A Simulative Framework for Data security using PSA in LAN using MATLAB and Distributed Firewall

Harjeet Singh,

Research Scholar, School of Computer Application & Technology, Career Point University, Kota (Raj.)

Dr. Abid Hussain,

Associate Professor, School of Computer Applications, Career Point University, Kota (Raj.)

Abstract: This approaches in the research article are to goal is to keep firewalls' enhancement from security attack while minimizing their drawbacks. A hybrid algorithm is created via comparative research and then applied in DLAN to enhance the network performance. The main aim is to achieve the study proposal's purpose. We plotted a LAN network using a MATLAB script. This study's distributed LAN was built with 100 nodes. The network is 1000 × 1000 meters in size and the nodes are randomly dispersed. A neural network, computer software, does the random processing. The built network now contains a wormhole attacker node and a DDoS setup. This paper induced packet security analysis (PSA) for security of distributed LAN. The Distributed Local Area Network (LAN) can be implemented in two ways using the structure described above. One with the PSA application and one without the PSA application. It is a modified version of routing algorithms, and it is defined as the packet security algorithm (PSA). When compared to the PSA -1, it has been noticed that the packet delivery for PSA – 0 (i.e., without packet security) is less frequent than the PSA -1. (With Packet Security). It is the same procedure that is followed in each and every attempt to transmit a packet that is being discussed here. Because of the increased rate of packet delivery in each round after the installation of security, the rate of packet delivery in each round is much greater than it was before. This paper uses the MATLAB simulation for study and implementation of LAN as network nodes framed in the MATLAB interface and do provide a communication with or without the packet security analysis to understand the distributed Firewall system. The overall paper demonstrated that the simulative frame work to estimated the network parameters and security analysis for distributed Firewall system using packet security analysis.

Keyword: Firewalls Enhancement, Hybrid protocol, Distributed Local Area Network (LAN), Wormhole Attacker, packet security analysis (PSA), Neural Network.

1. Introduction of Wireless Networks

Wireless networks are becoming increasingly popular as a result of their convenience. Because the consumer/user no longer needs to rely on cables, it is significantly easier for him/her to walk around while still remaining connected to the network. The portability of wireless networks distinguishes them from more traditional wired networks and contributes to their popularity. When enabled, this function allows the user to move around freely while still maintaining a connection to the network. When compared to the installation of a wired network, the installation of a wireless network is very straightforward. Fortunately, because wireless networks do not rely on cables or wires that are routed through walls and ceilings, this is not a concern. Wireless networks may be established in order to better serve the demands of customers [1]. There are many different sizes of networks, from small groups of clients to large networks with thousands of users. Using wireless networks has a number of advantages, particularly in remote areas where cable cannot be placed, such as hilly terrain.

1.1 Wireless Networks

Wi-Fi and other wireless networks are becoming increasingly popular, as individuals desire the flexibility of connecting from any location. Users of wireless networks can communicate and share data with one another without the requirement for a wired connection, so eliminating the necessity for a wired connection in the process. One of the reasons why wireless networks are so popular is the widespread use of wireless devices, which is one of the primary reasons for their popularity. A large number of wireless applications and devices are focused on wireless local area networks (LANs) (WLANs) [13]. There are two methods for accomplishing this: one involves the use of control modules (CMs), which are also known as base stations. The other involves the lack of control modules (CMs). These networks are not reliant on any pre-existing infrastructure in order to perform their duties effectively. These networks, which can be standalone or linked to one or more sites, enable internet access as well as connectivity to mobile networks. These networks have been proven to have the same wireless communication challenges as traditional wireless networks, including bandwidth restrictions, battery power, transmission quality enhancement, and coverage issues, amongst other things. A typical Wi-Fi network is made up of a number of mobile servers that communicate with one another either directly or through a central access point (base station) [2].

Instead of using physical connections to send and receive information, wireless networks make use of some type of stereo wavelengths in the air to transmit and receive data. Setting up wireless networks requires the usage of wireless routers and servers. A Wi-Fi network is a type of network in which computers can connect with one another without the use of cables or other wires. Wi-Fi is used to connect the PCs together and to communicate with one another. In order for a PC to connect to another network, there must be radio communication between the two networks. Customers of Wi-Fi networks exchange and receive information through the use of electromagnetic waves. A large number of Wi-Fi networks have sprung up in recent years, owing to its flexibility, simplicity, and ability to be set up at a low cost. Wireless networks are getting increasingly popular as a result of how simple they are to utilize. While the consumer/user is no longer tied to a single location by cables, he or she can still move freely while remaining connected to the network. Wi-versatility One of the characteristics that distinguishes it from typical wired networks is the use of Fi. Customers can transfer networks with ease while still remaining connected to the Internet thanks to this functionality. Wireless networks are easier to set up than wired networks, which is a significant advantage. You don't have to be concerned about removing the cables and wires that are embedded in the walls and roofs of your building. Each client can have their own customized wireless network, which can be established in-house. Depending on the extent of the network, these may have customers ranging from a few individuals to tens of thousands of users. Furthermore, wireless networks are a benefit in mountainous areas where traditional cable infrastructure would be impracticable due to the steepness of the terrain. Based on the size of the coverage area, the wireless network can be classified into the following categories:

a) Personal area network (PAN)

b. Local area network (LAN).

c) Computer Networks: Local Area Networks (LANs).

d) The third network type is the wide area network (WAN).

1.2 Components of Distributed Firewalls

In network domain security policy enforcement, a Distributed Firewall is a technique that employs the following components [3]:

- Policy Expressions
- Policy Distributed Schema (Policy Distributed Schema)
- Certificates

Traditional firewalls, on the other hand, typically use network components such as the IP address as a means of identifying a particular device.

1.3 Policy language

In order to set policies for each firewall, the Policy language must be utilized. These policies are a collection of rules that guide the firewall in its evaluation of network traffic as it traverses the network. It also specifies which inbound and outgoing connections on any component of the network policy domain are allowed, as well as which connections are not allowed [4].

1.4 Policy Distribution Scheme

The policy distribution scheme should include safeguards to ensure that the policy remains intact during the transfer process. Before any incoming or outgoing messages are processed, this policy is reviewed and approved. The policy can be distributed in a variety of ways, and the distribution can change depending on the implementation. Depending on the situation, it can be either directly pushed to end systems or pulled as necessary, or it can even be offered to users in the form of credentials that they must use when attempting to contact with the host systems. It is decided how policies are distributed based on one of the following distribution schemes [5].

- A policy domain can have several end points, and policies and credentials can be pushed to each of those end points.
- During the initialization process, policies and credentials can be retrieved from a trusted repository.
- Policies are retrieved at the initialization of the policy verifier, whereas credentials for authentication are retrieved during the initialization of the policy verifier.
- A trusted repository is maintained, and procedures are requested whenever communication traffic is received by a node from a previously unknown host.

1.5 Certificates

The possibility exists that the distributed firewalls will use the IP address to identify the hosts they are interacting with [14]. However, the existence of a security system is more vital. When identifying hosts, it is preferable to utilize a certificate. IPSec is a security protocol that delivers cryptographic certificates. While IP addresses may be readily spoof, digital certificates are far more secure than IP addresses and the authentication of the certificate cannot be easily forged. Policy distribution is accomplished through the use of these certificates. When implementing distributed firewall technology, policy languages are translated into some internal format by a compiler, which is then used to communicate with the firewall [6]. The system management software distributes this policy file to all of the protected hosts on a per-host basis. Upon receiving an incoming packet or connection, the mechanism applies the security policy to it, with each incoming packet accepted or denied by each host in accordance with the policy and the cryptographically validated identity of each sender (Ioannidis). It is possible that several variations in the deployment of distributed firewall technology will occur. A hybrid firewall, which combines the best features of both regular firewalls and distributed firewalls, is what these variations are referred to as.

1.6 Firewall Works

Security is implemented by the firewall through the use of established security policies, which offer filtering criteria for data transitions in the cloud networking environment. If the information that meets the organization's security standards is allowed to flow on the network with the rest of the packets, the information that does not fit the organization's security needs is prevented. In addition to being time-consuming, the firewall configuration process is also prone to error. Policy management is a difficult work due to the hundreds of rules that are always changing in their dynamic environment. These laws are in conflict with one another in nature, and they may overlap in the system that defines them at some point. Cloud computing requires free access to all data control services in order to achieve fat loss goals [15]. Also required are the requirements for safety and security. For this reason, it must be updated in such a way that it fulfils all of the features of the cloud in order to establish a security service. As a result of the complicated nature of policy anomalies, system administrators frequently confront a more difficult situation when it comes to the resolution of anomalies. This is especially true when it comes to the resolution of policy conflict anomalies. A natural technique for a system administrator to resolve policy conflicts is to adjust the conflicting rules in such a way that all of the conflicts are eliminated. As a result, the cloud-based firewall must be built to support the distributed processing environment, handle policy rule conflicts, and still effectively discover anomalies that occur as a result of the formulation of the rule while maintaining its effectiveness [7].

1.7 DDOS Attack

DDoS attacks, also known as distributed denial of service (DDoS) attacks [16], are malicious attempts to overwhelm target servers, administrations, or systems with a large volume of Internet traffic in order to bring the objective or the framework around it to a grinding halt. DDoS assaults are successful because they make use of a variety of traded-off PC frameworks as sources of attack traffic. Computers and other network resources, such as a local area network (LAN), may be included in the machines utilized. If carried out at a high level, DDoS assaults are comparable to traffic jams that clog roadways, preventing the intended destination from reaching normal traffic.

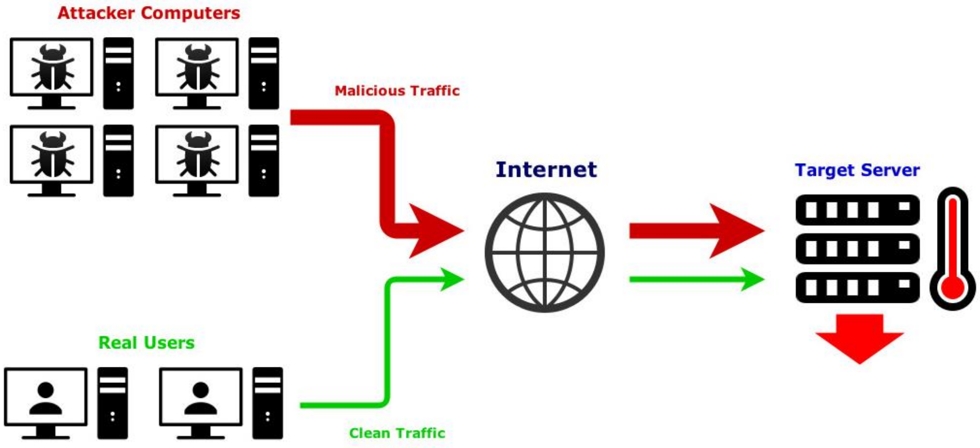


Figure 1. 1 DDoS attack work

A distributed denial-of-service (DDoS) attack allows an attacker to target an internet PC device in order to monitor it. Malware infects a variety of PCs, including desktop computers and Internet of Things (IoT) computers, transforming any PC into a bot (or zombie). An attacker can then take command of a bot group, often known as a botnet, from a distance.

Once the botnet has been established, an aggressor can send updated instructions to each robot using a remote-control approach to coordinate the machine. Each bot reacts by sending a request to the objective at the point in the process where the botnet has narrowed its attention to the IP address of the unlucky victim. As a result, the objective server or device will be subjected to a flood cap, and ordinary traffic will be denied administration as a result of this. Because each robot appears to be a real Internet gadget, it is impossible to distinguish between attack traffic and normal traffic [8].

1.8 Neural Net wok

An organized network assault known as a distributed denial of service (DDoS) is characterised by a huge packet stream that is formed by fusing together data from several sources. It is quite difficult to differentiate between a DDoS attack and a regular packet stream since the DDoS packet stream pattern acts in the same way as a normal packet stream pattern. The categorization of network packets is one of the network defence systems that may be used to protect against DDoS assaults. With the right mix of hidden layer neuron counts and training functions, a Neural Network (NN) may serve as an efficient tool for the categorization of network packets.

2. Research Backgrounds

Several authors have already looked into the effectiveness of services in a local area network (LAN). According to the most recent research in the field of network setup, data protection is the most important type of inquiry. The security function provided by a network is largely dependent on the reliability of the network in question. The study did not devote a significant amount of time to the various types of protection. Now, one day, no one will be able to conceive a world without computers and the Internet, which have all been disconnected from one another. The transmission of information is the primary function of the Internet; any computer anywhere in the world can be linked to any other computer anywhere in the world that is not connected to each other. As a result, both the client and the organisation stand to gain significantly. However, in this scenario, in the area of Network Protection [9], protected data transmission is required, which entails a straightforward procedure. Corrective action should be taken to safeguard you from viruses, hacking, and unauthorized access to your information and computer systems [10]. The firewall is the only device that may be enabled by network security. The firewall is a collection of artefacts that are formed between two networks that philtre traffic for the purpose of establishing unique security policies between the two networks. When a local system or network system is simultaneously connected to wide area networks and the Internet from outside the country, firewalls can be an effective means of protecting the system or network system from network security risks. Traditional network firewall devices are configured as a handle that only permits specific types of traffic to pass through and out of the network. These devices are often located at the network's perimeter. Fire wires whirling is another term for this phenomenon. The network is divided into two sections: one-sided and unstable, and the other-sided and stable. For this aim, they rely substantially on the topology of the network to achieve success. Aside from that, fireworks are used as a strategy for policy management. When fires are distributed, it is possible to impose security controls on the external network while constraining the network's topology to an inner or exterior perspective. In order to encourage the use of fire technologies in organizations for all network domain members, policy language and centralized distribution semantics are used to promote the use of fire technologies. Network devices communicate with unsecured channels while maintaining the logical separation of holdings in and out of the trusted domain. Distribute a fire to correct these problems and defend the network's end points when hackers attempt to infiltrate the system.

3. Research Gap Identified

Numerous academics have already conducted research into the quality of networks within a local area network (LAN). According to the most recent research in the field of network establishment, data security is the most important method of investigation. Computers and networks are getting increasingly intertwined as well. Every second, a slew of sensitive transactions take place, and machines are increasingly being used for data transportation rather than data processing purposes. Network protection is also essential in order to prevent computer hacking and to ensure that data transmissions are authenticated. Network Stability can be achieved through the usage of a Firewall. - It is possible to construct a network domain protection framework through the use of a policy vocabulary, a policy distribution scheme that allows policy regulation to be done from a central location, and certificates that allow every participant in the network policy domain to be identified. Because they protect sensitive network endpoints, distributed firewalls protect the network at the point where hackers seek to infiltrate it the most. The fact that the most disruptive and expensive hacking efforts are still coming from within the organisation causes traffic from both the Internet and the internal network to be philtered. They are capable of virtually unlimited scalability. Furthermore, the question of a single point of failure posed by the perimeter firewall has been answered. When a new regulation is introduced, a new policy is formed and appended to the existing regulation, according to the upgrade technology, which includes a number of features. New policy modifications are implemented in the absence of any associated protocols. In particular, the currently deployed firewall is distinguishable in that the firewall protection policy protocols are focused on the rules that have been constructed and created to manage the firewall that will be utilised after the firewall upgrade and new configuration. It is common for precision in identifying and deleting likely misconfigurations from changed policies to rely on rectification algorithms that analyse probable mistakes, as well as duplication and shadowing queries, to be critical. Developing tools to assist operators in the preparation of hybrid network identified software (SDN) topologies and in the simplification of the initial distribution of access control lists (ACLs) to SDN-capable protection regulation switches, which are described by a matrix of end-to-end flow reach capabilities, is essential. We want to conduct more extensive tests in field studies, such as those for mobile platforms, in addition to the general tests.

The network's safety feature is more dependent on the network's overall stability than on any other factor. The various security strategies were not thoroughly investigated in the course of the research. In the future, no one can imagine a world without computers and the internet, both of which have been severely restricted. Knowledge transmission occurs frequently; every gadget on the planet may be connected to any other computer on the planet, even if they are physically isolated from one another. This is a tremendous advantage for both the consumer and the organisation. As a result, secure data sharing is required in this case, though not in the traditional sense of network security. This includes a clear application of corrective measures to protect you against viruses, hacking, and unauthorised access to information. Only the firewall may be used to safeguard the network against intrusion. The firewall is a collection of objects that are placed between two networks with the purpose of filtering traffic between them in accordance with certain protection principles. When a local device or network system is simultaneously connected to wide area networks and the Internet outside of the region, firewalls can be extremely effective in protecting the device or network system from network protection threats. Standard network firewall modules, which are normally installed at the network's perimeter, are authorised to act as a handle, allowing only specific types of traffic to pass through the network and out of it. The turning of fire lines is a term that is sometimes used to describe this process. One-sided and one-sided and dysfunctional, the network is divided into two sections. As a result, they place a great deal of emphasis on the network's topology. Fireworks, on the other hand, are a method for decision control. Distributed fires enable the execution of protection policies on the external network, while restricting the network's topology to an inside or exterior view depending on the situation. Policy terminology and centralised distribution semantics are used by network devices to interact with untrusted networks in order to facilitate the use of fire technology in organisations for all network domain participants and to enable the logical differentiation of holdings in and out of the trusted domain. Fire should be distributed throughout the network so that it fixes these issues when hackers attempt in while also protecting network end points. For security reasons, it is extremely difficult and expensive to conduct internal investigations. Invasion and hacking are currently being established by sifting traffic from both the network of entrants and the internet. According to the findings of the above investigation, the use of customised hash codes for each dispersed network in order to make the firewall safer is insufficient.

As previously indicated, the study of various research of LAN and LAN-based securities has been studied through reviews of literature study, which has resulted in the findings of the study described above. The use of distributed firewalls for LAN security has been mostly unexplored, and there has been little in-depth investigation. The study discovered the following research gaps about the current scenario of technical necessity and demand.

a) The lack of a proper model or framework has been investigated in relation to LAN Securities.

b) A Distributed Firewall is required in order to execute data security in the local area network.

c) Distributed Firewalls are being used to evaluate data security in local area networks (LANs).

d) The preceding work does not include an analytical outcome (numerical).

e) DDoS (Distributed Denial-of-Service – DDoS) attack research on MANET has been investigated in a variety of studies, but only a small number of studies have been conducted on LAN setup.

It is hoped that this research investigation would provide a comprehensive grasp of the security algorithms taken collectively. The outcome of the comparative study allows for a more complete understanding of the behaviour analysis of the security algorithm as a whole.

4. Significance of Research

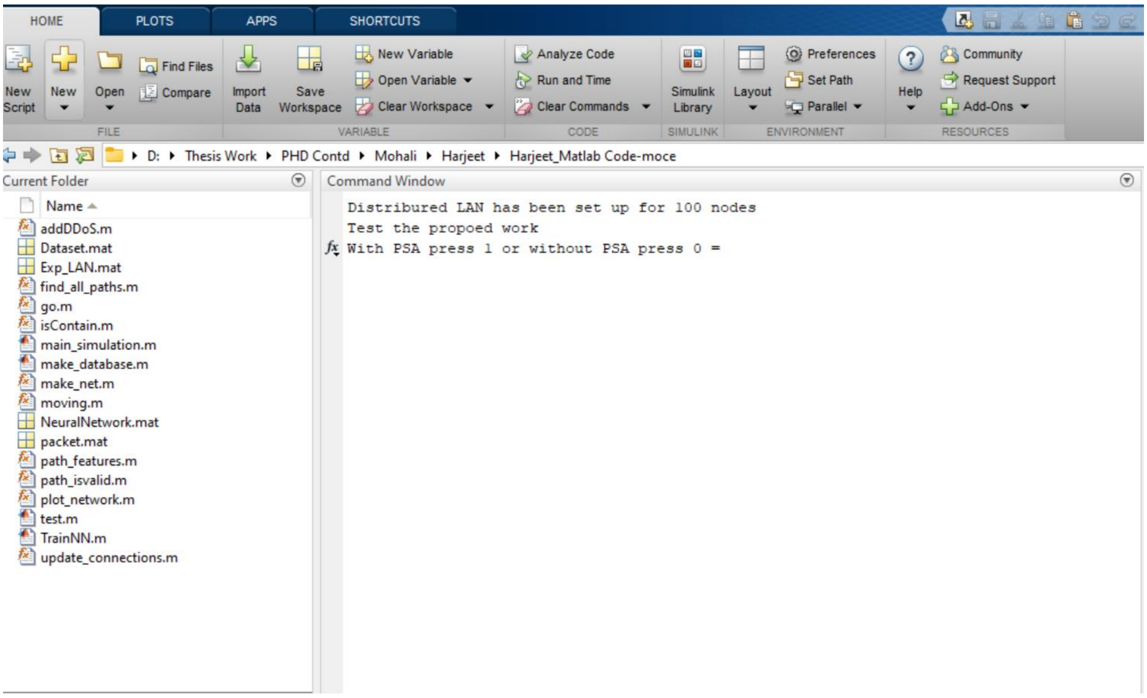
It is hoped that this research investigation would provide a comprehensive grasp of the security algorithms taken collectively. The outcome of the comparative study allows for a more complete understanding of the behaviour analysis of the security algorithm as a whole.

5. Neural Network to secure the DLAN

As the computer network grow, the encryption mechanisms are of notable importance. In particular, the asymmetric encryption models have been always deeply considered because of their wide range of usage. However, finding two pair functions for encryption and decryption that satisfy the necessary conditions for providing computational strength and safety that has always been a serious problem. In this work, we provide a new asymmetric encryption mechanism based on artificial neural networks. First, we presented the overall methods of encryption, and then we explored the necessary conditions of asymmetric methods. Next, we presented a model for the encryption mechanism that is based on Boolean algebra. We then used a neural network to learn the decryption mechanism. Finally, the simulation results showed that after training the artificial neural networks, it can be used effectively as a decryption function [11].

6. Simulation & Result

Obtaining the goal specified in the research proposal is the primary goal. Through the use of a MATLAB script, we were able to plot a LAN network. The number of nodes that have been launched for the construction of a distributed form of LAN in this study is 100 in total. The network has a dimension of 1000 * 1000 metres, and the nodes are distributed in a random manner. The random processing is carried out using a neural network, which is a computer programme. An attacker node has been allocated to the created network as the properties of a wormhole attack, and a DDoS configuration has been assigned to the network as well. The script has been executed in MATLAB 2013, as shown in the screenshot below.



```
Distributed LAN has been set up for 100 nodes
Test the propoed work
fx With PSA press 1 or without PSA press 0 =
```

Fig 5.1: MATLAB screen layout of execution of LAN

The Distributed Local Area Network (LAN) can be implemented in two ways using the structure described above. One with the PSA application and one without the PSA application. It is a modified version of routing algorithms, and it is known as the packet security algorithm (PSA).

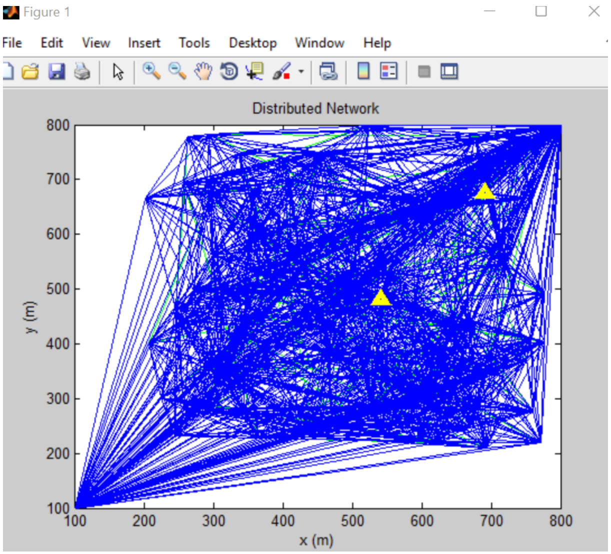


Fig 5.2: Distributed LAN presented in above figure along with 2 triangular nodes as attackers.

Now, the on-network test was initiated both with and without the use of a PSA [12]. The data packets in the group of 50 have been tossed to the receiver's end of the network connection. The parameters of the network have also been studied in greater depth. This should be repeated until 500 packets have been collected and evaluated.

Packet Bit: Range from 1 kb to 100 kb

Table 5.1: Evaluation of Data packet with absence of PSA

PSA (0)				
	Bits_Loss	Total_Time	Total_Energy	Packet_Delivery_Rate
Number of Data Packets 50	72	326.41	205.05	28
Number of Data Packets 100	79	311.38	466.88	21
Number of Data Packets 150	80.6667	280.45	394.03	19.3333
Number of Data Packets 200	77.5	553.61	544.50	22.5
Number of Data Packets 250	78.4	1020.60	831.26	21.6
Number of Data Packets 300	79	1217.70	1136.20	21
Number of Data Packets 350	78	1099.80	971.70	22
Number of Data Packets 400	78	1118.40	1574.00	22
Number of Data Packets 450	78.2222	969.12	1831.80	21.7778
Number of Data Packets 500	81.2	1029.20	1520.00	18.8

Table 5.2: Evaluation of Data packet with PSA

PSA (1)				
	Bits_Loss	Total_Time	Total_Energy	Packet_Delivery_Rate
Number of Data Packets 50	14.00	325.49	331.42	86.00
Number of Data Packets 100	20.00	77.95	728.72	80.00
Number of Data Packets 150	20.00	106.50	973.27	80.00
Number of Data Packets 200	6.00	302.40	1659.00	94.00
Number of Data Packets 250	14.80	189.94	3606.60	85.20
Number of Data Packets 300	2.00	560.78	**2279**.00	95.67
Number of Data Packets 350	21.14	256.03	3491.20	77.71
Number of Data Packets 400	1.75	479.02	9449.10	88.25
Number of Data Packets 450	3.11	481.86	9581.60	83.33
Number of Data Packets 500	2.00	414.34	8166.90	83.80

5.3 Comparative Analysis of Packet loss

	Bits_Loss PSA (0)	**Packet_Loss PSA (1)**
DP-50	72	14.00
DP-100	79	20.00
DP-150	80.6667	20.00
DP-200	77.5	6.00
DP-250	78.4	14.80
DP-300	79	2.00
DP-350	78	21.14
DP-400	78	1.75
DP-450	78.2222	3.11
DP-500	81.2	2.00

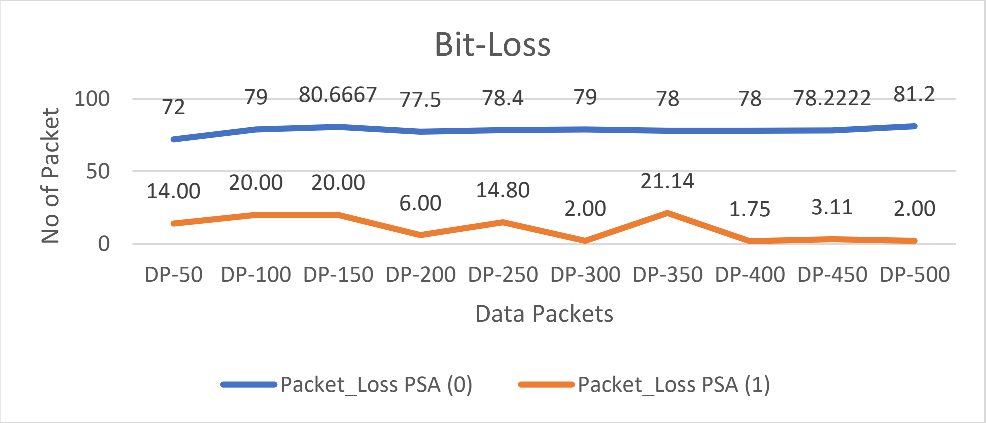
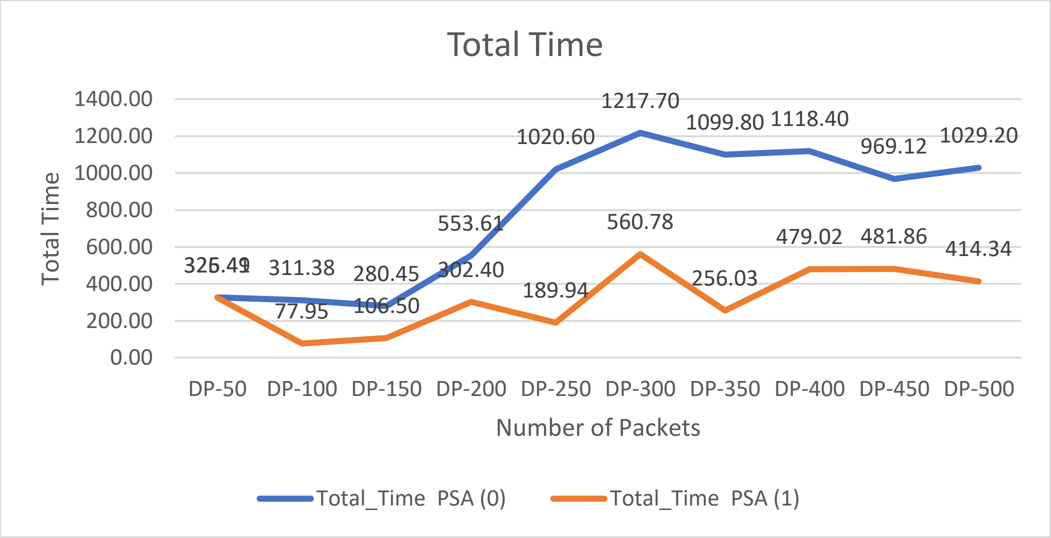


Fig 5.3: Comparative Analysis of Packet loss for nodes 500

As depicted in the preceding picture, the loss of a packet occurs after each throw of a 50*n round that is completed in MATLAB. As an example, in the situation of PSA – 0 (which is devoid of packet security), a significant amount of loss has been seen as compared to PSA -1. (With Packet Security). It is the identical pattern that is followed in each and every attempt at sending packets.

5.4 Comparative Analysis of Total Time

	Total_Time PSA (0)	Total_Time PSA (1)
DP-50	326.41	325.49
DP-100	311.38	77.95
DP-150	280.45	106.50
DP-200	553.61	302.40
DP-250	1020.60	189.94
DP-300	1217.70	560.78
DP-350	1099.80	256.03
DP-400	1118.40	479.02
DP-450	969.12	481.86
DP-500	1029.20	414.34



4.4 Comparative Analysis of Total Time

As depicted in the following picture, the total time spent in the network for each throw of the 50*n round run in MATLAB was calculated. As an example, the PSA – 0 (which is devoid of packet security) requires more time to be observed when compared to the PSA -1. (With Packet Security). It is the identical pattern that is followed in each and every attempt at sending packets.

5.5 Comparative Analysis of Total Energy

	Total_Energy	Total_Energy
DP-50	205.05	331.42
DP-100	466.88	728.72
DP-150	394.03	973.27
DP-200	544.50	1659.00
DP-250	831.26	3606.60
DP-300	1136.20	2279.00
DP-350	971.70	3491.20
DP-400	1574.00	9449.10
DP-450	1831.80	9581.60
DP-500	1520.00	8166.90

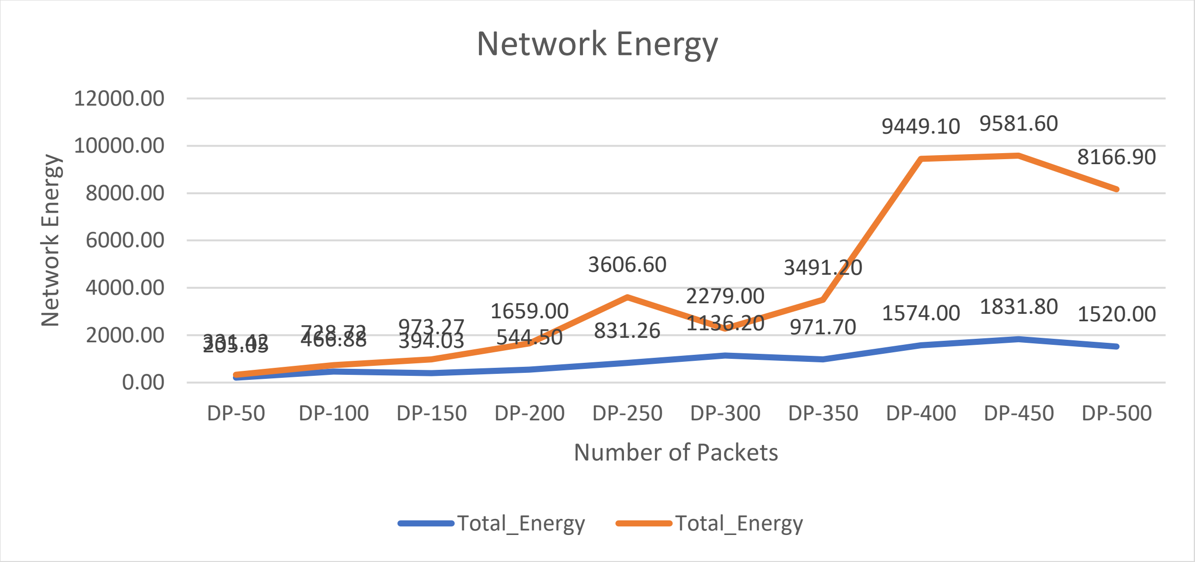


Fig 4.5 Comparative Analysis of Total Energy

As depicted in the preceding figure, the total energy expended in the network for each throw of the 50*n round executed in MATLAB was calculated. As an example, the PSA – 0 (which is devoid of packet security) has fewer observations when compared to the PSA -1. (with Packet Security). It is the identical pattern that is followed in each and every attempt at sending packets. Every time a packet is thrown, the total amount of energy expended in each round is significantly higher.

5.6 Comparative Analysis of Packet Delivery Rate

	Packet_Delivery_Rate	Packet_Delivery_Rate
DP-50	28	86.00
DP-100	21	80.00
DP-150	19.3333	80.00
DP-200	22.5	94.00
DP-250	21.6	85.20
DP-300	21	95.67
DP-350	22	77.71
DP-400	22	88.25
DP-450	21.7778	83.33
DP-500	18.8	83.80

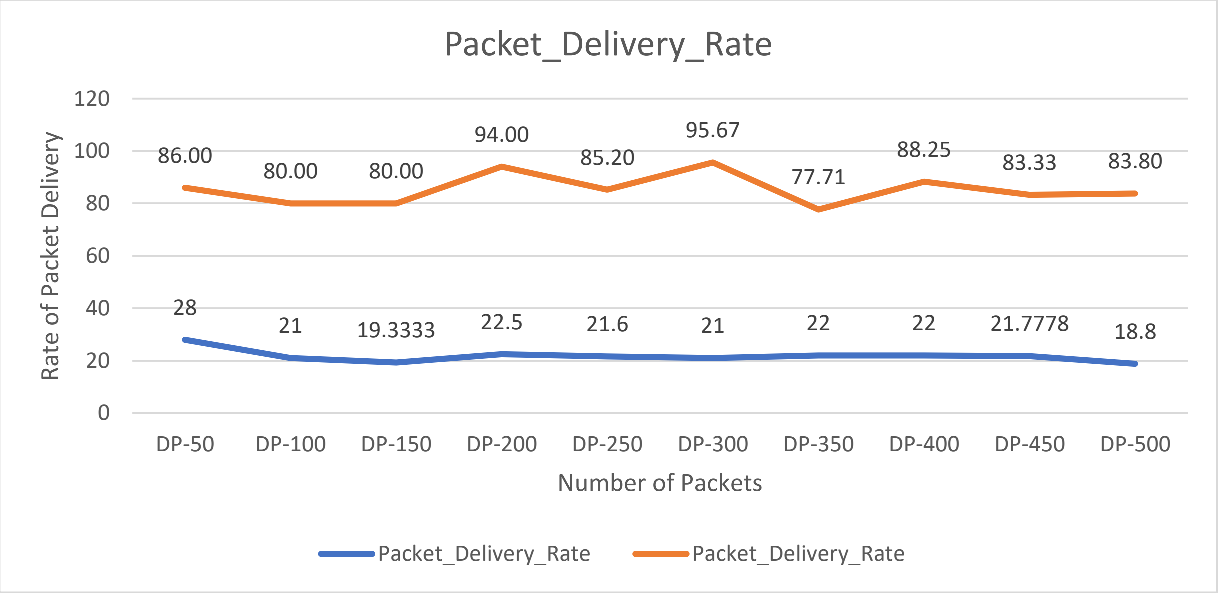


Fig 4.6: Comparative Analysis of Packet Delivery Rate

As depicted in the above figure, the rate of packet delivery consumed network resources in every throw of 50*n round completed in MATLAB was calculated. When compared to the PSA -1, the packet delivery for PSA – 0 (i.e., without packet security) has been observed to be less frequent (with Packet Security). It is the identical pattern that is followed in each and every attempt at sending packets. Every time a packet is thrown with the installation of security, the rate of packet delivery in each round is significantly higher than before.

7. Conclusion and Future Direction of Research

The primary goal of taking this method is to keep the benefits of firewalls while eliminating their drawbacks as much as possible. Rather than having a single point of entry into the network, the distributed firewall design is based on the concept of forcing policy rules to be applied at the endpoints. Network on client side is protected by a firewall that is dispersed throughout the network or server side provides unlimited access to the network. It can be used to restrict access points from being opened in order to secure important server data and applications. The purpose of the measures described in the study paper is to protect firewalls' enhancement from being compromised by a security assault while also limiting their disadvantages. A hybrid algorithm is developed via comparative study and then used in DLAN to improve the overall performance of the network. The primary goal is to accomplish the stated objective of the research proposal. Using a MATLAB script, we created a network diagram of a local area network. The dispersed local area network (LAN) for this investigation has 100 nodes. The network has a total area of 1000 x 1000 meters, and the nodes are distributed in a random manner. The random processing is carried out using a neural network, which is computer software. The network that has been constructed now incorporates a wormhole attacker node as well as a DDoS setup. In this research, we introduce packet security analysis (PSA) for the purpose of securing a dispersed local area network (LAN). The Distributed Local Area Network (LAN) may be implemented in two different methods, both of which make use of the above-described topology. One with the PSA application and one without the PSA application are available for use. A modified form of routing algorithms is known as the packet security algorithm, and it is stated as follows: (PSA). Compared to PSA-1, it has been observed that the delivery of packets for PSA – 0 (i.e., without packet security) is less frequent than the delivery of packets for the PSA -1. (With Packet Security). The technique that is followed in each and every attempt to send a packet is the same as the procedure that is detailed above. Because of the enhanced rate of packet delivery in each round after the installation of security, the rate of packet delivery in each round is much higher than it was before.

References

[1] Ahmed, A., Boulahia, L. M., & Gaiti, D. (2013). Enabling vertical handover decisions in heterogeneous wireless networks: A state-of-the-art and a classification. *IEEE Communications Surveys & Tutorials*, *16*(2), 776-811.

[2] Krumm, J., & Hinckley, K. (2004, September). The nearme wireless proximity server. In *International Conference on Ubiquitous Computing* (pp. 283-300). Springer, Berlin, Heidelberg.

[3] Caprolu, M., Raponi, S., & Di Pietro, R. (2019). Fortress: an efficient and distributed firewall for stateful data plane sdn. *Security and Communication Networks*, *2019*.

[4] Singh, S., & Verma, P. R. (2018). Data Security in Local Network through Distributed Firewalls: A Review.

[5] Sinha, M., Bera, P., & Satpathy, M. (2021, June). An Anomaly Free Distributed Firewall System for SDN. In *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-8). IEEE.

[6] Filipek, J. (2018). Security architecture for the distributed environments. *Information Sciences & Technologies: Bulletin of the ACM Slovakia*, *10*(1).

[7] Clincy, V., & Shahriar, H. (2018, July). Web application firewall: Network security models and configuration. In *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)* (Vol. 1, pp. 835-836). IEEE.

[8] Praseed, A., & Thilagam, P. S. (2022). HTTP request pattern based signatures for early application layer DDoS detection: A firewall agnostic approach. *Journal of Information Security and Applications*, *65*, 103090.

[9] Yue, X., Chen, W., & Wang, Y. (2009, November). The research of firewall technology in computer network security. In *2009 Asia-Pacific Conference on Computational Intelligence and Industrial Applications (PACIIA)* (Vol. 2, pp. 421-424). IEEE.

[10] Lavrov, E. A., Zolkin, A. L., Aygumov, T. G., Chistyakov, M. S., & Akhmetov, I. V. (2021, February). Analysis of information security issues in corporate computer networks. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1047, No. 1, p. 012117). IOP Publishing.

[11] Cao, W., Liu, Q., & He, Z. (2020). Review of pavement defect detection methods. *Ieee Access*, *8*, 14531-14544.

[12] Stephan, C., Xu, C., Brown, D. A., Breit, S. N., Michael, A., Nakamura, T., ... & Jung, K. (2006). Three new serum markers for prostate cancer detection within a percent free PSA-based artificial neural network. *The Prostate*, *66*(6), 651-659.

[13] Fikriyadi, F., Ritzkal, R., & Prakosa, B. A. (2020). Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method. *Jurnal Mantik*, *4*(3), 1658-1662.

[14] Hynek, K., Čejka, T., Žádník, M., & Kubátová, H. (2020, June). Evaluating Bad Hosts Using Adaptive Blacklist Filter. In *2020 9th Mediterranean Conference on Embedded Computing (MECO)* (pp. 1-5). IEEE.

[15] Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, *76*(12), 9493-9532.

[16] Khairi, M. H., Ariffin, S. H., Latiff, N. A., Abdullah, A. S., & Hassan, M. K. (2018). A review of anomaly detection techniques and distributed denial of service (DDoS) on software defined network (SDN). *Engineering, Technology & Applied Science Research*, *8*(2), 2724-2730.