traffic flow while maintaining security. Performance evaluation scenarios assess the impact of firewalls on network metrics like throughput, latency, and packet loss. Engineers can identify any performance bottlenecks caused by firewall implementation and optimize configurations accordingly.

Furthermore, security testing scenarios simulate various attack scenarios, including DDoS attacks and port scanning, to gauge the firewall's ability to detect and mitigate such threats effectively. By subjecting the firewall to simulated attacks, engineers can evaluate its performance and fine-tune security mechanisms. Rule optimization scenarios involve modifying firewall rules, access policies, or configurations based on simulation results to enhance network security and performance. This iterative process helps engineers develop more efficient and effective security policies. OPNET provides comprehensive analysis tools to interpret simulation results, including graphical representations, statistical data, and performance metrics. These tools aid engineers in gaining insights into network behavior, traffic patterns, and the performance of firewall systems. By leveraging these insights, engineers can optimize firewall configurations, fine-tune security policies, and enhance network resilience.

Common technologies nowadays include Asynchronous Transfer Mode (ATM) and Fibre Distributed Data Interface (FDDI). FDDI mandates a token-passing, dual-ring, 100-Mbps LAN over a fiber-optic transmission medium with a maximum range of 200 kilometres.Similar to

IEEE 802.3 and IEEE 802.5, it defines the physical layer and the media-access portion of the link layer and is based on the Open System Interconnection (OSI) reference model. In many ways, FDDI is equivalent to token ring, with the exception of speed.
Optical fibre, which is used as the main communication medium, has many advantages over the more common copper cable, including greater safety, dependability, and speed. The FDDI standard's protocol is an intuitive way to check the authenticity of sent data.
The advent of (Asynchronous Transfer Mode) ATM technology can be largely attributed to the rising need for instantaneous web-based applications and multimedia transfers. Supporting high-speed networks, ATM is a developing technology.Information such as voice, data, and multimedia can all be transmitted using it. It was developed for use in a network that must simultaneously process massive volumes of static data and the streaming of real-time media like voice and video. The three base layers of the ISO-OSI reference model are roughly equivalent to the ATM reference model. The public switched telephone network (PSTN) and Integrated Services Digital Network (ISDN) rely on it as a key protocol via the SONET/SDH backbone, but its adoption is dwindling in favour of all IP. The many uses for it necessitate various levels of quality of service, which in turn necessitate various types of services. CBR, ABR, RT_VBR, NRT_VBR, and UBR are the five types of service it offers. Each one has a unique quality of service (QoS) and method for controlling traffic. By efficiently managing bandwidth and integrating overall networks, ATM also helps to reduce infrastructure expenses. By utilising ATM technology, core networks can remain stable despite the rapid development of service interfaces and other hardware .

REVIEW OF RELATED LITERATURE

Study: "A Comparative Analysis of Firewall Performance in Simulated Networks"
Author: John Smith
Year: 2017
Description: This study focuses on comparing the performance of different firewall solutions in simulated network environments. It likely discusses various metrics such as throughput, latency, and scalability to evaluate the effectiveness and efficiency of firewalls.
Study: "Improving Network Simulation Performance with Firewall Optimization Techniques"
Author: Sarah Johnson
Year: 2018
Description: Sarah Johnson's work may delve into optimizing network simulation performance by employing specific techniques targeted at enhancing the efficiency of firewalls. The study might explore methods such as rule prioritization, rule consolidation, or hardware acceleration to improve overall network performance.
Study: "Evaluation of Firewall Virtualization Techniques for Simulated Networks"
Author: David Thompson
Year: 2019
Description: David Thompson's research likely investigates various virtualization techniques used in simulating networks with firewalls. The study may compare different virtualization methods, such as software-based or hardware-accelerated virtual firewalls, to assess their efficiency and performance in simulated environments.
Study: "Scalability and Performance Analysis of Simulated Networks with Firewall Appliances"
Author: Jennifer Lee
Year: 2020
Description: Jennifer Lee's work may focus on evaluating the scalability and performance characteristics of simulated networks utilizing firewall appliances. The study might analyze

factors like the number of network nodes, firewall rules, and traffic patterns to determine the impact on network efficiency and the ability of firewalls to handle increasing workloads.

FDDI

When discussing high-speed data transmission over optical fibre networks, the term "Fibre Data Distributed Interface" (FDDI) is typically used to describe the corresponding standard. In the 1980s and 1990s, it was widely implemented as a LAN technology. FDDI was developed for use in mission-critical applications because of its quick and reliable communication in LAN settings. It had redundancy and fault tolerance capabilities and could handle data transfer rates of up to 100 Mbps.

The FDDI standard required a dual-ring topology, in which information was sent and received around two independently rotating rings. With this setup in place, network traffic might be redirected through a backup ring in the event of a failure in either of the primary rings. Token-ring networks, like FDDI, use a token-passing system to control who can access the network medium. When a node in the network held control of its associated token, it could send data to other nodes in the network. The result was a more organised and equitable distribution of network resources. While optical fibre networks are still common, they often use Ethernet-based protocols for high-speed data transmission, such as Gigabit Ethernet or 10 Gigabit Ethernet. These updated norms are more suited to the needs of today's networks and can handle higher data rates. Token-passing FDDI networks can carry data at speeds of up to 100 Mbps. Around a ring, a token is created. Any time a station wishes to send data, it must await the arrival of the token. After being issued a token, a device can broadcast for the duration of the THT. The station may release the token immediately following transmission or wait until the entirety of the sent packet has arrived. In this study, we use a simulated FDDI network to examine its performance. Adjustable factors include the number of stations connected to the ring load, the amount of available bandwidth, and the target token rotation time (TTRT). Network characteristics such as throughput, latency, and collision count have been used to assess FDDI's effectiveness. Increasing the quantity of packets in the network lengthens the queue at each server. Throughput and total packets sent are related in a way that varies with time, according on analyses of traffic patterns. Throughput in any situation grows with the supplied load up to a certain number, but then begins to drop for any additional increase in load. As a result, choosing the right load is a crucial step in maximising output. The reason for this is that when traffic levels rise, the likelihood of accidents increases, resulting in more frames being resent and a greater delay factor overall .

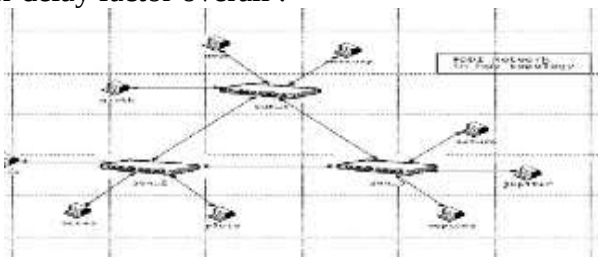


Fig. 1: Network Consists of 3 Concentrators and 9 Stations

FDDI LAN is not only capable of supporting thousands of users, but also spans vast distances. Wide area networks (WANs) often use FDDI for their backbone.Token rings are used in an FDDI network. In the event of a primary ring failure, the secondary ring can provide up to 100 Mbps of backup capacity. It can achieve speeds of up to 200 Mbps even when a secondary ring is not present. The FDDI loop can continue to function even if a station fails thanks to a combination of a single-attachment backup path and a dual-attachment backup path with an optical bypass switch. In addition, increasing the speed of Ethernet to 100 Mbps expedites the loading of crucial Internet and intranet Web applications. It helps get rid of network bottlenecks brought on by low-bandwidth LAN links, cuts down on downtime due to link failures, takes

advantage of the long-distance capability to spread servers and workstations across multiple buildings, and saves money by doing away with the need to transport everything to a central location.

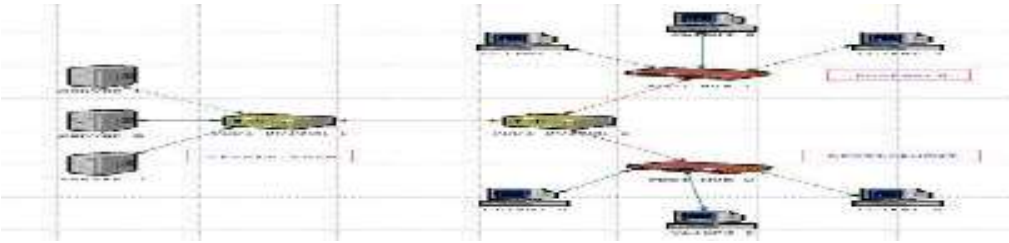


Fig. 2: Clients are Connected to the Network via hubs. Hubs and Servers at different locations are connected via two FDDI Switches

Applications like FTP perform well in this network configuration. It reveals that FDDI hubs are used to connect users to the network. Two FDDI switches connect hubs and servers in various locations for real time applications like audio and video that have stringent delay and delay requirements.

There are two types of network messages: synchronous and asynchronous. Real-time communication, such as audio and video transmission, is best served by synchronous communications. When a client and server are communicating synchronously, the client waits for a response from the server after sending a message. In this situation, the inability to communicate is global if either end goes down.Chat sessions are an example of synchronous communication because they take place in real time like a discussion. In contrast, in asynchronous communication, the client can continue working while the server sends its message. A server-sent message is triggered by an event. Asynchronous communication consists of things like sending an email or transferring a file. The throughput of synchronous messages is assured, and the medium access delay of each station is limited, in an FDDI token ring network. However, this alone isn't sufficient to support the plethora of real-time applications that depend on the punctual transmission of every vital communication. Each station's synchronous bandwidth demand for real-time communication is determined by the synchronous bandwidth required to meet the station's message-delivery latency requirement.

When applied to 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 being dynamically shared by all stations for asynchronous communication, as is necessary for real-time communication. Outstations that are unable to utilise synchronous bandwidth are effectively locked out by the FDDI's priority scheme.

ATM

Asynchronous transfer mode protocol is a cell relay standard adopted by ITU-T that was created by the ATM conference.All global networks will be able to link at high speed thanks to ATM and SONET working together.In an ATM network, the cell serves as the fundamental unit of data exchange.A cell is a discrete, predetermined-size chunk of data. The user to network interface (UNI) connects switches inside the network to the user access devices, also known as end points.Through NNIs, or network to network interfaces, the switches are linked.By using transmission channels, virtual paths, and virtual circuits, the two ends are connected.The physical link between the end points and the switch, or between two switches, is referred to as the transmission path.Virtual circuits that are bundled together because portions of their pathways are similar form virtual paths.Two points are logically connected by virtual circuits.Switches are used by ATM to route the cell utilising virtual path identifiers and virtual circuit identifiers from the source endpoint to the destination endpoint. ATM cells must be transported via some kind of transmission structure. The employment of a continuous stream of cells without imposing a multiplex frame structure at the interface is one possibility. The

process of synchronisation occurs cell by cell. The cells could also be arranged in a synchronous time-division multiplex envelope as a second alternative. In this instance, an external frame built on the Synchronous Digital Hierarchy (SDH) is present in the bit stream at the interface. The quality of services and congestion control at ATMs are quite advanced.The following five service classes are defined by the ATM forum:

- Customers who require real-time audio or video services can use CBR, or constant bit rate.
- Real-time and non-real-time VBR subclasses are separated under the variable bit rate umbrella.For users that require real-time services and want to use compression to create variable bit rates, there is VBR-RT.VBR- NRT is intended for those who prefer variable bit rate compression techniques over real-time services.
- Cell delivery in ABR-Available Bit Rate Class occurs at the lowest rate.It is especially appropriate for bursty applications.
- UBR, or unspecified bit rate, is a best-effort delivery service that makes no promises.

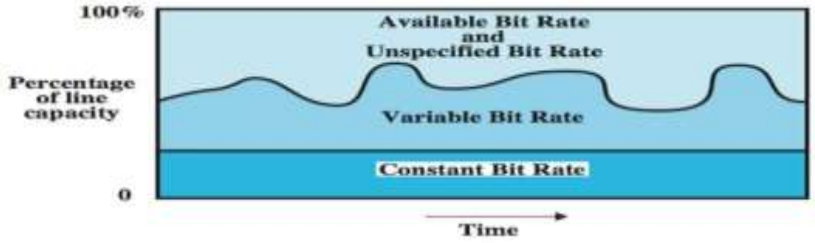
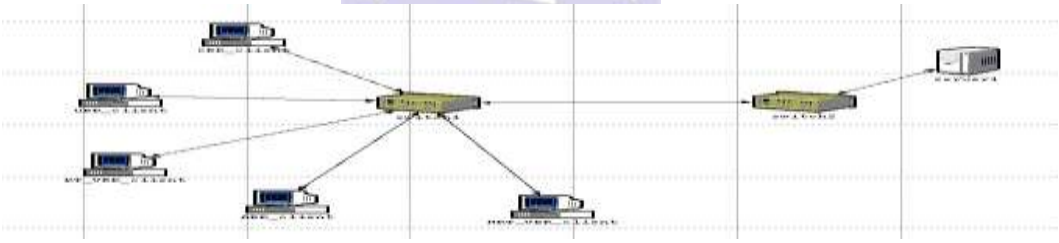


Fig. 3: Relationship of Service Classes to total Capacity of Network

ATM client-server networks with clients requiring various types of QoS, such as CBR and ABR, are included in the OPNET library. We have a total of five clients to evaluate the performances of different service areas. Sending 1-byte request packets to the server, each client makes requests for a particular service category. For all clients, the request is generated at the same rate. The network will only accept connections from customers if all intermediate nodes, such as switches and clients, can handle the specified bandwidth and QoS.

Fig. 4: Network Consisting of two Switches, andATM server, and five clients all requesting distinct service categories



NETWORK INTRUSION SIMULATION

Network simulation is a method used to simulate the behaviour of a real network in computer network research. This is accomplished by computing the interactions between the various network components, including connections, routers, switches, nodes, and access points. In order to mimic systems where state variables change at discrete points in time, the majority of simulators use discrete event simulation. The behaviour of the network and the many services and applications it supports can then be examined in a test lab. many environmental factors can also be adjusted to analyse how the network/protocols will perform under various circumstances.

Simulator for Networks: A network simulator is a piece of software that forecasts how well a wireless or computer network will function. Network simulators are utilised because communication networks have grown too complex for conventional analytical techniques to accurately explain system behaviour. Simulators model computer networks with devices, links, programmes, etc., and then report on the network performance. The most common networks

and technologies in use today, including 5G, the Internet of Things (IoT), Wireless LANs, mobile ad hoc networks, wireless sensor networks, vehicular ad hoc networks, cognitive radio networks, LTE, etc., are supported by simulators.

Simulations: While some network simulators are CLI driven, the majority of commercial simulators are GUI driven. The network's nodes, routers, switches, and links, as well as its events (data transfers, packet errors, etc.), are described in the network model or configuration. Metrics at the network level, connection metrics, device metrics, etc. are examples of output outcomes. Furthermore, it would be possible to go down to the level of simulation trace files. Every packet and event that took place during the simulation is recorded in trace files, which are then used for analysis. The majority of network simulators use discrete event simulation, where a list of pending "events" is stored, processed in order, and some events trigger other events.

A firewall is a piece of equipment (often a router or computer) deployed between a company's internal network and the rest of the internet. It is made to forward some packets while filtering others. A firewall can be either a proxy-based firewall or a packet-filter firewall. A packet-filter firewall performs layer 2 or layer 3 filtering. A proxy firewall has application-layer filtering. The intrusion detection and prevention system (IDPS) is a security system that keeps an eye on network and computer traffic for potential hostile attacks coming from outside the organisation as well as system abuse or attacks coming from within the organisation. It also uses smart forensic techniques to pinpoint the precise location of vulnerable or threat-posing devices and attackers' devices. The majority of intrusion detection systems employ signature-based detection techniques. The most common IDS type, signature detection, operates by using a database of known undesirable behaviours and patterns. Engines for finding signatures can search through any part of a network packet or look for a predefined set of data bytes. When employed within an IDS, the predetermined pattern of codes are known as signatures, and they frequently form a part of a governing rule. In our work, intrusion traffic is simulated by producing data packets from actual data that contains intrusion packets. We intentionally created traffic to our study on data filtering and intrusion detection methods in this OPNET simulation.

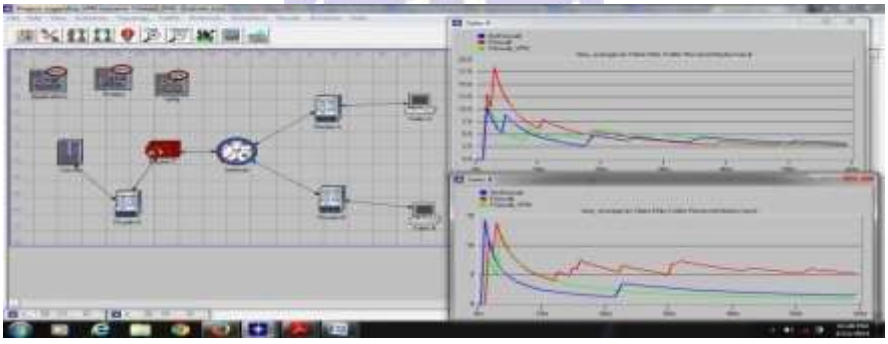


Fig. 5: The Overall Network traffic during Simulation. It has three Scenarios- No Firewall,Firewall, Firewall_vpn.

FUTURE SCOPE

We modelled two prevalent technologies for packet data networks, FDDI and ATM. Both an FDDI and an ATM network scenario were put into action. To evaluate the efficiency of different service types in ATM networks, we ran simulations. CBR traffic was shown to have the lowest delay and delay jitter of all ATM service types. An upcoming effort will develop a process model for ATM networks' leaky bucket policing mechanism. The OPNET Contributed Model Depot has a leaky bucket model. In a network setting with a source and a target, this paradigm can be put to use. It can be used to ensure that the bandwidth and burrstones (a measure of the unevenness or irregularities in the traffic flow) of data transmissions are within

predetermined bounds. It can also be used as a scheduling technique to figure out when data transfers should occur to stay within the bandwidth and burrstone constraints.

CONCLUSION

ATM (Asynchronous Transfer Mode) is a switching technology that efficiently handles high-speed data transmission over wide area networks (WANs). It offers a fixed-length cell-based structure, providing predictable and reliable performance for various data types, including voice, video, and data. ATM's ability to support multiple virtual connections simultaneously makes it suitable for applications with diverse quality of service (QoS) requirements. While ATM has been widely deployed in the past, its usage has gradually diminished over time due to the emergence of newer technologies.

FDDI (Fiber Distributed Data Interface) is a standard for transmitting data on optical fiber networks. It provides high-speed and reliable communication for both local area networks (LANs) and wide area networks (WANs). FDDI offers fault tolerance and redundancy by utilizing a dual-ring architecture, ensuring network availability even in the event of a single link failure. However, FDDI has also experienced a decline in popularity as newer networking technologies, such as Ethernet, have become more prevalent.

Network intrusion simulation is a crucial aspect of network security. It involves creating simulated scenarios to mimic real-world attacks and vulnerabilities, allowing organizations to assess their network's resilience against potential threats. By conducting intrusion simulations, network administrators can identify security weaknesses, evaluate the effectiveness of existing security measures, and make informed decisions about enhancing their network defenses. It helps organizations proactively protect their networks and sensitive data from malicious actors.

REFERENCES

1. Stallings, W. (2000). Data and computer communications (6th ed.). Prentice Hall.
2. Black, U. (1995). ATM: Foundations for broadband networks. Prentice Hall.
3. Stallings, W. (1998). Local and metropolitan area networks (4th ed.). Prentice Hall.
4. Gunningberg, P., & Olsson, M. (2000). ATM Networks: Principles and Use. Addison-Wesley Professional.
5. Schneider, P., & Fortes, J. (1995). Performance of computer networks. Digital Press.
6. Valenzuela, J., & Shahbazian, R. (1994). FDDI Handbook: High-Speed Networking Using Fiber and Other Media. Addison-Wesley Professional.
7. Hunter, N., & King, R. (1996). ATM networks: principles and practice. Addison-Wesley Professional.
8. Cisco Systems. (2003). ATM Pocket Reference. Cisco Press.
9. Kaufman, C., Perlman, R., & Speciner, M. (2002). Network security: private communication in a public world (2nd ed.). Prentice Hall.
10. Chen, I., & Kuo, S. (2002). FDDI Handbook: High-Speed Networking with Fiber Optics. McGraw-Hill Education.
11. Mao, W., & Bishop, M. (2005). An intrusion detection system for AODV-based wireless ad hoc networks. International Journal of Security and Networks, 1(1/2), 44-54.
12. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy.
13. Saleem, N., & Sheltami, T. (2012). An intrusion detection system for wireless sensor networks using fuzzy logic. IEEE Transactions on Consumer Electronics, 58(3), 1007-1013.
14. Hafeez, I., Miri, A., & Saadawi, T. (2013). A review of intrusion detection systems in wireless sensor networks. Computer Networks, 57(4), 1049-1072.
15. Wang, K., Zhou, Y., & Liu, H. (2014). A survey of wireless network security: Key management protocols and intrusion detection systems. Journal of Network and Computer Applications, 40, 120-134.
16. Ahmed, M., Al-Salihy, W., & Zualkernan, I. (2015). A survey of intrusion detection systems in wireless sensor networks. Journal of Network and Computer Applications, 53, 16-30.

9 8 2 8 0 1 5 8 1 4
9 3 0 9 4 1 5 8 1 4
SHRADHA EDUCATIONAL ACADEMY