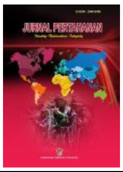

Jurnal Pertahanan: Media Informasi tentang Kajian dan Strategi Pertahanan yang Mengedepankan Identity, Nasionalism dan Integrity
Vol. 12 No. 1 (2026) pp.38-52
https://jurnal.idu.ac.id/index.php/DefenseJournal

Network Security Analysis Using PPTP and VPN on the Unmanned Aerial Vehicle PUNA MALE Simulation Prototype

Bita Parga Zen[1*], Iwan Nofi Yono Putro[2], Faisal Dharma Adhinata[3]
[1]Universitas Ma Chung
[2]Badan Riset dan Inovasi Nasional
[3]Universitas Telkom

bita.parga@machung.ac.id[1*], iwan.nofi.yono.putro@brin.go.id[2], faisaldharma@telkomuniversity.ac.id[3]
*Corresponding Author

Article Info

Article history:
Received : April 17, 2025
Revised : April 25, 2026
Accepted : April 30, 2026

Keywords:
Network Security,
PPTP,
Quality of Service,
UAV Puna Male,
VPN

DOI:
http://dx.doi.org/10.33172/jp.v12i1.19915

Abstract

Reliable and secure communication is a fundamental requirement for Medium-Altitude Long-Endurance (MALE) Unmanned Aerial Vehicle (UAV) operations, where real-time data transmission must be maintained despite network instability. Internet-Protocol (IP)-based communication networks commonly used in UAV systems are susceptible to delay, jitter, and packet loss, which can degrade mission performance in surveillance and reconnaissance scenarios. This study investigates the capability of a Point-to-Point Tunneling Protocol (PPTP) Virtual Private Network (VPN) to simultaneously enhance communication security and preserve network Quality of Service (QoS) for PUNA MALE UAV communications. A Hardware-in-the-Loop (HIL) simulation environment implemented in GNS3 was developed to emulate realistic operational conditions. Network performance was evaluated using ICMP, TCP, and UDP protocols, with metrics including delay, jitter, and packet loss. Experimental results show that ICMP achieved an average jitter of 0.0879 ms with zero packet loss, while TCP demonstrated superior stability compared to UDP, which exhibited a packet loss rate of 1.9708%. The findings reveal that PPTP VPN deployment can maintain stable QoS performance while providing secure communication channels, indicating its feasibility as a lightweight security solution for UAV communication systems operating in controlled network environments. This work provides empirical evidence supporting the secure integration of VPNs for reliable MALE UAV data communication architectures.

2549-9459/Published by Indonesia Defense University. This is an open-access article under the CC BY-NC license (https://creativecommons.org/licenses/by-nc/4.0/)

INTRODUCTION

Indonesia, as an archipelagic nation, faces significant challenges in maintaining effective territorial and maritime control given its vast oceanic expanse. The extensive maritime domain provides abundant natural resources; however, it also increases vulnerability to illegal fishing, resulting in considerable economic losses (Firmansyah et al., 2020). Consequently, maritime defense strategies must continuously adapt to technological advancements. One of the critical technological solutions supporting maritime surveillance operations is the utilization of uncrewed aerial vehicles (UAVs) equipped with modern sensing capabilities (Adil et al., 2024; Tomaszewski et al., 2022).

The PUNA MALE (Medium-Altitude Long-Endurance) design aims to fly for 24 hours, carrying out more detailed and accurate monitoring, reconnaissance, and mapping (ISR: Intelligence, Surveillance, and Reconnaissance) at an altitude of 3,000–9,000 m. The aircraft developed by the PUNA MALE National Research Program (PRN) consortium adopts a shape and configuration similar to the CH-4 aircraft (Debe & Ras, 2022). The combatant payload configuration for surveillance missions removes weapon system components and prioritizes the integrating of ISR sensors. These long-endurance ISR operations require reliable communication links and integration with satellite communication systems, thereby emphasizing the critical role of secure data transmission, communication network protection, and VPN-based security mechanisms to ensure operational integrity and information confidentiality (Hassan et al., 2022).

The need for a communication line for reliable data transfer will raises fundamental questions, including how to configure data transfer frequencies, the architecture of the data communication system, the choice of communication protocol, how to transmit data, how to manage the data communication lines, and the interface specifications. Therefore, preparing the architecture or topology of the long-range communication system and selecting its constituent components must be carried out from the start to produce a reliable communication system during gflight operations (Yue et al., 2020). The flight mission of a long-endurance UAV is closely related to range and the real-time processing of on-board data (Sulistiya et al., 2023).

In general, the concept of flight operations for PUNA MALE is shown in Figure 1. The proposed framework presents a satellite-assisted command, control, communication, and navigation architecture that enables reliable UAV operations beyond Visual Line-of-Sight (BVLOS). Initially, the UAV operates through a Direct Line-of-Sight (DLOS) link with the Ground Control Station (GCS) for real-time command and telemetry exchange. Upon exceeding LOS coverage, communication transitions to a Satellite Communication (SATCOM) system, where satellites relay bidirectional data between the UAV and the GCS over extended distances. Navigation is continuously supported by Global Navigation Satellite Systems (GNSS), providing accurate positioning and trajectory information.

The integration of satellite communication and navigation ensures operational continuity and situational awareness in areas with limited terrestrial infrastructure. Additionally, autonomous fail-safe mechanisms enable the UAV to perform predefined actions, such as loitering or Returning to Launch (RTL), in the event of communication loss. This hybrid architecture enhances operational range, reliability, and mission effectiveness for applications including surveillance, maritime monitoring, disaster response, and defense operations.

UAV communication is identical to radio communication; in this is known as Line-of-Sight (LOS) communication. In the context of UAV communications, satellite communications are also used, often referred to as Beyond Line-of-Sight (BLOS) communications (Tomaszewski et al., 2022). Popular mobile communication satellites use the L-band; however, its narrow channel capacity makes it diffult to utilize for high-bandwdth requirments. Satellit choices for large bandwidth are available in the C-band, and Ka-band, although these three bands lack specific regulations for mobile satellite communications (MSC) (Hartono & Darmawan, 2019; Mistri et al., 2023).

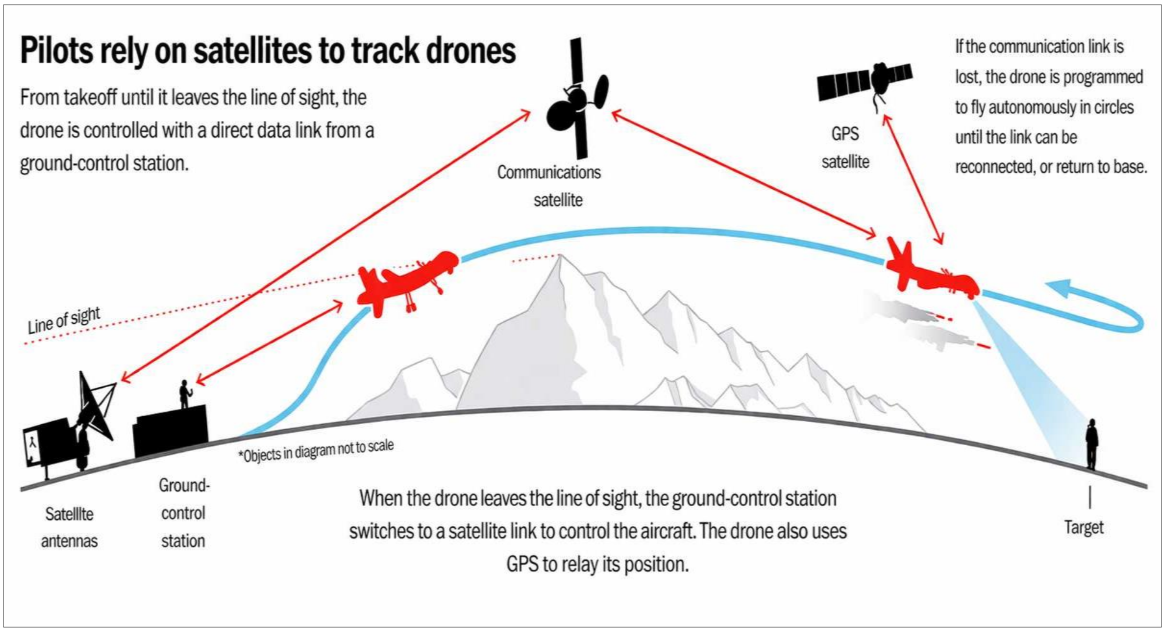

Figure 1. Outline of the PUNA MALE Flight Operation Concept
(de Zoysa & Siriwardana, 2024)

One way to test network quality on the PUNA MALE UAV is to perform a QoS (Quality of Service) analysis. QoS is a technique for optimizing network performance without altering the underlying physical network architecture (Gentile et al., 2024; Hassan et al., 2022). The essential QoS parameters include jitter, delay, and packet loss, which are utilized to assess network reliability. In addition to performance, network security requires significant attention; therefore, VPN implementation is employed to establish a private and secure communication channel over a public network or the Internet (Nurrobi et al., 2020; Suryani et al., 2018). Communication quality standards are generally regulated under the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) G.1010 standard (ITU-T, 2001) (Mumtaz et al., 2019; Wang et al., 2022).

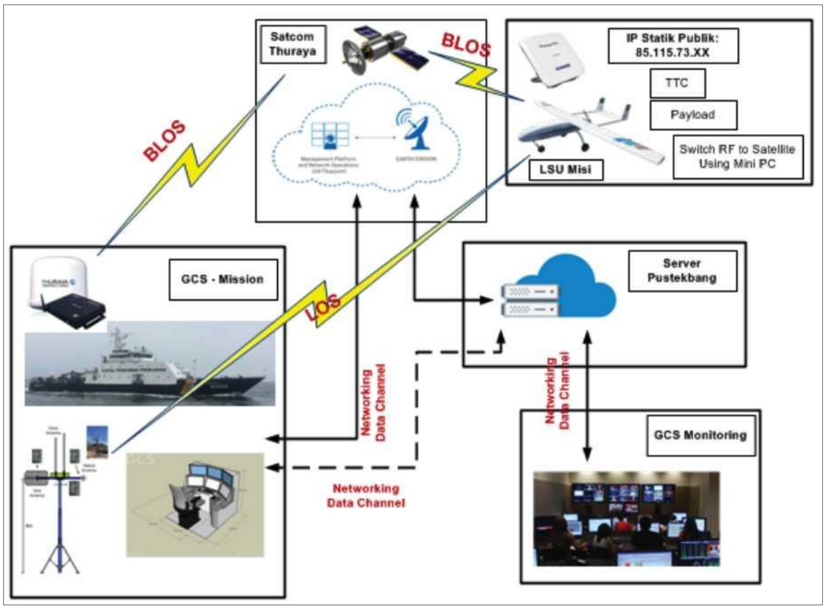

Figure 2. The operation concept of a Long-Range Communication System using satellites (Iida & Wakana, 2003)

This study uses the GNS3 network simulator integrated with the Hardware-in-the-Loop (HIL) simulations technique. This simulation utilizes external hardware to support PUNA MALE UAV research through the simulation and analysis of Quality of Service (QoS). To enhance data security, Point-to-Point Tunneling Protocol (PPTP) VPN is implemented. The PPTP protocol, as defined by the PPTP Forum, is capable of assigning channels, monitoring the status of the communication server, managing in-band signaling, initiating outgoing calls, and alerting the server during call arrivals or disconnections while enabling biderectional user data transmission (Padhiary et al., 2025; Shim et al., 2025; Yan, 2024).

The primary purpose of this study is to investigate the effectiveness of VPN implementation as a secure communication mechanism while maintaining acceptable QoS performance for MALE UAV operations. Despite the increasing adoption of satellite-assisted UAV communication for Beyond Visual Line-of-Sight (BVLOS) missions, challenges remain in ensuring both communication reliability and data security over long-range transmission links. Existing studies primarily focus on communication performance or security mechanisms in isolation, creating a research gap in evaluating their combined impact on operational UAV networks. Therefore, this research aims to analyze how VPN-based security integration influences critical QoS parameters, including delay, jitter, and packet loss, in long-range UAV communication systems.

METHODS

Quality of Service (QoS)

Quality of Service (QoS) refers to a set of network management mechanisms designed to measure, control, and guarantee communication performance by regulating key parameters such as throughput, delay, jitter, and packet loss. The primary objective of a QoS framework is to optimize these parameters to ensure network reliability without altering the underlying physical infrastructure. One widely recognized standard for evaluating network performance is the Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) TR 101329 V2.1.1 (1999-06), published by the European Telecommunications Standards Institute (ETSI) (QoS) standards (Marpaung et al., 2024).

Throughput: Throughput is calculated by dividing the total number of successfully received packets at a destination over a specific time interval by the duration of that period. While bandwidth represents the theoretical maximum capacity of a network, throughput measures the actual data transfer rate achieved under operational conditions (Adil et al., 2024). In practical UAV communication scenarios, throughput is frequently associated with effective bandwidth utilization.

$$Throughput=\frac{Data\ packet\ received}{Observation\ time} \tag{1}$$

$$Throughput=\frac{Throughput}{Bandwidth\ Total}\times 100\% \tag{2}$$

Table 1. Throughput

Throughput Category	Throughput	Index
Very good	76% - 100%	4
Good	51% - 75%	3
Medium	26% - 50%	2
Bad	< 25%	1

Source: (ETSI, 2006)

Packet loss: Packet loss is the inability of an IP packet to reach its destination within a netword. In the implementation of IP-based networks, the packet loss rate must be minimized to ensure data integrity and operational reliability. Based on the TIPHON standard, network degradation levels are categorized into four performance types, as detailed in Table 2. The equation for calculating packet loss is:

$$Packet\ Loss=\frac{packets\ sent\ -\ packets\ received}{packets\ received}\times 100 \tag{3}$$

Table 2. Packet Loss

Degradation Category	Packet Loss	Index
Very good	0% - 2%	4
Good	3% - 14%	3
Medium	15% - 24%	2
Bad	>25%	1

Source: (ETSI, 2006)

Delay: is the total time required for a packet to travel across a network from the source to its intended destination. In UAV communications, minimizing delay is critical for ensuring real-time command and telemetry synchronization. The average delay is calculated using the following equation:

$$Average\ delays = \frac{Total\ delays}{Total\ packets\ received} \quad (4)$$

Table 3. Latency

Latency Category	Delays	Index
Very good	<150 ms	4
Good	150 s/d 300 ms	3
Medium	300 s/d 450 ms	2
Bad	>450 ms	1

Source: (ETSI, 2006)

The network topology concists of eight distinch routers. Public routers, which are external to the server and client nodes, are identified by a gray background, while BRIN routers are highlited with a yellow background, and client-side routers are marked in green. In this experimental setup, Cloud3 acts as the client, while Cloud2 functions as the BRIN server. Each node represents a physical hardware component integrated into the GNS3 simulation environment via the Hardware-in-the-Loop (HIL) system.

To implement this topology, MikroTik Cloud Core Routers (CHR) are deployed within the QEMU hypervisor in GNS3. Each router is interconnected and configured according to the mission requirements. During the IP address assignment phase, a combination of private and public IP addresses is utilized to emulate realistic wide-area network (WAN) conditions (Andriyani et al., 2023; Luo et al., 2020; Yue et al., 2020; Zen et al., 2022).

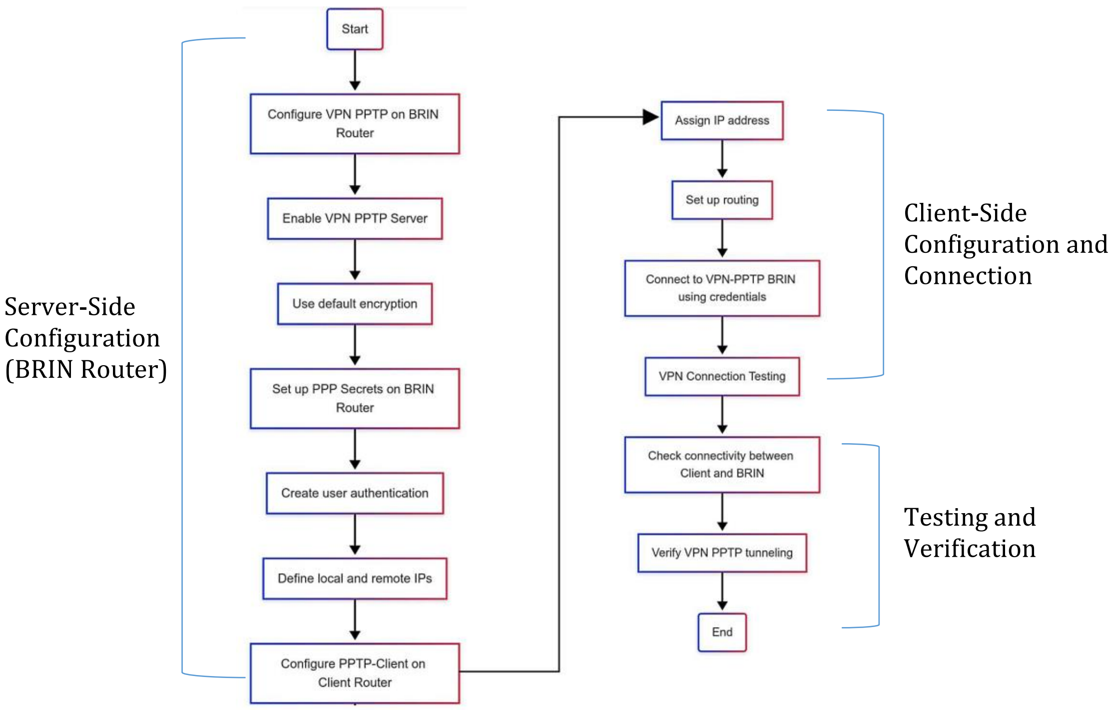

Figure 3. Research Flow
(By the author)

PPTP VPN Implementation and Configuration Parameters

The implementation of the PPTP VPN transitioned from a procedural setup to experimental execution by defining specific operational parameters. The VPN tunnel was established between the BRIN Router, acting as the VPN Server, and the Client Router. For tunnel security, the authentication phase utilized the MS-CHAPv2 protocol, while data payload encryption was enforced using 128-bit MPPE (Microsoft Point-to-Point Encryption), which is the standard mechanism for securing PPTP links on MikroTik RouterOS.

Furthermore, the IP addressing scheme for the virtual interface was rigidly defined to ensure predictable routing. Based on the simulation topology, the VPN tunnel used the local server IP 10.11.6.1/32 and assigned the remote client IP 10.11.6.2/32. To ensure that all relevant traffic traversed the secure tunnel rather than the public routing table, static routing policies were configured on the client router. Before initiating the QoS evaluation, tunnel integrity and payload encapsulation were empirically verified through ICMP ping sweeps and packet inspection using Wireshark, confirming that the VPN tunnel was fully operational and secure.

RESULT AND DISCUSSION

Network Topology Design and IP Address Classification

In Figure 4 shows the topological design. The network consists of eight distinct routers, where public routers, which are not part of the server or client nodes, are identified by a gray background. Meanwhile, BRIN routers are identified by a yellow background, client-side routers by a green background. Cloud3 serves as the client, and Cloud2 serves as the BRIN server in this experiment. Each node represents a physical hardware component integrated into the GNS3 simulation environment via the Hardware-in-the-Loop (HIL) system. A MikroTik router is deployed within the QEMU system in GNS3, with each router interconnected and configured according to the operational requirements. Private IPs and several public IPs are utilized for certain routers during the IP address classification stage.

Figure 4. Topology Design

The network service quality testing scheme uses the ICMP, TCP, and UDP protocols. The ICMP protocol is used to ping the Server-BRIN IP address as the destination. While testing, the TCP and UDP protocols use Iperf3 installed on the server and client. Each experimental trial was conducted for a duration of 100 seconds and repeated ten times to ensure data consistency and obtain a comprehensive dataset for QoS analysis. The service quality analysis is performed using Wireshark by capturing traffic on both the client and server nodes before testing begins.

Sending a test ping packet to the server with the command "ping 10.10.10.90" for 100 seconds tests the ICMP protocol (also known as "test ping"). Ten tests are run in total. Figure 5 displays ICMP protocol testing commands. For TCP evaluation, iperf3 was used to transmit packets to the server via port 5000 using the command "iperf3 -c 10.10.9.90 -p 5000 -t 100 > filename.txt" (Figure 6). The iperf3 application is used to test the UDP protocol by sending packets to the server on port 5000, while using the same bandwidth as when testing the TCP protocol with the command "iperf3 -c 10.10.9.90 -p -b bandwidth result -t 100 -u > filename.txt", as illustrated in Figure 7.

```
64 bytes from 10.10.9.90: icmp_seq=88 ttl=61 time=6.03 ms
64 bytes from 10.10.9.90: icmp_seq=89 ttl=61 time=10.2 ms
64 bytes from 10.10.9.90: icmp_seq=90 ttl=61 time=10.5 ms
64 bytes from 10.10.9.90: icmp_seq=91 ttl=61 time=9.16 ms
64 bytes from 10.10.9.90: icmp_seq=92 ttl=61 time=11.4 ms
64 bytes from 10.10.9.90: icmp_seq=93 ttl=61 time=11.0 ms
64 bytes from 10.10.9.90: icmp_seq=95 ttl=61 time=10.6 ms
64 bytes from 10.10.9.90: icmp_seq=96 ttl=61 time=10.6 ms
64 bytes from 10.10.9.90: icmp_seq=97 ttl=61 time=11.6 ms
64 bytes from 10.10.9.90: icmp_seq=98 ttl=61 time=11.9 ms
64 bytes from 10.10.9.90: icmp_seq=99 ttl=61 time=5.53 ms
64 bytes from 10.10.9.90: icmp_seq=100 ttl=61 time=10.6 ms
^C
--- 10.10.9.90 ping statistics ---
100 packets transmitted, 99 received, 1% packet loss, time 99189ms
rtt min/avg/max/mdev = 5.396/10.570/50.437/4.932 ms
```

Figure 5. ICMP Protocol Testing

```
[  5]  89.00-90.00  sec  2.88 MBytes  24.1 Mbits/sec   6   17.7 KBytes
[  5]  90.00-91.00  sec  2.34 MBytes  19.6 Mbits/sec   5   32.8 KBytes
[  5]  91.00-92.00  sec  2.52 MBytes  21.1 Mbits/sec   3   39.6 KBytes
[  5]  92.00-93.00  sec  2.34 MBytes  19.6 Mbits/sec   6   32.8 KBytes
[  5]  93.00-94.00  sec  2.34 MBytes  19.6 Mbits/sec   6   32.8 KBytes
[  5]  94.00-95.00  sec  2.70 MBytes  22.7 Mbits/sec   6   15.0 KBytes
[  5]  95.00-96.00  sec  2.16 MBytes  18.1 Mbits/sec   6   21.8 KBytes
[  5]  96.00-97.00  sec  2.16 MBytes  18.1 Mbits/sec   5   25.9 KBytes
[  5]  97.00-98.00  sec  2.34 MBytes  19.6 Mbits/sec   7   25.9 KBytes
[  5]  98.00-99.00  sec  2.70 MBytes  22.6 Mbits/sec   7   25.9 KBytes
[  5]  99.00-100.00 sec  1.98 MBytes  16.6 Mbits/sec   6   24.6 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-100.00 sec   252 MBytes  21.1 Mbits/sec  491             sender
[  5]   0.00-100.00 sec   251 MBytes  21.1 Mbits/sec                  receiver

iperf Done.
```

Figure 6. TCP Protocol Testing

```
[  5]  89.00-90.00  sec  2.52 MBytes  21.1 Mbits/sec  1887
[  5]  90.00-91.00  sec  2.52 MBytes  21.1 Mbits/sec  1887
[  5]  91.00-92.00  sec  2.51 MBytes  21.1 Mbits/sec  1886
[  5]  92.00-93.00  sec  2.52 MBytes  21.1 Mbits/sec  1887
[  5]  93.00-94.00  sec  2.52 MBytes  21.1 Mbits/sec  1887
[  5]  94.00-95.00  sec  2.51 MBytes  21.1 Mbits/sec  1886
[  5]  95.00-96.00  sec  2.52 MBytes  21.1 Mbits/sec  1887
[  5]  96.00-97.00  sec  2.51 MBytes  21.1 Mbits/sec  1886
[  5]  97.00-98.00  sec  2.52 MBytes  21.1 Mbits/sec  1887
[  5]  98.00-99.00  sec  2.52 MBytes  21.1 Mbits/sec  1887
[  5]  99.00-100.00 sec  2.51 MBytes  21.1 Mbits/sec  1886
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval          Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-100.00 sec   252 MBytes  21.1 Mbits/sec  0.000 ms  0/188661 (0%)  sender
[  5]   0.00-100.00 sec   250 MBytes  20.9 Mbits/sec  0.310 ms  1587/188661 (0.84%)  receiver

iperf Done.
```

Figure 7. UDP Protocol Testing

Delay, jitter, and packet loss metrics are used in the analysis of Quality of Service (QoS) test results for each tested protocol, particularly ICMP, TCP, and UDP.

Throughput

The bandwidth attained during each test of the TCP and UDP protocols is known as the throughput. Throughput results are given in Figure 8.

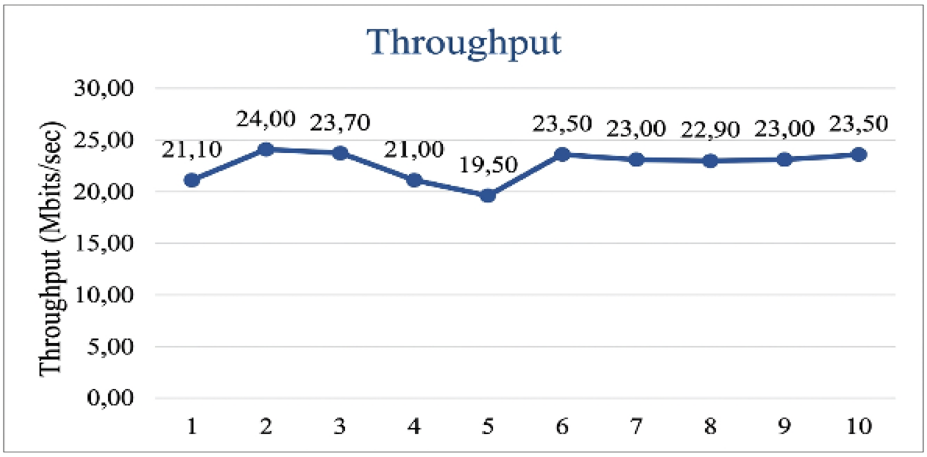

Figure 8. TCP and UDP Throughput Graph
(Processing by author)

ICMP Protocol

The results of the delay, jitter, and packet loss tests on the ICMP protocol are respectively given in Figure 9, Figure 10, and Figure 11. Based on the experimental results, the ICMP protocol exhibited a maximum average delay of 7.7900 ms and a minimum average delay of 2.4900 ms, resulting in a cumulative average delay of 4.4775 ms.

Regarding the jitter parameter, the data showed a maximum average of 2.8200 ms and a minimum of 0 ms, with an overall average jitter of 0.0879 ms. In the ICMP protocol packet loss parameter, no lost packets were found.

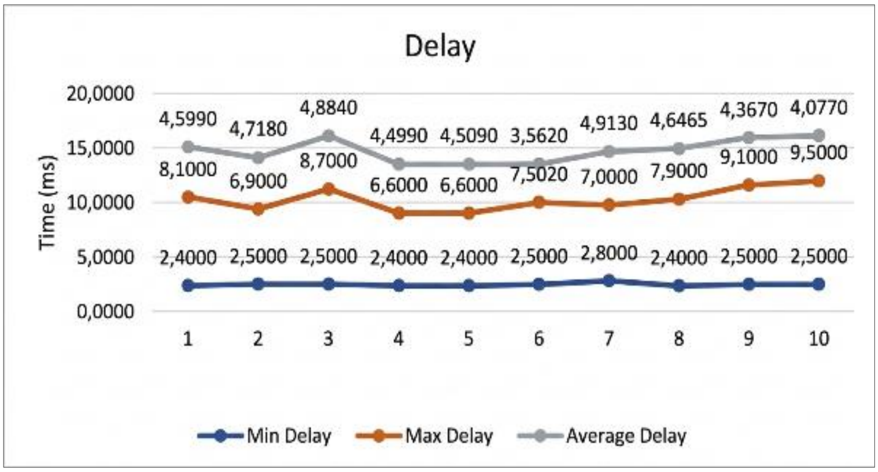

Figure 9. ICMP Delay Graph

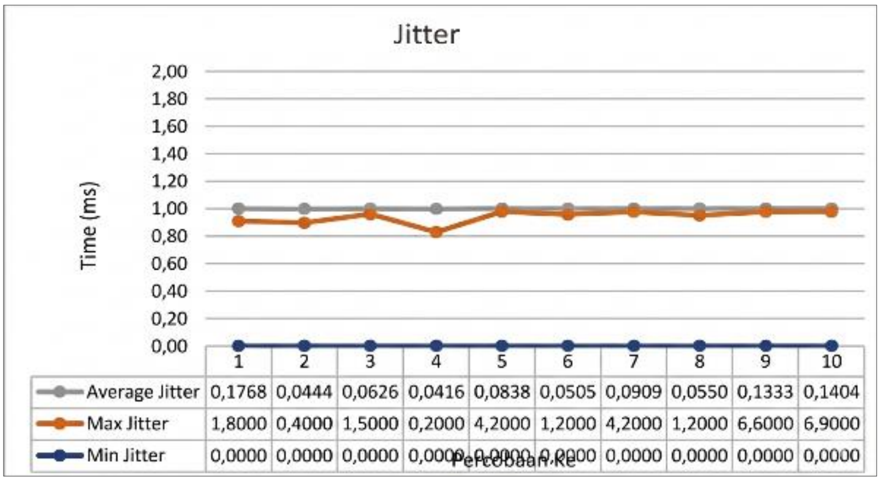

Figure 10. ICMP Jitter Graph

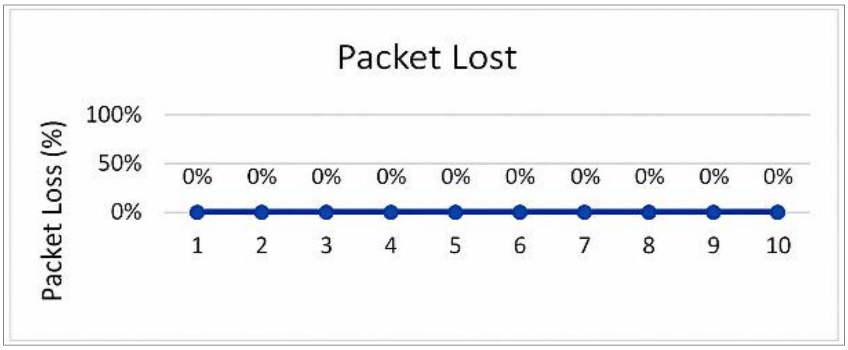

Figure 11. ICMP Packet Loss Graph

TCP Protocol

Figures 12, 13, and 14 illustrate the test results for TCP's delay, jitter, and packet loss, respectively. The test results for the TCP protocol show an average maximum delay of 70.3700 ms, a minimum average delay of 1.4800 ms, and a total average delay of 5.0873 ms. In terms of the jitter parameter, the maximum and minimum values were recorded at 67.9400 ms and 0 ms, respectively, with a remarkably low overall average of 0.0009 ms.

For packet loss parameters in the TCP protocol, the average total packet loss was 0.3507%. The highest packet loss was in the eighth experiment, and the lowest was in the ninth. The minimal packet loss observed is a direct outcome of TCP's robust mechanisms, such as retransmission of lost segments and flow control, which collectively ensure that data is delivered completely and in the correct sequence. This inherent reliability is crucial for critical applications, particularly in contexts such as UAV communications, where data loss can lead to severe operational consequences.

For instance, Nurrobi et al. (2020) emphasize that low packet loss and stable delay are primary indicators of network health. Furthermore, the necessity for reliable data transport in complex aerial systems, as underscored by Luo et al. (2020) in their research on hypersonic UCAV swarms, highlights the invaluable role of TCP's guaranteed delivery is maintaining the integrity of mission-critical communication links.

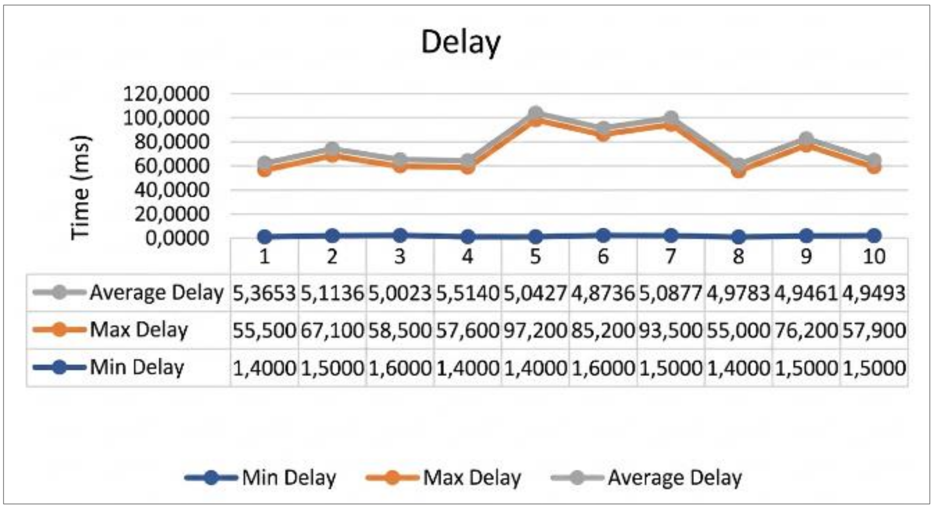

Figure 12. TCP Delay Graph

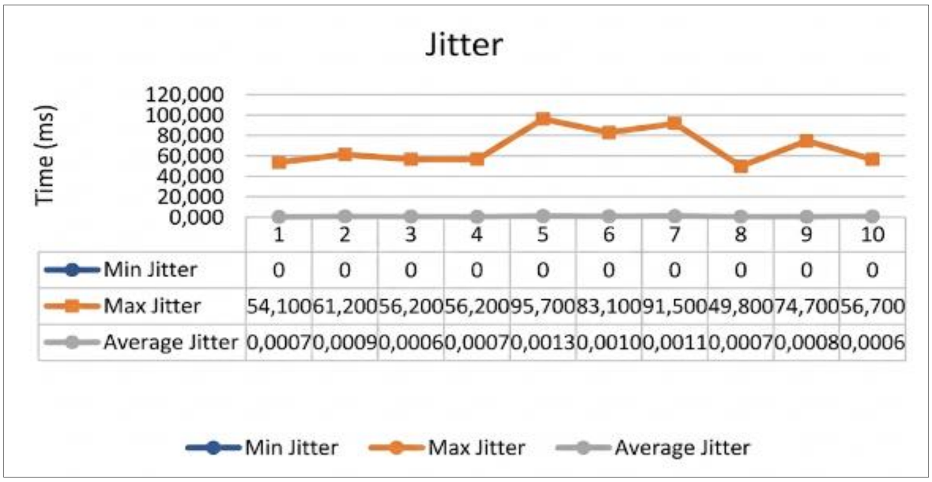

Figure 13. TCP Jitter Graph

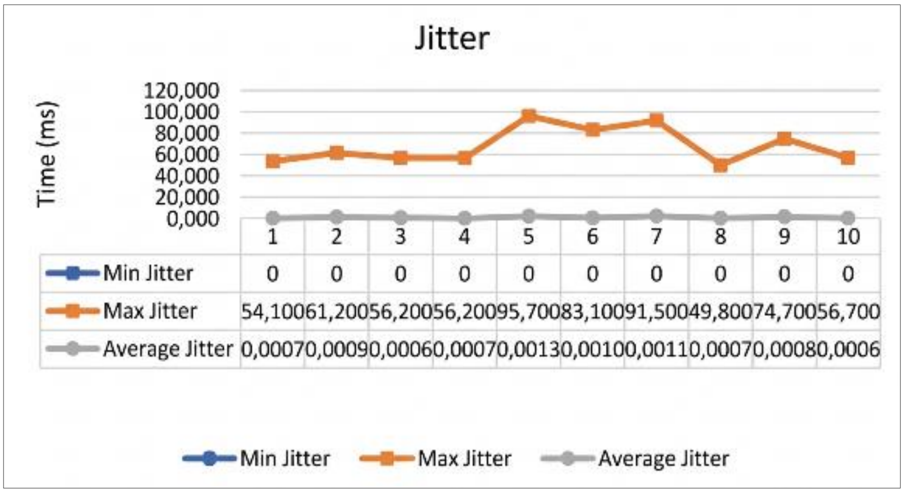

Figure 14. TCP Packet Loss Graph

UDP Protocol

The results of the delay, jitter, and packet loss tests on the UDP protocol are in Figure 15, Figure 16, and Figure 17. The experimental data for the UDP protocol shows a maximum average delay of 63.8400 ms and a minimum average delay of 1.3100 ms, with a cumulative average delay of 2.7178 ms. Regarding the jitter parameter, the maximum average was recorded at 66.2500 ms, while the minimum was 0.00 ms, resulting in an overall average jitter of 0.0007 ms.

For the packet loss parameter, the UDP protocol, protocol yielded an average total loss of 1.9708%. The highest packet loss was observed during the eighth trial, whereas the lowest loss rates occurred during the second, sixth, and ninth trials.

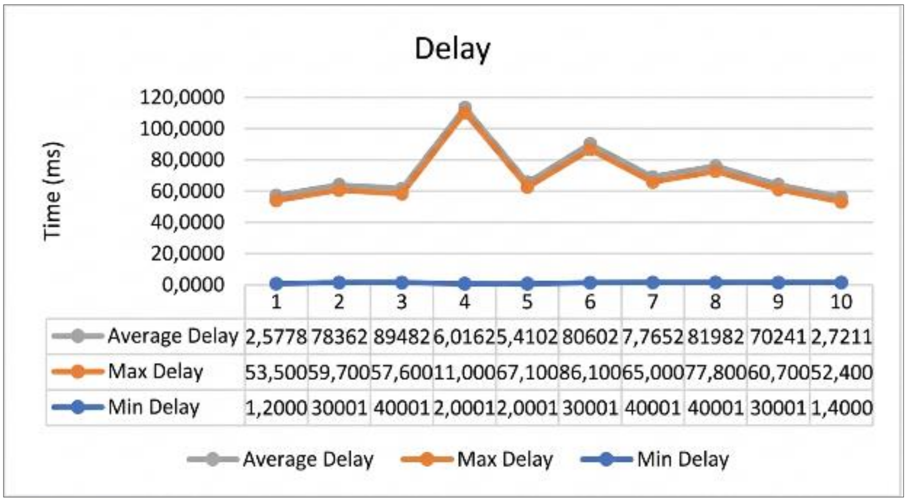

Figure 15. UDP Delay Graph

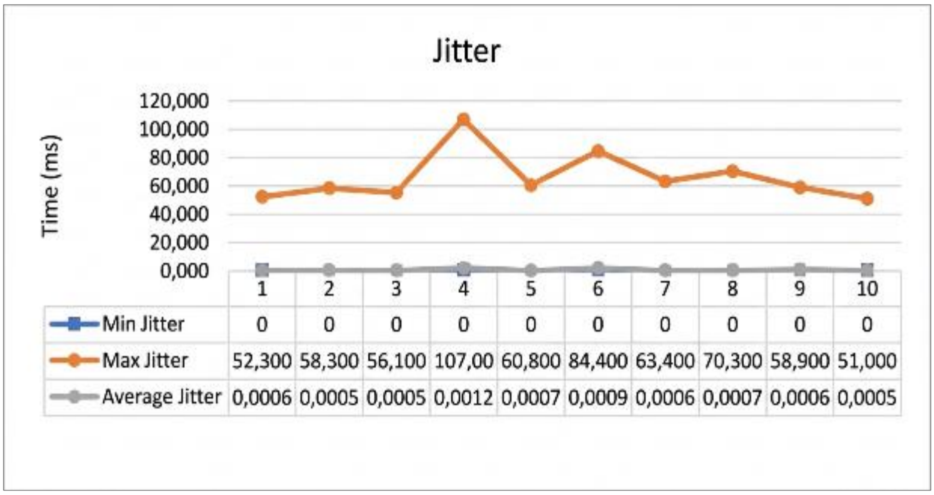

Figure 16. UDP Jitter Graph

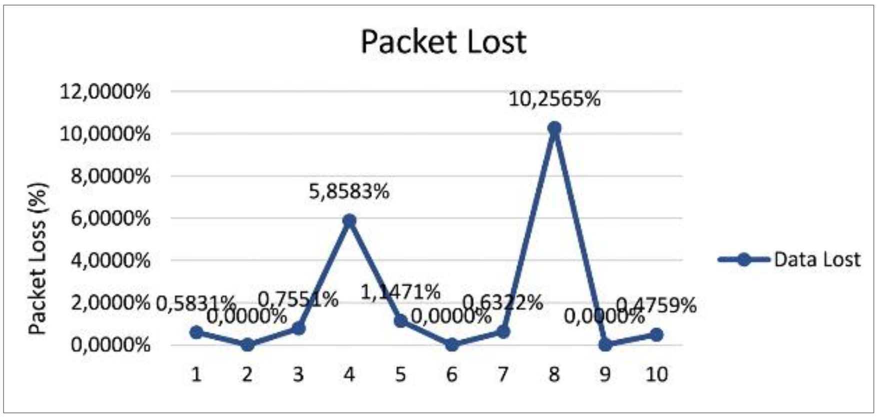

Figure 17. UDP Packet Loss Graph

CONCLUSIONS, RECOMMENDATIONS, AND LIMITATIONS

Based on the overall results obtained in this study, the implementation of the PPTP VPN demonstrates stable performance and reliability when tested using the ICMP, TCP, and UDP protocols. The evaluation based on throughput, packet loss, delay, and jitter parameters shows that the obtained Quality of Service (QoS) performance falls within the very good category according to QoS assessment standards. Specially, the recorded maximum delay of 7.79 ms and maximum jitter of 2.82 ms remain well below critical real-time communication thresholds. These findings confirm that secure VPN tunneling can be integrated into the PUNA MALE UAV simulation environment without significant degradation of the network performance required for telemetry, command, and data transmission. Furthermore, the results highlight that TCP offers superior stability in packet-loss performance compared to UDP, making it the more suitable choice for missions requiring high data integrity.

Despite the positive findings, several limitations exist in this research. The experiments were conducted in a simulation-based Hardware-in-the-Loop (HIL) environment using GNS3, which may not fully represent real operational conditions, such as variations in satellite latency, wireless interference, or UAV mobility dynamics. In addition, this study focuses exclusively on the PPTP protocol, which, despite its efficiency, possesses known security vulnerabilities compared to modern standards. The analysis also primarily addresses QoS metrics without extensive evaluation of encryption overhead, CPU processing efficiency, or scalability in multi-node UAV swarms.

Future studies should compare between PPTP and more modern VPN technologies, such as OpenVPN, L2TP/IPSec, and WireGuard, to identify the optimal balance between security and QoS. It is also recommended to validate these findings using physical network infrastructure and actual UAV flight tests to assess practical deployment challenges. Given the security profile of PPTP, integrating more robust protection mechanisms, such as IPSec tunneling or certificate-based authentication, is strongly advised for mission-critical defense operations and secure national surveillance systems.

REFERENCES

Adil, M., Song, H., Jan, M. A., Khan, M. K., He, X., Farouk, A., & Jin, Z. (2024). UAV-Assisted IoT Applications, QoS Requirements and Challenges with Future Research Directions. *ACM Comput. Surv.*, *56*(10). https://doi.org/10.1145/3657287

Andriyani, S., Sidiq, M. F., & Zen, B. P. (2023). *Analisis Celah Keamanan pada Website dengan Menggunakan Metode Penetration Testing dan Framework Issaf pada Website SMK Al-Kautsar* (Vol. 2, Issue 1).

de Zoysa, S., & Siriwardana, D. (2024). *Predictive Autonomous Drones for Cyber Espionage in Information Warfare: A 2026 Approach to Preemptive Threat Detection and Network Infiltration*.

Debe, R. G., & Ras, A. R. (2022). Pengembangan PUNA MALE Elang Hitam Klasifikasi Kombatan dalam Rangka Memperkuat Pertahanan dan Keamanan Indonesia. *Jurnal Pendidikan Tabusai*, *6*(2).

ETSI. (2006). Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); General aspects of Quality of Service (QoS). *Etsi Tr 101 329 V2.1.1*, *1*, 1–37.

Firmansyah, Y., Rahayu, N., Prabowo, Y., Putro, I. N. Y., & Kurniawan, F. (2020). Quality of Service (QoS) Analysis for Real-Time Telemetry by IP Satellite Communication. *Proceeding - 2020 International Conference on Radar, Antenna, Microwave, Electronics and Telecommunications, ICRAMET 2020*, 18–21. https://doi.org/10.1109/ICRAMET51080.2020.9298694

Gentile, A. F., Macrì, D., Greco, E., & Fazio, P. (2024). IoT IP Overlay Network Security Performance Analysis with Open Source Infrastructure Deployment. *Journal of Cybersecurity and Privacy*, *4*(3), 629–649. https://doi.org/10.3390/jcp4030030

Hartono, D., & Darmawan, S. (2019). Pemanfaatan Unmanned Aerial Vehicle (UAV) Jenis Quadcopter untuk Percepatan Pemetaan Bidang Tanah (Studi Kasus: Desa Solokan Jeruk Kabupaten Bandung). *Reka Geomatika*, *2018*(1), 30–40. https://doi.org/10.26760/jrg.v2018i1.2655

Hassan, A., Rawi, M. H. A. M., Mas'Ud, M. Z., Abu, M., Zakaria, Z., & Mansourkiaie, F. (2022). QoS Performance Evaluation of IoT-based Virtual Private Network for UAV Video. *Journal of Physics: Conference Series*, *2319*(1). https://doi.org/10.1088/1742-6596/2319/1/012022

Iida, T., & Wakana, H. (2003). Communications Satellite Systems. In R. A. Meyers (Ed.), *Encyclopedia of Physical Science and Technology (Third Edition)* (pp. 375–408). Academic Press. https://doi.org/10.1016/B0-12-227410-5/00882-6

ITU-T. (2001). G.1010: End-user multimedia QoS categories. *International Telecommunications Union*, *1010*.

Luo, S., Zhang, Z., Wang, S., Zhang, S., Dai, J., Bu, X., & An, J. (2020). Network for hypersonic UCAV swarms. *Science China Information Sciences*, *63*(4), 1–28. https://doi.org/10.1007/s11432-019-2765-7

Marpaung, N. L., Amri, R., Febrianzio, S., Ervianto, E., & Ali, N. D. (2024). Identification of internet network based on quality of service using TIPHON. *AIP Conference Proceedings*, *3026*(1), 50002. https://doi.org/10.1063/5.0199879

Mistri, R. K., Mahto, S. K., Singh, A. K., Sinha, R., Al-Gburi, A. J. A., Alghamdi, T. A. H., & Alathbah, M. (2023). Quad Element MIMO Antenna for C, X, Ku, and Ka-Band Applications. *Sensors (Basel, Switzerland)*, *23*(20). https://doi.org/10.3390/s23208563

Mumtaz, N., Perdana, D., & Bisono, G. (2019). Performance Evaluation of VoIP Traffic in 5G Millimeter Wave Network. *International Journal of Simulation: Systems, Science & Technology*, *18*(1), 6. https://doi.org/10.5013/ijssst.a.20.02.18

Nurrobi, I., Kusnadi, K., & Adam, R. (2020). Penerapan Metode QoS (Quality of Service) untuk Menganalisa Kualitas Kinerja Jaringan Wireless. *Jurnal Digit*, *10*(1), 47. https://doi.org/10.51920/jd.v10i1.155

Padhiary, M., Roy, P., & Kumar, K. (2025). Simulation Software in the Design and AI-Driven Automation of All-Terrain Farm Vehicles and Implements for Precision Agriculture. *Recent Progress in Science and Engineering*, *01*(02), 6. https://doi.org/10.21926/rpse.2502006

Shim, H., Kang, B., Im, H., Jeon, D., & Kim, S. (2025). TrustNet Virtual Private Network (VPN): Enhancing Security in the Quantum Era. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3530985

Sulistiya, Kusuma, Y. F., Yohanes, F. A., Daryanto, Y., Risnawan, N., & Baehaqi, F. A. (2023). Validation of the turbulence model in predicting aerodynamic characteristics of PUNA MALE using OpenFOAM software. *AIP Conference Proceedings*, *2941*(1), 20009. https://doi.org/10.1063/5.0181456

Suryani, I., Lindawati, L., & Salamah, I. (2018). Analisa QOS (Quality Of Service) Jaringan Internet Di Teknik Elektro Politeknik Negeri Sriwijaya. *It Journal Research and Development*, *3*(1), 32–42. https://doi.org/10.25299/itjrd.2018.vol3(1).1846

Tomaszewski, L., Kołakowski, R., Dybiec, P., & Kukliński, S. (2022). Mobile Networks' Support for Large-Scale UAV Services. *Energies*, *15*(14), 1–19. https://doi.org/10.3390/en15144974

Wang, K., Wang, Y., Li, Y., Fan, X., Xiao, S., & Hu, L. (2022). A review of the technology standards for enabling digital twin. *Digital Twin*, *2*, 4. https://doi.org/10.12688/digitaltwin.17549.1

Yan, L. (2024). UAV Detection with Radio Frequency Data and Deep Learning Techniques. *Proceedings of 2024 IEEE 6th International Conference on Civil Aviation Safety and Information Technology, ICCASIT 2024*, 234–239. https://doi.org/10.1109/ICCASIT62299.2024.10827957

Yue, L., Xiaohui, Q., Xiaodong, L., & Qunli, X. (2020). Deep reinforcement learning and its application in autonomous fitting optimization for attack areas of UCAVs. *Journal of Systems Engineering and Electronics*, *31*(4), 734–742. https://doi.org/10.23919/JSEE.2020.000048

Zen, B. P., Zafia, A., & Putro, I. N. Y. (2022). Network Security Analysis Simulation at the GCS in the UCAV to support the Indonesian Defense Area. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *6*(5), 824–831. https://doi.org/10.29207/resti.v6i5.4412