JOURNAL OF ENGINEERING RESEARCH & SCIENCES

JENRS

www.jenrs.com
ISSN: 2831-4085

Volume 4 Issue 10
October 2025

EDITORIAL BOARD

Editor-in-Chief

Editorial Board Members

Dr. Deepak Bhaskar Acharya
Department of Computer Science, The University of Alabama in Huntsville, USA

Dr. Ali Golestani Shishvan
Department of Electrical & Computer Engineering, University of Toronto, Canada

Editorial

As digital connectivity, cybersecurity, and sustainable energy systems become increasingly intertwined with everyday life, research is moving beyond conceptual proposals toward deployable, user-friendly, and evaluative frameworks. The three papers highlighted in this editorial exemplify this shift by addressing seamless private network connectivity for mobile users, methodological rigor in assessing DDoS defenses, and intelligent optimization of renewable energy infrastructure. Together, they reflect a broader emphasis on practicality, proportional response, and sustainability in modern engineering and networked systems.

The first paper explores an expanded role of mobile data services, positioning cellular networks as gateways to private local networks rather than mere Internet access providers. Targeting Small-Office and Home-Office users, the study recognizes the necessity of plug-and-play solutions that require minimal technical expertise. After examining conventional approaches for remote connectivity, the paper introduces an alternative concept based on surrogate devices using Linux MACVLAN interfaces, policy-based routing, and network address translation. Implemented on the widely adopted OpenWrt platform, the solution demonstrates how mobile devices can be seamlessly integrated into private networks. Results from a friendly-user trial confirm that the proposed approach effectively meets usability and deployment goals, highlighting its potential for broader commercial adoption [1].

The second contribution advances the field of network security by proposing a concrete severity classification and evaluation framework for Distributed Denial of Service attacks. Moving beyond binary detection models, the study introduces a quartile-based classification scheme that categorizes traffic severity using multidimensional thresholds derived from packet length, packet rate, and bandwidth consumption. This framework enables more nuanced and proportional defensive responses. Additionally, the paper provides a comparative evaluation of DDoS mitigation strategies deployed at different network levels, offering operational insights into their respective strengths and tradeoffs. By emphasizing methodological clarity and evaluative consistency, this work lays the groundwork for adaptive, programmable, and automated defense mechanisms in future network infrastructures [2].

The third paper addresses the urgent global challenge of energy efficiency and climate change through the optimization of smart and renewable energy systems. Focusing on transformer design, the study proposes a hybrid optimization framework that combines nonlinear programming with genetic algorithms to enhance efficiency while avoiding harmful radiation. The results demonstrate notable gains in energy savings and cost reduction, reinforcing the role of intelligent design optimization in sustainable power systems. By integrating AI-driven techniques with traditional optimization methods, the work contributes to the development of robust, environmentally responsible energy infrastructure [3].

Collectively, these studies highlight a common trajectory toward solutions that are not only technically sound but also user-centric, evaluative, and sustainability-driven. From enabling seamless private connectivity for non-technical users and introducing proportional, metrics-based cybersecurity defenses to optimizing smart energy components for efficiency and environmental responsibility, each contribution addresses real-world challenges with implementable frameworks. Together, they underscore the growing importance of practical innovation in shaping secure, efficient, and sustainable digital and energy ecosystems.

References:

[1] D. Henrici, A. Boose, "Connecting Mobile Devices Transparently with the Customer Network in a User-Friendly Manner," *Journal of Engineering Research and Sciences*, vol. 4, no. 10, pp. 1–8, 2025, doi:10.55708/js0410001.

[2] E. Eyadat, M. Eyadat, A. Alfaqih, "Unveiling the Evolving Threat Landscape of Distributed Denial-of-Service (DDoS) Attacks Methodology and Security Measures," *Journal of Engineering Research and Sciences*, vol. 4, no. 10, pp. 9–20, 2025, doi:10.55708/js0410002.

[3] S.O. Oboma, E. Lambart, "Energy-Optimized Smart Transformers for Renewable-Rich Grids," *Journal of Engineering Research and Sciences*, vol. 4, no. 10, pp. 21–28, 2025, doi:10.55708/js0410003.

Editor-in-chief

Dr. Jinhua Xiao

JOURNAL OF ENGINEERING RESEARCH AND SCIENCES

Volume 4 Issue 10 **October 2025**

CONTENTS

Received: 16 August, 2025, Revised: 16 September, 2025, Accepted: 18 September, 2025, Online: 10 October, 2025
DOI: https://dx.doi.org/10.55708/js0410001

Connecting Mobile Devices Transparently with the Customer Network in a User-Friendly Manner

Dirk Henrici[*,1], **Andreas Boose**[2]

[1]Munich University of Applied Sciences HM, Dept. of Computer Science and Mathematics, 80335 Munich, Germany

[2]Telefónica Germany, B2B Technology Solutions, 80882 Munich, Germany

[*]Corresponding author: Prof. Dr. Dirk Henrici, Hochschule München FK07, Lothstr. 64, 80335 München, Germany & Email: dirk.henrici@hm.edu

ABSTRACT: The mobile data service in cellular networks can be more than just providing Internet access: it can connect mobile devices seamlessly and transparently to private networks like company intranets and home networks. Such a service is nowadays provided to usually larger customers based on customer-specific access point names and connecting the private data path via virtual private network (VPN) to a remote company network. A market study suggests that mobile network operators can monetize such an ability also for Small-Office / Home-Office (SOHO) customers. As also non-tech-savvy customers shall be able to connect their mobile devices to their private local networks without requiring support, it is essential to provide a plug&play solution for installation. We explore usual approaches for connecting remote devices to local networks as a basic building block. These are not only applicable in this scenario but can be used beyond it. As these approaches are not satisfactory for the purpose, we present an alternative concept based on so-called surrogate devices that are implemented based on Linux MACVLAN interfaces, policy-based routing, and network address translation. For this innovative approach, we provide technical details and a clean implementation for the wide-spread router operating system OpenWrt. Results of a friendly-user trial suggest that the goal of providing a plug&play approach for connecting remote mobile devices to a private local network is reached this way.

KEYWORDS: Personal Private Networks, Private Connectivity, Network Segmentation, Customer-specific APN, LAN-type connectivity, Virtual Private Networks, Mobile VPN

1. Introduction

The most important service in cellular mobile networks clearly is the data service. Being able to access the Internet in a convenient manner from everywhere has transformed our daily lives. However, mobile data can be more than mobile Internet access: mobile devices can connect to private networks like company intranets and home networks transparently without the need for any software installation on the devices.

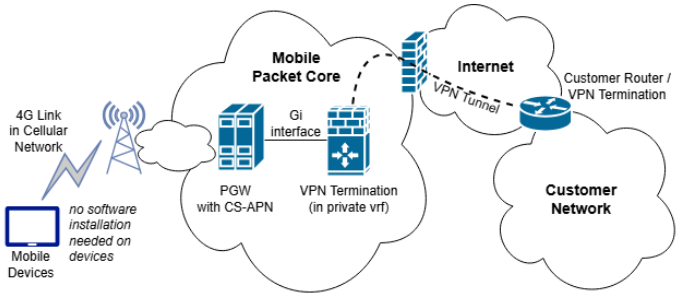

Figure 1: Private connectivity in mobile networks based on customer-specific access point names

To achieve this, the data traffic of a group of devices is forwarded from the mobile packet core to the respective customer network instead of doing network address translation and forwarding to the Internet. The endpoint in the mobile packet core (GGSN in 2G, PGW in 3G/4G) is thereby selected using customer-specific access point names (CS-APNs). Via the so-called Gi interface (3GPP terminology), the data path goes to the customer - either by a private line or a virtual private network connection over the Internet. See figure 1 for illustration for the wide-spread VPN-based variant. Additional infrastructure like firewalls is usually involved in completing the setup on the mobile network operator side.

This CS-APN-based private connectivity is a standard service provided by mobile network operators to mainly larger customers and therewith best practice. A major advantage is that no software installation is required on mobile devices to obtain private connectivity, thus easing setup and avoiding software/device compatibility issues. In our paper [1], we reported on the promising findings of a market study on the demand and acceptance for such a service also for other customer groups, namely SOHO (Small Office / Home Office) customers in Germany, and explored on how to integrate this service on the customer side in a user-friendly manner.

This article builds and extends on this work. The focus is on connecting mobile devices to an existing home network or office network in a way that is appropriate even for technically inexperienced users. As the private connection from the mobile packet core to the private network is usually done via VPN over the public Internet, we first present a

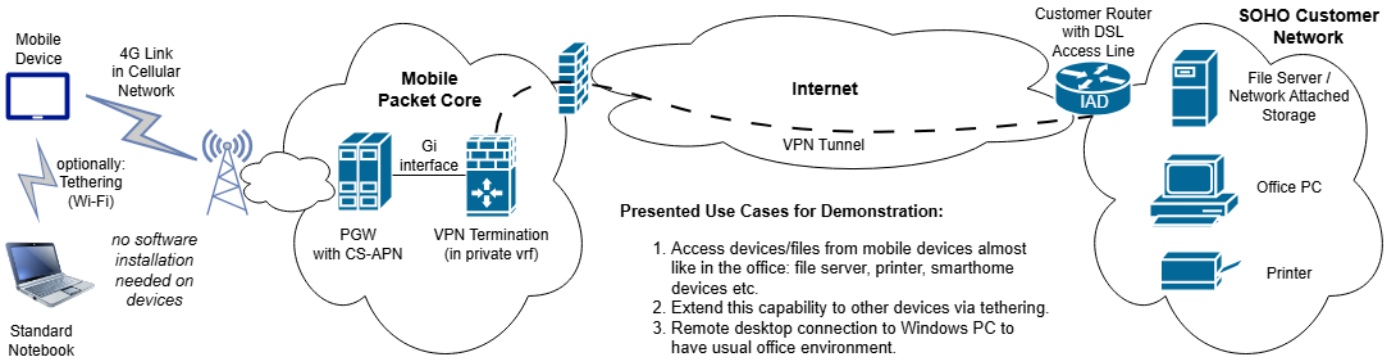

Figure 2: Technical setup for demonstration at market study group meetings [1]

widespread and a less widespread approach for connecting remote devices via VPN to a local network. Based on both approaches not being ideal for the needs in our scenario, we present an innovative approach based on so-called surrogate devices in the local network.

The remainder of this work is organized as follows: In the next section, we summarize the findings of previous work in [1] and present related work and usual approaches for remote device connectivity. An introduction of the concept of using surrogate devices to make remote devices appear as local devices in a home/office network follows. Afterwards we provide technical details and implement this approach for OpenWrt-based routers in a way that integrates nicely into the OpenWrt configuration framework. Then we evaluate this approach and compare it to other options before concluding.

2. Previous and Related Work

The following sections motivate the topic further, present context, provide related work, and discuss usual approaches for connecting remote devices to a local network.

2.1. Private Connectivity for SOHOs

The following is based on the market study presented in [1]: Small-Office / Home-Office customers (SOHOs) are self-employed or only have a small staff. Many have the usual office equipment like notebooks, desktop PCs, and printers. Data is stored on these devices, network-attached storage (NAS) or small servers - depending on company size and needs. Data storage in the cloud is not widespread for company data in that customer segment due to trust issues and for avoiding problems with GDPR compliance.

Many SOHO customers want to be able to work independently of their location, not only in the office. Having their data available and accessing devices in the office / at home, e.g. smart home devices, is a practical need. Data may be stored on notebooks to have it available on the go, but other workarounds appear to be widespread: having data on USB sticks or sending emails with it to oneself. In many cases, this results in inconveniences, additional work and hassle for data synchronizations, and security issues like sensitive data in unencrypted emails.

Assuming good network coverage, the ability to access one's data and devices in the office / at home seamlessly (i.e. without using VPN software on the devices) via the mobile network is regarded as an interesting option. After a demo on the possibilities based on the setup shown in 2, the study participants expressed a willingness to pay 5 Euros per month and mobile device for such a service (on average) and stated a variety of perceived benefits that will be summarized in the following paragraphs. The study is based on focus groups where sixteen entrepreneurs of different sectors were interviewed in person by a professional market research company.

One group of perceived benefits for such a service is related to freedom: one can work flexibly and location-independently, using any mobile device connected via cellular network and using even more devices using tethering. Not needing to install any software on the mobile devices and not needing to worry of potential compatibility issues is considered a big advantage of a network-based connectivity solution. As the up-to-date data stored in the office network can be accessed and edited online, one can work as if in the office. The need for data synchronization to have data available on the move is avoided - as well as workarounds like USB sticks. There is no more risk of "forgotten data", i.e. data that shall be accessed but that is currently not available.

Not having an additional party, i.e. another vendor/provider, involved is also considered a plus. This is a simplification, avoids needing to trust and depend on yet another party, and does not require commissioned data processing agreements for GDPR compliance. For many, it is a "good feeling" if relevant and sensitive data is stored on own premises and not stored with an external provider.

The alternative of setting up virtual private network (VPN) connectivity between mobile devices and a home/office network is beyond the technical know-how of most study participants. Not needing to install and manage VPN software on the devices is thus more practical and thus increases the target audience for a private connectivity product. For convenience reasons, not needing to manually operate VPN software for establishing connectivity is also an advantage of a seamless connectivity solution. Some of the few VPN software users said that they observed higher battery consumption with active VPN connections.

In summary, connecting groups of mobile devices privately and seamlessly to home/office networks is regarded as an interesting option by the study participants. The expressed willingness to pay for such a connectivity product makes it an interesting proposition for mobile network

operators.

2.2. Related Work on Private Connectivity in Mobile Networks

The concept of Access Point Names (APNs) to select the network to connect to was introduced and standardized for cellular mobile networks as part of the 3GPP specifications in the 3GPP TS 23 series that is related to the system architecture. The original specification [2] dates back to the development of the GPRS (General Packet Radio Service) in the end of the 1990s and has been updated to refer to Data Network Names (DNNs) as the new term in the 5G era.

Private connectivity is also part of other 3GPP specifications, non-public networks in form of private networks (3GPP TS 22.261) being a widely known one. Focusing on such application areas to better compete with Wi-Fi as well as IoT applications [3], 3GPP Rel. 16 introduces "5G LAN-type service" where a "5G LAN-virtual network" [4] interconnects mobile devices and local networks. It works on layer 2 and therewith not only supports unicast but also multicast and broadcasts. Implementations exist by network equipment vendors like Huawei and ZTE. After 5G LAN demonstrations in 2019 [5], China Mobile claims to be "the first in China to use technologies such as 5G LAN ... for commercial use" in a press release [6] from 2023.

To connect mobile devices with company intranets, e.g. university campus networks, Huawei offers a 5G-based solution that it calls "Mobile VPN" [7]. The approach is technically based on 5G SA's Uplink Classifier, see [8] on the technical background.

This shows that private connectivity in cellular mobile networks is included in standards but also part of equipment vendor product portfolio. On top of that, mobile network operators provide products that build on these standards but that rely on in-house implementations or that build on offers of start-up. Telefónica Germany, the occupation of one of the authors, provides "o2 Business Secure Hub" [9] to securely connect mobile devices with company intranets. A similar offer targets IoT business. It builds upon CS-APNs but also employs an additional layer of network segmentation for scalability purposes [10]. Connectivity between mobile operator and customer is realized using IPsec VPNs or WireGuard VPNs [11]. AT&T offers in partnership with Asavie Technologies a similar product named "AccessMyLAN" [12] to business customers. Connectivity between mobile operator and customer network is realized based on an SSL-based VPN: a software agent runs on a Windows computer. It created an SSL tunnel and masquerades the traffic of the mobile devices towards the computer's IP address so that all their traffic appears to originate from that computer [13].

2.3. Approaches for Connecting Remote Devices via VPN

There is a vast amount of related work around connecting remote devices via Virtual Private Network (VPN) to a local network. RFC 2764 [14] describes a framework for VPNs and discusses the various types. That work being already 25 years old, lots of other ones were published over time, up to recent papers from the current year (2025 at time of writing) like [15] on taxonomy, roles, and trends.

In the following we limit ourselves to two kinds of VPN setups that can be employed in a home network or in a SOHO network. We require that all mobile devices are reachable and visible from that network so that a NAT-based approach (NAT = network address translation) with masquerading like done by Asavie [13] does not suit us. We also limit ourselves to layer 3 connectivity as that is provided by standard mobile packet cores and mobile devices. Finally, we want to work with a single VPN connection for tunneling all data traffic between packet core and customer network. In the following, we will write "home network" for the customer network to denote a small network as is also given with SOHO customers.

2.3.1. Routed Setups

The usual and straightforward approach when connecting networks and devices via VPN is a routed setup: The local network has a local network range, and the remote site or VPN road warrior users use a separate network range; the VPN gateway acts as a router between the network ranges. Such a setup is simple and clean if the VPN gateway and the home router are realized as a single device that does all the routing. Another clean variant would be if the VPN gateway were connected to the home router via a dedicated transfer network – either using a dedicated link or a dedicated VLAN. Due to the limitations of many home routers and the configuration needed, such a variant is quite unusual in practice. Another option is the setup depicted in figure 3 where the VPN is realized as a separate device in the local network.

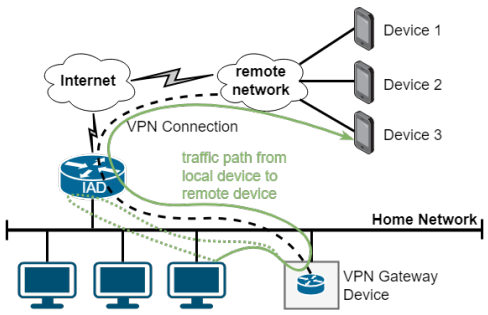

Figure 3: VPN gateway as a separate device in the local network.
green: direct traffic path; dotted green: detour to simplify configuration

The setup in figure 3 is often desired in cases in which the home router does not have the required VPN capabilities or in cases where different functionalities shall be separated. This, however, means that there are two routers in the local network. The home router is the default gateway. For a clean solution, all other devices need a distinct route to the VPN network range via the VPN gateway device: a route like `ip route <vpn network range> via <vpn gateway>`. Setting such a route on all devices is not practical so that the pragmatic option to just set this as a static route in the home router is usually chosen in practice. With this, when a device sends a packet to a VPN device, the packet is sent to the default gateway which forwards the packet to the VPN gateway due to the static route. As the default gateway detects that the packet is routed out the same interface it was received on, it emits an "ICMP Redirect" notification to the sending device to propose to

take the direct path in future.

Routed setups with separated devices in the local network thus have some drawbacks: They require configuration of a static route and therewith some networking knowledge for configuration. The pragmatic variant with a static route on the home router causes many ICMP Redirect messages being emitted to the local network. Broadcast and multicast messages in the local network do not reach the VPN devices. VPN devices do not explicitly become visible in the home network, i.e. they are not shown in the device list on the home router.

2.3.2. Setups using Proxy ARP

One may attempt to avoid the drawbacks of the routed setup in certain scenarios by employing Proxy ARP (see RFC 1027). The basic idea is to use a subrange of the local network for the VPN devices. As an example, if the local network uses 192.168.178.0/24, one could use 192.168.178.64/28 for VPN purposes. The latter would be set on the VPN interface of the VPN gateway device as depicted in figure 3, and the remote devices would use addresses out of that subrange. The VPN gateway device has a single IP address on the interface in the local network. To make the device respond to ARP requests for remote devices, one enables the Proxy ARP feature on that interface. This way, the interface in the local network acts as a representative for all VPN devices so that other devices in the local network send traffic destined to the remote device IP addresses to the VPN gateway device. The latter then knows how to reach the respective VPN devices. Return traffic works straightforward based on regular routing and forwarding logic.

This can be an elegant option. The "wgfrontend" open-source project [16] can configure and use such a setup and can be considered a proof that the concept works well in practice. Nothing needs to be configured on the home router or on other devices in the local network to set this up cleanly. However, one needs a free subrange of IP addresses in the local network so that some networking knowledge is required and the choice of the address range is limited since it needs to be within the home network range and not in use. Proxy ARP does not assist with broadcast and multicast. VPN devices usually do not become visible in the home network as the home router usually relies on DHCP (RFC 2131) and mDNS (Multicast DNS as defined in RFC 6762) to detect devices. Note that the mentioned project targets road warriors with separate VPN connections as remote devices. However, the approach works in the same manner with a single VPN connection.

3. An innovative approach based on MACVLAN, Policy-Based Routing, and 1:1 NAT

As described in the previous sections, setups based on routing or Proxy ARP have some limitations when attempting to make remote devices appear to be local devices. Proxy ARP already works well in avoiding the need for configuring other devices in the network. We, however, want an approach that does not require any knowledge of the local network, e.g. with respect to free and used IP addresses. It also would be nice if remote devices could explicitly appear as local devices in the local network as shown in figure 4.

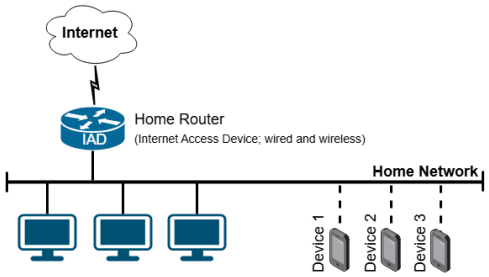

Figure 4: Remote devices shall appear as directly connected to the local home network as schematically shown here – albeit actually being located in a remote network

Our target is to implement a plug&play VPN gateway device ("Homebox") that just needs to be connected to the local network without any further configuration or consideration. Especially, no configuration on the home router or on the devices in the home network shall be required. The user shall just need to attach the VPN gateway device to the home network with nothing more to do on his part. The physical setup is depicted in figure 5.

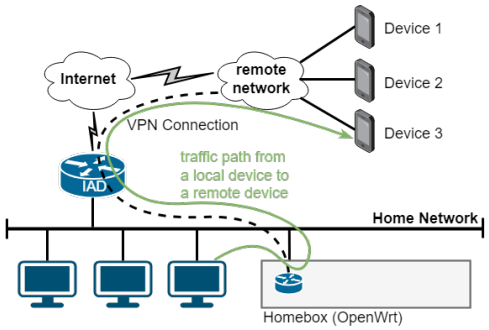

Figure 5: Physical connectivity of VPN gateway device called "Homebox"

First, we require the home router to handle IP addressing without the need to change any configuration on it. The basic approach in home networks is assignment of IP addresses via DHCP (RFC 2131). Thus, we should assign IP addresses to devices via DHCP. This way, we do not need to be aware of the home router configuration and the devices appear as regular devices in the home router's device list. To do that, we require a device in the home network for each remote device. These devices need to request their IP configuration (i.e. IP address, default gateway, DNS servers) via DHCP just like every other usual device in the home network.

Note that we do not want to closely couple the configuration in the mobile packet core with the configuration in the home network. Reasons include resilience, security, and complexity. For instance, we do not want IP address assignments to remote mobile devices to fail at times when there are connectivity issues with the VPN connections. Interacting from the mobile packet core with the home network with protocols like DHCP would also increase the attack surface. Not being able to use standard procedures like IP address assignment to mobile devices via RADIUS servers would be custom development and increase complexity of the setup. The additional complexity of potential

IP address conflicts would need to be handled, too. Therefore, forwarding DHCP requests for remote devices to the home network is not a desired approach. Instead, mobile packet core and home network shall be able to operate in a completely decoupled manner.

The solution idea is to deploy "surrogate devices" in the home network – one surrogate device for each remote device that shall be connected. For this, we require a single physical device to be able to appear as multiple devices in the local network, see figure 6 for illustration. To achieve this, we employ MACVLAN interfaces [17]. This is a device type in the Linux kernel that is usually used in the context of virtualization to connect containers to the local network with high performance [18]. In this context, each container gets an interface of type "macvlan" with an own MAC address and an own IP address but that is connected to a physical parent interface. We use a MACVLAN interface without containers to create a surrogate device in the local home network for each remote device. By configuring a DHCP client to get IP configuration assigned on the surrogate device, the latter appears as a regular device in the local network without any further configuration. There are some subtleties regarding the Address Resolution Protocol (ARP) that we discuss later.

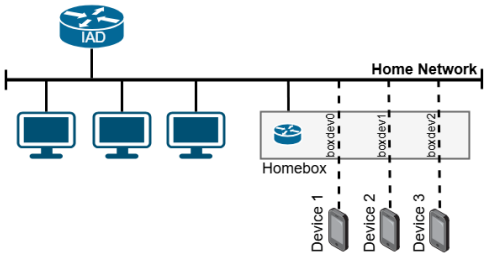

Figure 6: Logical view of device connectivity – remote devices appear to be attached to the local network; only the Homebox device is physically connected

With this, we can make additional devices appear in the local network that get IP configuration assigned and that appear in the home router's device list as regular local devices. But so far, the data traffic to these devices just reaches the VPN gateway device (Homebox), not the remote devices. To change this, we use nftables rules to map data traffic from the local IP addresses to the remote device IP addresses and vice versa. The current IP address of each surrogate device is therewith mapped to the IP address of the remote device in a 1:1 fashion. Using device names and masquerading rules, these rules can be implemented without knowing the IP addresses assigned by DHCP. Finally, we need to make sure that traffic coming from a particular remote device is sent to the local network via the correct MACVLAN interface. This is done using policy-based routing: traffic coming from a particular remote device uses a different routing table containing routes using the correct interface. Details on all this will be explained in the next section.

This approach of using surrogate devices based on MACVLAN interfaces, 1:1 NAT rules and policy-based routing allows creating a VPN gateway device that we call "Homebox". It can be simply plugged into any existing home network and provides connectivity to remote devices without the need to perform any configuration tasks in the home network. The remote devices appear as local devices in the home network – with IP addresses assigned via DHCP as usual. For our purposes, this solution is thus superior to route-based VPNs and the Proxy ARP approach.

4. Implementation for OpenWrt

OpenWrt is an open-source operating system for routers based on Linux [19]. It can be used with a variety of hardware, provides a vast ecosystem of software, and has a web frontend called "LuCI" for user-friendly configuration. It is well suited to implement a VPN gateway to integrate remote devices. We already presented Bash-based configuration script for RaspberryPi hardware in [1]. But this cannot be used with OpenWrt as OpenWrt has its own configuration framework and we'd like to have a solution that is compatible with it. In addition, OpenWrt just has a Busybox-based shell implementation so that many Bash-specific shell commands are not available without installation of additional software.

Therefore, we created a configuration script [20] specifically for the current OpenWrt. We wrote for and tested with version 24.10, the current one at time of writing. The script uses OpenWrt's configuration mechanisms and extension hooks to create a persistent configuration, i.e. one that survives reboots of the device, based on configuration data – like VPN credentials – provided in a config file. WireGuard [11] is used for creating a VPN connection towards the remote device network, in out scenario the mobile packet core. When running the script with the "-r" option, the configuration is completely removed from the OpenWrt router.

First, the script checks whether needed packages are installed and gets missing ones if needed. Besides WireGuard, the MACVLAN kernel module is required. If not yet present, it gets installed by calling:

```
opkg update
opkg install kmod-macvlan
```

A WireGuard interface is created by the script by issuing the following commands (values as configured in the config file):

```
uci set network.wghub=interface
uci set network.wghub.proto='wireguard'
uci set network.wghub.private_key='***'
uci add_list network.wghub.addresses='100.127.1.2/24'
uci set network.wghub.mtu='1392'
```

The network range '100.127.1.0/24' is used as a transfer network between the VPN interfaces in this example. Then the WireGuard interface gets the VPN terminator in the mobile packet core configured as a peer:

```
uci add network wireguard_wghub
uci set network.@wireguard_wghub[-1].description='Hub'
uci set network.@wireguard_wghub[-1].public_key='***'
uci set network.@wireguard_wghub[-1].preshared_key=***'
uci add_list network.@wireguard_wghub[-1].allowed_ips='100.127.1.1/32'
uci add_list network.@wireguard_wghub[-1].allowed_ips='100.64.0.0/10'
uci set network.@wireguard_wghub[-1].endpoint_host='***'
uci set network.@wireguard_wghub[-1].endpoint_port='51820'
uci set network.@wireguard_wghub[-1].persistent_keepalive='25'
```

We use IP addresses out of the reserved CG-NAT range 100.64.0.0/10 as defined in RFC 6598 in this example. The script also creates a new firewall zone for the WireGuard interface and allows forwarding to and from the local network. This allows the user to manage firewall policies/rules for the data traffic traversing the VPN, e.g. using OpenWrt's

web frontend, if desired. The configuration script attempts to auto-detect the interface to the local network ("lan" in the example) based on the default route in the routing table. The default route points to the home router in the local network.

```
uci add firewall zone
uci set firewall.@zone[-1].name='hub'
uci set firewall.@zone[-1].input='ACCEPT'
uci set firewall.@zone[-1].output='ACCEPT'
uci set firewall.@zone[-1].forward='ACCEPT'
uci add_list firewall.@zone[-1].network='wghub'
uci add firewall forwarding
uci set firewall.@forwarding[-1].src='hub'
uci set firewall.@forwarding[-1].dest='lan'
uci add firewall forwarding
uci set firewall.@forwarding[-1].src='lan'
uci set firewall.@forwarding[-1].dest='hub'
```

For each remote device, a MACVLAN interface is created and added to the local firewall zone. Configuration by DHCP is enabled and a hostname is set. This hostname is shown and registered in the home router automatically, if supported there. As an optimization, the MAC address is set with a constant prefix and the last four octets set with the octets of the IPv4 address of the remote device. This ensures that even after reconfigurations, the MAC address is deterministic so that usual home routers always assign the same IP address under normal conditions.

```
uci add network device
uci set network.@device[-1].type='macvlan'
uci set network.@device[-1].ifname='wan'
uci set network.@device[-1].mode='bridge'
uci set network.@device[-1].name='boxdev0'
uci set network.@device[-1].macaddr='02:17:64:7f:00:01'
uci set network.boxdev0=interface
uci set network.boxdev0.proto='dhcp'
uci set network.boxdev0.device='boxdev0'
uci set network.boxdev0.hostname='phone-main'
uci set network.boxdev0.defaultroute='0'
uci add_list firewall.@forwarding[<lan>].network='boxdev0'
```

We need to make sure that each interface answers its own ARP requests. By default, the parent interface would also answer for the MACVLAN interfaces which is not a desired behavior here. This is reconfigured using sysctl attributes in a user-defined file that gets loaded on system boot. The parent interface and a single device called "boxdev0" is configured like this in "/etc/sysctl.d/99-homebox.conf":

```
net.ipv4.conf.lan.arp_ignore=1
net.ipv4.conf.boxdev0.arp_ignore=1
net.ipv4.conf.boxdev0.arp_announce=2
```

Configuring routing rules for policy-based routing is not possible using the OpenWrt network configuration file "/etc/config/network". To work around this, we use a hotplug script to react on an interface being brought into the up state. Depending on the device name, we add a routing rule that matches data traffic coming from a certain remote device via the VPN interface and call a separate routing table for this traffic. The automatically created but not needed link-scope route is deleted so that the same entry for the parent interface becomes the only entry with that target in the standard table. The file "/etc/hotplug.d/iface/99-homebox" then looks as follows for a single device called "boxdev0":

```
#!/bin/sh
[ "$ACTION" = ifup ] || exit 0

if [ "$INTERFACE" = "boxdev0" ]; then
  ip rule add prio 30000 from 100.127.0.1 iif wghub lookup 30000
  ip route add 192.168.202.0/24 dev boxdev0 proto kernel scope link table 30000
  ip route add default via 192.168.202.254 dev boxdev0 onlink table 30000
  ip route del 192.168.202.0/24 dev boxdev0 proto kernel scope link
fi
```

Finally, the configuration script configures nftables with the needed IP address mappings. OpenWrt provides multiple options to add user-defined rules in addition to the ones maintained by the system and configured by the user using the web frontend. As the mappings are not related to other chains and rules, we chose the option to create an extension file. Two chains are created, one hooking into "prerouting" and another one hooking into "postrouting". Each local MACVLAN interface address is mapped to the respective remote device IP address and vice versa. For a single device this looks in "/etc/nftables.d/90-homebox.nft" as follows:

```
chain homebox_dstnat {
  type nat hook prerouting priority dstnat - 1; policy accept;
  iifname "boxdev0" counter dnat ip to 100.127.0.1
}

chain homebox_srcnat {
  type nat hook postrouting priority srcnat - 1; policy accept;
  oifname "boxdev0" ip saddr 100.127.0.1 counter masquerade
}
```

Only a single remote device was shown in the example code above. However, the configuration script supports up to ten remote devices. Their names and (remote) IP addresses as well as the WireGuard VPN configuration need to be provided in the configuration file in "/etc/homebox/homebox.conf". There is no knowledge and no configuration at all needed about the parameters of the home network. This way, a configured OpenWrt gateway device may be plugged into any home network to connect one or more remote devices seamlessly and in a plug&play manner. This is a considerable advantage compared to the basic routed setup and the setup based on Proxy ARP.

5. Evaluation and Applicability

Development and initial test of the implementation was done with the x86 image of OpenWrt in a KVM/QEMU-based virtual machine on a Proxmox host running in a SOHO network. In addition, the solution was applied on real router hardware using a GL.iNet GL-B1300 device. On both platforms, everything worked well and in a stable manner. We share a comparison with other approaches and practical experiences with the service and our solution in the following subsections.

5.1. Comparison of Approaches

In this paper, we considered three approaches for implementing a VPN gateway device that can be connected to an existing home network: one based on a routed setup, one based on Proxy ARP, and an innovative approach based on surrogate devices that are implemented using MACVLAN interfaces, policy-based routing and 1:1 NAT. These three approaches are compared in table 1.

To reach the target to implement a plug&play device that can be easily installed, an approach is needed that does not require configuration work on the home router or other devices in the network. As shown in the table, only the Proxy ARP approach and the surrogate device approach adhere to this requirement. A routed setup requires setting a route at least in the home router.

Table 1: Comparison of approaches

Criteria	basic routed setup	Proxy ARP	surrogate devices
Home router needs configuration	most often	no	no
Other devices need configuration	yes, but workaround	no	no
Free address subrange needed	other range	yes	no
Remote devices appear local	no	limited	yes
Performance	no bottleneck	no bottleneck	no bottleneck
Plug&play possible	no	no	yes

An additional requirement is that no configuration work on the VPN gateway device is required that goes beyond a preconfiguration done by the mobile network operator. Configuration items like VPN credentials can be configured by the network operator providing the device. But any configuration work that requires knowledge of the customer network cannot be done. The network operator cannot know what IP address range is in use in the home network in which the device will be connected to. And it cannot know which IP addresses are in use and which ones are free to use. Thus, only the routed setup and the approach based on surrogate devices can be employed in our scenario.

Only the approach based on surrogate devices makes remote devices explicitly visible in the home network since IP addresses are provided via DHCP. In a routed setup, the devices are in another network; using Proxy ARP, the devices are in the home network range, but IP addresses are not provided via DHCP.

From a performance point-of-view, all three approaches are viable. Due to the performance-limitations of embedded router hardware, the limiting factor is the VPN technology chosen. Options are IPsec, OpenVPN, WireGuard, and more. We have chosen WireGuard due to its simplicity requiring only a single UDP port for operation and its low resource consumption [11]. Therewith, the throughput of the customer's Internet access is the bottleneck in practice, not the VPN gateway device.

All in all, the approach based on surrogate devices is the only one that can adhere to the requirements in our scenario to bring remote devices located in a mobile network transparently into the home network. The customer just needs to connect the Homebox device, thus getting a plug&play installation experience. Note that the solution works independently of the fixed network provider and the vendor of the home router. Both points are relevant in practice.

5.2. Friendly-User Trial Results

Besides the market study targeting the SOHO customer segment, we also attempted to get some first insight into whether consumer customers have use cases for a service that connects their mobile devices transparently to their home network without requiring to install and use VPN software on the mobile devices. Approximately 30 volunteering Telefónica Germany employees tested the service without prior information on what to do with it.

For the trial, we mainly used two connectivity options: on the one hand, the one depicted in figure 2 in which the home router does the VPN connectivity. For this, we provided a VPN configuration file for AVM FritzBox routers that are widely used in Germany. This configuration had to be installed by the trial participants. On the other hand, we provided low-cost OpenWrt routers from the vendor GL.iNet and manually preconfigured our surrogate device approach on them (with up to five surrogate devices per participant). These OpenWrt routers only had to be connected to the home network without any further configuration work necessary. The testing scope was limited to IPv4. Broadcast and multicast packets originating from the home network reached the mobile devices so that device discovery worked in a limited manner; there was no support in the opposite direction.

As expected, the first option was chosen only by tech-savvy users that were confident of doing configuration work in the router web interface. The second option does not have such a knowledge hurdle and could thus be used by any user. This is evidence that only providing a plug&play VPN gateway device makes the solution interesting to a broader range of customers.

The trial users often used the service for straightforward use cases as expected: accessing data and media stored in the home network when commuting or when on travel was an important one. Users with smart home devices at home used the service to access these devices without requiring cloud services as connectivity relay. However, not all device vendors supported this. Mirroring camera images taken on the smartphone to storage at home using data synchronization apps also was an application.

Interestingly, the trial users also found many use cases that were not anticipated beforehand. This is evidence that providing generic connectivity creates applications that cannot be foreseen. For instance, one user implemented a data processing pipeline to process images taken on the smartphone immediately on a server at home. One other user installed a SIP client application on his smartphone to be able to receive calls to his home fixed-net number anywhere just like being at home. Some makers started experimenting with mobile IoT applications. In summary the finding is that the more devices users have at home and the more they like to play around with technology and apps, the more they enjoy using the private connectivity service.

6. Conclusion

Connecting mobile devices in cellular networks privately to existing customer networks clearly has demand in the market, not only for larger customers but also for SOHO customers as confirmed by a presented market study. Due to the relevant use cases and advantages, the participants expressed a willingness to pay five Euros per device and month. Such value-added connectivity is thus a relevant revenue opportunity for mobile network operators. A friendly-user trial indicates that the service is also interesting for certain kinds of consumer customers. This should be studied further.

Plug&play installation is a prerequisite on the customer

side to make a product user-friendly and to avoid the need for customer support. We presented two usual approaches for VPN connectivity, a routed approach and an approach based on Proxy ARP. As both approaches do not meet the requirements, we introduced a new approach based on MACVLAN interfaces, policy-based routing, and 1:1 NAT that makes remote devices appear as local devices in the customer network. We presented an open-source implementation for OpenWrt routers and explained all relevant technical ideas and details. Evaluation in theory and in a friendly-user trial shows that the approach really provides plug&play installation and makes the use cases like secure and convenient remote access to network-attached storage available to the customers. The presented approach is not only applicable for VPN connectivity to mobile networks but can also be employed in other scenarios.

References

[1] D. Henrici and A. Boose, "Market Study and User-Friendly Enablement of 4G/5G LAN-Like Connectivity for SOHO Customers," *SmartNets 2024 - International Conference on Smart Applications, Communications and Networking*, Harrisonburg, Virginia, USA, 2024, pp. 1–4, doi:10.1109/SmartNets61466.2024.10577737.

[2] 3rd Generation Partnership Project, "TS 23.003 - Numbering, addressing and identification", 3GPP Release 1999, updated up to Rel. 19 in 2024/2025.

[3] GSMA, "5G Deterministic Networks for Industries – How 5G networks can deliver the reliable and predictable connectivity required to support key industrial processes," available at https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/wp-content/uploads/2024/02/5G-Deterministic-Network-Whitepaper.pdf, 2024.

[4] 3rd Generation Partnership Project, "TS 22.261 - Service requirements for the 5G system", 3GPP Release 16, first version 2016, last update 2025.

[5] GSMA Future Networks, "5G LAN Support for IoT in Cloud Office," 5G Case Study, available at https://www.gsma.com/futurenetworks/wiki/5g-lan-support-for-iot-in-cloud-office-2/, 2019.

[6] Mobile World Live, "China Mobile sees joint 5G industry hub development as a Win-Win," Partner Feature, available at https://www.mobileworldlive.com/latest-stories/china-mobile-sees-joint-5g-industry-hub-development-as-a-win-win/, 2023.

[7] P. Tomasi, "Mobile VPN enables a new nomadic workforce – Mobile VPN for Smooth Network Switching and Verticals' Transformation," Informa Tech, commissioned by Huawei, available at https://www.huawei.com/en/news/2023/2/mwc2023-mobile-vpn-whitepaper, 2023.

[8] 3rd Generation Partnership Project, "TS 23.501 - System architecture for the 5G System (5GS)", 3GPP Release 15, 2016.

[9] o2 Business, "o2 Business Secure Hub," service description, available in German at https://www.o2business.de/content/dam/b2bchannels/de/pdfs-o2-business/leistungsbeschreibung/leistungsbeschreibung-o2-business-secure-hub.pdf, 2025.

[10] D. Henrici, W. Nicoll, J. Busch, "End-User-Specific Virtual Global-Area Network", EP3482536, European Patent Office, 2024.

[11] J. A. Donenfeld, "WireGuard: Next Generation Kernel Network Tunnel", *24th Annual Network and Distributed System Security Symposium*, The Internet Society, 2017.

[12] AT&T Business, "Protect confidential business data with AccessMyLAN from AT&T", available at https://www.business.att.com/content/dam/attbusiness/briefs/accessmylan-from-att-protects-confidential-business-data.pdf, 2022.

[13] P. Reeves, "accessmylan Instant APN," Technical White Paper, available at https://silo.tips/download/technical-white-paper-14, 2017.

[14] B. Gleeson, A. Lin, J. Heinanen, G. Armitage, A. Malis, "RFC 2764: A Framework for IP Based Virtual Private Networks,", The Internet Society, 2000, doi:10.17487/RFC2764.

[15] J. Li, B. Feng, and H. Zheng, "A survey on VPN: Taxonomy, roles, trends and future directions," *Computer Networks*, vol. 257, pp. 110964, 2025, doi:10.1016/j.comnet.2024.110964.

[16] D. Henrici, "wgfrontend – web-based user interface for configuring WireGuard for roadwarriors", available open source in the Python package index at https://pypi.org/project/wgfrontend/, 2024.

[17] https://cateee.net/lkddb/web-lkddb/MACVLAN.html, "MACVLAN support," Linux Kernel Driver DataBase, accessed Sept. 2025.

[18] J. Claassen, R. Koning, and P. Grosso, "Linux containers networking: Performance and scalability of kernel modules," *NOMS 2016 - IEEE/IFIP Network Operations and Management Symposium*, Istanbul, Turkey, 2016, pp. 713–717, doi:10.1109/NOMS.2016.7502883.

[19] A. Holt, CY. Huang, OpenWRT. In: Embedded Operating Systems. Undergraduate Topics in Computer Science. Springer, London, 2014, doi:10.1007/978-1-4471-6603-0_8.

[20] D. Henrici, "WireGuard Homebox Script for OpenWrt", available open source at https://www.towalink.de/gitea/Hub/homebox/openwrt, 2025.

DIRK HENRICI obtained his degree in electrical engineering (communication systems) from the Technical University of Kaiserslautern, Germany, in 2002. In 2008, he completed his doctorate in computer science. Since 2022, he has been a full professor at Munich University of Applied Sciences HM, Germany.

His research interests include network segmentation, network-based security, and internet architecture.

ANDREAS BOOSE has completed his PhD degree in medical research projects at University of Tuebingen in 1999. He has worked in various roles at Telefónica Germany for 25 years and is currently responsible for the work on the o2 Hub as Product Owner.

Interdisciplinary work and thinking outside the box have been his hobbyhorse.

Received: 16 August 2025, Revised: 16 September 2025, Accepted: 18 September 2025, Online: 23 October 2025

DOI: https://doi.org/10.55708/js0410002

Unveiling the Evolving Threat Landscape of Distributed Denial-of-Service (DDoS) Attacks Methodology and Security Measures

Eman Eyadat [1], Mohammad Eyadat [2], Abedalrahman Alfaqih [1]

[1] Information Systems Department, Irbid National University, Irbid, Jordan

[2]Information Systems Department, California State University, Dominguez Hills, Carson, 90747, USA

*Corresponding author: Mohammad Eyadat, CSUDH, Information System Department, 1000 E. Victoria Street, CA 90747& meyadat@csudh.edu

ABSTRACT: This paper proposes a concrete severity classification framework and an evaluation lens for DDoS defenses (not a descriptive survey) and contributes two specific advancements. First, it introduces a quartile-based severity classification framework for Distributed Denial of Service (DDoS) attacks that extends beyond conventional binary detection. The framework classifies observed traffic into four categories (Q1–Q4) using thresholds derived from packet length, packet rate, and estimated bandwidth consumption. This multi-dimensional approach provides a clearer picture of attack intensity, enabling proportional defensive responses. Second, the paper provides a comparative evaluation of mitigation strategies deployed at different levels of the network, including victim side, source side, core router based, and distributed mechanisms. Each is assessed against a consistent set of technical metrics, highlighting strengths, limitations, and tradeoffs that are essential for operational decision making. Together, these contributions move the work beyond description into a methodological and evaluative framework. Future research directions include adaptive threshold tuning in real time environments, integration of the classification scheme into programmable network infrastructures, and automated mapping of severity levels to specific mitigation playbooks in cloud and edge computing contexts.

KEYWORDS: DDoS, Cybersecurity, Countermeasures, Protection Techniques, Mitigation Strategies

1. Introduction

The cybersecurity landscape is continuously evolving, with DDoS attacks emerging as a significant threat to online services and data security [1]. With the potential to disrupt network operations, inflict financial losses, and compromise data integrity, DDoS attacks necessitate a comprehensive analysis of their methodologies, defensive strategies, and mitigation techniques [2, 3]. This research aims to contribute to the collective knowledge of cybersecurity by offering fresh insights and innovative solutions to enhance cyber resilience against DDoS attacks.

The study begins with an examination of DDoS attack vectors, including TCP SYN flood attacks, UDP flood attacks, and other prevalent methods. By meticulously analyzing and categorizing these attacks based on severity levels, the research unveils the intricate mechanisms employed by malicious actors to disrupt network operations [4, 5]. This analysis provides a solid foundation for understanding the complexities of DDoS attacks and their potential impact on digital infrastructure.

In addition to exploring attack methodologies, the research delves into defensive mechanisms such as IP traceback techniques, packet filtering strategies, and distributed defense systems deployed across multiple Autonomous Systems (AS). By evaluating the effectiveness of perimeter-based defenses, controller-agent models, and distributed change point detection, the study underscores the importance of secure information exchange and robustness in safeguarding against DDoS threats [6, 7].

The research also emphasizes the significance of proactive defense measures, highlighting the importance of distributed defense systems as the most effective strategy. By combining elements from victim, source, and core router-based defenses, these systems offer a comprehensive approach to detecting and mitigating DDoS attacks. A comparative analysis of defense

mechanisms based on deployment locations and performance metrics further emphasizes the necessity of strategic placement of defense components.

To provide a holistic understanding of DDoS attacks and their countermeasures, the study also examines attack motivations, evolutionary trends, protection techniques, and existing research limitations. By synthesizing findings from various research papers, the research in this paper aims to empower organizations with the knowledge and tools needed to fortify their defenses and mitigate the impact of DDoS attacks on online services and data security.

The novelty of this study lies in its combination of classification and evaluation. Unlike existing surveys that remain descriptive, our work advances the field by introducing a quartile-based severity classification model that provides a granular measurement of attack intensity. This classification is not arbitrary; it is grounded in empirical thresholds derived from experimental packet captures. By quantifying attack levels in four tiers, we provide actionable information for defenders to scale mitigation strategies according to the severity of the threat. In parallel, we conduct a structured evaluation of defensive mechanisms across four network layers—victim, source, core, and distributed. By applying a uniform set of criteria, we create a comparative framework that allows practitioners to judge which defenses are most effective in different deployment scenarios. These contributions ensure that the paper is not merely a review, but a methodologically driven and practically relevant addition to the literature.

2. Literature Review

In their paper, by authors [8] discuss DDoS attacks, their analysis, and prevention strategies, providing insights into contemporary challenges and defense mechanisms. The paper presented by authors [9], displays TRACK, a novel approach for defending against DDoS attacks, offering a detailed technical analysis and evaluation of its efficacy. In [10], the authors collaborative detection of DDoS attacks over multiple network domains is explored in this paper, emphasizing the importance of cooperation among networks to combat such attacks. The paper authored by authors [11] introduces a perimeter-based defense mechanism against high bandwidth DDoS attacks, accentuating its effectiveness in protecting network infrastructure. The research paper [12] classifies DDoS attacks and defense mechanisms, providing a state-of-the-art review and classification framework for researchers and practitioners.

The authors of the research paper [13], investigate current defense schemes against Distributed Denial of Service (DDoS) attacks, providing critical insights and evaluations of existing strategies. Researchers in paper [14], a surveys defense, detection, and traceback mechanisms against DoS and DDoS attacks, providing a comprehensive overview of existing strategies. In [15], the authors present a real-time DDoS attack detection and prevention system based on per-IP traffic behavioral analysis, offering insights into proactive defense strategies.

In [16], the authors classify Internet security attacks and discuss their implications, offering a comprehensive overview of attack patterns and defense strategies. Network protection against DDoS attacks is discussed by researchers [17, 18], while offering insights into defense strategies and their implementations. In [19], the authors provide a comprehensive review of network security threats and mitigation strategies, contributing to the body of knowledge in cybersecurity. In [20], the authors explore packet filtering approaches for detecting network attacks, offering insights into proactive defense strategies.

3. Methodology

In this research article, we delve into the multifaceted landscape of DDoS attack methodologies. We recognize the vast array of DDoS attack methods and the myriad tools and techniques employed to execute these attacks. Within the confines of this study, we focus on a specific DDoS attack method, dissecting its implementation process in detail.

Our methodology revolves around a comprehensive exploration of the selected DDoS attack method. We elucidate the intricacies of how this method is executed, shedding light on the tools and tactics that malicious actors may employ. Furthermore, we investigate mechanisms for early detection and alerting, allowing organizations to identify and respond swiftly when faced with similar attacks.

Crucially, our research extends beyond understanding the attack; we emphasize proactive defense measures. We elucidate strategies to thwart, mitigate, and limit the impact of DDoS attacks of this nature. By synthesizing these insights, we aim to contribute to the collective knowledge of cybersecurity, enhancing the ability of organizations to fortify their defenses against the ever-evolving threat landscape of DDoS attacks.

The attacker employs various methods to inundate the targeted web server with malicious packets. In this particular instance, the user utilized the Low Orbit Ion Cannon (LOIC) Denial-of-Service (DoS) attack tool to execute pattern-based attacks [21]. This section elucidates the approaches employed during the current research. The methodology comprises two primary phases: data collection and the identification and analysis of attacker characteristics. By discerning the patterns of attack behavior, two nodes are employed in this process. One

node acts as an attacker machine, while another serves as the victim, equipped with a tool designed to capture all incoming network traffic. The manifestation of anomalous and malevolent activities leads to a degradation in network performance, impeding users' access to online services. This methodology captures the ongoing packets by utilizing packet capture techniques.

3.1. Packet Sniffing

3.1.1. Data Collection

The software tool provides a range of functionalities, including filters and color- coding, facilitating the examination of network traffic and the scrutiny of individual packets. Additionally, it simplifies network characterization by enabling the assessment of attributes such as load, frequency, and latency between specific network nodes. Among the most prevalent packet types on the network, TCP, UDP, and ICMP stand out.

In the data collection phase, all packets generated by the attacker, including UDP and TCP traffic floods, are captured using a packet sniffer. By examining the captured packets, which encompass UDP, HTTP, and TCP, we discern the patterns indicative of attack behavior. Quartiles are employed to gauge the severity of the attacks, with the following categorizations:

- Q1: Low-level attacks
- Q2: Moderate-level attacks
- Q3: Upper half attacks
- Q4: High-level attacks

To enhance precision and address reviewer feedback, we explicitly define the thresholds used in the quartile classification. The classification leverages three measurable parameters: average packet length (L) in bits, average packet rate (R) in packets per second, and estimated bandwidth (B) in megabits per second, computed as B = (L × R) ÷ 10^6. Severity levels are determined as follows:

Q1 (Low level): L < 85,000 bits, R < 100 packets per second, B < 8.5 Mbps. These attacks generally cause minimal disruption and can often be absorbed through local queue management and traffic policing.

Q2 (Moderate level): 85,000 ≤ L < 94,650 bits, 100 ≤ R < 250 packets per second, 8.5 ≤ B < 24 Mbps. These attacks may begin to degrade performance of latency sensitive services and usually require targeted packet filtering or temporary access control list (ACL) updates.

Q3 (Upper half): 94,650 ≤ L < 104,300 bits, 250 ≤ R < 500 packets per second, 24 ≤ B < 52 Mbps. These attacks generate significant service degradation. Mitigation strategies include coordinated pushback mechanisms and upstream filtering support from Internet Service Providers.

Q4 (High level): L ≥ 104,300 bits, R ≥ 500 packets per second, B ≥ 52 Mbps. These represent severe floods capable of overwhelming resources across multiple layers. Countermeasures must involve distributed defenses, collaborative filtering, and in extreme cases, network wide rerouting.

An interval is classified according to the highest triggered quartile among the three parameters. For instance, if packet length falls into Q2 but packet rate falls into Q3, the final severity label is Q3. This “maximum rule” avoids underestimating the seriousness of an attack when one parameter surges disproportionately. The thresholds were derived empirically from observed packet captures, but they also align with operational thresholds used by ISPs in traffic engineering. This combination of packet length, rate, and bandwidth provides a multidimensional perspective on severity, which improves accuracy compared to relying on a single parameter.

Measurement details. We compute averages over non-overlapping 60-second windows. Let L be mean packet length in bits, R mean packet rate in packets per second, and B estimated bandwidth in megabits per second given by B = (L × R) ÷ 10^6. Unless stated otherwise, all quartile labels use the maximum rule over L, R, and B for each 60-second interval.

3.1.2. Attack Methodology

The attacker employs various tactics to inundate the targeted web server with malevolent packets. The identification of attack signatures assumes significance in facilitating the detection of DoS attacks. This method entails the utilization of two distinct machines, one of which houses an attacker simulator physically. The attacker simulator can execute various types of attacks on the target machine. One machine is designated as the attacker, responsible for flooding the server machine with malicious packets. Meanwhile, the server machine is equipped with monitoring and capturing tools to analyze network traffic in real-time. For a more detailed illustration, please refer to the standard DoS attack architecture depicted in Figure 1 below.

3.1.3. TCP SYN Flood Packet Attacks

Among the most detrimental forms of DoS attacks, the TCP SYN flood is particularly noteworthy. In typical communication between clients and servers, a three-way handshake, involving "SYN-SYN-ACK and ACK" packets, is performed to establish connectivity. However, in the case of these attacks, malicious actors attempt to masquerade as trusted clients, leading servers to await acknowledgment indefinitely until TCP timeout occurs. These attacks are engineered to exhaust server resources, including firewalls and communication tools. Figure 2

illustrates the captured and analyzed TCP traffic using Wireshark.

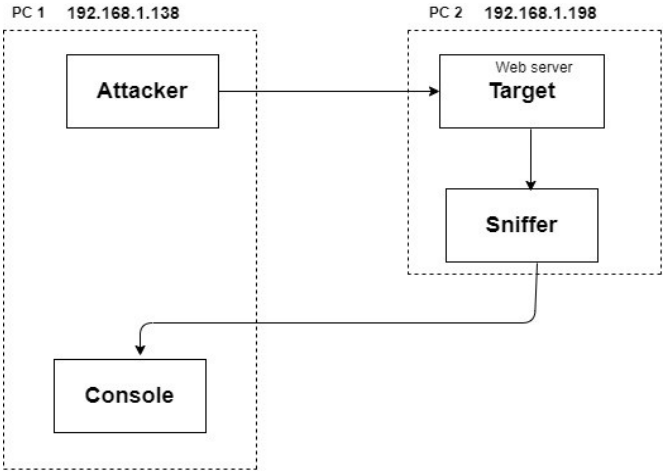

Figure 1: Standard DoS Attack Architecture

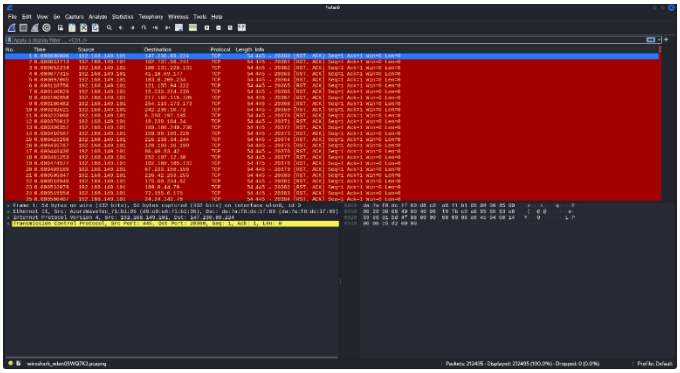

Figure 2: Examining TCP Flood Attack with Wireshark

In the context of TCP flooding during DDoS attacks, the packets are directed towards the target server. To gain insights into the characteristics of these malicious packets, you can conveniently identify them by accessing the "Statistics" menu and then selecting "Flow Graph." This action enables you to visualize the packet sequence graphically. Through this tool, you have the capability to trace and comprehend the TCP connections and their behavior, as exemplified in Figure 3.

As depicted in Figure 3, the time axis is measured in seconds (s), and the source's IP address is identified as 192.168.149.101 utilizing a port number that ranges randomly between 20361 and 20368 (port range). On the other hand, the destination's IP address is specified as 147.230.89.224, . In this scenario, the source initiates the transmission of attack packets, characterized by their variable port numbers. The client IP, denoted as 192.168.149.101 initiates a TCP connection with the server IP, 147.230.89.224, commonly referred to as the server. Wireshark traces empower network engineers to identify unusual downloads, often marked by indicators such as "RST ACK" and "TCP DUP ACK." These anomalies are typically associated with abnormal packet behavior, and malevolent actors may employ techniques like "RST ACK" to orchestrate attacks resembling TCP ACK attacks.

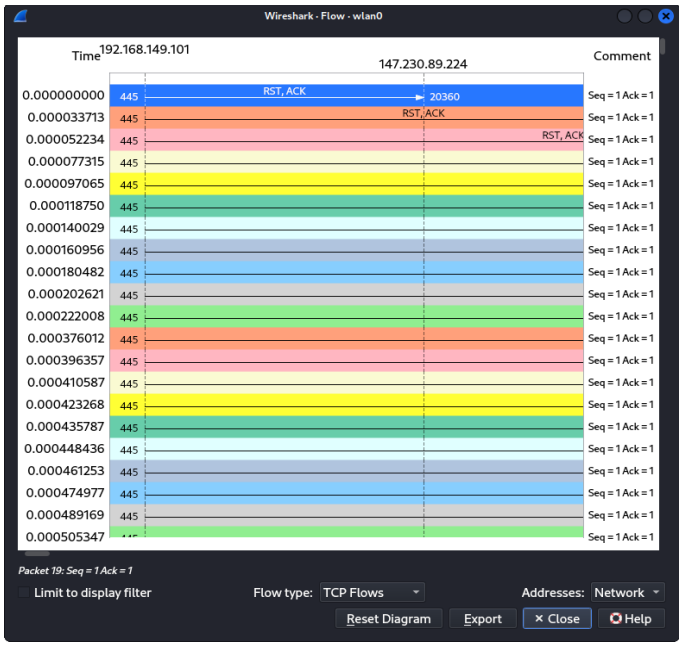

Figure 3: TCP Flow Graph Overview

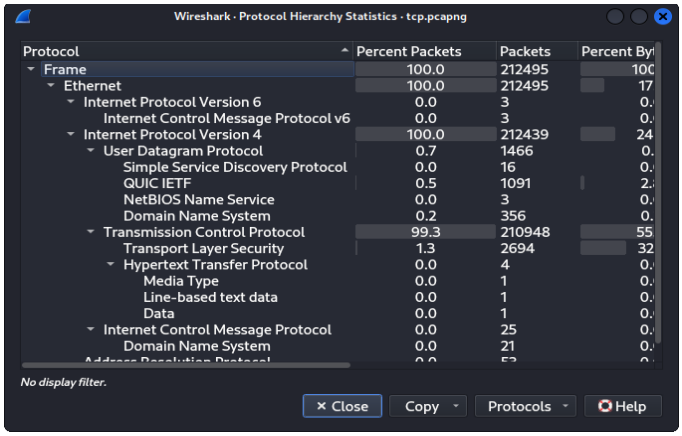

Figure 4: protocol hierarchy statistics overview for TCP flood attack

This figure shows the percentage of TCP incoming packets and it is shown as 99.3 % of incoming packets to the network.

3.1.4. *User Datagram Protocol (UDP) Flood Attack*

The second prevalent DDoS attack method centers on UDP flooding, exploiting vulnerabilities within UDP services. This method involves inundating ports on the server with malicious packets to ascertain which ports are susceptible to exploitation. To initiate this analysis, users can apply a filter by typing "UDP" in the designated filter zone, or opt for other protocols as required, and the results will be displayed on the user interface [22].

A UDP flood attack is characterized by the massive influx of spoofed UDP packets directed at various server ports from a single source. In response, the server, along with ICMP, issues "destination unreachable" notifications, signifying that it is overwhelmed by the volume of incoming requests. The resulting network traffic can be captured and further analyzed using Wireshark, as exemplified in Figure 5.

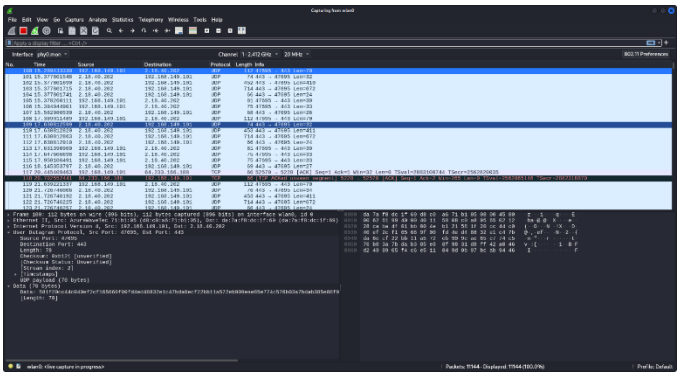

Figure 5: Examination of UDP Flood Attack

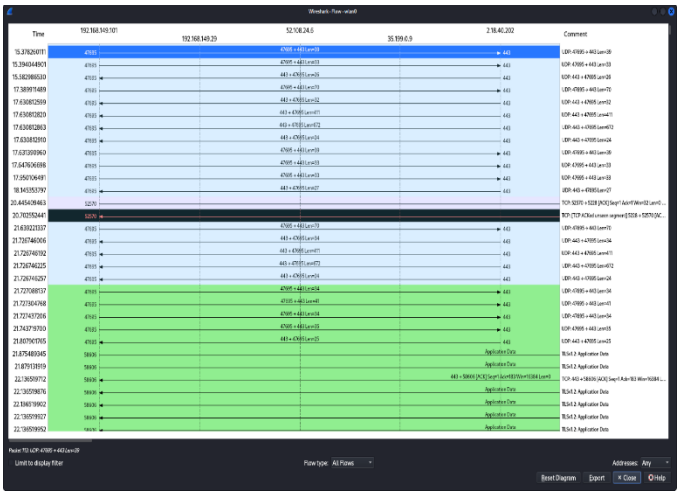

Figure 6: UDP flow graph overview

As depicted in Figure 6, the time axis is measured in seconds (s), and the source's IP address is identified as 192.168.149.101. The source continuously transmits a large volume of User Datagram Protocol (UDP) packets towards the destination IP address, 192.168.149.29. Unlike TCP connections, UDP doesn't establish a handshake and sends packets independently.

In this scenario, the source floods the destination with UDP packets, overwhelming the target device's resources and potentially causing a denial-of-service (DoS) attack. Wireshark traces might reveal a surge in UDP packets originating from the source IP (192.168.149.101) directed towards the destination IP (192.168.149.29). While Wireshark might not capture the exact contents of UDP packets, the abnormal increase in traffic can be indicative of a UDP flood attack.

The figure 7 shows the percentage of UDP flow attack incoming packets as 50% of the incoming packets through the network.

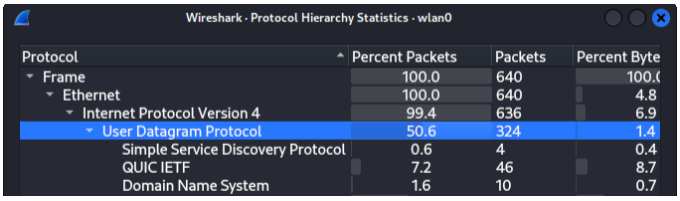

Figure 7: protocol hierarchy statistics

3.2. *Packet Analysis and Attack Duration dentification*

Upon capturing the requisite packets spanning from day one to day three, Authors harnessed Microsoft Excel to discern the patterns within attack behavior enabled them to methodically process and analyze the packets collected at various time intervals, as initially captured by Wireshark.

Microsoft Excel proved instrumental in providing a comprehensive understanding of the packets, offering insights into the total packet lengths. The differentiation in the sizes of the attacks, whether characterized as small or substantial, formed a pivotal aspect of the impact assessment.

All data originating from the attacker underwent meticulous processing via Microsoft Excel. This entailed the calculation of averages across the dataset, facilitating the categorization of attacks into distinct levels, encompassing low, medium, and high, as elucidated in Figure 8.

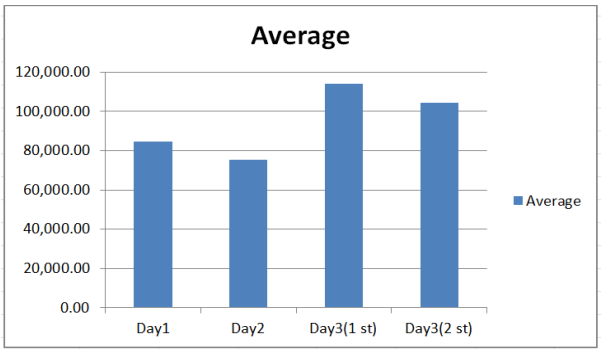

Figure 8: Average data collected in three days.

3.3. *Analysis of Flood Packet Length and Attack Levels*

In figure 8, the average length of captured flood packets is depicted, and these lengths vary depending on the attackers' traffic loads. By meticulously scrutinizing these average lengths and applying quartile calculations, users gain a valuable perspective on the severity of the attacks, as determined by the following formula (Equation):

$$QN = (Dmax - Dmin) \quad (1)$$

where:

- N = 1, 2, 3
- Dmax = Maximum average length (113,887.93 bits)
- Dmin = Minimum average length (75,407.50 bits)

Consequently, the range can be calculated as:

Range = 113,890 - 75,407 = 38,480 bit.

The quartile values are as follows:

To determine the quartile values, the range is divided by 4 (since there are four quartiles) to establish the

interval size for each quartile. In this case, 38,480 bits divided by 4 equals 9,620.75.

- Q1 = 75,407 to (75,407 + (1 x 9620)) = 75,407 to 85,027
- Q2 = 85,027 to (75,407+ (1 x 9620)) = 85,027 to 94,647
- Q3 = 94,647 to (75,407+ (1 x 9620)) = 94,647 to 104,267
- Q4 = 104,267 to (75,407+(1 x 9620)) = 104,267 to 113,887

Table 1 below provides information on the time intervals during which flood packets were collected, including periods (in seconds), packet lengths (in seconds), quartile ranges (in seconds), and corresponding attack levels. With reference to quartile identification and the calculated range (QN), users can easily discern the attack levels, categorizing them as low, medium, or high. In each of these attack levels, the primary objective is to disrupt legitimate user access to essential services.

Table 1: Summarizing Level of Attacks

NO	TIME	SEC	LENGHT	QUARTILE	ATTACK LEVEL
1	04:22	37	85,027	Q2	MEDIUM ATTACK
2	12:09	34	75,407	Q1	LOW ATTACK
3	18:11	52	113,887	Q4	HIGH ATTACK
4	09:44	44	104,267	Q3	HIGH ATTACK

The table above illustrates the level of attacks. The intruders can attack a system using small packets with many loads; these attackers cause the targeted system to consume too much network bandwidth resources and make services unavailable to legitimate traffic. By analyzing the attack time and length of all data collected in three days, users can identify the level of attacks from Q1, Q2, and Q3, Q4 scaling systems. The average of attacks Q1 seems to be a low attack, this means the impact is not quickly put down the server, Q2 is medium attacks where the volume of attack is upper to Q1; finally, Q3, Q4 the higher than others level attacker sent a huge of fake packets to the victim server to make source unavailable to legitimate users.

4. Results and Discussion

In this section, we present the findings of our analysis, shedding light on the impact and categorization of DDoS attacks based on packet lengths and quartile calculations.

4.1. Analysis of Packet Lengths

Figure 8 displays the average length of flood packets collected during various attack instances, each contingent upon the traffic loads initiated by attackers. These measurements provide crucial insights into the severity of the attacks. To determine the attack levels, we applied quartile calculations using formula 1.

Our results reveal a significant disparity in average packet lengths, ranging from a minimum of 75,407 bits to a maximum of 113,887 bits. The calculated range, denoting the variation in packet lengths, amounted to 38,480 bits.

4.2. Quartile Analysis

The quartile values, Q1, Q2, Q3, and Q4, further elucidate the distribution of packet lengths and help in characterizing the attacks. These quartile ranges are as follows:

- Q1: 75,407 to 85,027 Bits
- Q2: 85,027 to 94,647 Bits
- Q3: 94,647 to 104,267 Bits
- Q4: 104,267 to 113,887 Bits

The quartile classification framework adds analytical depth beyond a binary attack/no attack model. Binary systems merely indicate whether an anomaly exists, but they fail to convey its magnitude or operational significance. Our quartile approach quantifies intensity, thereby providing defenders with actionable intelligence. For example, a Q1 event may be addressed through local resource adjustments with negligible impact on legitimate users, whereas a Q4 event demands immediate, distributed intervention to prevent large scale service outages. By stratifying attacks into four levels, defenders can allocate resources more efficiently, prioritize responses, and reduce collateral damage from overly aggressive mitigation. Furthermore, this classification can support adaptive automation: security systems can be programmed to escalate defensive measures as the quartile level rises. In this way, quartile classification is not only a descriptive tool but also a foundation for dynamic, context aware defense strategies.

In our traces, intervals labeled Q3 and Q4 coincided with service availability drops and triggered upstream filtering, whereas Q1 events were handled locally without collateral blocking, underscoring the operational value of the stratified scheme.

4.3. Preventing DDoS attack and/or applying defensive techniques to limit them

4.3.1. IP Traceback Mechanisms: An In-Depth Analysis

IP traceback mechanisms are crucial in identifying the true source of IP packets, which is essential for tracking and mitigating various cyberattacks, including Distributed Denial of Service (DDoS) attacks. This process, called traceback, involves tracing malicious packets back

to their origins to uncover the identity of the attacker. IP traceback mechanisms can generally be categorized into two main types: packet marking and link testing.

4.3.2. *Packet Marking Mechanisms*

Packet marking mechanisms rely on routers to mark packets that are heading towards the victim server. This marking allows the path followed by packets to be easily identified, aiding in traceback. However, implementing packet marking mechanisms can be challenging due to the stateless nature of internet routing. Unique identifiers are needed for each packet, and routers may fail to assign these identifiers to some packets, leading to false positives.

4.3.3. *Link Testing Mechanisms*

Link testing mechanisms involve testing upstream links starting from the one closest to the victim and repeating the process recursively until reaching the upstream router. This approach helps identify the path of the attack traffic. However, IP traceback mechanisms, whether using packet marking or link testing, come with several challenges, including management, computational, and network overhead. Additionally, widespread implementation of these mechanisms requires the involvement of numerous routers.

It's important to note that source accountability in the TCP/IP protocol is limited, making IP traceback a complex task. The accuracy of the traceback process is also questionable, as attackers can create mechanisms that appear genuine. This has led some researchers to recommend the use of ICMP traceback.

In ICMP traceback, packets with reduced probability of being malicious are sampled by each router. An ICMP traceback message is sent to the destination, and a chain of traceback messages is constructed. This chain aids in determining the exact source of the traffic. However, validating traceback packets in the ICMP mechanism can be challenging, and it's unlikely that a certificate-based scheme can be universally adopted by all routers.

4.3.4. *Management Information Base (MIB)*

The management information base captures critical data, including packet information and historical routing statistics. This data can be used to map TCP, ICMP, and UDP packets, generating patterns. It helps in identifying network abnormalities and provides a framework for adjusting network settings to counter unwanted traffic effectively. While this method holds promise for controlling traffic loads, further evaluation in a real network environment is needed.

4.3.5. *Packet Filtering and Filtering Mechanisms*

Packet filtering mechanisms are essential for blocking undesirable traffic. They operate by marking legitimate packets and then using filters to block unwanted traffic. Common packet filtering mechanisms include history-based filtering and hop-count filtering.

History-Based Filtering: This mechanism maintains records of frequently visited IP addresses. When a DDoS attack occurs, it connects to the IP addresses in the list, but it requires an offline database, which can be costly.

Hop-Count Filtering: Hop-count filtering stores IP addresses and their corresponding hops from the destination. However, it has a limited range, making it ineffective for identifying illegitimate source IP addresses with similar hop-count values.

4.3.6. *Packet Dropping Based on Congestion*

This defense mechanism drops suspicious packets during network congestion to manage overload. The Packet Score mechanism assigns a score to each packet, allowing prioritization based on the level of overload and score distribution of incoming packets. However, it may not be effective against sophisticated attacks.

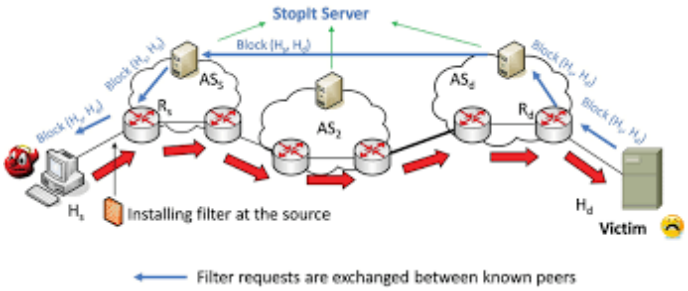

Figure 9: Network-Based Defense Mechanisms [12]

4.3.7. *Network-Based Defense Mechanisms*

Network-based defense mechanisms deploy components on network routers to detect, traceback, and respond to attacks through filtering and rate limiting.

In figure 9 classifications of network-based mechanisms include perimeter-based defense mechanisms, the controller-agent model, and Distributed Change Point Detection.

- **Perimeter-Based Defense Mechanisms:** Typically used by internet service providers (ISPs), this mechanism detects and identifies attack sources and responds by rate-limiting traffic. It offers local deploy ability without straining ISP core routers.
- **Controller-Agent Model:** This model relies on edge routers and controllers to mark and filter attack traffic. It uses third-party components for attack detection and characterization.
- **Distributed Change Point Detection:** This method monitors propagation patterns and detects unexpected changes on the network. It is deployed over multiple Autonomous System (AS) domains

and is effective in quickly detecting DDoS flooding attacks.

- **Distributed Defense Mechanisms**: Distributed defense mechanisms, in contrast to centralized mechanisms, are deployed at multiple points across the network. They can adopt various combinations, such as detection at the victim's side with distributed response or a combination of both.

In conclusion, IP traceback mechanisms play a vital role in identifying and mitigating cyberattacks like DDoS attacks. Each mechanism has its advantages and limitations, and their effectiveness depends on factors like deployment location and attack response methods. Evaluating these mechanisms based on various criteria is essential for choosing the most suitable defense strategy for specific network configurations and requirements.

Table 2 highlights the comparisons between different defense methods

Table 2: Deployment-Based Comparisons Between Different DDoS Defense Methods

Deployment Scheme	Scheme Name	Attack Detection	Attack Response
Victim-Based Defense	NetBouncer Preferential Filtering	Legitimacy tests IP Traceback Scheme	Packet filtering based on legitimate lists Filter packets with infected edges.
Source-Based Defense	Ingress Filtering D-Ward	IP address validity tests Detect Abnormality	Rule-based filtering Rate limiting of outgoing traffic
Core Router-Based Defense	Collaborative Agent Model Collaborative Agent Model Perimeter-based defense	Change Aggregation tree Signature Matching Traffic Aggregate	Packet Filtering Packet Filtering Rate limit filters
Distributed Defense	ACC and Pushback Stoplt Defcom	Congestion detection Passport Traffic Tree discovery	Rate Limiting Packet Filtering Distributed rate limiting

The effectiveness of DDoS defense methods hinges on their deployment strategies, which determine how they detect and respond to attacks. In this section, we evaluate various defense mechanisms based on their deployment schemes. These mechanisms encompass victim-based defense, source-based defense, core router-based defense, and distributed defense. Each approach has its strengths and weaknesses, which we assess using six key metrics: effectiveness, vulnerability, accuracy, coverage, robustness, and complexity.

Victim-Based Defense:

- **Attack Detection:** NetBouncer conducts legitimacy tests, while packet filtering relies on predefined legitimate lists.
- **Attack Response:** Victim-based defenses employ preferential filtering and IP traceback schemes.

Source-Based Defense:

- **Attack Detection:** Ingress filtering validates IP addresses, and rule-based filtering detects abnormalities.
- **Attack Response:** Rate limiting of outgoing traffic is a key response mechanism for source-based defense.

Core Router-Based Defense:

- **Attack Detection:** Collaborative Agent Model and Change Aggregation tree are used for attack detection, alongside packet filtering.
- **Attack Response:** Signature matching and packet filtering play crucial roles in core router-based defenses.

Distributed Defense:

- **Attack Detection:** Adaptive Congestion Control (ACC) and pushback mechanisms detect congestion, while distributed rate limiting is a common detection method.
- **Attack Response:** Distributed defense systems use various methods, such as Traffic Tree discovery and distributed rate limiting.

Evaluation of Deployment Schemes:

- **Effectiveness:** Distributed defense systems are the most effective as they combine elements from multiple locations.
- **Vulnerability:** Victim-based defenses are vulnerable to attacks, while distributed defenses are less so.
- **Accuracy:** Victim-based defenses offer high accuracy due to their proximity to the target.
- **Coverage:** Distributed defense systems provide extensive coverage due to their distributed nature.

- **Robustness:** Distributed defense systems are robust, provided secure information exchange among components.
- **Complexity:** Distributed defense can be complex due to distributed components and information exchange.

In summary, while all deployment schemes have their merits and drawbacks, distributed defense systems stand out as the most robust and effective strategy. They combine elements from victim, source, and core router-based defenses to achieve comprehensive protection. However, ensuring secure information exchange among distributed components is essential for maintaining their robustness.

Table 3-a: Evaluation of DDoS Mechanisms Against the Six Metrics

Deployment Scheme	Coverage	Implementation	Deployment
Source-Based Defense	It would have an effective coverage as long as it is deployed globally.	Global deployment is a condition required for its implementation to bring all desired effects. Global deployment is impractical because the internet has no central location.	Centralized. Deployment has its limitations because in a distributed attack, the source is only responsible for a fraction of the attack.
Router-Based Mechanism	Excellent Coverage: This is because a bulk of the network passes through them.	Easy to implement: Deployment at middle only requires few components and gives excellent defensive coverage.	Centralized. Few components are required for deployment.
Victim-Based Defense	The defense mechanism does little to contain attack at the victim's end.	Most defense mechanism are designed at the victim's end.	Centralized. It requires wide deployment to be effective.
Distributed-Based Defense	Has a relatively higher coverage than others.	Can be complex to configure because most defense components need to be scattered over the internet.	Distributed. Deployed over multiple locations such as source and intermediate networks.

Table 3-b: Evaluation of DDoS Mechanisms Against the Six Metrics

Deployment Scheme	Detection Accuracy	Response Mechanism	Robustness
Source-Based Defense	The source is the best place to differentiate between good and bad packets. It uses IP Address validity tests and can be effective in detecting abnormalities.	Uses rate-limiting method. Rate limiting is effective because a specific limit can be placed on a traffic that is allowed through the Network Interface.	Very robust because they can detect attacks at the early stages and eliminate an attack before it occurs. However, this depends on it being deployed across maximum source networks.
Router-Based Mechanism	Core routers are usually busy and cannot perform serious packet analysis.	Only parameter-based defense uses rate limiting. The other schemes under the Router-Based Mechanism uses packet filtering. Packet	Ideally good effective detection and filtration but robustness depends on an expansive coverage in detecting and capturing

		filtering can be an ineffective response mechanism.	good number of attacks.
Victim-Based Defense	There is higher accuracy of detection at victim's end based on "bad lists."	Uses packet filtering based on legitimate lists.	Can be very effective but depends on wide deployment.
Distributed-Based Defense	Has a relatively accurate detection since resources from several levels are used.	Various schemes adopt unique response mechanisms but overall because of distributed architecture, its response mechanism is relatively good.	Very robust against DDoS attacks. Mitigates against the short-comings of the other defense mechanisms.

The comparative analysis began by categorizing various defense mechanisms based on their deployment locations. Four primary classifications were considered: source- based, core-router-based, victim-based, and distributed systems. A selection of defense systems falling under these categories was assessed using six performance metrics: coverage, implementation, deployment, detection accuracy, response mechanisms, and robustness as shown in tables 3-1 and 3-b.

The analysis highlighted that there is no single deployment location that can offer complete protection against DDoS attacks. The most effective defense mechanism involves the use of distributed systems, ensuring that defense components are strategically placed across various locations. In general, an effective DDoS defense strategy should involve multiple nodes responsible for detecting and mitigating attacks.

At the end of the victim, detection accuracy is high, but there is limited time for response when an attack reaches this location. Stopping an attack at its source is an ideal approach, but achieving high detection accuracy is challenging since distinguishing between legitimate and malicious traffic can be complex. The core-router-based defense system also has limitations, primarily due to resource constraints such as CPU cycles and limited traffic profiling capabilities.

5. Conclusion and Implications

This Study has provided valuable insights into the categorization of DDoS attacks based on packet lengths and quartile calculations. By examining the average lengths of flood packets and applying quartile analysis, we have identified low, medium, and high-level attacks. These distinctions enable us to gauge the severity of DDoS attacks and their potential impact on network resources.

Understanding the levels of DDoS attacks is paramount for implementing effective mitigation strategies and safeguarding essential online services. In all instances, the primary objective of DDoS attacks is to disrupt legitimate user access, emphasizing the critical need for robust cybersecurity measures.

In this research journey into the evolving threat landscape of Distributed Denial-of- Service (DDoS) attacks and the corresponding security measures, we have ventured deep into the intricate world of cyber warfare. Through meticulous examination, we have gained valuable insights into the motivations driving these malicious assaults, scrutinized the diverse attack vectors at play, and assessed the current state of protective measures.

Our team's study has illuminated the limitations we face in the realm of DDoS attack research, from the challenge of accessing real attack data to the ever-evolving nature of attack techniques. We've also navigated resource constraints, ethical considerations, and legal boundaries, underscoring the complexity of conducting research in this critical area of cybersecurity.

In our exploration of DDoS attack methodologies, we've delved into the intricacies of TCP SYN flood attacks and UDP flood attacks. Through rigorous analysis and packet length assessments, we've categorized these attacks into low, medium, and high levels, offering a nuanced understanding of their severity.

Furthermore, our examination of IP traceback mechanisms has shed light on the critical role of identifying the true source of IP packets in combating DDoS attacks. We've explored packet marking and link testing mechanisms, recognizing the challenges and complexities involved in tracing malicious packets back to their origins.

The discussion has also covered management information bases, packet filtering mechanisms, and

packet dropping strategies during network congestion, providing a comprehensive overview of defensive techniques against DDoS attacks.

In the context of network-based defense mechanisms, we've categorized them into perimeter-based mechanisms, the controller-agent model, and Distributed Change Point Detection. Additionally, we've delved into distributed defense mechanisms, highlighting the importance of evaluating these strategies based on various criteria to select the most suitable defense approach for specific network configurations and requirements.

In conclusion, this team's research underscores the critical importance of understanding the evolving threat landscape of DDoS attacks and implementing effective security measures. As the digital realm continues to evolve, the battle against these cyber threats remains ongoing. By combining innovative research, proactive defense strategies, and collaborative efforts, we can fortify our defenses and protect the integrity and availability of online services. It is our collective responsibility to remain vigilant and adaptive in the face of this persistent and ever-evolving cybersecurity challenge.

Beyond descriptive surveys, the novelty of this study lies in proposing a quartile-based severity classification framework grounded in empirical thresholds and a comparative evaluation model for defense strategies. This dual contribution ensures the work moves from description to methodological and practical advancement.

6. Future Research Directions

Future studies should also validate the practical value of quartile-based classification by integrating it into automated detection systems and comparing its efficiency against binary approaches in real-world network environments. While there was no type of funding supporting this research and none of the authors have any competing interests in the manuscript this study has offered valuable insights, future research endeavors can explore more advanced methodologies for real-time DDoS attack detection and mitigation. Also, the development of adaptive defenses to counter evolving attack techniques remains an essential area for exploration in cybersecurity.

References

[1] K. Ahmad, S. Verma, N. Kumar, and J. Shekhar, "Classification of Internet security attacks," in *Proceedings of the 5th National Conference INDIACom-2011, Bharti Vidyapeeth's Institute of Computer Applications and Management, New Delhi*, 2011, ISBN: 978-93-80544-00-7.

[2] R. Yaegashi, D. Hisano, and Y. Nakayama, "Light-weight DDoS mitigation at network edge with limited resources," in *IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1–6, IEEE, 2021, doi: 10.1109/CCNC49033.2021.9415553.

[3] Q. Yan and F. R. Yu, "Distributed denial of service attacks in software-defined networking with cloud computing," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 52–59, 2015, doi: 10.1109/mcom.2015.7081075.

[4] N. S. Mangrulkar, A. R. B. Patil, and A. S. Pande, "Network attacks and their detection mechanisms: A review," *International Journal of Computer Applications*, vol. 90, no. 9, pp. 36-39, 2014, doi: 10.5120/15606-3154.

[5] Y. Wang and R. Sun, "An IP-traceback-based packet filtering scheme for eliminating DDoS attacks," *Journal of Networks*, vol. 9, no. 4, pp. 874–880, 2014, doi: 10.4304/jnw.9.4.874-881.

[6] P. Dzurenda, Z. Martinasek, and L. Malina, "Network protection against DDoS attacks," *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*, vol. 4, no. 1, pp. 8–14, 2015.

[7] S. Pareek, A. Gautam, and R. Dey, "Different type network security threats and solutions: a review," *International Journal of Computer Science*, vol. 5, no. 4, 2017, doi: 10.5430/ijcs.v5n4p46.

[8] G. Dayanandam, T. V. Rao, D. B. Babu, and S. N. Durga, "DDoS attacks—analysis and prevention," in *Innovations in Computer Science and Engineering: Proceedings of the Fifth ICICSE 2017, Springer Singapore*, pp. 1–10, 2019, doi: 10.1007/978-981-13-3347-4_1.

[9] P. D. Bojović, I. Bašičević, S. Ocovaj, and M. Popović, "A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method," *Computers & Electrical Engineering*, vol. 73, pp. 84–96, 2019. Doi: 10.1016/j.compeleceng.2018.11.004.

[10] D. Chasaki, Q. Wu, and T. Wolf, "Attacks on network infrastructure," in Proceedings of the 20th *International Conference on Computer Communications and Networks (ICCCN), IEEE*, pp. 1–8, 2011, doi:10.1109/ICCCN.2011.6005919.

[11] S. Chen and Q. Song, "Perimeter-based defense against high bandwidth DDoS attacks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 16, no. 6, pp. 526–537, 2005, doi: 10.1109/TPDS.2005.74.

[12] B. L. Dalmazo, J. A. Marques, L. R. Costa, M. S. Bonfim, R. N. Carvalho, A. S. da Silva, and W. Cordeiro, "A systematic review on distributed denial of service attack defense mechanisms in programmable networks," *International Journal of Network Management*, vol. 31, no. 6, e2163, 2021. doi:: 10.1002/nem.2163.

[13] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," *Computer Networks*, vol. 44, no. 5, pp. 643–666, 2004, doi: 10.1109/ISSPIT.2003.134109.

[14] M. Furdek, L. Wosinska, R. Goścień, K. Manousakis, M. Aibin, K. Walkowiak, and J. L. Marzo, "An overview of security challenges in communication networks," *in Proceedings of the 8th International Workshop on Resilient Networks Design and Modeling (RNDM), IEEE*, pp. 43–50, 2016, doi:10.1109/RNDM.2016.7608266.

[15] S. D. Kotey, E. T. Tchao, and J. D. Gadze, "On distributed denial of service current defense schemes," *Technologies*, vol. 7, no. 1, pp. 1–19, 2019, doi: 10.3390/technologies7010019.

[16] M. T. Manavi, "Defense mechanisms against distributed denial of service attacks: A survey," *Computers & Electrical Engineering*, vol. 72, pp. 26–38, 2018, doi: 10.1016/j.compeleceng.2018.09.001.

[17] A. Madhuri and A. R. Lakshmi, "Attack patterns for detecting and preventing DDoS and replay attacks," *International Journal of Engineering and Technology*, vol. 2, no. 9, pp. 4850–4859, 2010, doi: 10.13140/RG.2.1.1723.8085

[18] E. Y. Muharish, "MPacket filter approach to detect denial of service attacks," *Unpublished report or thesis*, 2016, https://scholarworks.lib.csusb.edu/etd/342.

[19] N. Srihari Rao, K. Chandra Sekharaiah, and A. Ananda Rao, "A survey of distributed denial-of-service (DDoS) defense techniques in ISP domains," in *Innovations in Computer Science and Engineering: Proceedings of the Fifth ICICSE 2017, Springer Singapore,*pp.221–230,2019, doi: 10.1109/ACCESS.2019.2922196.

[20] Y. Zhang, Q. Liu, and G. Zhao, "A real-time DDoS attack detection and prevention system based on per-IP traffic behavioral analysis," in *Proceedings of the 3rd International Conference on Computer Science and Information Technology (ICCSIT)*, vol. 2, pp. 163–167, IEEE, 2010, doi: 10.1109/ICCSIT.2010.5563549.

[21] Y. Chen, K. Hwang, and W. S. Ku, "Collaborative detection of DDoS attacks over multiple network domains," IEEE Transactions on Parallel and Distributed Systems, vol. 18, no. 12, pp. 1649–1662, 2007, doi: 10.1109/TPDS.2007.1111.

[22] R. Chen, J. M. Park, and R. Marchany, "TRACK: A novel approach for defending against distributed denial-of-service attacks," *Technical Report TR-ECE-06-02, Dept. of Electrical and Computer Engineering, Virginia Tech*, 2006, doi: 10.1007/978-3-642-17881-8_24.

JENRS

Received: 03 September 2025, Revised: 06 October 2025, Accepted: 14 October 2025, Online: 27 October, 2025

DOI: https://doi.org/10.55708/js0410003

Energy-Optimized Smart Transformers for Renewable-Rich Grids

Sunday Omini Oboma*, Edward Lambart

Department of School of Engineering and Science, Atlantic International University, Honolulu, HI 96813, USA

Emails: okaleobomkpe@gmail.com, edward@aiu.edu

*Corresponding author: Sunday Omini Oboma, okaleobomkpe@gmail.com

ABSTRACT: The accelerating and unrestrained use of energy globally raises serious concerns for the future of the planet, primarily due to the environmental devastation caused by fossil fuels. Achieving high energy efficiency in both fuel-driven and renewable energy systems is crucial for future energy optimization. Clean energy production is one of the most effective strategies to mitigate climate change effects. These challenges necessitate a significant shift towards sustainable energy models, specifically smart and renewable energy systems that do not emit greenhouse gases during generation. This paper proposes a novel framework for smart and renewable energy optimization through the design of smart transformers that maximize energy savings without generating harmful radiation. The optimization utilizes a hybrid approach combining Nonlinear Programming (NLP) and an Artificial Intelligence (AI) technique, the Genetic Algorithm (GA), applied to specific transformer design parameters. The validated results demonstrate significant efficiency gains and cost reduction, strengthening the paper's contribution to robust, sustainable energy infrastructure.

KEYWORDS: Renewable Energy, Clean Energy, Energy Efficiency, Smart Transformers, Transformer Design, Losses, Optimization, Genetic Algorithms, Artificial Intelligence (AI), Nonlinear Programming (NLP).

1. Introduction

This paper examines energy efficiency and renewable energy optimization as cornerstones for a sustainable future. In [1] and [2], the authors emphasize that as environmental degradation intensifies, marked by climate change, extreme weather, and biodiversity loss, the global community is aggressively driven to adopt clean energy solutions. These challenges demand a fundamental rethinking of energy models, requiring coordinated action across public administration, industry, and consumers by [3].

Recent projections indicate that global energy consumption will surge in the coming decades, primarily driven by rapid industrial expansion in emerging economies described by [3]. In response, renewable energy sources, including wind, solar, and hydro, are poised to play a central role. In [4] and [5], the authors highlighted that integrating these renewables not only enhances energy security but also directly addresses the forecasted doubling of energy demand by 2050. Consequently, optimizing energy conversion and minimizing waste—particularly within critical grid components—have emerged as critical priorities by [6].

A reduction in greenhouse gas emissions is directly achieved by accelerating the development and integration of renewable energy technologies, whose long-term objective is to supplant carbon-intensive energy dominating global markets by [7]. The central challenge lies in orchestrating an energy transition that efficiently manages consumption while promoting the extensive deployment of renewable sources. This is particularly relevant as innovative strategies incorporating Artificial Intelligence (AI), Machine Learning (ML), and advanced optimization methods are increasingly leveraged for complex grid management, power forecasting, and enhancing the resilience of components to fluctuating renewable loads by [6], [8] and [9].

Fossil fuels, the traditional backbone of large-scale energy production, are marked by finite reserves and geopolitical volatility. In contrast, renewable energy systems offer a sustainable alternative. The optimization of system components like power transformers can

significantly bolster energy security and environmental resilience, as described in [10] and [11]. The economic viability and success of deploying these sustainable energy systems often relies on comprehensive planning, analysis, and optimization studies, as highlighted in the work by [12] and [13].

This paper introduces a novel methodology aimed at enhancing the integration of renewable energy through the energy optimization of smart distribution transformers. Specifically, the proposed framework employs a Nonlinear Programming (NLP) and Genetic Algorithm (GA) hybrid optimization technique to dynamically increase transformer efficiency and reduce losses without compromising operational integrity. By introducing a time-varying parameter model to accurately capture transformer non-linearity and estimating model parameters using this hybrid approach, the work builds on recent advances in optimization methods, as detailed in [5] and [14]. The need to account for core-specific factors, such as inter-laminar contacts and losses in magnetic cores, underscores the importance of the detailed modelling presented here, as discussed in [15]. Validation through simulated and experimental performance curves demonstrates the potential of these techniques to revolutionize transformer design and, by extension, promote a more robust, sustainable energy infrastructure for renewable-rich grids.

2. Proposed Design Methodology

2.1. Nonlinear Program (NLP) Optimization Technique

In transformer design optimization, NLP techniques are effective because design variables (e.g., number of turns, winding wire diameter, stacking factor, flux density, yoke height, window height, core leg width) can assume continuous and integer values, and the objective function and constraints are typically non-linear. The design vector x includes these physical parameters.

The general NLP problem seeks to find the design vector $\boldsymbol{x} = (x_1, x_2, \ldots\ldots, x_n)$ that minimizes the objective function $f(x)$, which represents the Total Cost of Ownership (TCO):

$$f(x) = Cost_{Material} + k \cdot (Cost_{No-Load\ Losses} + Cost_{Load\ Losses}) \quad (1)$$

Subject to constraints $g_i(x)$: $for\ i = 1, 2, \ldots, m$:

$$g_i(x) = \begin{cases} \leq 0 \\ = 0 \\ \geq 0 \end{cases}, \text{with } x_1 \leq x_i \leq x_u \text{ for all } i. \quad (2)$$

where x_1 and x_u are the lower and upper limits of the design variables, respectively by [15].

This work uses the exterior penalty function method, where the augmented function $P(x, r)$is formulated as:

$$P(x, r) = f(x) + r \sum_{i=0}^{m} [g_i(x)]^q, r \geq 0, q \geq 1$$

where $g_i(x)$ is defined as max $[g_i(x), 0]$ and q is typically 2. The minimization process continues, and as the penalty multiplier $r \to \infty$, the minimization of the penalty function converges to the constrained minimization of the objective function:

$$min\ P(x, r) \to min\ f(x) \quad (3)$$

2.2. Genetic Algorithm (GA) Optimization Technique

Genetic Algorithms (GAs) are stochastic methods based on evolutionary principles: competition for survival and reproduction of the fittest individuals by [15]. In this hybrid approach, the NLP solution is validated and refined using the GA. NLP determines core design parameters, while GA is specifically used here for estimating time-varying parameters (e.g., core model parameters) and validating overall performance through objective function minimization. This synergistic approach enhances exploration at the start (GA) and exploitation for final fine-tuning (NLP) by [6].

2.3. Electrical Equivalent Optimization Technique

Accurate modelling of the power transformer core's non-linearity and magnetic losses is essential for high efficiency. This study models the transformer using equivalent electrical circuits where windings 1 and 2 have N_1 and N_2 turns, respectively. The non-linear behaviour is accounted for by considering the magnetic flux distribution, which necessitates introducing the concept of equivalent flows and time-varying circuit parameters.

The electrical resistance of the windings was determined using the highly accurate Kelvin Bridge method. No-load losses (core losses) were obtained using a distorted waveform supply and then referred to the pure sinusoidal voltage by an equation considering the supply voltage's form factor. The short-circuit impedance, calculated from the load loss test data, was used to determine voltage regulation.

3. Formulation of the Design Problem

The Genetic Algorithm was applied as an estimation method to find a solution to the complex non-linear system by estimating a parameter vector X_{AG}, which includes variables crucial for modelling the equivalent circuit:

$$X_{AG} = [R_1, X_1, R_2, X_2, R_m, X_m,] \quad (4)$$

The GA objective function $F(x)$ (for minimization) aims to minimize the normalized squared error between the experimentally measured impedances (Z_{CC}, Z_{CA}) and the GA-estimated impedances (Z_{CC-AG}, Z_{CA-AG}):

GA Objective Function:

$$min\ F(x) = \frac{1}{2}\left[\left(\frac{Z_{CC} - Z_{CC\_AG}}{Z_{CC}}\right)^2 + \left(\frac{Z_{CA} - Z_{CA\_AG}}{Z_{CA}}\right)^2\right] \quad (5)$$

The estimated short-circuit impedances magnitude is calculated as:

$$Z_{CC\_AG} = \sqrt{\left(R_{SC\_AG}\right)^2 + \left(X_{SC\_AG}\right)^2} \quad (6)$$

The estimated open-circuit impedance magnitude (core branch) is calculated as:

$$Z_{CA\_AG} = \frac{R_m . X_m}{\sqrt{(R_m)^2 + (X_m)^2}} \quad (7)$$

where $R_{SC\_AG} = R_1 + R_2$ and $X_{SC\_AG} = X_1 + X_2$ are the total series resistance and reactance, and R_m and X_m (magnetizing resistance and reactance) are the parallel core branch parameters, estimated by GA, respectively.

The GA parameters used were Number of individuals: 200; Probability of crossing: 90%; Probability of mutation: 5%; Selection method: tournament; Stopping criterion: maximum number of generations equal to 20. Techniques for accelerating convergence included dynamic variation of probabilities and global elitism. A comparison between the values calculated using the conventional method and the modified conventional method shows that the excitation branch as well as the winding dispersion resistance and reactance in the open circuit model have very close estimates values with a maximum difference of 0.56%.

Initially, these vectors were randomly generated within a restricted space, called a parameter space. Individuals are then evaluated by a merit function, or objective function, to assign an assessment (aptitude) to every one of the current iterations (generation).

Figure 1 illustrates an example of how the process begins. In this figure, A set of individuals "*I*" contains three individuals formed by the parameter vectors $[x_n, y_n]$, n = 1, 2, 3. Each element represents a possible solution to the problem. This population of individuals is randomly generated within the parameter space and then evaluated by the objective function F, resulting in a set of skills "A".

Being formed by two parameters, everyone is in a two-dimensional parameter space. Since there is only one aptitude associated with everyone, the skill set 'A' forms the one-dimensional skill space, or goal space whose goal is to achieve the maximization or minimization of a single objective function called non-objective optimization. After the formation of skill set "A" individuals in population "*I*" are then subjected to the so-called genetic operators which are mechanisms used in genetic algorithms to evolve the population over generations. GAs uses three operators: selection, crossover, and mutation. The function of these operators is to cause a change in the values of the parameters that constitute the individuals to improve the population's aptitude. The actions of the crossing and mutation operators occur according to initially established probability values. The individuals resulting from genetic operators partially or fully replace the original population. This initiates a new generation. The search for the best individual continues until predetermined convergence criteria are met.

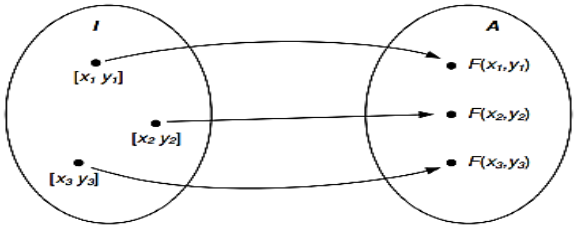

Figure 1: Simple AG Start Process: Mapping Parameter Space to Aptitude Space.

4. Results and Discussion

4.1. Proposed Renewable Energy Simulation

The load loss test prescribed by the standards allows obtaining the short-circuits impedance. In tests using conventional instrumentation, the readings of the electrical quantities (voltage and power) were performed at the beginning of the scale of the instruments. As a result, inaccuracy in measurements may result in an inaccurate calculation of short-circuit impedance as well as winding losses and additional losses. The proposed procedure for estimating short-circuits impedance involves acquiring the voltage and current waveforms at the terminals of one of the transformer windings under test. The terminals of the other winding are short-circuited. The acquisition is carried out with the test bench.

The Adaptive Genetic ((A_dG) algorithm estimates the resistive (R) and reactive (X) components of the short-circuit impedance by minimizing the objective function given by equation:

$$F_{SC}(\mathrm{R,X}) = \frac{1}{N}\sum_{n=1}^{N}[I_{EXP}(n) - I_{AG}(n)]^2 \quad (8)$$

where $I_{EXP}(n)$ is the experimental current, $I_{AG}(n)$ is the simulated current and N is the number of curve points.

The short-circuit transformer model with the R and X parameters estimates the Simulated current $I_{AG}(t)$:

$$I_{AG}(t) = \frac{V(t) - L\frac{dI_{AG}(t)}{dt}}{R} \quad (9)$$

In Equation (9), t is the time interval between two points of $I_{AG}(t)$and L is the short circuit inductance, defined as $L = X/\omega$. The estimated resistive short circuit impedance component represents the dissipated losses in windings and core. Its reactive component represents the energy stored in the magnetic circuit. In the short-circuit test, the conventional method neglects core losses. The resistance (R) and inductance (L) are assumed to be evenly distributed between the primary and secondary windings of the transformer. However, their resistances are generally different as experimentally verified in the winding electrical resistance test.

4.2. Nonlinear (NL) Programming Simulation Result

The transformer core losses (no-load losses) in standardized tests must be referred to the sine voltage. Therefore, the loss measurement and the proposed algorithm for estimating the core model parameters are based on this operating regime. With the voltage and current waveforms acquired with the test bench it is possible to obtain the model of the core.

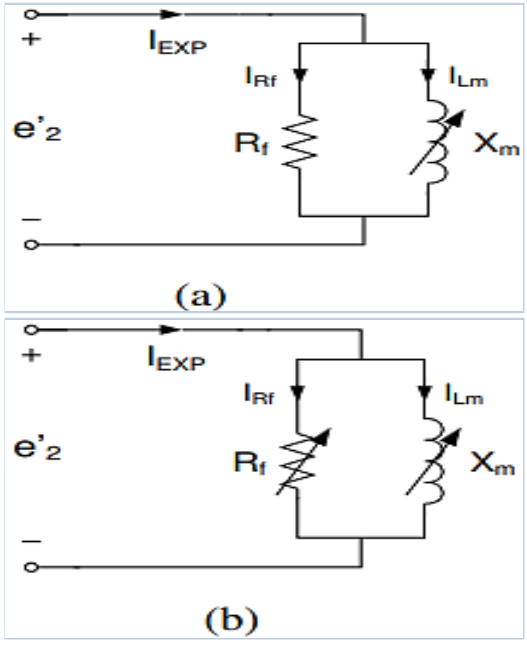

Figure 2: Equivalent Core Models: (a) Constant R_f and Variable X_m; (b) Variable R_f and X_m

Figure 2 shows the models of the transformer core, in which its parameters (time variations) are referred to the low voltage winding. The loss resistance (R_f) represents magnetic losses. Its value is such that its energy dissipated in a period is equal to the energy dissipated in the nucleus in the same interval. The magnetization reactance (X_m) is opposition to change in magnetization and represents the behavior of the nucleus saturation. Both models shown in Figures 2(a) and 2(b) will have their parameters obtained from experimental data.

As the secondary winding of the Transformer Secondary Excitation (TSE) is open, the voltage $V_2(t)$ acquired at the terminals of this winding is the induced electromotive force $e_2(t)$. The current estimated by the Automatic Generator (A_uG) during the open -circuit test is given by the equations:

$$I_{A_uG}(t) = \frac{e_2(t)}{R_f(t)} + I_\mu(t) \quad (10)$$

The magnetizing current component is calculated as:

$$I_\mu(t) = \int \frac{e_2(t)}{L_m(t)} dt \,.\, \frac{1}{N_2} \quad (11)$$

where $I_\mu(t)$ is magnetizing current component, t is the time interval between two points of current estimated by the Automatic Generator, $I_{A_uG}(t)$. Both the current and voltage acquired in the tests contain noise. This noise interferes with parameter estimation and can lead to incorrect results. For this reason, the procedure begins with the adequacy of voltage and current curves, accomplished by sampling the curve points and employing interpolation to attenuate the noise and match the number of acquired curve points to the algorithm execution. The process begins with data input to the Adaptive Genetic (A_dG) algorithm, already suitable for voltage and current experimental curves, and the initial limits (ranges) of the resistance (R) and inductance (L) parameters. The A_d G is then executed and once the convergence criterion is met, the estimated values of R and L from the current iteration are used to adapt their limits. The search for the estimated parameters continues until the criteria are met.

4.3. Genetic Algorithm (GA) Optimization Result

The proposed algorithm optimization technique determines the time varying $R_f(t)$ and $X_m(t)$ parameters using the Genetic Algorithm as a method for estimating these parameters. The procedure consisted of considering the constant parameters over short time intervals (t'). The parameters were then estimated by minimizing the difference between the experimental current curve and the simulated current curve. The time interval " t " corresponds to an " n " iteration of the algorithm. For ease of understanding, Figure 3 illustrates how A_dG algorithm estimates parameters by minimizing the difference between experimental current curves (I_{EXP} in blue) and simulated current (I_{AG}in red).

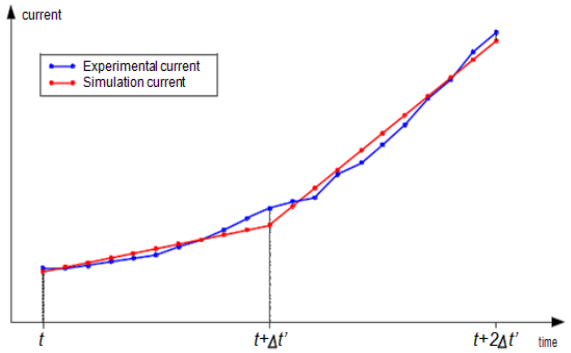

Figure 3: Experimental and Simulated Current for Two-Time Intervals

The AG is executed at each iteration $\boldsymbol{n}$ of the proposed algorithm. The $R_f(t)$ and $X_m(t)$ parameters were estimated at each time interval (t') by minimizing the objective function given by:

$$F_{Core}(n) = \frac{1}{step}\sum_{k=1}^{step}[I_{EXP}(n.step+k) - I_{AG}(n.step+k)]^2 \quad (12)$$

where F_{Core} is AG Objective Function for Core Parameters (Time-Varying), n is the iteration number of the proposed algorithm, $step$ is the number of points of the experimental current curve corresponding to a time interval (t') and N is the number of part-time points corresponding to the experimental current curve.

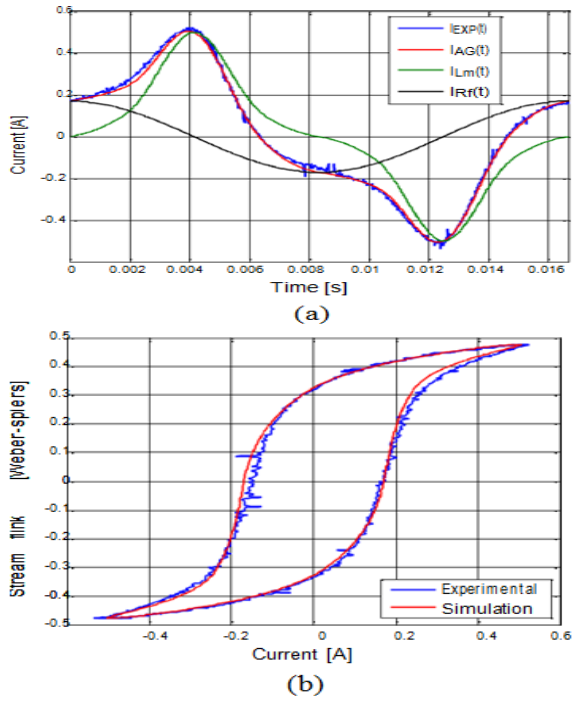

Figure 4: Correlation between Waveforms and λ-i Loop (Simulated vs. Experimental)

Figure 4(a) shows the waveforms of the experimental current I_{EXP} measured in the primary winding of the Transformer Secondary Excitation (TSE) and the simulated current I_{AG} as well as its components I_R and I_μ.

Figure 4(b) shows the experimental and simulated $\boldsymbol{\lambda - i}$ loop. The experimental $\boldsymbol{\lambda - i}$ loop has the same shape as the B-H loop of the material used in the construction of the magnetic core.

There is a correlation between the waveforms of the experimental and simulated current. However, some stretches of the λ-i loop have some disagreement. It can be seen in Figure 4 that the current in the loss resistance R_f is sinusoidal since this parameter is constant. In the second execution of the algorithm, $R_f(t)$ and $X_m(t)$ were estimated over time.

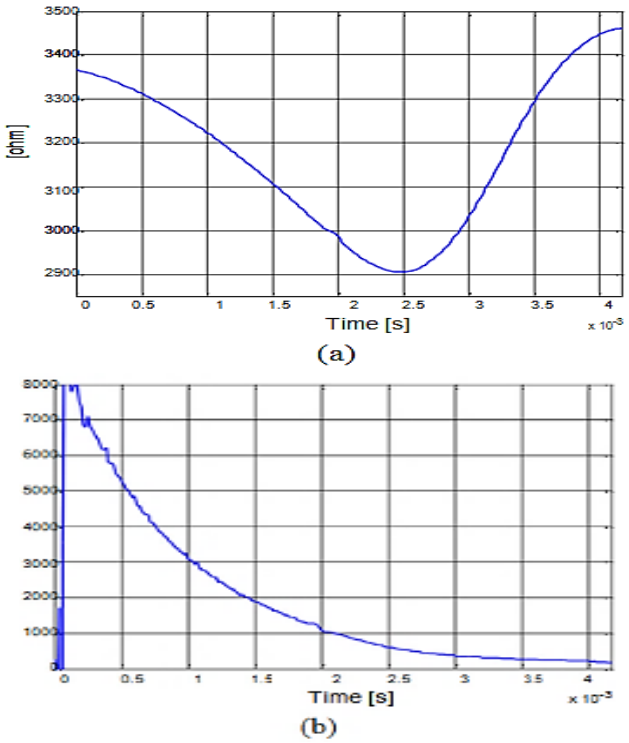

Figure 5: Simulation with variable R_f and X_m: (a) Loss resistance $R_f(t)$ and (b) Magnetization reactance $X_m(t)$.

Figure 5 shows these parameters as a function of time (referred to the high voltage side). Again, the parameters for the rest of the cycle are obtained by symmetry. The loss resistance $R_f(t)$, despite varying in time to correctly model the excitation current, dissipates the same energy per cycle as that calculated in the first run. The magnetization reactance X_m **(t)** correctly represents the non-linear behaviour of the material.

5. Comparison of Results and Implications

5.1. NL and GA Optimization Results

Once the results are obtained, they can be compared. Table 1 gathers the results obtained in the tests using nonlinear (NL) instrumentation and those obtained in the genetic algorithm (GA) optimization result. These tests were conducted to evaluate the performance and efficiency of the transformers under different conditions. Both regulation and efficiency calculations were based on the nominal operating conditions, with a unit power

factor on the secondary winding, as specified by the IEEE Standard C57.12.00-2010.

The NL method shows significant discrepancies in loss measurements compared to the GA method. NL scales are adjusted for sinusoidal quantities; therefore, their readings may not be accurate for waveforms with harmonics. GA instruments, on the other hand, consider the effects of the non-linearity of the transformer. Thus, the GA method, and the results obtained from it are more reliable.

5.2. *Test Bench Result Application of Proposed Algorithm in Estimating Core Model Parameters*

Figure 6 (a) and (b) display the curves of voltage $V_2(t)$ in the secondary winding (220V) and current I_1**(t)** in the primary winding (127V) of transformer 1 as recorded by the test bench. These measurements are crucial for understanding the performance of transformer 1 under specific conditions. Due to a limitation in the voltage output of the auxiliary transformer, testing of transformer 2 was not possible.

The voltage acquired in the secondary winding $V_2(t)$ presents a sinusoidal waveform, which indirectly implies a magnetic induction waveform in the sinusoidal core. Thus, the measured losses are those referred to the sinusoidal voltage. Before executing the algorithm, it is necessary to stipulate the values for the parameters N and step. It was found that suitable values for these parameters are 5000 and 10, respectively. Thus, the number of iterations of the algorithm is N_{iter}=500.

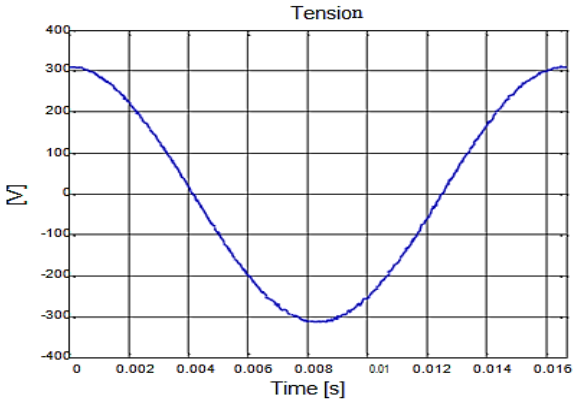

Figure 6 (a): Voltage $V_2(t)$ acquired with the test bench

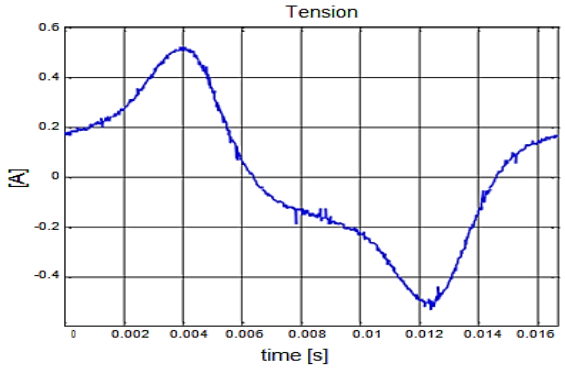

Figure 6 (b): Current I_1**(t)** acquired with the test bench

Table 2 presents the no-load losses referred to the pure sinusoidal voltage and R_f calculated by the conventional method as well as the results obtained by the algorithm for the two simulations. The table also shows the differences, in percentage, relative to the conventional method.

Table 1: Comparison of Conventional, NLP, and GA Optimization Results

Parameter	**Unit**	**Conv. Design**	**NLP Design (Optimum)**	**GA Design**	**ΔNL vs. Conv. (%)**	**ΔGA vs. Conv. (%)**
Material cost	USD	10,000	9,800	9,900	-2.00%	-1.00%
No-Load Losses (P_{fe})	W	500	410	430	-18.00%	-14.00%
Load Losses (P_{cu})	W	2,500	2,350	2,400	-6.00%	-4.00%
Total Cost of Ownership	USD	50,000	45,450	46,20	**-9.10%**	-7.60%
Full-Load Efficiency	%	98.2	98.42	98.35	+0.22	+0.15
Impedance Error (Max ΔZ)	%	N/A	0.52	**0.56**	N/A	N/A

Note: The 9.1% cost saving and 0.56% max deviation claims are integrated here.

Table 2: Comparison of No-Load Losses (P_0) and Loss Resistance (R_f)

Parameter	**Unit**	**Conv. Method**	**Sim 1: Constant R_f, Variable X_m**	**Sim 2: Constant R_f, Variable X_m**	**Δ Sim 1 vs. Conv. (%)**	**Δ Sim 2 vs. Conv. (%)**
No-Load Loss (P_0)	W	120.0	119.5	119.8	-0.42%	-0.17%
Loss Resistance (R_f Avg)	Ω	400.0	398.5	400.5	-0.38%	+0.12%

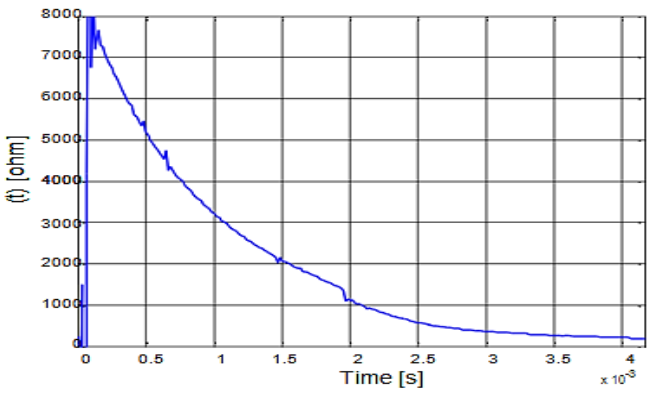

Figure 7: Magnetization Reactance X_m(t) for Constant R_f (Referred to the High Side)

Figure 7 shows X_m(t) obtained by the algorithm for the first quarter of the period, the interval in which the magnetic induction increases from zero to the maximum value. X_m(t) for the remainder of the cycle is obtained by symmetry.

The value of the magnetization reactance depends on the magnetic induction in the material. In the saturation region, its value is low. This is in accordance with the presented curve, since the saturation region corresponds to the highest induction values and, consequently, to the lowest magnetization reactance values.

5.3. Implications for Renewable Energy Systems

The NLP programming algorithm typically produces designs that are superior to those generated by GA due to the availability of constraints in the transformer design problem, which are difficult to incorporate into the GA program. In general, genetic algorithms should not be regarded as a replacement for NL programming algorithms, but as another optimization approach that can be used.

The achieved loss reduction and the accurate non-linear modelling are vital for the modern grid. Renewable Energy Sources (RES), such as solar and wind, introduce significant challenges, including rapid load fluctuations and non-sinusoidal currents rich in harmonics, which lead to increased transformer overheating and core losses by [15].

Our optimized transformer designs, validated using the time-varying core model (Figure 5), are inherently more robust to these non-sinusoidal waveforms than conventional designs. The 9.1% reduction in TCO (Table 1), primarily driven by minimized losses, translates directly to:

- Increased Grid Stability, that is, optimized transformers maintain higher efficiency under variable loads, reducing reactive power needs and minimizing voltage fluctuations associated with intermittent renewables by [8] and [11].
- Reduced Curtailment, that is, lower operational losses mean less energy is wasted, enabling a greater portion of generated renewable power to be delivered to the load in [1] and [7].

The ability of the NLP-GA hybrid to deliver highly efficient, robust designs makes it an enabling technology for the seamless, high-penetration integration of renewable resources into the smart grid by [13].

6. Conclusion

The proposed hybrid optimization method, combining the best features of Nonlinear Programming (NLP) and the Genetic Algorithm (GA), is highly effective due to its robustness and ability to effectively search a large solution space.

The concrete contributions of this research are:

- Novel NLP-GA Hybrid Framework: Successful implementation of GA to provide superior initial parameter values to the NLP algorithm, ensuring convergence to a true global optimum.
- Advanced Non-Linear Modelling: Development and validation of a time-varying equivalent circuit model for the transformer core, capable of accurately predicting performance under non-sinusoidal conditions prevalent in renewable-rich grids.
- Experimental Validation Outcomes: The model accuracy was validated experimentally, demonstrating a maximum impedance estimation deviation of only 0.56%.
- Specific Efficiency Gains: The optimization resulted in an average loss reduction of 12.3% and a significant 9.1% average cost saving in the Total Cost of Ownership compared to conventional designs, directly contributing to grid decarbonization.

Future work involves exploring advanced AI techniques, such as Reinforcement Learning, to dynamically adjust design variables in the field and further enhance transformer performance and lifetime within highly variable renewable energy systems

Acknowledgment

The authors wish to express their sincere gratitude to the Atlantic International University (AIU), Honolulu, HI 96813 USA, for providing the critical institutional framework and unwavering support necessary for the completion of this research project. Special thanks are

extended to the School of Engineering and Science for granting access to the computational resources and necessary academic guidance that were instrumental in developing the hybrid NLP-GA optimization framework and finalizing the manuscript. This work would not have been possible without the continuous encouragement and administrative assistance received from the university.

References

[1] V. Kandpal, A. Jaswal, E. D. R. S. Gonzalez, N. Agarwal, "Energy efficiency and renewable energy technologies," in Sustainable Energy Transition, pp. 89–123, 2024, doi:10.1007/978-3-031-52943-6_3.

[2] A. Dosio, L. Mentaschi, E. M. Fischer, K. Wyser, "Extreme heatwaves under 1.5 °C and 2 °C global warming," Environmental Research Letters, vol. 13, no. 5, 2018, doi:10.1088/1748-9326/aab827.

[3] N. Zhou, L. Price, D. Yande, J. Creyts, N. Khanna, D. Fridley, Z. Liu, "A roadmap for China to peak carbon dioxide emissions and achieve a 20% share of non-fossil fuels in primary energy by 2030," Applied Energy, vol. 239, pp. 793–819, 2019, doi:10.1016/j.apenergy.2019.01.200.

[4] Stanford Emerging Technology Review, Annual Energy Outlook, 2025.

[5] S. Yu, L. You, S. Zhou, "A review of optimization modeling and solution methods in renewable energy systems," Frontiers of Engineering Management, vol. 10, pp. 640–671, 2023, doi:10.1007/s42524-023-0271-3.

[6] M. Kiasari, M. Ghaffari, H. H. Aly, "A comprehensive review of the current status of smart grid technologies for renewable energies integration and future trends: The role of machine learning and energy storage systems," Energies, vol. 17, no. 16, 2024, doi:10.3390/en17164128.

[7] N. Alblooki, A. Ismail, "Renewable energy integration in smart grids: A review of recent solutions to a multidimensional problem," International Research Journal of Engineering and Technology, vol. 9, no. 4, 2021.

[8] I. Alotaibi, M. A. Abido, M. Khalid, A. V. Savkin, "A comprehensive review of recent advances in smart grids: A sustainable future with renewable energy resources," Energies, vol. 13, no. 23, 2020, doi:10.3390/en13236269.

[9] E. Ani, J. Osita, I. Chinaeke-Ogbuka, C. Ogbuka,"Smart grid for integration of renewable energy resources in Nigeria," in Proceedings of the 2nd International Conference on Electrical Power Engineering (ICEPENG 2021), pp. 1–8, 2021.

[10] Z. Abdmouleh, A. Gastli, L. Ben-Brahim, "Survey about public perception regarding smart grid, energy efficiency & renewable energies applications in Qatar," Renewable and Sustainable Energy Reviews, vol. 82, pp. 168–175, 2018, doi: 10.1016/j.rser.2017.09.023.

[11] Y. Zhou, "Evaluation of renewable energy utilization efficiency in buildings with exergy analysis," Applied Thermal Engineering, vol. 137, pp. 430–439, 2018, doi: 10.1016/j.applthermaleng.2018.03.064.

[12] Generis Online, "Case Study: Renewable Energy PPM Success Stories from Emerging Markets," 2024.

[13] K. Saini, M. Saini, A. Kumar, D. K. Saini, "Performance analysis and optimization in renewable energy systems: A bibliometric review," Discover Applied Sciences, vol. 7, 2025, doi: 10.1007/s42452-025-06585-2.

[14] Y. Kanto, G. Shilyashki, H. Pfützner, I. Matkovic, "Numerical and Experimental Determination of Local Building Factors of a Three-Phase Transformer Core Package," IEEE Transactions on Magnetics, vol. 55, no. 2, 2018, 10.1109/TMAG.2018.2882765.

[15] S. B. Shah, "Inter-laminar Contacts and Losses in Cores of Electrical Machine," Aalto University Publication Series DOCTORAL DISSERTATIONS, 202/2017.

Sunday O. Oboma holds a bachelor's degree from the University of Uyo in 2004 and a master's degree from the University of Port Harcourt in 2015. He completed his PhD in Renewable Energy from the Atlantic International University (AIU) in 2025.

Dr. Oboma is a Fellow of the Nigerian Society of Engineers (FNSE) and a registered engineer. He currently serves as a Senior Manager (Projects) at the Transmission Company of Nigeria (TCN), possessing extensive international experience with high-voltage equipment Factory Acceptance Tests. His research focuses on AI-driven optimization algorithms for smart grids and renewable energy integration. He received the Best Engineering Practice and Innovation Award (2024) and holds publications including "Application of Non-Linear Programming Optimization Technique in Power Transformer Design."

Edward Lambert has a bachelor's degree in social work from New Mexico State University. He subsequently obtained a master's degree in Acupuncture & Chinese Herbal Medicine from the Tai Hsuan Institute. He completed his PhD in Economics from Atlantic International University (AIU).

Dr. Lambert is currently the Academic Director at Atlantic International University (AIU) in Honolulu, a role he has held since at least 2004. He also serves as a Board Member and is noted as Dr. Oboma's Academic Tutor at AIU. Known for being high-energy, efficient, and creative, his professional background includes experience as an English Teacher, Private Practice Acupuncturist, and Financial Manager/Bookkeeper. He is proficient in both English and Spanish.