International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

Analyzing the Performance of Wireless and Wired Security Models using OPNET

Moram Sunil Kumar Reddy[1]

[1] Research Scholar, Department of Computer Science & Engineering, Dr. A. P. J. Abdul Kalam University, Indore, Madhya Pradesh

Dr. Manoj Eknath Patil[2]

[2] Supervisor, Department of Computer Science & Engineering, Dr. A. P. J. Abdul Kalam University, Indore, Madhya Pradesh

ABSTRACT

The effectiveness of different security models is crucial in today's network security environment for protecting data and preventing cyber-attacks. We simulated wired and wireless network systems under different security situations using OPNET. Traditional firewall systems for wired networks and WPA2 for wireless networks were among the well-established security methods tested in the research. Using the OPNET simulation tools, this article mimics an evaluation of both wireless and wired networks. This article compared two cases; one used a firewall gateway using TLS encryption using MD5_RSA, while the other used wireless mobile clients. The study's findings illuminate the process by which hybrid security protocol ensures end-to-end protection for web servers and wireless clients.

Keywords: Security, Server, Wireless, Wired, Delay, Throughput

I.INTRODUCTION

Protecting networks against the constantly changing cyber environment is of the utmost importance in today's world. In order to run their apps and provide their services, businesses, government agencies, and nonprofits rely on wired and wireless networks. Attack techniques used by bad actors to take advantage of security holes are always evolving in tandem with technology. An in-depth familiarity with the various security types and how they function is crucial for mitigating these dangers. When it comes to protecting the availability, confidentiality, and integrity of data, there is a wide variety of approaches that make up network security. There are advantages and disadvantages to applying security measures in wired networks (those that use physical connections like Ethernet cables) and wireless networks (those that use radio waves for communication). Protecting data transmission in a wired network from prying eyes is easier because of the regulated physical environment. However, due to their dependence on radio frequencies, wireless networks are intrinsically more susceptible to interference and eavesdropping, calling for sophisticated security measures to reduce hazards.

One of the most well-known programs for simulating and analyzing networks is OPNET, or the Open Network Simulator. Network engineers and researchers may use it to model, simulate, and assess how alternative security models and network topologies function in different circumstances. A better knowledge of the practical performance of various security measures may be achieved with the help of OPNET, which offers a virtual environment free from real-world restrictions for testing network settings and security protocols. Thanks to this, it's a great tool for comparing wired and wireless security approaches.

The physical infrastructure of the network and the data transferred across the cables are the usual targets of security measures in a wired network setting. Implementing encryption protocols, intrusion detection systems (IDS), and firewalls are common security approaches. In contrast to intrusion detection systems (IDS), firewalls are able to manage and monitor all network traffic, both incoming and outgoing, according to a set of predefined security rules. Data communicated over the network is encrypted and less likely to be intercepted using encryption protocols like Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

Conversely, wireless networks have extra difficulties because of their intrinsic openness and the possibility of remote unwanted access. Common encryption algorithms in wireless network security models include Wi-Fi Protected Access (WPA) and WPA2, which encrypt data sent over wireless channels to ensure safe connection. Additionally, authentication methods are used to confirm the identity of users that access the network, for example, Extensible Authentication Protocol (EAP). A multi-layered security strategy integrating authentication, encryption, and intrusion detection is essential for protecting wireless settings from possible dangers such as eavesdropping and illegal access.

These security models may be thoroughly tested using OPNET's network simulation capabilities, which can handle both wired and wireless scenarios. Researchers may evaluate the efficacy of these models in addressing possible vulnerabilities and threats by developing comprehensive network scenarios and evaluating the effectiveness of different security solutions. If you want to know how a firewall handles heavy network traffic or how encryption algorithms affect the speed and safety of wireless connections, OPNET simulations are a great tool to use.

Tests of numerous attack channels and security breaches are also possible in OPNET's simulation environment, which sheds light on how resilient different security solutions are. To test a network security model's resilience to Distributed Denial of Service (DDoS) assaults—which may overload a network's resources and interrupt services—one might run simulations. In addition, researchers may evaluate the efficacy of security measures in detecting and mitigating network breaches and unauthorized access attempts using OPNET's ability to predict their Impact.

II.REVIEW OF LITERATURE

Jaiswal, Rupesh et al., (2023) This study examines several performance assessment metrics of wireless network applications, with a focus on file sharing methods like Bit-Torrent and client-server techniques. The benefits and drawbacks of the client-server model, as well as the need of a peer-to-peer model, are discussed in this project. We display many performance evaluation parameters in an OPNET environment, including latency, traffic delivered and received, and the influence of traffic on servers, for both wired and wireless client-server networks. The performance of the Bit-Torrent network is examined using various analytical modeling techniques, including the Queueing network model and the fluid flow model. The impact of seed and peer arrival and departure on parameters such as downloading speed, transition rates, and delay is then assessed using Matlab.

Sun, Yi & Sun, Yue et al., (2013) One emerging area of focus in wireless networking is the wireless sensor network. Wireless HART, ISA100.11a, IEEE1451, and ZigBee/IEEE802.15.4 are among the few communication protocols used by wireless sensor networks, in comparison to other network technologies. IEEE802.15.4 is a two-way wireless communication standard that was developed for short-range, low-complexity, low-power, low-rate, and low-cost wireless networks. This research uses the OPNET simulator to examine how well IEEE 802.15.4 works. The simulation results show how various network loads affect system performance metrics including end-to-end latency, packet reception ratio, and node-wide performance, which may be used as a theoretical foundation for building real networks.

Vohra, Rajan et al., (2012) To conduct a thorough analysis of WLAN performance, one must first determine which network configuration parameters have the potential to alter the network's quality of service. When dealing with subpar network performance, it's important to keep an eye out for symptoms like slow throughput, high packet loss rate, delayed round trip time (RTT), more retransmissions, and more collisions. Examining the impact of processing delay and media access delay on WLAN performance is the primary goal of this article. By adjusting metrics like buffer size, fragmentation threshold, and request to send (RTS) thresholds, simulations show that WLAN performance may be improved using the simulation program OPNET. The impact of buffer size on service quality is the main focus of this article. Reducing WLAN latency and media access time with hardly perceptible changes in throughput is possible by changing the buffer size to a number different than what is specified in the standards.

Rahul, Malhotra & Gupta, Vikas et al., (2011) In this research, we try to use OPNET, a simulation tool, to analyze the performance of wired and wireless computer networks. Different transmission connections and load balancers have been tested for wired networks in order to determine performance metrics such as throughput and latency. The load-balancing has been examined using metrics such as the study of sent and received traffic. Wireless networks have used a variety of physical characteristics and buffer sizes to estimate metrics including throughput, retransmission attempts, and latency. The findings show that wired networks function well with server-load balancing policies and high-speed Ethernet cables like 1000 Base X, but wireless LANs may be fine-tuned for better performance with careful parameter selection. We found that wireless networks with infra-red type physical features and larger buffer sizes performed better in the simulated scenarios we evaluated (1024Kb).

Kirubanand, V.B. & Senniappan, Palaniammal. (2011) A high-performance client-server network using hubs, switches, Bluetooth, WI-Fi, and Wimax, as deduced by the steady algorithms, is the primary objective of this research. Approach: Finding performance on wired and wireless technologies in terms of service rate, arrival rate, expected waiting time, and busy period is the major emphasis of this work. The model primarily involves an M/M (a,b)/1 markovian with adaboost and user selection algorithms. Wireless technologies have been determined to be superior than cable technologies when comparing inter-arrival and inter-service times. When there is network congestion, the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

Adaboost algorithm between the client and server may increase the data packets' delivery speed to the destination and ensure that they reach their destination without loss. Finding the user with the greatest queue priority is the primary goal of user selection algorithms. A user is chosen at random from among those with uniform probability if more than one person has the greatest priority. Implementing wireless technologies with adaboost and a user selection algorithm has also shown to be highly efficient in terms of arrival rate, service rate, expected waiting time, and busy period implementation for data transactions between clients and servers using Wimax technology in M/M (a,b)/1. The results show that various wireless technologies may have their performance evaluated using the numbers computed by bluetooth. Final Thoughts/Suggestions: Utilizing the RSA method, which offers enhanced security measures, we ensure the safety of data packets as they travel over the network.

Ghwanmeh, Sameh & Alzoubaidi, A. (2006) Many new applications are rapidly adopting wireless technology. An essential component of WLAN design and operation is performance optimization. This research presents performance optimization strategies utilizing OPNET modeler, a state-of-the-art network simulator. A number of simulation experiments with various parameters, such as the RTS/CTS threshold, fragmentation threshold, and data rate, have shown the optimization of WLAN performance. When the environmental factors are fine-tuned, the simulation results demonstrate that the WLAN performs well.

III.RESEARCH METHODOLOGY

Our study's primary emphasis was on implementing a hybrid security protocol to measure performance between wireless clients and wired servers in order to accomplish the set of goals. We have taken two kinds of situations into account in our study. The first step is to evaluate the efficacy of RSA encryption techniques in wireless mobile client communication via a WTLS gateway. Second, the use of the message digest technique to deliver TLS encryption for the firewall gateway. Opnet is a robust and feature-rich program that allows users to model whole heterogeneous networks using a variety of protocols, allowing for accurate simulation of the resulting systems.

Simulation Parameters

The OPNET simulation environment is used to construct the model. Four client nodes and four server nodes make up the network diagram. The model employs both client-side and server-side encryption and decryption. The encrypted data is sent from the wireless client to the web server via the gateway. Various throughput and wireless LAN delay-based metrics form the basis of the studied findings. The ability to model networks in their heterogeneous state using any of the available protocols is a hallmark of OPNET, a robust and feature-rich simulation tool. The program has evolved from its military origins to become the preeminent commercial tool for simulating networks. OPNET is a packet-level network simulator that includes an extensive library of realistic simulations of fixed network gear and protocols that are commercially available. You may use this program to set up a big network in your computer.

IV.RESULTS AND DISCUSSION

Throughput of wireless client and wired server

What we mean by "network throughput" is the efficient rate at which various forms of mobile communication streams (e.g., Ethernet) can transmit lucrative messages.The throughput is measured in bits per second, data packets per time slot, or data packets per second. Any number of physical and virtual connections, as well as specialized routing protocols, may carry this data. The total bit rates sent by all network terminals constitute the aggregate or machine output.

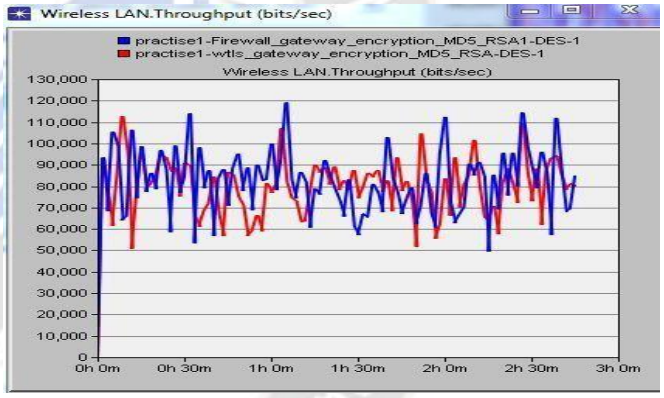

Figure 1: Throughput of wireless client and wired server

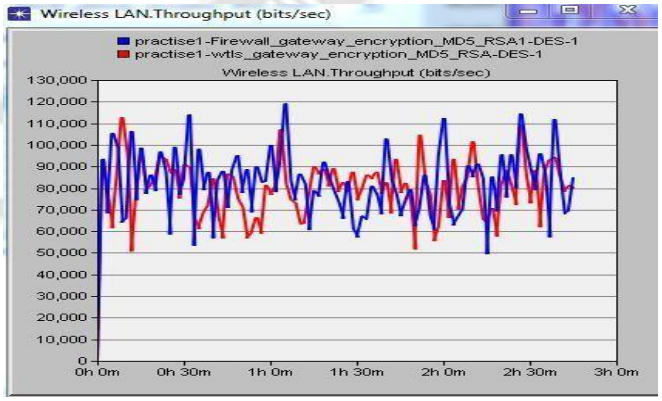

Figure 2: Network Throughput of wireless client and wired server

Delay

A network's latency is the amount of time it takes for data bits to transition between different transmission modes. Seconds

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

are the units of delay. Depending on where the connection node is located, the delay could vary somewhat. Data transmission delays occur between servers because, as shown in figure, the WTLS gateway has a much larger delay than firewall encryption.

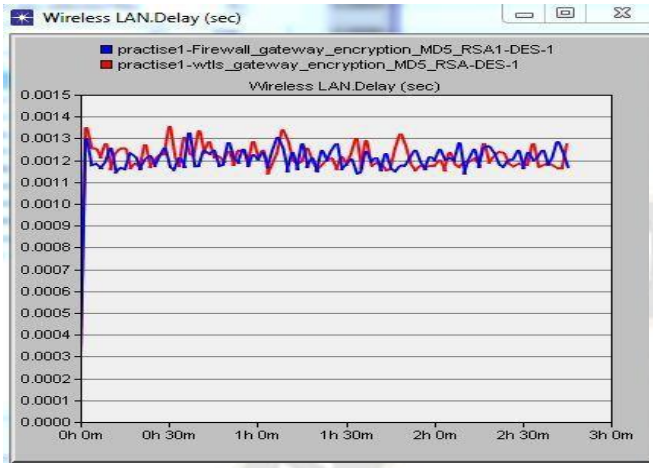

Figure 3: WLAN Delay

Load in wireless local area network

According to the data shown in the picture below, the firewall gateway has a larger load than the WTLS gateway in both scenarios. Although the WTLS gateway can handle loads as low as 49,000 bits per second, they can go as high as 120,000 bits per second. In contrast, both the minimum and maximum values for firewall gateway encryption are 110,000 bits per second.

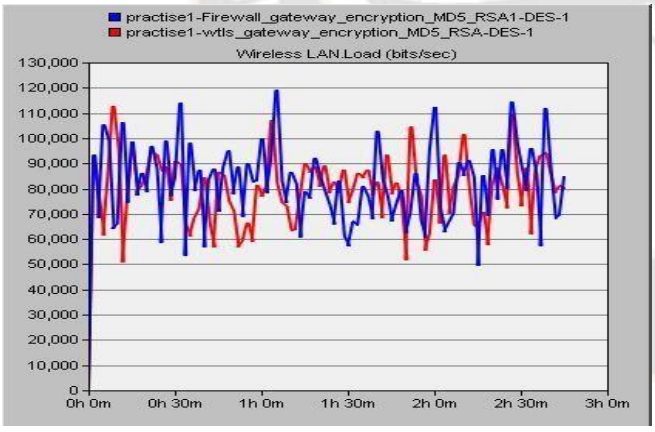

Figure 4: Load in wireless local area network

Wireless LAN Media Access Delay

See below for a visual representation of the concept that wireless LAN media access delays are measured in seconds. It also demonstrates that the media access latency is weak in the firewall encryption scenario and quite significant in the WTLS gateway encryption scenario. The maximum and lowest values for WTLS gateway encryption are 0.00053 and 0.00024 seconds, respectively. On the other side, the lowest possible time for firewall encryption is 0.00025 seconds, while the highest time is 0.00046 seconds.

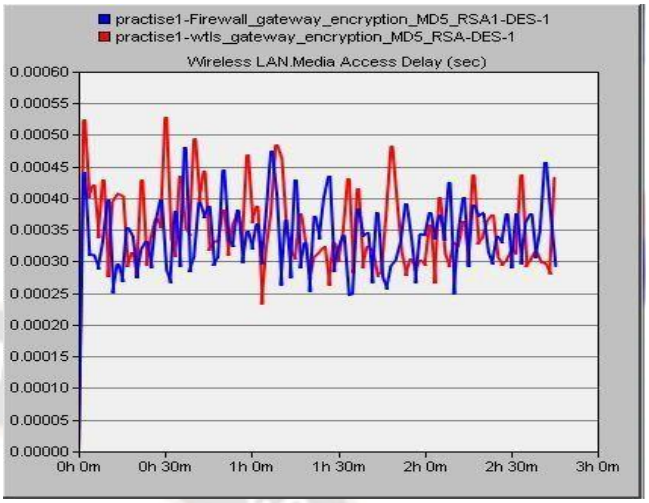

Figure 5. Wireless LAN Media Access Delay

The results of a hybrid protocol, WTLS MD5_RSA, and TLS MD5_RSA are compared in Table 1. A throughput of 90 bits/sec is achieved by WTLS MD5_RSA, but TLS MD5_RSA and the Hybrid Protocol both reach 120 bits/sec, suggesting that the latter two are more efficient when it comes to data transfer. Compared to WTLS MD5_RSA (0.0013 sec), the latency for TLS MD5_RSA with the Hybrid Protocol is somewhat smaller at 0.0012 sec. When compared to WTLS MD5_RSA, TLS MD5_RSA and the Hybrid Protocol both perform better in terms of WLAN load and WLAN media access latency, with lower values for each parameter. Compared to WTLS MD5_RSA, which has a throughput of 70,000 bits/sec, TLS MD5_RSA and the Hybrid Protocol have a throughput of 75,000 bits/sec. Nonetheless, WTLS MD5_RSA has somewhat better firewall-to-router channel consumption than the other two protocols, coming in at 4.5 seconds instead of 5 seconds. In terms of throughput and latency, the Hybrid Protocol and TLS MD5_RSA both perform better than WTLS MD5_RSA, which demonstrates improved channel use.

Table 1: Comparison of Simulation Results

Parameters	**WTLS MD5_RSA**	**TLS MD5_RSA**	**Hybrid Protocol**
Throughput	90 Bits/Sec	120 Bits/Sec	120 Bits/Sec
Delay	0.0013 Sec	0.0012 Sec	0.0012 Sec
Load in WLAN	120,000 bits per sec	110,000 bits per sec	110,000 bits per sec
WLAN Media	0.00053 sec	0.00046 sec	0.00046 sec

Access Delay			
Firewall to Router Throughput	70,000 Bits/Sec	75,000 Bits.sec	75,000 Bits.sec
Firewall to Router Channel Utilization	4.5 Sec	5 Sec	5 Sec

V.CONCLUSION

To better understand the efficacy and resilience of various security measures in many network contexts, it is essential to analyze the OPNET performance of wired and wireless security models. It is becoming more and more critical to understand how different security models function under different scenarios as the landscape of network security continues to grow with technology and the complexity of cyber-attacks. By virtue of its extensive simulation capabilities, OPNET provides a potent instrument for the controlled virtual evaluation of these security models, facilitating in-depth study and optimization. The simulation features of OPNET also make it possible to test out various network setups and security measures, which helps to understand how they affect the network's performance and safety. By proactively identifying the best security configurations and methods, risks may be reduced and overall security can be improved before they are implemented in actual network settings.

REFERENCES: -

[1] R. Jaiswal, S. Lokhande, and S.V. Mitkari, "Performance Evaluation of Wireless Networks," International Journal of Computer Applications, vol. 7, no. 8, pp. 1237-1242, 2023.

[2] Y. Sun, Y. Sun, P. Xu, and H. Liu, "Performance Analysis of Wireless Sensor Network Based on OPNET," Communications and Network, vol. 5, no. 3, pp. 512-516, 2013, doi: 10.4236/cn.2013.53B2094.

[3] R. Vohra, R. S. Sawhney, and G. Saini, "OPNET based Wireless LAN Performance Improvisation," International Journal of Computer Applications, vol. 48, no. 1, pp. 27-31, 2012, doi: 10.5120/7314-9912.

[4] R. Malhotra, V. Gupta, and R. Bansal, "Simulation and Performance Analysis of Wired and Wireless Computer Networks," International Journal of Computer Applications, vol. 14, no. 7, pp. 1-9, 2011, doi: 10.5120/1897-2528.

[5] V. B. Kirubanand and P. Senniappan, "Study of Performance Analysis in Wired and Wireless Network," American Journal of Applied Sciences, vol. 8, no. 8, pp. 826-832, 2011.

[6] T. Velmurugan, H. Chandra, and S. Balaji, "Comparison of Queuing disciplines for Differentiated Services using OPNET," in IEEE ARTComm. 2009, pp. 744-746, 2009.

[7] U. Din, S. Mahooz, and M. Adnan, "Performance evaluation of different Ethernet LANs connected by Switches and Hubs," European Journal of Scientific Research, vol. 37, no. 3, pp. 461-470, 2009.

[8] Z. Ren, Y. Huang, Q. Chen, and H. Li, "Modelling and Simulation of fading, Pathloss and shadowing in wireless networks," in Proceedings of ICCTA 2009, vol. 14, no. 7, pp. 335-343, 2009.

[9] S. Shaban, H. M. El Badawy, and A. Hashad, "Performance Evaluation of the IEEE 802.11 Wireless LAN Standards," in Proceedings of the World Congress on Engineering 2008, vol. I, July 2-4, 2008.

[10] M. N. Ismail and A. M. Zin, "Emulation network analyzer development for campus environment and comparison between OPNET Application and Hardware Network Analyzer," European Journal of Scientific Research, vol. 24, no. 2, pp. 270-291, 2008.

[11] P. Jurcik, A. Koubaa, M. Alves, E. Tovar, and Z. Hanzalek, "A simulation model for the IEEE 802.15.4 Protocol: Delay/Throughput Evaluation of the GTS Mechanism," in Proceedings of the 15th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS07), Istanbul, Turkey, vol. 14, no. 7, pp. 109-116, October 2007.

[12] S. Ghwanmeh and A. Alzoubaidi, "Wireless Network Performance Optimization Using Opnet Modeler," Information Technology Journal, vol. 5, no. 1, pp. 18-24, 2006, doi: 10.3923/itj.2006.

[13] W. Hneiti and N. Ajlouni, "Performance Enhancement of Wireless Local Area Networks," in Proceedings of IEEE ICTTA'06, 2nd International Conference on Information & Communication Technologies: from Theory to Applications, Damascus, Syria, vol. 2, no. 7, pp. 2400-2404, April 2006.