SIMULATED CHARACTERIZATION OF 5G NETWORK RESILIENCE TO ADVERSARIAL ATTACK

Okafor, C. J.[1], Abonyi, D.O.[2] , and Ene P.C.[3]
[1*,2,3,]Department of Electrical and Electronic Engineering, Enugu State University of Science and Technology, Enugu State, Nigeria.
Email: [1]c4okafor4@gmail.com, [2]abonyi.dorathy@esut.edu.ng, [3]eneh.princewill@esut.edu.ng

Article Info
Received: 18/10/ 2025
Revised: 02/11/2025
Accepted 08/11/2025
Corresponding Authors
[1*]Email:
c4okafor4@gmail.com
Corresponding Author's Tel:
[1*]+2347019443335

ABSTRACT

Adversarial attack is an attack tactics employed by cybercriminals to deceive modern network security systems and penetrate networks for cyber attack. While several studies focused on known threats, there has been gap in their inability to detect unknown threat features, but this weakness can only be identified through characterization of a testbed network. The aim of this study is simulated characterization of 5G network resilience to adversarial attack. The testbed are the Networks of Nigerian immigration service's passport offices at Awka and Enugu, both in Nigeria. The testbed characterization involved simulation of diverse adversarial attack vectors on the network. The parameters considered for data collection are latency, throughput, packet loss, Mean Time to Response (MTTR), error rate and Mean Time to Detect (MTTD). The results obtained for the Enugu network showed that throughput, latency, packet loss, MTTR, error rate and MTTD recorded values of 68.87Mbps, 87.09ms, 7.9%, 393ms, 3.89, and97.10ms respectively. Similarly, the Awka network recorded a throughput of 90.26Mbps, latency of 39.45ms, packet loss of 1.65%, MTTR of 183ms, error rate of 0.685, and MTTD of 35.6ms. Overall, these results implied that during the penetration test on the two network facilities, the quality of service was affected as it degrades, showing that the traditional security solution was not sensitive to adversarial threat features. To address this problem, this paper recommends development of adaptive adversarial attack detection system and then integrating to the testbed for the improved security against adversarial attack.

Keywords: Adversarial attack, Awka, penetration test, simulation, throughput, Latency, MMTD, MMR

1. INTRODUCTION

Adversarial attacks represent a formidable challenge to the security and reliability of machine learning systems, spanning various domains from image recognition to natural language processing. These attacks exploit vulnerabilities in models, data, or the learning process itself, aiming to deceive or manipulate the behavior of AI systems (Hemberg and O'Reily, 2021). Evasion attacks, for instance, involve subtly perturbing input data to cause misclassification by the model, often with imperceptible changes that evade human detection (Cappers et a., 2019). Extraction attacks target the confidentiality of models, attempting to extract sensitive information or intellectual property from them. Poisoning attacks manipulate the training data, injecting malicious samples to compromise the model's performance or introduce vulnerabilities. Inference attacks leverage model outputs to deduce sensitive information about the training data or individuals, posing privacy risks (Dzhaparov, 2020). The dynamic landscape of adversarial attacks underscores the critical need for robust defenses and ongoing research to mitigate these threats and foster trust in AI technologies (Buchanan, 2020).

Due to the prohibitive cost, scale, and risk of experimenting on live 5G infrastructure, simulation environments have become the preferred method of studying network resilience. Platforms such as ns-3, OMNeT++, MATLAB Simulink, and custom 5G testbed allow researchers to replicate realistic network behaviors, evaluate adversarial attack strategies, and measure resilience under controlled conditions. Simulated characterization provides a safe and scalable way to assess vulnerabilities, test mitigation strategies, and compare system performance under both benign and adversarial scenarios (Demir et al., 2021).

Although several studies have explored 5G security, most focus on protocol vulnerabilities, cryptographic solutions, or high-level policy frameworks. Limited research has systematically quantified the resilience of 5G networks to adversarial machine learning attacks within simulated environments (Feijoo et al., 2023). Furthermore, existing work often overlooks cross-layer perspectives, the dynamic behaviour of adaptive adversaries, and the role of

resilience metrics in guiding defense strategies. These gaps highlight the need for a comprehensive characterization framework that integrates simulation, adversarial modelling, and resilience assessment (Dzhaparov, 2020).

Given the rapid global deployment of 5G and its role in critical digital ecosystems, there is a compelling need to investigate its resilience against adversarial attacks. Simulation-based characterization provides an effective methodology for identifying vulnerabilities, quantifying impacts, and designing robust countermeasures without jeopardizing live systems (Feldsar et al., 2023). This study aims to contribute to the body of knowledge by developing a simulation framework that characterizes 5G resilience, evaluates performance metrics under adversarial stress, and informs the design of secure and adaptive 5G architectures.

2. Related Works

Kong et al., (2021) surveyed on the execution of adversarial attack in the age of artificial intelligence. The study included the ideas and varieties of adversarial assaults, such as backdoor attacks, poisoning attacks, evasion attacks, targeted attacks, untargeted attacks, real-world attacks, black-box attacks, and detection models. The categorization of malware-based adversarial assaults, including attacks on neural network models and training data, was also included in the study. The defence strategies include input pre-processing, model pruning, differential privacy, model watermarking, PATE, input reconstruction, adversarial training, network distillation, adversarial example detection, training data filtering, regression analysis, ensemble learning, iterative retraining, and Deep Neural Network (DNN) verification. The study is a methodical survey that is offered to further the complete investigation and provide scholars with in-depth discourse on the subject.

Maiorca et al., (2020) researched on the lesson learned from pdf-based attacks towards the detection of adversarial attacks. The study focused on malware that is embedded in PDF files as an example of this kind of arms race. The first section of the study offered a thorough taxonomy of the various techniques that can be used to create PDF malware, including white-box, gray-box, black-box, GA-based, white mimicry, black-box reverse mimicry, and black-box mimicry. It also includes a description of the corresponding learning-based detection systems, such as those that detect optimization-based and heuristic-based attacks. Using a well-established methodology in the field of adversarial machine learning, it then classifies attacks that are especially aimed against learning-based PDF malware detectors. This methodology may be used to classify existing vulnerabilities of learning-based PDF malware detectors, as well as to find new assaults that could pose a danger to these systems and possible defences that could lessen their effects. As a result of the study's findings, developers and security analysts have been motivated to create stronger defences and investigate previously undiscovered details about malware that may be helpful in its categorization.

Martins et al., (2020) presented a systematic review on the application of adversarial machine learning for the intrusion and malware scenarios. Examining previous research on the use of adversarial machine learning for malware and intrusion detection scenarios was the main goal of the work. The study covered a few foundational ideas that are useful for comprehending the fundamentals of adversarial attacks and defending tactics. The study found that malware and intrusion classifiers can be affected by adversarial attacks. Almost all of the classifiers involved produced nearly identical results when tested against normal data. However, decision trees, linear SVM, and Naïve Bayes were the most affected. The study suggested that future investigations examine adversarial defence strategies using defensive distillation in malware detection more thoroughly. After that, the defence model should be trained using more recent, standardized datasets.

Chen et al., (2020) researched on the generation of adversarial examples against machine learning based IDS in Industrial Control Systems. The study began with a brief overview of the three types of assaults, the basic structure of an ICS, a GAN, and a black-box scenario. The study found that Black-box attack tactics depend on adversarial instances' transferability, or the potential for adversarial examples produced by a local learning model to confound other models. Determining the attacker's background knowledge, objective, and capabilities is a step in the black box attack process. Next, before creating the initial assault via injection, function code, and reconnaissance attacks, the control subnet was invaded. Then, utilizing an ensemble model, Random Forest, Extra Trees, GBDT, and

AdaBoost classifiers, a detection technique and surrogate classifier were provided. The result of the system implementation showed that the system achieved a precision of 0.9886, recall of 0.9882 and F1-score of 0.9883.

McCarthy et al., (2022) surveyed on the functionality-preserving of adversarial machine learning algorithm for classification in intrusion detection and cybersecurity. Addressing adversarial machine learning attacks and examining the resilience of machine learning models in the cybersecurity and intrusion detection sectors were the primary goals of this survey. In this study, the major research trends that was identified was examined in relation to the unresolved research difficulties for future investigations. Articles pertaining to functionality-preservation in adversarial machine learning for cybersecurity or intrusion detection with knowledge of robust categorization were required for inclusion. The survey's main finding was that improved robustness metrics are required. While some researchers only report accuracy, others may report a higher F1-Score. Nevertheless, F1-Score was skewed by unbalanced datasets, which are common in intrusion detection and partly caused by a high number of benign samples. As a result, defences against adversarial examples must take into account the likelihood that adversaries will adapt and use new tactics.

Liu et al., (2020) researched on interpretation perspective of adversarial attacks and defenses. In this study, they combined the latest developments in interpretable machine learning with an examination of adversarial assaults and countermeasures. The work specifically divided interpretation methods into two categories: feature-level interpretation and model-level interpretation. The article looked at how the interpretation may be applied to developing defensive strategies or launching aggressive attacks within each category. Subsequently, a further relationship between adversarial disruption and resilience was briefly discussed. The study's conclusion is that future research projects should take into account adversarial assault scenarios, improved interpretability of models, and model enhancement through the use of adversaries.

3. Research Methodology

The methodology for this work began with the characterization of the enterprise network managed by the Nigerian immigration service through penetration scan testing, and then results were analyzed to model vulnerabilities against adversarial attack. Recommendations were made to solve the problem and make the network resilient to adversarial attack. Figure 1 presents the block diagram of the characterization process.

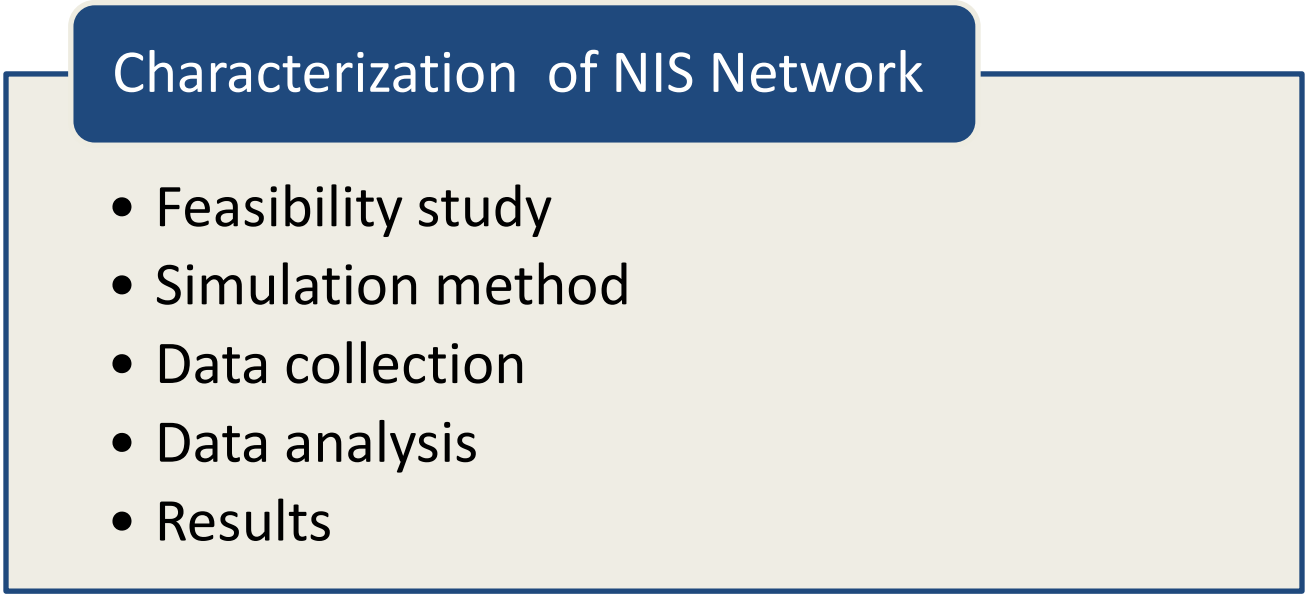

Figure 1: Block diagram of the research design mind map

The Figure 1 presents the research design block diagram. The first component is the characterization of NIS networks in Enugu and Awka as the testbed. The methods of characterization began with feasibility study to collect

data of the network and then carry out the penetration scan test through simulation method. Data was collected and then analyzed to report results of characterization.

3.1 Materials used for the study

The materials used for this work are classified into hardware and software requirements. Their version and description are presented in Table 1 for hardware and Table 2 for software.

Table 1: Hardware Materials

Material	Version	Description
Computer System	Intel Core i7, 11th Gen	High-performance system used to run simulations, data collection, and analysis.
RAM	16GB	Memory used for data storage, network simulations, and running attack simulations.
Storage	1TB SSD	Storage for data sets, logs, and tool installations.

Table 2: Software materials

Materials	Version	Description
OS	Linux-v11 and windows 10	Operating system running the entire simulation environment.
Cisco Packet Tracer	v8.2.2.040	Simulation tool used to design and emulate network configurations and traffic.
Wireshark	v4.0.2	Network traffic analyzer and inspect packets during attack scenarios.
Excel	V2007	Used for visualizing network traffic and attack impacts on KPIs.
Google Colab	V2022a	Programming language used to write custom scripts for traffic generation, attack simulation, and KPI monitoring.
Google Earth	2024	Software used to visualized the case study centre of this research
Nmap	v7.94	Scanning of the network to look for vulnerabilities
Masscan	v1.3.2	Sending malicious packets to the network

a. The case study methodology

The case study used for this work is the Nigerian Immigration Services (NIS) passport office, located at Lat. 6.23457 and Long. 7.10873. The address is 6-4M5, Nnewi Street, Odera Estate, Off Enugu-Onitsha, Express Way, Awka, Anabara State, Nigeria. The second data source is Nigerian Immigration service passport office, located at Lat. 6.43432 and Long. 7.53104. figure 2 presents the location of NIS, Awka, Passport office while figure 3 presents the location of NIS Enugu, passport office in Google Earth view.

3. Characterization of the NIS networks under study

This work characterized the NIS passport processing centres at Awka, and Enugu. The method of characterization is feasibility study and penetration testing. The purpose of the characterization is to identify weakness of the current security firewall which makes the network vulnerable against different adversarial attacks. The parameters considered for the characterization are packet penetration time, throughput, latency, packet loss, and error rate, and labels for detected vulnerabilities. The Figure 4 presents the method of characterization using block diagram.

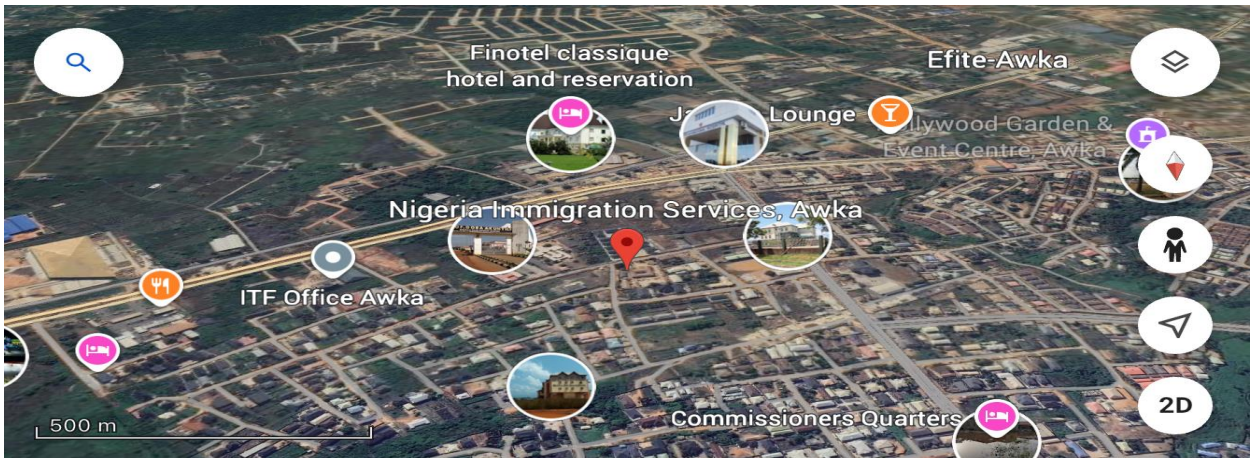

figure 2: NIS Geographical location, Awka (Source: Google Earth)

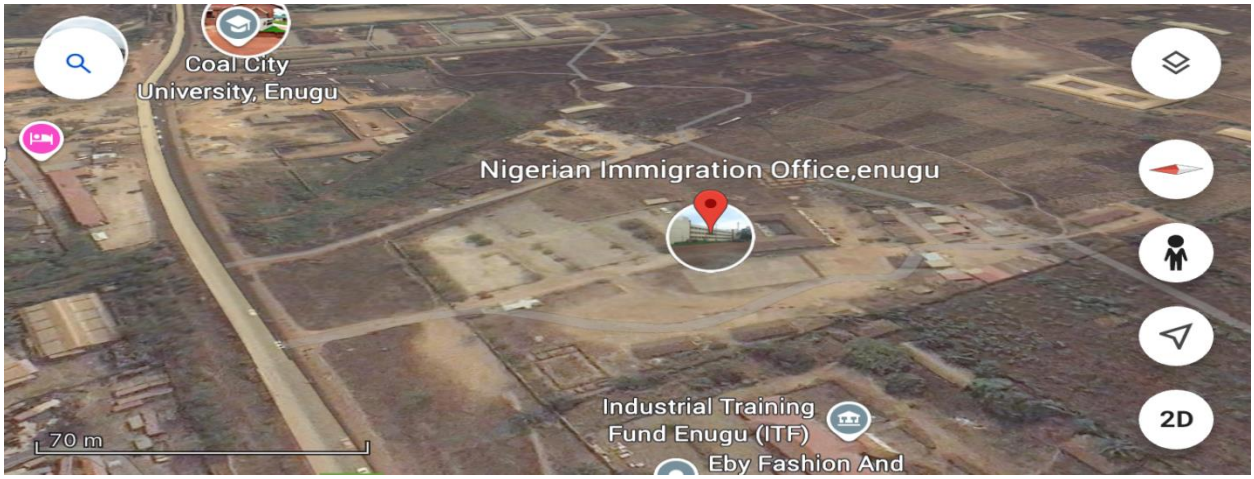

Figure 3: NIS Geographical location, Enugu (Source: Google Earth)

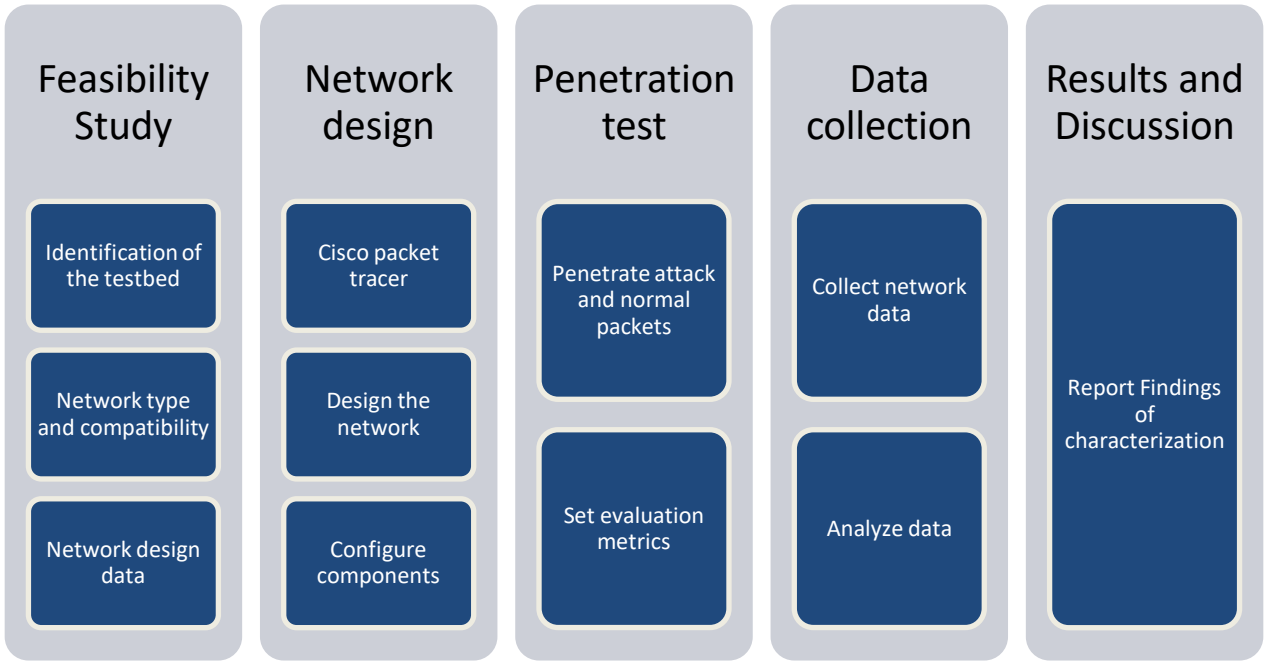

Figure 4: Block diagram of the characterization process

3.1 Feasibility study of the NIS passport offices

Feasibility study was carried out at the NIS office to evaluate the network's infrastructure and capacity to support the network attack penetration test. This was carried out on the 14th October, 2024, for Awka office and then on the 3rd November, 2024 for Enugu office. The study assessed the software tools for simulating network traffic and attacks as well as the hardware that was available, such as high-performance servers and storage systems. The outcomes demonstrated that the NIS network infrastructure was strong enough to manage the project's computational requirements, enabling efficient network testing under different condition. The Passport processing section of the organization was selected as the enterprise network for data collection. The collected data from Awka were reported in Table 3, and then used to develop the virtual network, while the Table 4 reported the data of the network collected from Enugu.

Table 3: Awka Network Architecture Data (Source: NIS Awka)

Component	Parameter	Description	Value/Configuration
Attacker Node	IP Address	The attacker node that simulates adversarial attacks.	192.168.1.20
	Traffic Type	Type of attack traffic generated by the attacker node.	DDoS Flood, MITM, Poison
	Attack Rate	The rate at which attack traffic is sent to the target server.	5000 packets/second
	Payload Size	Size of each malicious packet sent to the server.	64 bytes (for DoS), 128 bytes (for MITM and Poison)
Router	IP Address	The router responsible for routing traffic between nodes.	192.168.1.40
	Routing Table	Configuration for routing traffic between nodes.	Static routes, routing based on destination IPs
	Link Speed	The bandwidth capacity of the connection passing through the router.	1 Gbps
	Latency	Delay introduced by the router when forwarding packets.	10 ms
Server	IP Address	Server receiving legitimate requests from the client node and attacks from the attacker node.	192.168.1.30
	Request Rate	Number of requests the server can handle per second under normal conditions.	100 requests/second
	Throughput	The amount of data transferred from the server to the client node.	100Mbps
	Latency	Time taken for the server to respond to requests.	30 ms
Cables	Cable Type	Type of cables used to connect the nodes (e.g., Ethernet).	Cat 6 (Ethernet)
	Bandwidth	The bandwidth of the cables linking each node.	1 Gbps
Switches	Switch Type	Type of switch used to connect nodes together.	Layer 2 Ethernet Switch
	Switching Speed	The speed at which the switch forwards data packets.	1 Gbps
	Port Configuration	The number of ports on the switch connecting the nodes.	4 ports
Network Topology	Topology Type	The arrangement of nodes within the network.	Star (with Router as central node)
	Packet Loss	The percentage of packets lost during transmission between nodes.	0% (under normal conditions), 10% (under attack)
	Error Rate	The rate of errors in transmitted packets,	0.1% (normal), 5% (under attack)

		typically caused by attacks or network overload.	
Simulation Time	Duration	Total time duration of the simulation test (for each scenario).	30 minutes
	Traffic Monitoring	The method for monitoring the network traffic during the simulation.	Wireshark (for packet capture)
Legitimate Node	IP Address	The four nodes that simulate legitimate packet and their IP addressed.	192.136.1.20 192.136.1.37 192.136.1.22 192.136.1.17
	Traffic Type	Type of packet.	HTTP
	Data Rate	Data rate	100 Mb/second
	Payload Size	Size of each packet sent to the server.	32 bytes

Table 4: Enugu Network Architecture Data (Source: NIS, Enugu)

Component	**Parameter**	**Description**	**Value/Configuration**
Attacker Node	**IP Address**	The attacker node that simulates adversarial attacks.	192.168.1.20
	Traffic Type	Type of attack traffic generated by the attacker node.	DDoS Flood, MITM, Poison
	Attack Rate	The rate at which attack traffic is sent to the target server.	5000 packets/second
	Payload Size	Size of each malicious packet sent to the server.	64 bytes (for DoS), 128 bytes (for MITM and Poison)
Router	IP Address	The router responsible for routing traffic between nodes.	192.168.1.40
	Routing Table	Configuration for routing traffic between nodes.	Static routes, routing based on destination IPs
	Link Speed	The bandwidth capacity of the connection passing through the router.	1 Gbps
	Latency	Delay introduced by the router when forwarding packets.	10 ms
Server	IP Address	Server receiving legitimate requests from the client node and attacks from the attacker node.	192.168.1.30
	Request Rate	Number of requests the server can handle per second under normal conditions.	100 requests/second
	Throughput	The amount of data transferred from the server to the client node.	100Mbps
	Latency	Time taken for the server to respond to requests.	30 ms
Cables	Cable Type	Type of cables used to connect the nodes (e.g., Ethernet).	Cat 6 (Ethernet)
	Bandwidth	The bandwidth of the cables linking each node.	1 Gbps
Switches	Switch Type	Type of switch used to connect nodes together.	Layer 2 Ethernet Switch
	Switching Speed	The speed at which the switch forwards data packets.	1 Gbps
	Port Configuration	The number of ports on the switch connecting the nodes.	5 ports
Network Topology	Topology Type	The arrangement of nodes within the network.	Star (with Router as central node)
	Packet Loss	The percentage of packets lost during transmission between nodes.	0% (under normal conditions), 10% (under attack)

	Error Rate	The rate of errors in transmitted packets, typically caused by attacks or network overload.	0.1% (normal), 5% (under attack)
Simulation Time	Duration	Total time duration of the simulation test (for each scenario).	30 minutes
	Traffic Monitoring	The method for monitoring the network traffic during the simulation.	Wireshark (for packet capture)
Legitimate Node	IP Address	The four nodes that simulate legitimate packet and their IP addressed.	192.147.1.22 192.147.1.37 192.147.1.47 192.147.1.50
	Traffic Type	Type of packet.	HTTP
	Data Rate	Data rate	100 Mb/second
	Payload Size	Size of each packet sent to the server.	32 bytes

3.2. Testbed Network design and Simulation

The data collected from the feasibility study were respectively applied to simulate the NIS network for Enugu and Awka, using Cisco packet tracer. The process started with the network configurations, through the selection of components such as legitimate nodes, attacker nodes, servers, firewall, then interconnect them to create the network using cables. IP address was assigned to each of the nodes, routers and servers, before simulation. Figure 5 presented the network model of NIS at Awka, while Figure 6 presents the network model of Enugu NIS. These two networks were respectively tested for 30mins, and data were collected for analysis using wireshark tool.

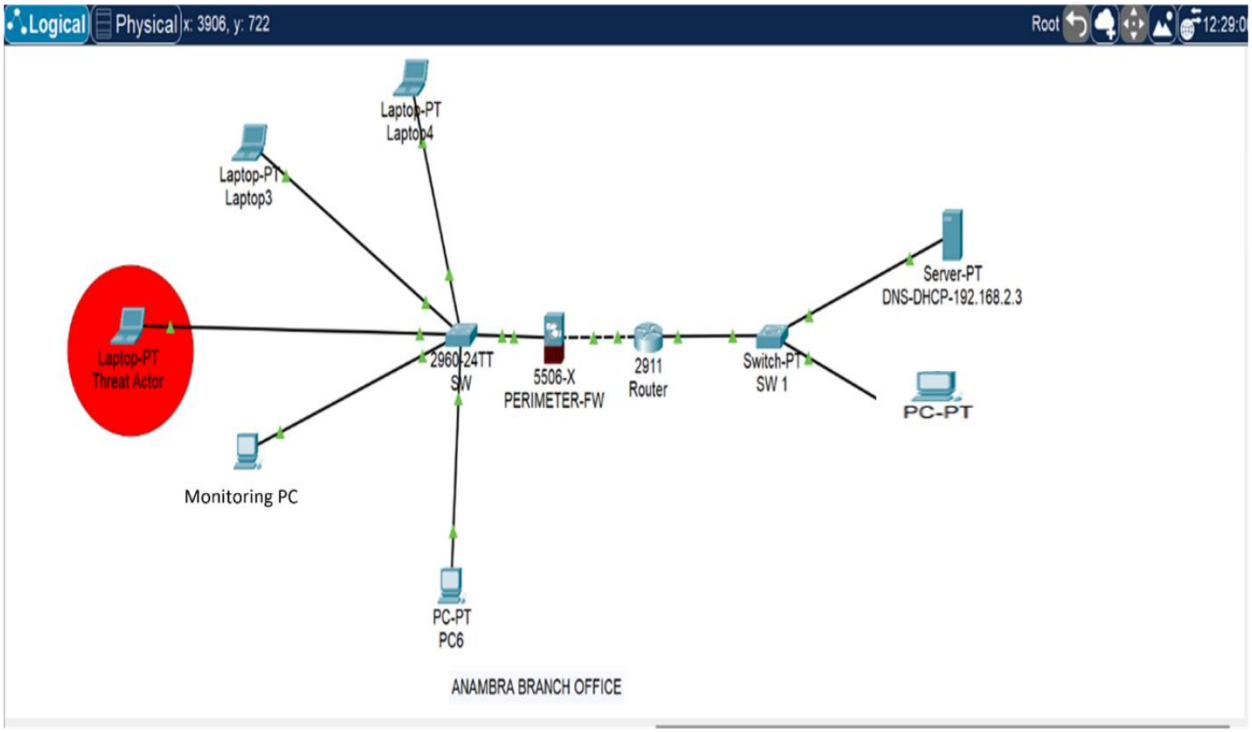

Figure 5: The testbed network at NIS, Awka with packet tracer simulator

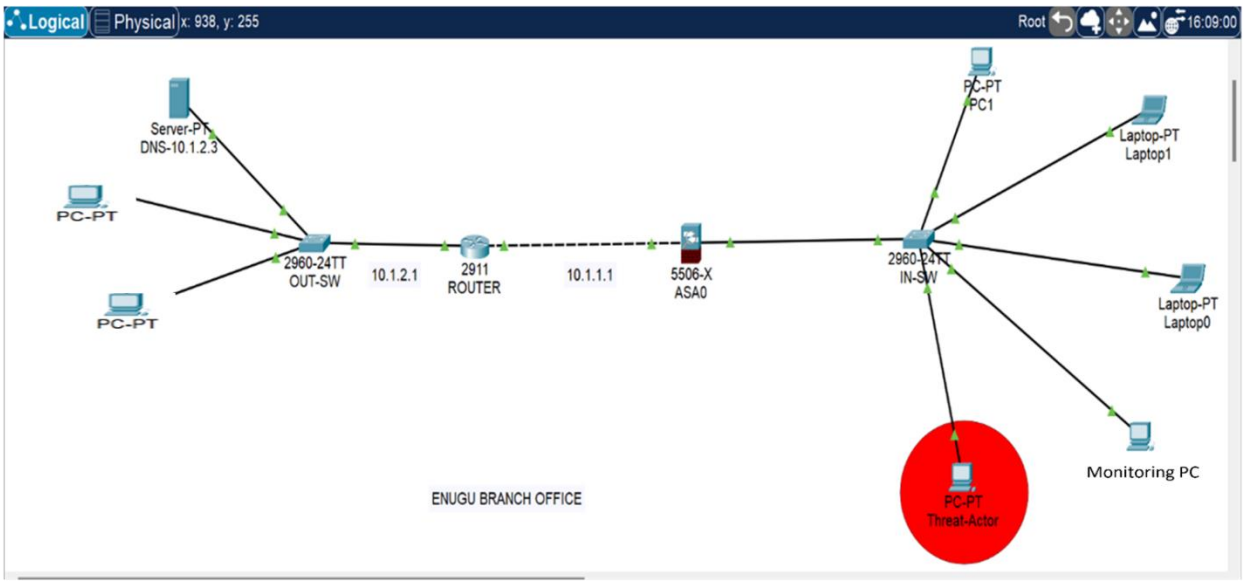

Figure 6: The Testbed Network at Enugu with packet tracer simulator

3.3 Data collection of Characterization Results

This section presents how measurements on the network were carried out during penetration test. This was achieved by pinging the different nodes which routes through the routing system to the server. The attack nodes were pinged using 5000 packets per seconds to induce different attacks. For the DDoS, each packet size was 64 bytes, while for the MITM and Poison attack, each packet size was 128bytes. These attack features and normal packet features were induced to the network at interval of one minute each randomly using Masscan tool, while Wireshark software was applied for data collection and analysis. This method was applied for both the Enugu and Awka NIS networks. The metrics used for data collection were defined in Equation1 to Equation5while the results were reported in tables 4 and table5.

3.4 Justification for the two Different Networks Characterized

The justification for the two different networks considered for this work was to improve the dependability of results. The way vulnerabilities appear in comparable attack scenarios can vary depending on the specific characteristics of each network environment, including different hardware configurations, software stacks, topologies, or traffic patterns. Researchers can evaluate the flexibility of protection measures, spot patterns and anomalies in attack behaviour, and ascertain whether a given vulnerability is unique to a given network configuration or generalizable by testing across multiple networks. Additionally, this method offers a larger dataset for evaluating threat detection models' performance, guaranteeing that the created solutions are reliable and efficient in a variety of real-world scenarios.

3.5 Metrics for threat detection models performance evaluation

Evaluating the performance of the network requires a set of well-defined metrics to measure their efficiency in identifying, mitigating, and withstanding adversarial attacks. These metrics are critical to understanding how a network performs under normal conditions and during simulated attacks. Below is an explanation of key metrics used for this purpose:

1. Mean Time to Detect (MTTD) (ms): MTTD measures the average time taken to detect an attack after it begins, expressed in milliseconds. A lower MTTD indicates faster threat detection, enhancing the network's ability to respond promptly to intrusions. Conversely, a high MTTD suggests delays in identifying threats, leaving the system vulnerable for extended periods. Equation 1 presents the model of MTTD.

$$MTTD(ms) = \frac{Detectiontime - Atackstarttime}{Numberofattacksdetected} \quad 1$$

2. Mean Time to Respond (MTTR) (ms):MTTR represents the average time taken to mitigate or neutralize an attack after detection, also in milliseconds. Low MTTR values demonstrate the efficiency of response mechanisms, minimizing the attack's impact. High MTTR reflects inefficiencies in stopping ongoing threats, which may exacerbate their consequences. Equation 2 presents the MTTR.

$$MTTR(ms) = \frac{Resolutiontime - detectiontime}{Numberofissuesresolved} \quad 2$$

3. Error Rate (%): This metric indicates the proportion of corrupted data packets during transmission. High error rates, often observed in adversarial conditions like data poisoning, signify compromised data integrity and successful interference. A low error rate suggests reliable communication and resilience against attacks. Equation 3 presents the Error rate.

$$Errorrate(\%) = \frac{Numberoferrors}{Totalpacketsent} * 100 \quad 3$$

4. Throughput (Mbps): Throughput measures the amount of data successfully transmitted across the network per second, expressed in megabits per second (Mbps). A decline in throughput during an attack (e.g., DDoS) reflects the network's struggle to process malicious and legitimate traffic simultaneously. Stable throughput under stress indicates robust defenses against malicious activity. Equation 4 presents the throughput performance.

$$Throughput\ (Mbps) = \frac{Totaldatatransferred\ (bits)}{Transfertime\ (s)} \quad 4$$

5. Latency (ms): Latency is the time it takes for a data packet to travel from the source to the destination and back, measured in milliseconds. During attacks such as "Man-in-the-Middle" (MITM), increased latency signals potential interception or delays due to malicious activities. Monitoring latency spikes helps identify real-time threats.

6. Packet Loss (%): This metric represents the percentage of data packets that fail to reach their destination during transmission. High packet loss rates during attacks may indicate network congestion or deliberate tampering, while low packet loss demonstrates the network's ability to maintain integrity and handle adversarial interference effectively. Equation 5 presents the loss percentage.

$$Loss(\%) = \frac{Numberoflostpackets}{Totalpacketssent} * 100 \quad 5$$

4. Results of characterization

This section presents the results of characterization carried out at the NIS, Enugu and Awka passport offices during the penetration test on their networks while considering various types of adversarial attack and their impact on quality of service. The impacts were accessed considering KPI such as throughput, latency, packet loss, MTTR, Error rate, and MTTD at the different interval of the penetration testing process. The results collected from Awka NIS passport office was reported in Table 5.

Table 5: Results of characterization (Source: NIS, Awka)

Time Stamp	Throughput (Mbps)	Latency (ms)	Packet Loss (%)	MTTR (ms)	Error Rate (%)	Attack Type	MTTD (ms)	Output
0:00:00	66.10371039	126.0913	11.69534	722.9164	0.49987	Poison	219.370	1
0:01:00	97.70375554	13.33708	0.0714334	0.0000	0.00544	No Attack	0.0000	0
0:02:00	99.7179421	17.21998	0.4692763	0.0000	0.00038	No Attack	0.0000	0
0:03:00	95.0389422	16.1748	0.305826	0.0000	0.00353	No Attack	0.0000	0
0:04:00	99.88468787	15.2477	0.1999304	0.0000	0.02333	No Attack	0.0000	0
0:05:00	56.31790047	130.6583	2.9951067	796.2073	0.63225	Poison	202.846	1
0:06:00	96.96227574	11.70524	0.0325257	0.0000	0.07444	No Attack	0.0000	0
0:07:00	95.17183983	18.08397	0.1523068	0.0000	0.04883	No Attack	0.0000	0
0:08:00	96.57883487	14.40152	0.0610191	0.0000	0.24758	No Attack	0.0000	0
0:09:00	99.82805739	19.09320	0.1293899	0.0000	0.33126	No Attack	0.0000	0
0:10:00	67.24532377	98.71474	8.5155049	921.1424	2.24877	MITM	106.262	1

0:11:00	98.02424882	19.26658	0.3636359	0.0000	0.16327	No Attack	0.0000	0
0:12:00	97.14778013	15.2083	0.4805860	0.0000	0.42226	No Attack	0.0000	0
0:13:00	96.26339945	15.39692	0.2933755	0.0000	0.48262	No Attack	0.0000	0
0:14:00	96.96482876	12.75999	0.1481367	0.0000	0.0826	No Attack	0.0000	0
0:15:00	68.3933919	119.0202	2.9807352	907.7307	3.53428	DDoS	151.213	1
0:16:00	96.35496416	17.71270	0.0370223	0.0000	0.17923	No Attack	0.0000	0
0:17:00	99.4206547	18.63103	0.3116490	0.0000	0.16544	No Attack	0.0000	0
0:18:00	99.68220825	13.10982	0.1625916	0.0000	0.16480	No Attack	0.0000	0
0:19:00	96.81221264	18.87212	0.2361074	0.0000	0.05979	No Attack	0.0000	0
0:20:00	64.53258527	124.5563	3.5397737	520.2168	3.55331	MITM	137.314	1
0:21:00	99.4455459	14.39336	0.1008596	0.0000	0.44788	No Attack	0.0000	0
0:22:00	97.62314888	15.63273	0.3477580	0.0000	0.06966	No Attack	0.0000	0
0:23:00	96.9779131	15.39841	0.1015306	0.0000	0.47142	No Attack	0.0000	0
0:24:00	97.00567267	16.94784	0.4402339	0.0000	0.31217	No Attack	0.0000	0
0:25:00	60.9978873	118.3145	12.055081	946.2795	2.6967	MITM	137.314	1
0:26:00	95.96279922	18.96033	0.1590017	0.0000	0.05502	No Attack	0.0000	0
0:27:00	98.86032419	14.27107	0.4090073	0.0000	0.43036	No Attack	0.0000	0
0:28:00	99.96523935	15.10747	0.2087055	0.0000	0.11105	No Attack	0.0000	0
0:29:00	99.40067316	13.37615	0.4714548	0.0000	0.16160	No Attack	0.0000	0
0:30:00	67.88491487	125.4030	3.8087312	848.1521	3.56130	DDoS	149.375	1
Average	90.26689	39.4533	1.654312	182.666	0.68517		35.603	

Table 5 present the results collected from the penetration testing of the NIS network at Awka while considering the penetration of adversarial attacks such as MITM, DDoS, poison and then normal packet without attack. This penetration test was carried out for 30mins and at every minute interval, different packet type was injected into the network. The results showed that every minute presents a different version of the network behaviour. While major part of the network performance was stable with the penetration of normal packet, it was, however, observed that the behaviour of the network was affected upon injection of adversarial attack. For instance, it was observed that the error rate of the network increased at every point of the attack injection. Also, the throughput of the network was reduced each time attack was injected to the network. The MTTR reported an average of 182.666ms, while the MTTD reported 35ms. Overall, the results showed that the poor qualities of KPI such as throughput, loss, latency are all indications of successful attack penetration on the network, which is a major problem. Secondly, the MTTD and MTTR values recorded indicated the vulnerability of the existing firewall in detecting threat at the delay response time, allowing threats to penetrate. The implication of this is that data confidentiality and integrity of customer information at the NIS Awka are at high risk and hence requires urgent network security solution. Graphical analysis was also applied to further explain major metrics for quality of service and revealed patterns of the network through threats as shown in Figure 7.

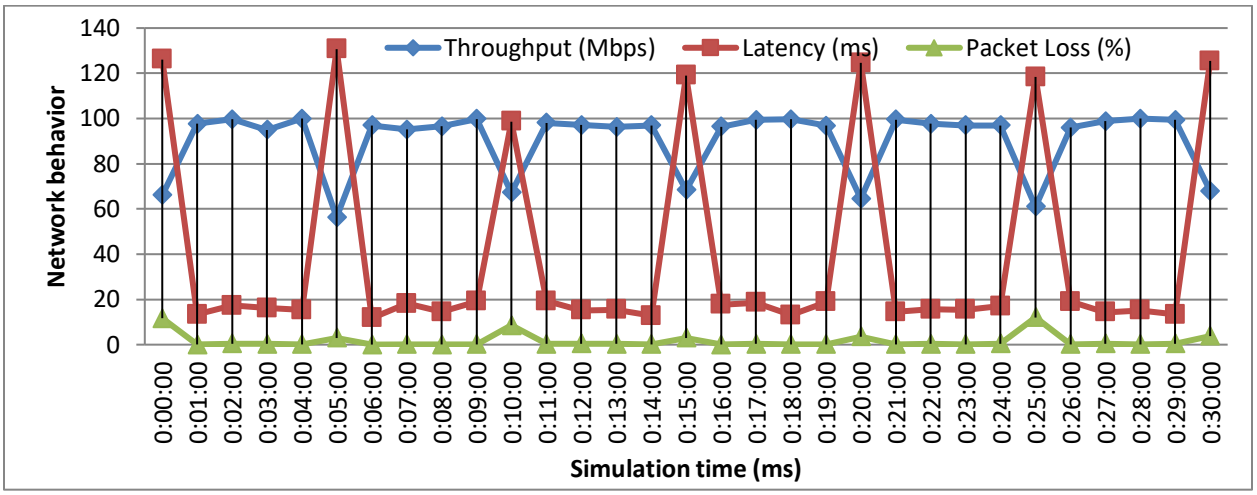

Figure 7: Result of network performance with adversarial attack

Figure 7 presents the penetration test result of the NIS network with adversarial attack injection. From the results, it was observed that at every point of attack injection, the latency and packet loss increases, while the throughput drops. The results implies that the existing firewall is vulnerable to adversarial attack, which is a big issue. Also, the Figure 8 analyzed the response time to MTTR and MTTD of the firewall during attack. The reason was to measure the time it takes for the firewall to respond to threat injection to the network. This is very important as a delay response time will allow the threat to penetrate and affect quality of service.

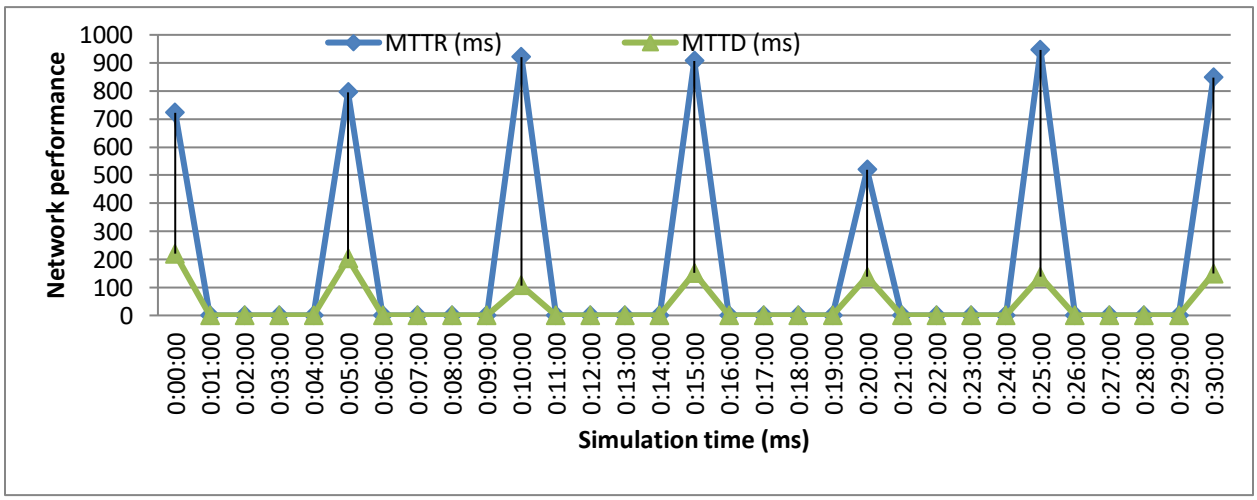

Figure 8: Firewall Response to Attack

Figure 8 graphically displays the existing system response time to threat. From the results it was observed that the response time of the firewall always increased with threat. This implied that the time it takes for the firewall to process the packet and then detect threats already gives room for the threat to penetrate to the network. This is the reason, the quality of service metrics such as throughput, latency and losses were all very poor during the same period, because attack was successful in penetrating the network. The impact of this problem cannot be over emphasized as elements of computer network security which are confidentiality, integrity, availability and even reliability cannot be guaranteed with this type of existing security solution. In addition, customer information, organization's data are at risk and they can be accessed anytime by hackers through adversarial attack, thus

necessitating the need for this research. To validate the data analysis for the existing system, data for another test of NIS in Enugu was collected and reported in Table 6 using the same penetration testing.

Table 6: Results of characterization (Source: NIS, Enugu)

Time stamp	Throughput (Mbps)	Latency (ms)	Packet Loss (%)	MTTR (ms)	Error Rate (%)	Attack Type	MTTD (ms)	Output
0:00:00	89.3	2.5	0.50065	0.00	0.25646	Normal	0.000	0
0:01:00	58.5	125.1	7.29933	600	2.55685	DDoS	120.0	1
0:02:00	60.2	118.4	7.35600	450	2.15365	Poison	0.000	1
0:03:00	60.8	130.3	9.54003	750	2.88645	MITM	180.0	1
0:04:00	92.5	1.50	0.74305	0.53	0.05540	Normal	0.000	0
0:05:00	65.1	135.8	13.00044	900	2.24541	DDoS	200.0	1
0:06:00	58.4	120.0	10.44504	550	2.36466	Poison	0.000	1
0:07:00	52.3	129.7	12.02211	800	2.96634	MITM	160.0	1
0:08:00	55.0	114.8	10.24432	350	5.07654	DDoS	0.000	1
0:09:00	60.5	140.2	14.09004	620	5.54654	Poison	250.0	1
0:10:00	58.7	119.2	10.65453	505	4.45642	MITM	0.000	1
0:11:00	58.0	128.5	11.80043	570	5.80045	DDoS	150.0	1
0:12:00	91.8	1.71	0.30022	0.00	0.20566	Normal	0.000	0
0:13:00	92.7	3.83	0.54340	0.05	0.30775	Normal	220.0	0
0:14:00	96.2	4.30	0.34309	0.35	0.15604	Normal	0.000	0
0:15:00	58.9	142.1	14.52430	510	9.65406	DDoS	260.0	1
0:16:00	53.5	116.0	10.24345	540	8.05006	Poison	0.000	1
0:17:00	56.4	134.0	12.84500	485	8.06604	MITM	210.0	1
0:18:00	54.7	122.5	10.50773	450	5.35650	DDoS	0.000	1
0:19:00	53.2	129.0	11.90944	575	7.96566	Poison	180.0	1
0:20:00	59.9	118.7	10.33400	650	7.26545	MITM	0.000	1
0:21:00	51.5	139.5	13.70555	595	7.46563	DDoS	230.0	1
0:22:00	57.4	114.0	10.05323	630	6.02454	Poison	0.000	1
0:23:00	54.8	135.6	12.50442	485	8.06406	MITM	190.0	1
0:24:00	60.0	117.5	10.22201	540	7.15564	DDoS	0.000	1
0:25:00	57.6	143.2	15.00954	620	6.00564	Poison	280.0	1
0:26:00	92.1	1.65	0.44509	0.40	0.10643	Normal	0.000	0
0:27:00	89.3	2.78	1.54372	0.70	0.74653	Normal	140.0	0
0:28:00	95.5	1.53	0.27709	0.35	0.10653	Normal	0.000	0
0:29:00	93.7	3.67	0.55110	0.42	1.25055	Normal	240.0	0
0:30:00	96.4	2.22	0.40991	0.55	0.35007	Normal	0.000	0
Avg.	68.86774	87.09	7.869944	392.85	3.89251		97.0967	

Table 6 presents the results of the network characterized at Enugu NIS centre. From the results it was observed that the network performance changes at every interval based on the penetration tool data inputs. The results showed that, averagely, the network throughput performance drop at every instance of threat. Also, the packet loss rate when there is threat increases at every instance of threat input while the loss rate increased as well. These metrics behaviour implied that the network firewall is vulnerable to threat as it allows the penetration of adversarial threats

to the network, which impacts on the overall quality of service. The results also reported that the MTTR and MTTD are all very high with an average of 393ms for MTTR and 97ms for MTTD respectively. These results showed that the firewall in the existing system takes lots of time to process packet and then classify threat. To address this problem there is need for an adaptive firewall which is intelligent to classify legitimate packet, normal attack and adversarial attacks respectively. The Figure 9 graphically analyzed the network performance KPI, while Figure 10 reported the response time of the firewall to each attack injection.

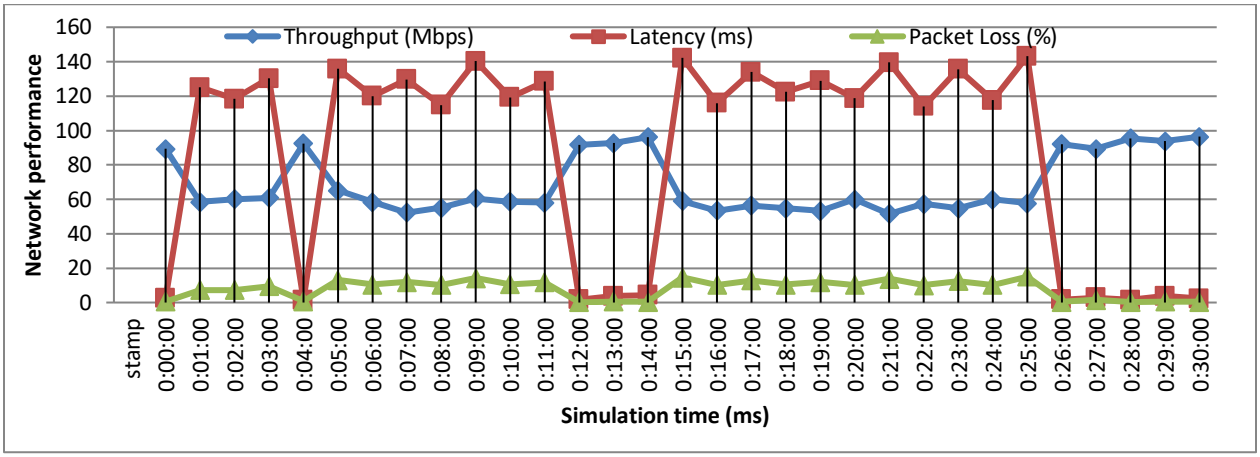

Figure 9: Results of NIS Enugu network during characterization

Table 9 reported the NIS network performance during the penetration testing. The results showed that at every point of attack penetration, the KPI tends to perform very poor as the throughput drops, latency increased and packet loss increased. Overall, these are signs of the firewall vulnerability and present the need for improved adaptive and smart firewall solution. The Figure 10 also reported the network firewall response time to threat penetration.

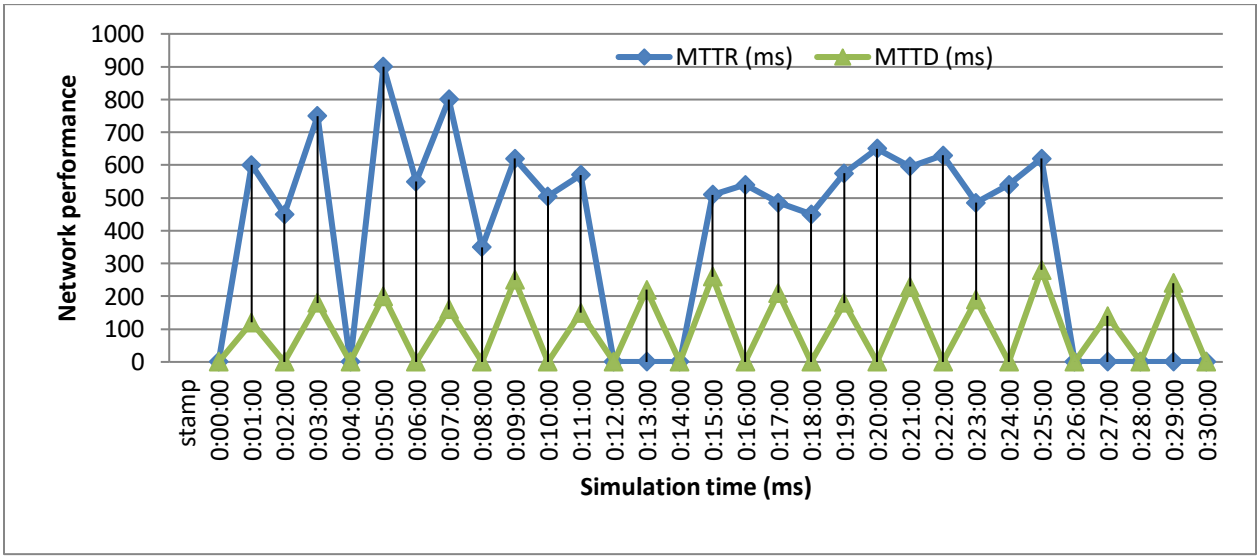

Figure 10: Result of the NIS Enugu Network Firewall Response time

Figure 10 illustrates the NIS Enugu Network Firewall's response times, specifically highlighting the MTTD and MTTR under threat penetration scenarios. The analysis indicates that at every instance of an attack, both MTTD and MTTR are significantly high, raising concerns about the system's efficiency in identifying and mitigating threats promptly. This delay suggests vulnerabilities in the firewall's real-time classification capabilities, potentially leaving the network exposed for extended periods. The impact of these delays is far-reaching for the NIS as it increases the risk of data breaches, operational disruptions, and financial losses due to extended downtime and costly remedial actions. For customers, prolonged response times can compromise the security of sensitive data, erode trust, and

damage the organization's reputation. Addressing these shortcomings is critical to ensuring robust threat management and maintaining stakeholder's confidence.

5. Conclusion

This study presented a simulated characterization of 5G network resilience to adversarial attacks using testbeds from the Nigerian Immigration Service networks in Enugu and Awka passport offices. The findings revealed that adversarial attack vectors significantly degraded the quality of service, as observed in the variations of throughput, latency, packet loss, mean time to response, error rate, and mean time to detect across both testbeds. While the Enugu network demonstrated higher vulnerability, the Awka network exhibited relatively better resilience, though still affected under adversarial conditions. These results confirm that traditional security solutions are insufficient in detecting and mitigating unknown adversarial threat features, thereby exposing 5G infrastructures to operational risks. Consequently, this work underscores the need for adaptive adversarial detection mechanisms capable of learning unknown attack patterns and dynamically integrating into live network environments. By doing so, 5G networks can achieve improved robustness, faster incident response, and enhanced security resilience against evolving cyber threats.

5.1 Ethical Clearance

Ethical clearance for this study was obtained to ensure compliance with institutional research policies and national data protection guidelines. The simulated characterization of 5G network resilience to adversarial attacks was carried out using testbed environments within the Nigerian Immigration Service networks at Enugu and Awka. No personally identifiable information (PII) or sensitive user data was collected, stored, or processed during the experiments. All data generated and analyzed were strictly technical parameters such as throughput, latency, packet loss, mean time to response, error rate, and mean time to detect, which pose no ethical or privacy risks. Access to the simulated testbed and collected data was restricted to authorized research personnel, and results were reported in aggregated form to avoid exposure of operational details that could compromise system security. These measures ensured that the research adhered to ethical principles of confidentiality, data protection, and responsible use of network resources.

REFERENCE

Buchanan, B. A National Security Research Agenda for Cybersecurity and Artificial Intelligence. *Cent. Secur. Emerg. Technol. Issue Brief* **2020**, 7.

Cappers, B.; Mengerink, J.G.; van de Pasch, J. Why algorithms are dangerous: What the role of AI should be in cybersecurity. *Eur. Cyber Secur. Perspect.* **2019**, *2019*, 76–78.

Chen J., Gao X., Deng R., He Y., Fang C., & Cheng P., (2020)Generating Adversarial Examples against Machine Learning based Intrusion Detector in Industrial Control Systems. IEEE XploreDOI 10.1109/TDSC.2020.3037500, IEEE Transactions on Dependable and Secure Computing

Demir, A.K.; Alam, S. Advancing Artificial Intelligence-Enabled Cybersecurity for the Internet of Things. In *Handbook of Research on Advancing Cybersecurity for Digital Transformation*; IGI Global: Hershey, PA, USA, 2021; pp. 118–143.

Dzhaparov, P. Application of blockchain and artificial intelligence in bank risk management. *ИкономикаУправление* **2020**, *17*, 43–57.

Dzhaparov, P. Application of blockchain and artificial intelligence in bank risk management. *ИкономикаУправление* **2020**, *17*, 43–57.

Feijoo-Martínez, J.R., Guerrero-Curieses, A., Gimeno-Blanes, F., Castro-Fernández, M., &Rojo-Álvarez, J.L. (2023). Cybersecurity Alert Prioritization in a Critical High Power Grid With Latent Spaces. IEEE Access, 11, 23754–23770.

Feldsar B., Mayer R.,&Rauber A., (2023) Detecting Adversarial Examples Using Surrogate Models. Mach. Learn. Knowl. Extr. 2023, 5, 1796–1825. https://doi.org/10.3390/make5040087

Hemberg, E.; O'Reilly, U.M. Using a Collated Cybersecurity Dataset for Machine Learning and Artificial Intelligence. *arXiv* **2021**, arXiv:2108.02618.

Kong Z., Xue J., Wang Y., Huang L., Niu Z., & Li F., (2021) A Survey on Adversarial Attack in the Age of Artificial Intelligence. Hindawi Wireless Communications and Mobile Computing Volume 2021, Article ID 4907754, 22 pages https://doi.org/10.1155/2021/4907754

Liu, H.; Lang, B. Machine learning and deep learning methods for intrusion detection systems: A survey. *Appl. Sci.* **2019**, *9*, 4396.

Maiorca D., Biggio B., &Giacinto G., (2020) Towards Adversarial Malware Detection: Lessons Learned from PDF-based Attacks. ACM Comput. Surv. 1, 1, Article 1 (January 2019), 35 pages. https://doi.org/10.1145/3332184

Martins N., Cruz J., Cruz T., & Abreu P., (2020) Adversarial Machine Learning Applied to Intrusion and Malware Scenarios: A Systematic Review. IEEE Access: Digital Object Identifier 10.1109/ACCESS.2020.2974752

McCarthy, A.; Ghadafi, E.; Andriotis, P.; Legg, P. Functionality-Preserving Adversarial Machine Learning for Robust Classification in Cybersecurity and Intrusion Detection Domains: A Survey. *J. Cybersecurity Priv.* **2022**, *2*, 154–190.