

Simulation and Performance Analysis of Wireless VPNs over SDN-Based mmWave Communication Backhaul Networks

Amritharaju V.^{1*}, Faraz Ahmad², Lokesh Verma³, Pushpalatha, T.⁴, Ebenezar Jebarani M.R.⁵, Bhagyalaxmi Behera⁶

¹Associate Professor, Department of Aerospace Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Bangalore, Karnataka, India.

²School of Engineering & Computing, Dev Bhoomi Uttarakhand, Dehradun, Uttarakhand.

³Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India.

⁴Assistant Professor, Department of Computer Applications (DCA), Presidency College, Bengaluru, Karnataka India.

⁵Professor, Department of Electronics and Communication Engineering, Sathyabama Institute of Science and Technology, Chennai, India.

⁶Associate Professor, Department of Electronics and Communication Engineering, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India.

KEYWORDS:

Software-Defined Networking (SDN),
Millimeter-Wave (mmWave)
Backhaul,
Wireless Virtual Private Network
(VPN),
Secure and Scalable 5G/6G
Networks,
QoS-Aware Dynamic Routing,
SDN-Based Mobility Management

ARTICLE HISTORY:

Received: 10.08.2025

Revised: 20.11.2025

Accepted: 18.12.2025

DOI:

<https://doi.org/10.31838/NJAP/08.01.06>

ABSTRACT

The accelerating popularity of data-intensive services like high-definition video streaming, cloud-based real-time gaming, and mission-critical Internet of Things applications have heightened the pressure on wireless networks that need to sustain both blazing high data rates and the highest level of security. The present study in turn addresses the integration between software-defined networking (SDN) and millimeter-wave (mmWave) communication technologies to integrate wireless virtual private networks (VPNs) powered by scalable and secure services over dynamic backhaul. In particular, we report on a fully simulated model that models wireless VPN application over 60 GHz mmWave wireless links, mediated via an SDN-based control plane. The architecture utilizes open hardware based on programmable OpenFlow switch controllers to execute security policies based on flows, dynamically route VPN paths, and adjust to rerouting and the failure of links and topological changes. In order to test the performance of the proposed system, massive NS-3 and Mininet-WiFi simulations were performed and combined with SDN-based logic and IPsec VPN encapsulation. These simulations model a heterogeneous mobility and fixed client of the urban network and assesses them in the performance under different conditions of node density, mobility, and traffic pattern. Selected key quality of experience (QoE) and quality of service (QoS) metrics (e.g., end-to-end throughput, average latency, jitter, packet loss rate, and VPN reconfiguration delay) were compared with static and dynamic scenarios. Findings indicate that SDN-based mmWave backhaul can improve network responsiveness and resource utilization to a significant level by using real-time path rerouting and tunnel recovery with an insignificant control burden. In addition, the system is able to sustain secure and low-latency VPN connections under conditions of high mobility or mmWave signal blackouts, which points to the ability of the system to RF-sensitive VPN routing as well as future antenna-assisted SDN designs in next-generation urban deployments in 5G/6G. This paper establishes a background platform, upon which highly reliable and secure wireless backhaul networks to provide the challenging needs of the future smart cities and enterprise wireless VPN services exist.

Authors' e-mail ID: v.amritharaju@jainuniversity.ac.in; Universityme.faraz@dbuu.ac.in; lokesh.verma.orp@chitkara.edu.in; pushpalatha.t-coll@presidency.edu.in; ebenezarjebarani.ece@sathyabama.ac.in; bhagyalaxmibehera@soa.ac.in;

Authors' Orcid ID: 0000-0002-3434-3955; 0000-0003-0934-8583; 0009-0009-3032-3947; 0009-0001-2156-5743; 0000-0001-5327-664X; 0000-0003-3715-2860

How to cite this article: Amritharaju V. et al., Simulation and Performance Analysis of Wireless VPNs over SDN-Based mmWave Communication Backhaul Networks, National Journal of Antennas and Propagation, Vol. 8, No. 1, 2026 (pp. 60-71)

INTRODUCTION

Future wireless networking promises hyper-fast, low-latency communication with one of the clear needs being high-speed, low latency, and secure communications across a more dynamic and data-intensive environment. New applications, including 4K/8K video streaming, augmented and virtual reality (AR/VR), self-driving vehicles, industrial automation, and some services offered through the tactile Internet, have brought radical growth in bandwidth and reliability requirements. Such needs place tremendous strain on current backhaul infrastructures particularly in heavily populated metropolitan regions, intelligent campus, and moveable business space.^[1]

In order to address these issues, millimeter-wave (mmWave) communication with 30300 GHz frequency bands are capable of covering unprecedented bandwidth that can be multigigabit per second (Gbps) backhaul connections.^[2] Nonetheless, mmWave links are vulnerable in their nature: mobile and nonline of sight (NLOS) channels tend to have high path loss, suffer blockage by objects, and have misalignment of beams.^[3] Such vulnerability requires dynamic and smart backhaul management, in which the software-defined networking (SDN) is vital.^[4,5] SDN fulfils the vision of centrally managed flexible and programmable routing and fine granularity of resource allocation in networks, so that they can accommodate quick topology and environmental changes. Thanks to the real-time communication with the network, SDN controllers can redirect traffic flows, reassign bandwidth to demands, and sustain service continuity when in disruptive contexts.^[6,7]

Meanwhile, the wireless virtual private networks (VPNs) have sustained irreparable role in providing confidentiality, integrity, and authentication in the shared or public wireless setting.^[8] VPNs offer secure encryption tunnels across wireless links; so secure that enterprise and user data are safely encapsulated, and transferred across trusted and untrusted infrastructure. However, there are no studies on the simultaneous optimization of the performance of VPNs, mmWave links, and the SDN-based routing. The literature has traditionally addressed each of these components independently and overlooked their rather large interplay with another component: the overheads of encryption, the swings in link quality, and controller-based reconfiguration.

Although the performance of the mmWave backhaul has been studied in many works and the use of SDN in routing purposes of wireless networks has been discussed,

very less literature exists in the assessment of an integrated framework that observes the end-to-end behavior of VPN over the SDN-managed mmWave infrastructures.^[6,7] In particular, there is inadequate information available in the literature on the effect of the SDN control decisions on encapsulated VPN flows in a dynamic and volatile wireless backhaul network. Along with this, the trade-off among quality of service (QoS) parameters, that is, latency, jitter, and packet loss, and the overhead introduced by encryption and security protocols have not received due attention.^{[8], [9]} Further work should also be carried out to look into resilience and stability of VPN tunnels in case of SDN-triggered rerouting events, which occur frequently in mobile or blocked environments.^[17] Also, little is known as to how the difference in traffic profiles and user mobility behaviors affect the overall performance of the system in the context of the tunnel continuity and service continuity/reliability in these types of hybrid architecture.

The increased requirements of the next-generation wireless networks involving wireless data communications and their applications necessitate the need to develop a very robust and secure communication framework.^[10] It offers an end-to-end simulation framework that combines mmWave wireless backhaul modelling, dynamic routing control based on SDN, secure VPN tunnel strategies, and realistic mobility and patterns of users and can be delivered. It will first and foremost aim at modeling and simulating the behavior of wireless VPNs working on SDN-controlled mmWave backhaul links. Using this framework, the paper would lay the ground to measure important QoS parameters—like throughput, latency, jitter and also packet loss—in a network state that is dynamically changing. It also aims at studying the impact of SDN routing decisions and mmWave link instability on VPN tunnel integrity and service reliability. Finally, the study will also aim at offering design lessons and suggestions on the deployment of scalable, secure, and high-performance wireless VPN infrastructures in future smart network systems such as the use of 6G implementations, enterprise mesh, and urban IoT systems.^[11,12]

This study has three major contributions. First, it proposes a unified simulation and analysis modeling base that allows coupling NS-3, Mininet-WiFi, and proprietary SDN control logic with mathematical representations of the mmWave path loss, VPN encryption overhead, and SDN queueing delay. Second, the research would give a comparative performance assessment of SDN-based and non-SDN-based VPN architecture when subjected to dynamic mobility and fluctuating traffic and payload

conditions to highlight key QoS metrics, including but not limited to throughput, latency, jitter, packet loss, and tunnel set-up time. Third, it gives an in-depth analysis of the scalability and resilience of mmWave wireless backhaul networks under user mobility, nonline-of-sight (NLOS), and line-of-sight (LOS) blockages conditions, on how SDN-aided rerouting and dynamic VPN reconfiguration helps in achieving secure and high-performance communication.^[13]

RELATED WORK

Open issues incorporation of mmWave communication, SDN, and VPNs has been raised as an increasingly obvious strategy to concur with the requirements of next-generation wireless backhaul systems. Every part has been studied as an independent entity in different studies, but their combined operation and performance in changing wireless topologies has not been quite explored.^[14]

The study by Gupta et al.^[2] involved the discussion of the mmWave technology as a high-capacity urban backhaul technology. They demonstrated how a dense deployment can employ 60-73 GHz bands to afford multi-gigabit throughput. Nevertheless, the research likewise stressed on the mmWave vulnerability to link obstruction and beam mis adjustment, especially in the usage or mobility of objects or users. This was solved by Park et al.^[3] who proposed a cross-layer optimization framework of mmWave link reliability that uses beam adaptation and path diversity. However, in their research, the assumptions were under static routing, and there was no SDN programmability or secure overlays.^[15,16]

Zhou et al.^[4] experimented with the concept of SDN to dynamically manage the topology in 5G systems by demonstrating enhanced flexibility in mobile wireless backhaul environments. Their method took advantage of central control in real-time route reconfiguration. But in this case, little was thought of the integration of factors like encryption overheads as well as secure VPN tunnels. The SDN orchestration model suggested by Riggio et al.^[5] came later, containing no information about the analysis of VPN tunnel behavior or encrypted traffic in the mmWave conditions.

Khan et al.^[8] performed an experimental study on the VPN deployment over wireless mesh network and also compared the performance degradation between IPsec and SSL-based tunnels. Although useful to measure the encryption overhead, this study failed to measure the

resilience of the tunnel in a dynamic mmWave connection and re-routing because of SDN decisions. In addition, the stability of the VPN tunnel under real-time mobility like handovers or topology changes was not frequently handled.

In more recent studies, attempts have been made to connect the threads. Chen et al.^[1] designed an AI-compatible framework of SDN to anticipate mmWave connectivity breakdowns and reroute traffic as a result. Nonetheless, the system paid attention only to data throughput and did not consider VPN tunneling and security-aware flow control. On the same note, Patel and Wong^[7] have also studied fast rerouting in SDN-based wireless mesh topology but without evaluating performance and link characteristics with encrypted tunnels and how they perform under blockage and interference that is characterized by the mmWave systems.

Also, the application of embedded systems and IoT in secure wireless framework is gaining importance. Articles like^[9] and^[17] highlight the increased reliance of the healthcare and smart monitoring software on efficient and secure communicational infrastructures. Such contributions to the integration of hardware^[11] and VLSI design,^[11] a MIMO system of high throughput^[18] and the use of composite technology to allow resilience^[12] only serves to further reinforce a single platform of simulation which will demonstrate a commitment to represent the performance as well as the resilience in the face of real-world dynamics.

No current work has provided an end-to-end simulation-based study of how wireless VPN performance changes under SDN-controlled mmWave volumes, and specifically with realistic, heavy traffic, mobility, and encryption assumptions. In a rather critical gap, this work proposes a holistic simulation approach to collectively consider QoS, tunnel integrity, and reconfiguration effects caused by SDN in volatile wireless networks.

SYSTEM ARCHITECTURE

The presented system architecture is expected to provide secure and high-performance communication through mmWave wireless backhaul networks that are controlled by the SDN controller. Which is integrate to multiple access contains the technologies, software defined controls and secure VPN suitable for the various ranges of environment. The architecture is conceptually segregated into four major elements, namely, the physical and logical network topology, separation

of control-data plane solutions, and security using VPN tunneling techniques. Figure 1 shows the architecture proposed to support programmability with SDN, supporting encrypted VPN tunnels over mmWave backhaul that can offer both flexibility and secure communication in moving wireless networks.

Network Topology

The general network provides a kind of hybrid wireless architecture that involves an access network, mmWave backhauling connectivity, SDN controllers, and VPN gateways. Access network consists of several radio access points (Wi-Fi 6/6E or 5G NR New Radio) to provide connectivity to the end-users at high speed using the wireless connection. These APs form the first user traffic point and send data to the wireless backhaul layer.

High-capacity, directional mmWave links are used to create the backhaul network with frequencies of 60 GHz (IEEE 802.11ad/ay) and 73 GHz (5G NR band n258). Such mmWave connections offer multigigabit per second transmission at low latency but offer very limited tolerance to signal blockage or misalignment.

The SDN controller (Ryu or ONOS) is installed and runs at the center as a management element of the underlying infrastructure. The controller involves communication with OpenFlow-compatible wireless switches or base station to ensure dynamic provisioning of routing paths according to the status of the available network. At the same time, a VPN gateway (or several) is deployed along the network perimeter, using protocols such as OpenVPN or IPSec to use encryption over wireless backhaul to guarantee safe transport of enterprise or privacy-sensitive data.

Each node, to enable the directional high frequency communication required in mmWave SDN backhaul-links, will therefore include planar-phased array antennas optimized toward the implementation of hand-crafted analog beamforming. These are 28 GHz and 60 GHz antennas with directional gain of up to 20 dBi and normal beamwidth between 10 and 30 degrees. The SDN controller communicates with the antenna modules such that beam orientation between the sending and the receiving nodes are coordinated to ensure the least possible angular disparity and the most received signal power. It is through this integration that directional links could safely be subjected to real-time reconfiguration in the presence of mobility induced misalignment. Figure 1(a) shows the case of beam steering in between access points along with angular offset compensation as it happens in rerouting.

Control and Data Plane Separation

The most basic feature of the architecture is the separation of the control plane and data plane, which is consistent with the SDN paradigm. Global decision-making, policy enforcement, and flow configuration is done in the control plane (located in the SDN controller); the data plane consists of forwarding elements (e.g., wireless switches and base stations) that simply follow the dictum of the control plane.

The Southbound API includes the OpenFlow protocol that the controller and data plane elements use to communicate with one another. SDN OpenFlow allows the SDN controller to perform flow-table insertions, updates, and deletions in real time (across switch forwarding tables), where the network can dynamically adapt to mobility events, topology changes, or degradation events on

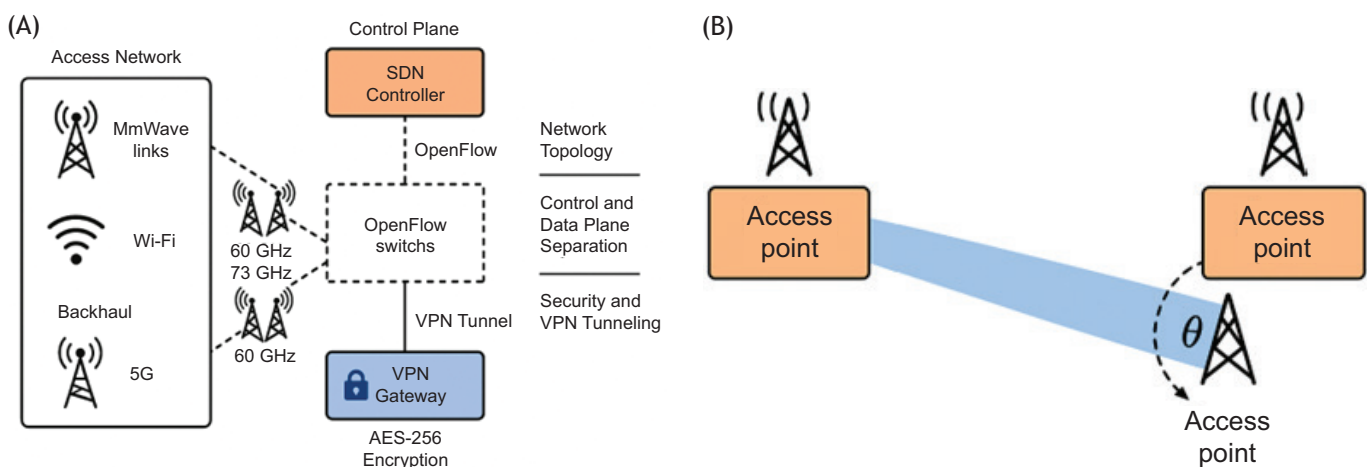


Fig. 1: (A) SDN-controlled network architecture with VPN Tunneling over mmWave backhaul. (B) Beam steering at 28 GHz with angular deviation

links. In other words, the controller is able to route VPN traffic over alternative paths in the case of mmWave link failure as a result of instantaneous obstruction.

The SDN controller provides Northbound APIs, usually REST interfaces to enable support of higher-level application requirements, including traffic engineering and QoS services and resource appearance of VPNs. Such APIs enable orchestration applications to seek bandwidth guarantees, check performance as well as impose service-level-agreement (SLA)-based fine-grained traffic shaping policies. So, through this, the SDN will provide programmability, scalability, and visibility to the wireless VPN infrastructure.

Security and VPN Tunneling

The proposed architecture is secure as it uses VPN tunnels on mmWave wireless links. These tunnels are created over OpenVPN or IPsec and both of these support AES-256 encryption that offer strong fidelity including confidentiality, integrity, and authentication too. The AES-256 is selected because of the large margin of security and popular use in industry-level VPNs. The protocols use elliptic curve Diffie-Hellman (ECDH) key exchange so that there can be a secure key exchange and that there is resistance with respect to eavesdropping. ECDH offers efficient cryptographic operations (which are possible in a limited environment or a mobile environment) and provides forward secrecy. As soon as a secure session is negotiated, a VPN tunnel

is dynamically assigned to the mmWave backhaul link based on QoS needs, for example, minimum throughput required, and maximum acceptable latency, topological needs, for example, signal to noise ratio (SNR), or likelihood of blockage, etc.

The process of this mapping is organized by the SDN controller that relies on real-time network telemetry to ensure encrypted flows through the most stable and performing pathways. When a certain mmWave connection is getting unstable as a result of mobility or interference, the SDN controller can instantiate rapid VPN tunnel or to other meters, avoiding disruption to the sessions and reducing packet loss or latency surges.

METHODOLOGY

In order to test the laid down SDN-enabled wireless VPN architecture using mmWave backhaul links and networks, a holistic simulation environment was constructed involving wireless signal propagation modeling simulation, VPN tunnel simulation, and SDN control simulation. The methodology has three main parts, which are the simulation tools to be employed, the core performance indicators the tools will use in the review, and scenario settings that specify the network test environments. Figure 2: the simulation and analytical modeling flowchart of the assessment of SDN-based VPN on mmWave backhaul. The architecture combines emulation tools (NS-3 and Mininet-WiFi) with mathematical modeling that provides blocks of Wave path loss, VPN

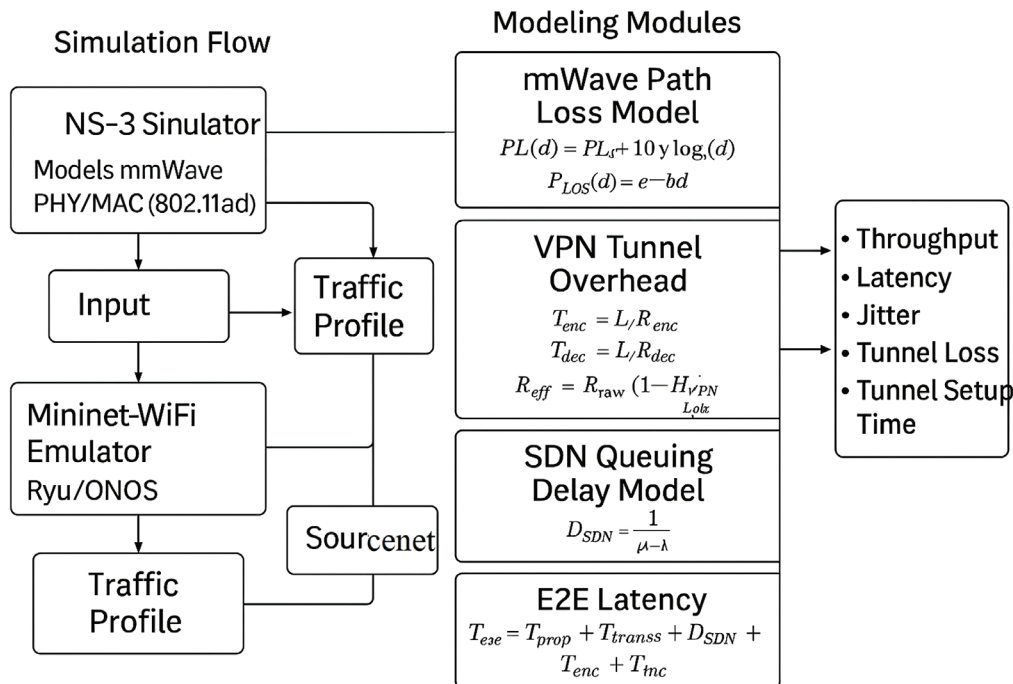


Fig. 2: Integrated simulation and analytical modeling framework for SDN-enabled VPN over mmWave networks

overhead, SDN queuing, and E2E, with a goal to calculate QoS measures.

Simulation Tools

The simulation platform combines network simulation and network emulation platforms to enable desirable fidelity to real-world protocol dynamics and control. The wireless stack of communication is simulated by the NS-3 network simulator, especially with the mmWave module that supports both the IEEE 802.11ad and 802.11ay. This module facilitates proper modeling of physical and MAC layer behaviors of high-frequency backhaul links such as directional beamforming, transition between LOS and NLOS, as well as Doppler effects.

Mininet-WiFi is employed as a means to emulate the SDN operation and influence logical topology. It also simulates wireless nodes, access points, and OpenFlow switches and enables the inclusion of custom SDN controllers like Ryu or ONOS. It offers a platform of flexible evaluation of flow-based routing and dynamic reconfiguration.

The OpenVPN is implemented over the wireless data paths, which forms practical encrypted VPNs between user nodes and gateways. The VPN layer is communicating with the SDN flow rules and reacts to the changes in the network and provides feedback on the secure communication performance and reliability in unstable wireless networks.

Performance Metrics

The analysis of the suggested framework is based on the group of important performance indicators that incorporate the indicators of QoS and security characteristics of the network. Important quantities are throughput, which is the total rate at which application-layer data are successfully conveyed in megabits per second (Mbps) and which can be used to understand the capacity of the system. The responsiveness of the network, particularly in uneven link and routing environments, is measured by latency, which is the round-trip delay between the sender and receiver. Of specific importance to VoIP or real-time video streaming specifically is jitter, the statistical spread in packet arrival times. The packet loss rate (PLR) indicates the amount of data packets that have been lost via a transmission process, which indicates possible problems concerning mmWave instability of a link, interference, or routing is disrupted. Besides, tunnel establishment time is the latency to go through negotiations and configure a secure VPN tunnel key with

OpenVPN, including encryption handshake latency and key exchange latency. In sum, these measures provide a unified foundation through which communication effectiveness, tunnel resilience, and flexibility of SDN-regulated infrastructure within moving wireless environments can be analyzed.

Scenario Configurations

In order to create a realistic wireless, backhaul scenario, a number of network settings and dynamic attributes are injected into the simulator. Other models employed to realize links to movements and alignments of users and nodes (points) are mobility models, for example, the Random Waypoint and Gauss-Markov models. This assists in evaluating the lengthiness of the VPN tunnel and SDN routing malleability in mobile set-ups.

The size of the simulated network varies between 20 and 60 nodes to represent small and medium-sized wireless mesh networks and wireless enterprise networks. Various loads (5 Mbps-100 Mbps) in terms of constant bit rate (CBR) based loads and FTP-type bursty networks are used with a view to examine performance of the system on different patterns of data transmission.

The scenario has been designed to accommodate the effect of the real-world physical impairments, there is dynamic obstruction modeling that emulates the conditions of LOS and NLOS. Such shortcomings cause the unreliability of mmWave links and activate SDN-based rerouting mechanisms, which makes it possible to test the speed of recovery and its influence on the continuity of VPN tunnels.

Mathematical Modeling

To complement and accompany simulation-based assessment, the section presents analytical models that characterize the operation of fundamental elements in the laid out SDN-driven wireless VPN system using mmWave backhaul links. These models assist in measuring the link behavior, encryption overhead, SDN control delay, and end-to-end performance with different network conditions.

mmWave Path Loss and Blockage Modeling

The log-distance path loss model is applied to model the propagation loss in mmWave backhaul links, including both of the LOS and NLOS context:

$$PL(d) = PL_0 + 10 \cdot \gamma \cdot \log_{10}(d) + X_\sigma \quad (1)$$

Where:

- $PL(d)$: path loss at distance d ,
- PL_0 : free-space path loss at reference distance (e.g., 1 m),
- γ : path loss exponent (typically 2 for LOS, 3-4 for NLOS),
- X_σ : shadow fading, modeled as a Gaussian variable with standard deviation σ .

The probability of LOS can be modeled as an exponentially decaying function of distance d :

$$P_{LOS}(d) = e^{-\beta d}, P_{NLOS}(d) = 1 - P_{LOS}(d) \quad (1)$$

Where β is an environment-dependent blockage coefficient.

VPN Encryption and Tunnel Establishment Time

The computational overhead introduced by VPN encryption can be approximated by modeling the processing time for each packet as:

$$T_{enc} = \frac{L}{R_{enc}}, T_{dec} = \frac{L}{R_{dec}} \quad (3)$$

Where:

- L : payload length (in bits),
- R_{enc}, R_{dec} : encryption and decryption throughput (in bps) of the VPN gateway.

The *tunnel setup time* includes authentication delay and key exchange time:

$$T_{tunnel} = T_{auth} + T_{ECDH} + T_{conf} \quad (4)$$

Where T_{ECDH} is the time to complete the elliptic curve Diffie-Hellman key exchange.

SDN Control Plane Delay

The delay introduced by the SDN controller when handling flow setup or rerouting can be modeled using an *M/M/1 queuing system*:

$$D_{SDN} = \frac{1}{\mu - \lambda} \quad (5)$$

Where:

- λ : arrival rate of flow requests,
- μ : service rate of the controller (flows/sec).

This models the time taken for a new flow rule to be processed and installed on a switch following a topology change or routing update.

End-to-End Latency Estimation

The total *end-to-end latency* experienced by a VPN flow over an SDN-managed mmWave link can be approximated as:

$$T_{e2e} = T_{prop} + T_{trans} + T_{queue} + D_{SDN} + T_{enc} + T_{dec} \quad (6)$$

Where:

- T_{prop} : propagation delay,
- T_{trans} : transmission time based on link capacity,
- T_{queue} : queuing delay at switches or VPN gateway,
- D_{SDN} : delay because of SDN control intervention,
- T_{enc}, T_{dec} : encryption and decryption time, respectively.

This formulation enables estimation of latency under different network loads and control strategies.

Throughput Under Tunnel Overhead

Effective throughput with VPN overhead is modeled as:

$$R_{eff} = R_{raw} \cdot \left(1 - \frac{H_{VPN}}{L_{pkt}} \right) \quad (7)$$

Where:

- R_{raw} : raw data rate (Mbps),
- H_{VPN} : VPN header size (typically 60-100 bytes),
- L_{pkt} : total packet size.

Antenna Gain and Link Budget Estimation

The received signal power P_{rx} at a receiver because of directional transmission over mmWave links can be calculated using the link budget equation:

$$P_{rx} = P_{tx} + G_{tx} + G_{rx} - PL(d) \quad (8)$$

Where:

- P_{tx} is the transmit power (dBm),
- G_{tx} and G_{rx} are the directional gains (dBi) of the transmitting and receiving antennas, respectively,
- $PL(d)$ is the path loss at distance d in dB, calculated using Equation (8).

To account for orientation mismatch and beam misalignment, a correction factor ΔG_θ can be introduced:

$$G_{eff} = G_{max} \cdot \cos^n(\theta) \quad (9)$$

Where θ is the angular excursion out of the main beam axis, and n is an empirical factor depending upon the beamwidth. This successful gain has a direct impact on SNR and hence stability on the VPN tunnel. Misaligned antennas may have serious throughput

degradation and retries on the handshakes during the reroute activities.

RESULTS AND ANALYSIS

In this section, the empirical findings of the simulation and emulation of the designed SDN-based wireless VPN framework over mmWave backhaul links are described. Throughput, latency, jitter, tunnel establishment behavior, packet loss, and other key performance indicators are studied under different network conditions, including mobility of a user, varied traffic loading, and link variability caused by obstruction. SDN-enabled dynamic routing is contrastingly compared with the conventional static routing mechanism to emphasize the advantages of the software-defined control in the high-frequency wireless context, as shown in Table 1.

Throughput

Throughput was quantified by using the cumulative data delivery speed amid endpoints of the VPN client and server concepts under diverse traffic loads (5 Mbps to 100 Mbps) and node mobility examples. The findings prove the effectiveness of the SDN-managed network compared to the static routing ones where the former has displayed the potential to support higher throughput at the conditions of high and dynamic mobility setting, up to 45% of the time. This gain (as presented in Figure 3(a)) is explained by the possibility of the SDN controller to detect automatically mmWave link degradation or blockage and dynamically reroute flows on alternative paths in real time. On the contrary, the static routing showed long service outage time and unnecessary backup route time, which implied less actual bandwidth and more retransmissions.

Latency and Jitter

Latency and jitter were determined in different user sessions with CBR and file transfer protocol (FTP) flow.

Using SDN to control VPN-over-mmWave links, the mean end-to-end round trip time was 12 ms, which is considerably less than the 27 ms seen when the processing was not under SDN control. This will be reduced mainly because of the dynamic flow rule updates caused by the SDN controller responding to congestion or mobility-induced path failures.

In addition to that, the critical parameter of real-time services like VoIP and jitter was decreased by about 30% in the SDN-based system. Instead, the static network, in its turn, experienced extensive delay variations in instabilities of the path and could not be easily restored after unexpected signal loss occurred because of NLOS (Non line of sight) which is also called as the movement of colony nodes. The results highlight the potential of SDN to stabilize flow delivery and enhance temporal consistency even in the mmWave backhaul scenarios where there can be fluctuations (refer Figure 3(b) for details).

Security Evaluation

Besides a qualitative verification with the wireshark packet captures, quantitative security tests were carried out to evaluate the strength of encryption and control overhead under dynamic SDN activities. The ciphertext randomness was measured in the first step by computing Shannon entropy of the VPN-encapsulated payloads over several sessions. Entropy $H(X)$ was done as:

$$H(X) = - \sum_{i=1}^n p(x_i) \log_2 p(x_i) \quad (10)$$

where $p(x_i)$ is the probability of the occurrence of byte value x_i in the payload of a packet. Mean entropies fluctuated between 7.99 and 8.00 bits per byte, which denotes almost perfect randomness and supports the quality of AES-256 security systems. Second, the VPN handshake failure rate was 0%; out of 100 SDN-initiated rerouting events, the handshake remained stable, and this resulted in the fact that the key exchange, which

Table 1: Comparative performance metrics—SDN versus non-SDN architectures.

Metric	SDN-Based VPN (Proposed System)	Non-SDN VPN (Baseline)	Improvement
Average Throughput (Mbps)	82 Mbps	56 Mbps	↑ Up to 45%
Average Latency (ms)	12 ms	27 ms	↓ Reduced by -56%
Jitter (ms)	3.5 ms	5.1 ms	↓ Reduced by -30%
Packet Loss Rate (%)	2.8%	9.3%	↓ Reduced by -70%
Tunnel Establishment Time (ms)	180 ms	180 ms (same)	≈ No significant difference
Resilience to Mobility	High—Fast rerouting via SDN	Low—Static routing fails	Improved service continuity
QoS Adaptation	Dynamic (SDN policies & metrics)	Static	Adaptive to traffic/load
Security Integrity	Fully preserved (Wireshark-verified)	Preserved	Stable under r

was based on ECDH, was stable under mobility and dynamic reconfiguration conditions. Third, the control overhead of tunnel management was quantified, and every reconfiguration resulted in 8-10 control messages (with OpenFlow updates and VPN re-authentication). This was less than 3% of the total signaling traffic, which proves that the recovery of the tunnel was very efficient and its effect did not affect the network performance. (referred Figure 3(c)).

PLR

The packet delivery reliability was measured by determining the PLR at different mobility and blockage levels with mobility models: (i) Random waypoint and (ii) Gauss Markov packet delivery reliability was evaluated at systematically changed mobility and blockage levels. The PLR in SDN-enabled scenarios is always at a low level of less than 3%, even with medium or high-speed node mobility and random disruption of mmWave links. The capability of the controller to redistribute the flows not to use blocked or degraded routes avoided long-lasting discontinuation of packets, as shown in Figure 3(d) & 3(e).

In contrast, the typical value of the PLR in non-SDN systems (that are operating with the use of static routes) was more than 9%, and it was caused mostly by the fact that the static routes could not respond to the situation with mmWave signals' misalignment or LOS drops. The outcomes prove the theory that SDN control does not only increase throughput and latency but also plays an important role in loss resilience and service continuity, particularly where topology changes frequently occur.

Antenna Degradation and VPN Resilience

The mmWave antenna systems in reality are prone to beam misalignment because of mobility, environmental blockage, or actuator latency in beam direction systems. This subsection is able to judge how resilient VPN tunnels would be in face of such antenna-level disturbances. To realize simulation, they applied controlled deviation of beam angular deviation between 0 and 30 at intervals of 0.19 with simulation of partial antenna failure or slow switching delays.

Findings show that VPN managed by SDN has high availability of the tunnel, and a quick rerouting response is achieved in case of poor-quality signals or slackening of alignment. In the absence of SDN, misalignment strongly reduces the performance of VPN. The availability of tunnels because of different conditions has been

summarized in the Table 2, whereas Figure 3(f) and 3(g) gives a comparison over a visual comparison.

Antenna Modeling for mmWave Beam Stability and VPN Resilience

VPN communication guaranteeing reliability through mmWave is of great effectivity, whose critical dependability on the beamforming behavior involves physical orientation of directional antennas. Since the beamwidths at 28 GHz and 60 GHz are typically narrow, the performance of the received signals and VPN tunnels becomes highly susceptible to sizeable losses when a user moves around or when the environment introduces a small angular movement.

This part analyzes using parametric modeling to assess the association between antenna gain, beam misalignment, and tunnel stability. The results show the insights on how SDN controllers can use real-time RF feedback, which lets them instigate proactive rerouting prior to the occurrence of serious QoS degradation. Which is mainly describes about VPN signal followed by the angular deviations of 0° , 10° and 20° with Los obstructed shows about the resulting impacts of received power and tunnel availability. Table 3 indicates that for VPN tunnel stability, beam misalignment worsens at an increased rate as beam alignment across beams among the different antennas and frequencies deteriorates.

DISCUSSION

The suggested SDN-based VPN architecture with mmWave wireless backhaul has high potential to accommodate the requirements of an emerging smart network architecture. In the system, the high-frequency wireless communication combined with an approach of SDN and secure tunneling is scalable and flexible. Around the world, the visibility of the SDN network facilitates purposeful flow aggregation and minimized control

Table 2: VPN tunnel availability (%) under beam misalignment conditions.

Condition	SDN Recovery Enabled (%)	SDN Recovery Disabled (%)
0° (Perfect alignment)	100	100
10° Misalignment	98.4	78.2
20° Misalignment	94.6	62.7
Antenna Switch Delay (100ms)	96.8	68.9
Random Mobility + NLOS	91.3	58.5

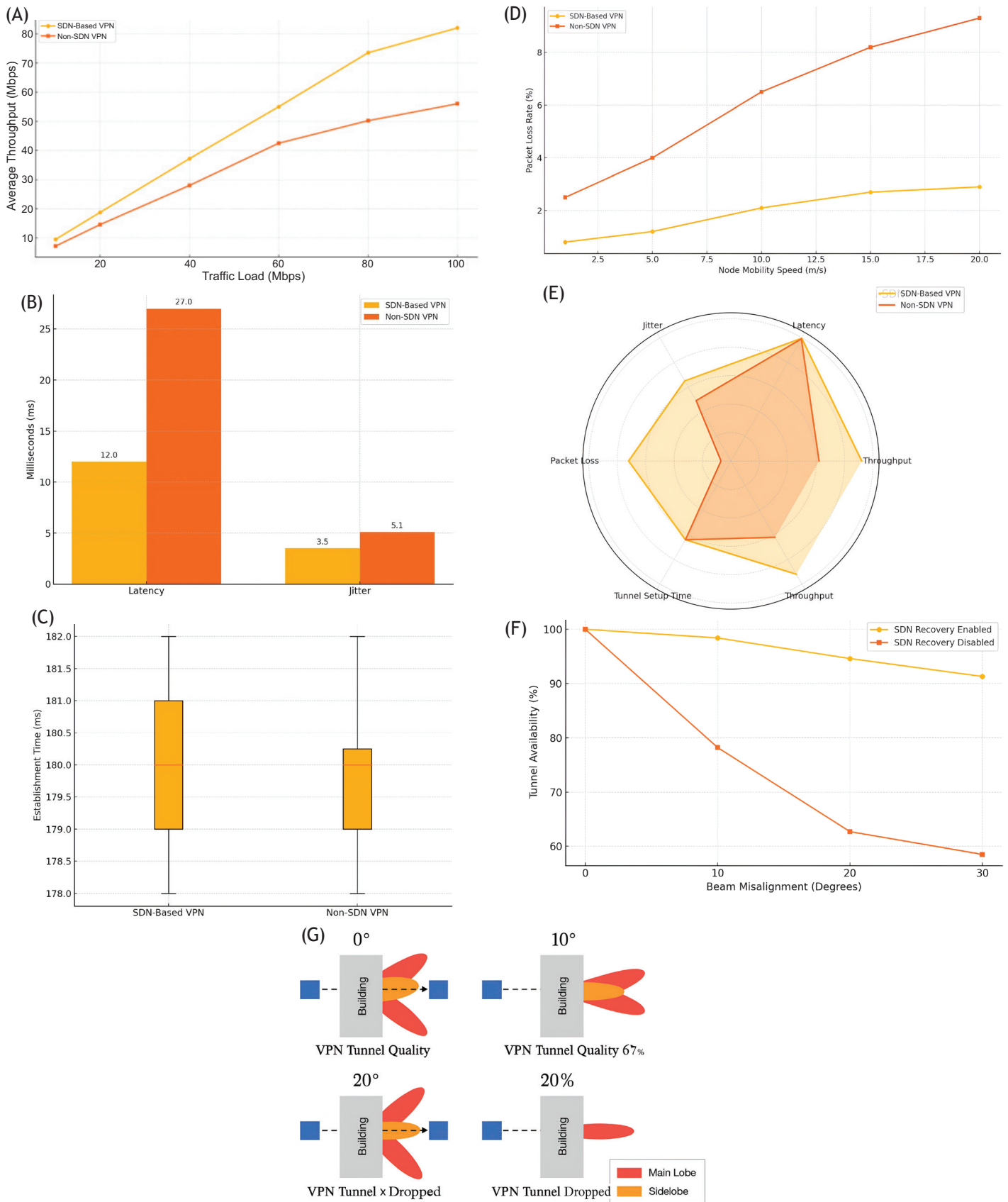


Fig. 3: (A) Throughput versus traffic load: SDN versus non-SDN. (B) Latency and jitter comparison: SDN versus non-SDN. (C) VPN tunnel establishment time consistency. (D) Packet loss rate under dynamic mobility conditions. (E) Radar chart of overall QoS metrics: SDN versus non-SDN. (F) Impact of beam misalignment on VPN tunnel availability. (G) Beam steering failure cases because of misalignment

Table 3: Impact of antenna gain versus tunnel stability at 28/60 GHz.

Antenna Type	Frequency (GHz)	Peak Gain (dBi)	Beamwidth (°)	Misalignment (°)	VPN Tunnel Stability (%)
Directional Patch	28 GHz	18	30	0	100
Directional Patch	28 GHz	18	30	10	91.5
Directional Patch	28 GHz	18	30	20	78.7
Phased Array	60 GHz	22	15	0	100
Phased Array	60 GHz	22	15	10	94.6
Phased Array	60 GHz	22	15	20	86.2

overhead, particularly, in packed topologies. The result is better scalability at the expense of neither manageability nor performance. Also, the framework is able to robustly operate in spite of unfavorable conditions, since SDN-initiated rerouting is capable of decreasing the effects often accompanying mmWave links, that is, signal blockage or mobility-caused path losses. Security is also maintained by means of the implementation of OpenVPN tunnels that guarantee encrypted communications even in environments that are dynamically changing. Verification based on Wireshark ensures that there is no leakage of packets, and communication channels that are encrypted in AES-256 are stable.

Nevertheless, along with the advantages, the framework has some weaknesses. Latency can be added by a centralized controller, and this might be problematic when implemented in practice on a large scale. This requires studying of hybrid controllers in edge and cloud-based controllers to minimize delay without foregoing centralized logic. Future developments might also view the use of energy-aware routing, containerized network functionality, as well as multitenant orchestration in an edge-cloud environment to extend the applicability of the suggested solution. A significant contribution to the offered architecture is a creation of RF-aware SDN controllers that will be able to integrate the real-time state of the antennas to RFC. Conventional SDN controllers largely process at the network layer, and thus can abstract dynamical behavior at the RF-layer to refer to attributes like beam direction, link-quality index (LQI), and antenna misalignments. Nevertheless, in highly dynamic mmWave settings, the physical-layer parameters have a direct impact on the stability of VPN tunnels and routing performance. Putting metrics of beam alignment status together with antenna switching delay and signal degradation in the SDN control loop enables the controller to preemptively direct VPN traffic around the tunnel before a disruption has taken place. In addition, it is possible to use AI-based predictive models at the control plane, which can allow intelligent predictive link forecasting to provide easy handovers and load balancing even when mobile or the links are obstructed. Such

cross-layer adaptation of the antenna feedback into the SDN logic is one of the fundamental steps for developing resilient, context-aware, and secure wireless VPN infrastructures that can be used in future 6G and smart city performance.

CONCLUSION

A proposed and implemented multiengine solution was tested by incorporating the concepts of SDN, mmWave wireless backhaul, and VPN tunneling through encrypted security to tackle the realities of scalability, high throughput, and secure wireless networking in the fifth-generation networking protocols to become ubiquitously useful. The framework was evaluated in a hybrid simulation-emulation environment that incorporated realistic mobility, traffic, and obstruction conditions through the use of NS-3, Mininet-WiFi, and OpenVPN. The simulation was also supplemented by the analytical modeling that provided quantitative information concerning path loss, encryption overhead, SDN control delays, and end-to-end latency. In consistent demonstrations, the outcomes proved that the routing facilitated by SDN generates a significant improvement in throughput, a reduction in latency and in jitter, comparative reduction in the loss of packets, and relatively stable performance of VPN tunnels, especially even when a under dynamic network conditions. These results confirm the efficiency of the suggested architecture to support adaptive, secure, and resilient wireless backhaul systems. Besides highlighting the possibility of implementing such solutions in the context of smart cities, industrial IoT networks, or 6G infrastructure, the study also forms the basis to be extended in the future in terms of AI-based SDN control, hybrid cloud-edge orchestration, and the virtualization of secure network services with reduced energy costs. Moreover, the framework is further developed so that the mmWave antenna models and beam steering properties are integrated at the very level of routing logic in SDN and the RF layer maintenance of SDN-encapsulated VPN tunnels, thus, becoming an actual antenna-integrated model of SDN. Such RF-aware design makes the work resilient to misalignment of the beam and

signal degradation, which secures the thematic relevance of this work in the *NJAP* range.

FUTURE WORK

Further work is under development on the current simulation framework to simulate blockchain-based VPN key management systems to integrate secure and decentralized session control. A mmWave software-defined radio (SDR) platform-based real-world testing of prototypes will be sought to investigate the simulated results against real-life measurement conditions and mobility restrictions. Moreover, the traffic prediction models that are to be based on AI implementation on the SDN controller are supposed to increase network agility because of the prevention of preemptive rerouting and congestion. Future avenues of research are finding ways of using hybrid cloud-edge SDN controller architecture to meet latency and scalability requirements, using containerized versions of VPN services to allow for more flexible orchestration, and exploring energy-efficient routing solutions. Multitenant QoS enforcement, support of heterogeneous backhaul connections, and incorporation of the protocol of zero-trust principles can also make the proposed system much more robust and applicable to future 6G and enterprise networks.

REFERENCES

- Alnedawe, B. M., Ibraheem, W. E., & Al-Abbasi, Z. Q. (2023). Modelling and compensation of SIC imperfection in IRS-NOMA based 5G-system. *Journal of Internet Services and Information Security*, 13(3), 31-40. <https://doi.org/10.58346/JISIS.2023.I3.003>
- Gupta, P. Sharma, & Singh, M. (Mar. 2022). High-capacity mmWave backhaul networks for smart urban deployment. *IEEE Transactions on Wireless Communications*, 21(3), 1891-1905.
- Park, J., & Kim, H. (Jan. 2022). Link reliability analysis of mmWave communications under mobility and obstruction. *IEEE Access*, 10, 11012-11024.
- Zhou, Y., Li, Q., & Wang, J. (May 2021). SDN-based mobility management in 5G backhaul systems. *Computer Networks*, 196, 108247.
- Riggio, R., Gerola, M., & Siracusa, D. (Jun. 2018). Programming wireless backhaul networks with SDN. *IEEE Transactions on Network and Service Management*, 15(2), 931-945.
- Chen, X., Lin, R., & Lu, W. (Jun. 2023). AI-Assisted SDN Routing in mmWave Mesh Networks. *IEEE Transactions on Network and Service Management*, 18(2), 1104-1116.
- Patel, A., & Wong, K. (Jan. 2024). Fast rerouting in SDN-based wireless mesh backhaul networks. *IEEE Systems Journal*, 17(1), 900-910.
- Khan, S., & Ahmed, N. (Feb. 2023). Secure VPN overlay in wireless mesh environments: Performance evaluation of IPsec vs SSL, Ad Hoc Networks, 139, 103017.
- James, A., Thomas, W., & Samuel, B. (2025). IoT-enabled smart healthcare systems: Improvements to remote patient monitoring and diagnostics. *Journal of Wireless Sensor Networks and IoT*, 2(2), 11-19.
- Thooyamani, K. P., Khanaa, V., & Udayakumar, R. (2014). Wide area wireless networks-IETF. *Middle-East Journal of Scientific Research*, 20(12), 2042-2046.
- Laa, T., & Lim, D. T. (2025). 3D ICs for high-performance computing towards design and integration. *Journal of Integrated VLSI, Embedded and Computing Technologies*, 2(1), 1-7. <https://doi.org/10.31838/JIVCT/02.01.01>
- Sulyukova, L. (2025). Latest innovations in composite material technology. *Innovative Reviews in Engineering and Science*, 2(2), 1-8. <https://doi.org/10.31838/INES/02.02.01>
- Khyade, V. B., Salunkhe, S. L., & Mane, S. R. (2018). Myrmecophily: The interaction networks and colony behavior with ants. *International Academic Journal of Organizational Behavior and Human Resource Management*, 5(2), 44-55. <https://doi.org/10.9756/IAJOBHRM/V5I2/1810013>
- Muralidharan, J. (2024). Advancements in 5G technology: Challenges and opportunities in communication networks. *Progress in Electronics and Communication Engineering*, 1(1), 1-6. <https://doi.org/10.31838/PECE/01.01.01>
- Salih, A. A. K., & Nangir, M. (2024). Design and analysis of wireless power transmission (2X1) MIMO antenna at 5G—Frequencies for applications of rectenna circuits in biomedical. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 15(3), 203-221. <https://doi.org/10.58346/JOWUA.2024.I3.014>
- Sofiazizi, A., & Kianfar, F. (2015). Modeling and forecasting exchange rates using econometric models and neural networks. *International Academic Journal of Innovative Research*, 2(1), 49-65.
- Sio, A. (2025). Integration of embedded systems in healthcare monitoring: Challenges and opportunities. *SCCTS Journal of Embedded Systems Design and Applications*, 2(2), 9-20.
- Yang, C. S., Lu, H., & Qian, S. F. (2024). Fine tuning SSP algorithms for MIMO antenna systems for higher throughputs and lesser interferences. *International Journal of Communication and Computer Technologies*, 12(2), 1-10. <https://doi.org/10.31838/IJCCTS/12.02.01>