Network Security Analysis Simulation at the GCS in the UCAV to support the Indonesian Defense Area

Bita Parga Zen¹, Anggi Zafia², Iwan Nofi Yono Putro³
¹² Informatics Engineering, Faculty of Informatics, Telkom Purwokerto Institute of Technology
³ National Research and Innovation Agency
¹ bita@ittelkom-pwt.ac.id , ²zafia@ittelkom-pwt.ac.id, ³iwan.nofi.yono.putro@brin.go.id

Abstract

An unmanned Combat Aerial Vehicle (UCAV) is an unmanned aircraft that has a serial control communication device that can be seen directly in real-time. In carrying out UCAV flights, it requires good and stable data transmission security so that signal loss does not occur during the communication process. Researchers create a concept of a security scheme in communication at the Ground Control Station (GCS) that can be used for the use of UCAV communication at long distances, using the Quality of Service (QoS) method from OPEN VPN with parameters Throughput, Packet Loss, Delay (Latency) and Jitter can determine the reliability of a UCAV communication network. Based on the results of Quality of Service (QoS) testing with OpenVPN Autopilot UCAV objects on the ICMP protocol have the smallest packet loss value of 0%, the delay parameter is 5.2ms, the jitter parameter gets a high value of 4.68 ms higher than the TCP protocol and UDP. The TCP protocol has a relatively small packet loss value of 0.3% and ranks second to the ICMP protocol, then the delay value is 8.48 ms greater than the ICMP and UDP protocols, and the jitter parameter value is 0.0013 ms smaller than the ICMP and UDP protocols. The use of VPN OVPN is a good recommendation. Still, researchers suggest that should use not only OPEN VPN but also L2TP VPN and PPTP VPN for security at the Ground Control Station at UCAV as a comparison.

Keywords: Unmanned Combat Aerial Vehicle; Quality of Service; Defense; Ground Control Station; OPEN VPN

1. Introduction

The Republic of Indonesia has maritime and land borders with ten countries in the region (Thailand, Malaysia, Vietnam, the Philippines, East Leste, Papua New Guinea, Australia, and the Republic of Palau) [1] is the 7th largest country in the world based on geographical location and has waters as one of the trades. which makes Indonesia vulnerable to border problems related to regional border issues which have always been a problem for the beneficiary parties, the real threat of armed criminal groups and separatism currently has the potential to disrupt the country's defense and security system.[2], entering the industrial revolution 4.0 where all have used technology as the main component in various fields, especially industrial production, information, and communication technology [3], anticipating national defense to maintain the sovereignty of the nation [4], this certainly cannot be separated from the modern defense equipment owned by developed countries, one of which is the development of unmanned aircraft technology Unmanned Combat Aerial Vehicle (UCAV).

UCAV aims to be a control serial communication tool that can be seen directly in real-time [5] and can monitor if there is a threat in the defense area. UCAV is controlled by the Ground Control Station (GCS) which can be used for the use of UCAV communications at long distances [6], but the obstacle is that it is vulnerable to interference, both from damage to the device and from security factors. In GCS, a computer network is needed for stability and security when sending and receiving data to ensure that the data sent reaches its destination [7], and the data sent is confidential.

For this reason, it is necessary to test network quality and data security on the network at GCS using Quality of Service (QoS) analysis [8]. The quality of data delivery services is the key to the attack area that affects the operational performance of the Unmanned Combat Aerial Vehicle (UCAV). Data transmission service area refers to the distance at which a missile on a UCAV, if this is neglected, can hit and damage a target with a certain probability under specific environmental parameters, including altitude, missile and target speed,
ballistic tilt angle, entry angle, and off-axis angle, in an air combat environment [9].

One way to test network quality is to perform a QoS analysis. Quality of Service (QoS) is a technology that allows network administrators to deal with the effects of congestion on packet flow traffic from various services to make optimal use of network resources, rather than increasing the physical capacity of the network. [10]. defines that QoS is a technique for managing bandwidth, delay, jitter, and packet loss for packet flow in a network [10]. The purpose of the QoS mechanism is to influence at least one of the four basic QoS parameters that have been determined. In addition to testing network stability using QoS, data transmission security needs to be implemented to ensure data safety from unauthorized parties [11]. One way to secure data on a network is to implement a Virtual Private Network (VPN) which can make a network private and secure using a public network or the internet.

![Figure 1. GCS to UCAV Communication Scheme](image1)

This is one of the basics of making simulations and analyses of QOS (Quality Of Service) throughput, delay, jitter, and packet loss stages. [12] with the addition of data security using VPN OpenVPN using the GNS3 network simulator application with the Hardware In The Loop Simulations technique which is a simulation involving some external hardware as support that will be applied to the Ground Control Station to control UCAV.

2. Research Method

This research will build a simulation and analysis of the Quality of Service on Unmanned Combat Aerial Vehicle Communication Networks for Data Security by explaining the levels or sequences starting from Throughput, delay, jitter, and packet loss at Ground Control Station Using OPENVPN with Hardware In The Loop Technique, Design This simulation will be a study that will be used for testing, and identify needs by providing detailed and accurate research figures. Figure 2 below are the stages of the process carried out by the researcher.

![Figure 2 Research Process Flow](image2)

2.1 Modeling IP and Network

In the IP address classification stage Configure all router interfaces connected to multiple ports by assigning an IP address to each port connected to the router. [13]. regarding the IP address to be used, there are several public IPs used for certain routers and private IPs. The following table classifier IP Address used.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interfaces</th>
<th>IP Adress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router Pustekbang BRIN</td>
<td>ether1</td>
<td>103.16.223.107/29</td>
</tr>
<tr>
<td></td>
<td>ether1</td>
<td>10.10.5.136/27</td>
</tr>
<tr>
<td></td>
<td>local VPN</td>
<td>10.11.6.1/32</td>
</tr>
<tr>
<td>Router1</td>
<td>ether1</td>
<td>103.16.223.108/29</td>
</tr>
<tr>
<td></td>
<td>ether2</td>
<td>103.51.131.107/29</td>
</tr>
<tr>
<td>Router 2</td>
<td>ether1</td>
<td>103.51.131.108/29</td>
</tr>
<tr>
<td></td>
<td>ether2</td>
<td>10.0.0.1/30</td>
</tr>
<tr>
<td>Router 3</td>
<td>ether1</td>
<td>10.0.0.2/30</td>
</tr>
<tr>
<td></td>
<td>ether2</td>
<td>10.0.0.5/30</td>
</tr>
<tr>
<td>GCS Sat</td>
<td>ether1</td>
<td>10.0.0.6/30</td>
</tr>
<tr>
<td></td>
<td>ether2</td>
<td>10.0.0.9/30</td>
</tr>
<tr>
<td>Satellite</td>
<td>ether1</td>
<td>10.0.0.10/30</td>
</tr>
<tr>
<td></td>
<td>ether2</td>
<td>10.0.0.13/30</td>
</tr>
<tr>
<td>Modern Sat UCAV</td>
<td>ether1</td>
<td>10.0.0.14/30</td>
</tr>
<tr>
<td></td>
<td>ether2</td>
<td>10.0.0.17/3</td>
</tr>
<tr>
<td>Router Client</td>
<td>ether1</td>
<td>10.0.0.18/30</td>
</tr>
<tr>
<td></td>
<td>ether2</td>
<td>10.11.12.1/29</td>
</tr>
<tr>
<td></td>
<td>remote VPN</td>
<td>10.11.6.2/32</td>
</tr>
</tbody>
</table>

In Figure 2 there are 8 device routers, where the
Pustekbang BRIN router is marked with a yellow background, while the client router side is marked with a green background. For public routers or routers outside the server and client are marked with a gray background (gray). Furthermore, for the Server and Client in this simulation, Cloud2 is the Pustekbang Server and Cloud3 is the Client. Each device is external hardware connected to the GNS3 simulation software with the concept of Hardware in The Loop System. This topology design is implemented in the GNS3 software by adding a Mikrotik Router to the Qemu system contained in the GNS3. Then each router is connected and configured as needed.

![Image](image_url)

Figure 2. Communication Network Topology Design

2.2 Quality of Service (QoS)
Quality of Service (QoS) is an attempt to define the characteristics of a network quality by measuring how good the network quality of service is using certain parameters [14]. The International Telecommunication Union-Telecommunication (ITU-T) G.1010 standards are discussed in this paper as they relate to the quality of service (QoS) performance from telemetry data utilizing UDP protocols both with and without VPN on Ground Control Station (GCS) communication with UCAV [15]. G.1010 is an ITU-T standard. [16].

A guarantee for zero information loss or the absence of packet loss is a parameter that must be taken into account for data transfer. Then, the delay that happens must be less than 1 second and the fluctuation of the delay (jitter) that occurs must adhere to certain guidelines [15]. It is anticipated that the reliability performance of satellite communications that are intended and may be beneficial for long-range UCAV communication applications would be known from the findings of testing and analysis [17].

There are 3 levels of QoS that are often used, namely Best-effort service, which is a service model where each application for each data transmission is required without asking permission from the computer network. a service that can meet all the requirements of different QoS rules [18]. The ultimate goal of QoS is to provide a better and more planned network service with controlled dedicated bandwidth, jitter, and latency and increase loss characteristics centered on network characteristics. [19]

<table>
<thead>
<tr>
<th>Category Delay</th>
<th>Delay</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very good</td>
<td>&lt; 150 ms</td>
<td>4</td>
</tr>
<tr>
<td>Good</td>
<td>150 s/d 300</td>
<td>3</td>
</tr>
<tr>
<td>Fair</td>
<td>301 s/d 450 ms</td>
<td>2</td>
</tr>
<tr>
<td>Poor</td>
<td>&gt; 450 ms</td>
<td>1</td>
</tr>
</tbody>
</table>

b. Delay
Delay (Latency) is the time it takes for data to travel the distance from the sender to the receiver. delay can be affected by long distances, physical media, data congestion, or also long processing times [18]. The equation to calculate the delay is:

\[
\text{Avaragedelay} = \frac{\text{Totaldelay}}{\text{Totalpacketsreceived}}
\]  (1)

<table>
<thead>
<tr>
<th>Category Delay</th>
<th>Delay</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very good</td>
<td>76%–100%</td>
<td>4</td>
</tr>
<tr>
<td>Good</td>
<td>51% s/d 75%</td>
<td>3</td>
</tr>
<tr>
<td>Fair</td>
<td>26% s/d 50%</td>
<td>2</td>
</tr>
<tr>
<td>Poor</td>
<td>&lt;25%</td>
<td>1</td>
</tr>
</tbody>
</table>

The total variation of the delay is obtained from:

\[
\text{Total Variation Delay} = \text{Delay} - (\text{Average Delay})
\]  (3)

Table 2. Category Jitter

<table>
<thead>
<tr>
<th>Kategori Jitter</th>
<th>Peak Jitter</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very good</td>
<td>0 ms</td>
<td>4</td>
</tr>
<tr>
<td>Good</td>
<td>1 s/d 75 ms</td>
<td>3</td>
</tr>
<tr>
<td>Fair</td>
<td>76 s/d 225 ms</td>
<td>2</td>
</tr>
<tr>
<td>Poor</td>
<td>&gt; 225 ms</td>
<td>1</td>
</tr>
</tbody>
</table>

DOI: https://doi.org/10.29207/resti.v6i5.4412
Creative Commons Attribution 4.0 International License (CC BY 4.0)
Packet loss is a parameter that shows the condition of a data packet that is lost from the total number of packets that can occur due to collision and congestion on a network [23]. The equation to calculate packet loss is:

\[
\text{Packet Loss} = \frac{\text{Packaged} - \text{Packagerceived}}{\text{Receivedpackage}} \times 100\% 
\]

(4)

Table 3. Category Packet Loss

<table>
<thead>
<tr>
<th>Category</th>
<th>Packet Loss Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very good</td>
<td>0% - 2%</td>
</tr>
<tr>
<td>Good</td>
<td>3% - 14%</td>
</tr>
<tr>
<td>Fair</td>
<td>15% - 25%</td>
</tr>
<tr>
<td>Poor</td>
<td>&gt; 25%</td>
</tr>
</tbody>
</table>

2.3 Open VPN type VPN configuration

VPN configuration is carried out on the BRIN pustekbang router as a VPN Open VPN Server. VPN Open VPN Server is made using the default settings on the Pustekbang router so that it can be accessed by the client side as a tunnel that connects the network. The security used only uses default encryption to be able to connect to the network without using additional security such as IPsec or certificates. The following is the VPN Server OVPN configuration that has been created on the Pustekbang router. First, to increase the security of this OpenVPN connection, we will add certificates to the server as well as the client. After we create the certificate, we will first activate the OpenVPN Server on the main gateway router at 'Server-Pustekbang'. Type in SSL Linux PPP → on the Interface Tab of the OVPN Server Command. Then to enable OpenVPN Server check the Enabled option. Also, add a certificate for OpenVPN connection in 'Router-Pustekbang' as OVPN Server in parameter 'Certificate' as shown below.

Figure 3 OPENVPN Server Configuration

Routing configuration is also carried out on the UCAV Satellite Modem router to connect to other router networks to be connected. The following is a picture of the routing configuration used on the UCAV Satellite Modem router. As with other VPN connections, we will also create a 'PPP secret' to dial a connection from the OVPN Client

Figure 4 OPENVPN Authentication Configuration

Next, do the configuration for the 'Client' as an OpenVPN Client. Because we use the terminal, we go to the PPP menu → Interfaces → Add [+] → OVPN Client. Then fill in each parameter. If OpenVPN is successfully connected then we can see the OpenVPN Server router in the PPP → Active Connections menu. There will be displayed information from client devices that have successfully connected to OpenVPN Server.

Schematic on the Ground Control Station as the main link to the Unmanned Combat Aerial Vehicle (UCAV) which functions as reconnaissance and helps map out areas [24] at the time of combined operation which has 3 main components: 1. UCAV as the main component that can be flown for monitoring by air; 2. Ground Control Station as a computer for the control room in the UCAV remote control which can be viewed with a monitor in real-time both for taking pictures and for video, then the routing configuration is carried out on the UCAV Satellite Modem router to connect other router networks to be connected. The following figure shows the routing configuration used on the UCAV Satellite Modem router. 3. Ground Data Terminal as a distance determinant, namely the antenna for connecting the Ground Control Station to UCAV

Figure 5 UCAV satellite modem router configuration.

This research focuses on simulating the network design on GNS3 simulation software. In QoS, there are 3 main parameters used to analyze the quality of the service, namely, parameters of delay, jitter, and packet loss in the UCAV satellite modem router. In the analysis stage...
of the results of the Quality of Service (QoS) test the parameters used are the parameters of delay, jitter, and packet loss in each of the tested protocols, namely the routing configuration protocol is also carried out on the UCAY Satellite Modem router to connect other router networks so that they are connected. The following figure is the routing configuration used on the UCAY Satellite Modem router.

3. Result and Discussion

ICMP testing is done by sending a ping test packet to the server using the command: "ping 10.10.10.90" for a time interval of 100 seconds and is carried out 10 times. This test aims to maximize the data later in processing QoS. Parameters

TCP testing is done by sending packets via port 5000 using the iperf3 application to the server using the command “iperf3 -c 10.10.9.90 -p 5000 -t 100 > filename.txt”. This test is carried out with a time interval of 100 seconds and is carried out ten times to get maximum data on QoS processing.

UDP testing is done by sending packets via port 5000 using the iperf3 application to the server using the bandwidth obtained from the TCP protocol testing. This test is carried out with a time interval of 100 seconds and is carried out ten times to get maximum data on QoS processing.

In the analysis phase of the Quality of Service (QoS) test results, the parameters used are the delay, jitter, and packet loss parameters in each of the tested protocols, namely the Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP) and User Data Protocol (UDP). The following are the results of the test graph for each protocol obtained:

a. Throughput is the bandwidth obtained in each trial of the TCP and UDP protocols

b. Protocol ICMP

Delay ICMP

The following is the result of measuring the QoS parameters of the ICMP protocol delay based on a predetermined test scheme, the test results above the resulting graph show that the maximum average delay is 7.75 ms, the minimum average delay is 2.81 ms, and the average delay is 2.81 ms. total delay is 5.20 ms

Figure 8 UDP Protocol Test

Figure 9 TCP and UDP Throughput Graph

Figure 10 ICMP Delay Graph
Jitter ICMP
The following are the results of the ICMP protocol jitter parameter QoS measurements based on a predetermined test scheme. In the parameters of the jitter, the maximum average jitter is 12.75 ms, the minimum average jitter is 0 ms, and the overall average jitter is 4.68 ms.

![ICMP Jitter Graph](image1)

Packet Loss
The following is the result of measuring the QoS parameters of the ICMP packet loss protocol based on the test scheme that has been determined based on the graph below, in the ICMP packet loss protocol parameter, no packet loss was found at 0%.

![Packet Loss ICMP](image2)

c. Protocol TCP

Delay TCP
The following is the result of measuring the QoS parameters of the TCP protocol delay based on the test scheme that has been determined from the graph above, the delay results from the TCP protocol obtained the maximum delay on the 7th experiment with a value of 112.00 ms, the minimum delay on the 8th experiment with a value of 1.8000 ms, the maximum average delay on the 9th experiment with a value of 8.8153 ms, and the minimum average delay on the 2nd experiment with a value of 8.1801.

![Delay TCP](image3)

Jitter TCP
The following is the result of measuring the QoS parameters of the TCP protocol jitter based on a predetermined test scheme. Based on the graph above, the results of the jitter of the TCP protocol obtained the maximum jitter on the 7th experiment with a value of 109.400 ms, the minimum jitter of all tests got a value of 0.0000 ms, the maximum average jitter on the 7th experiment with a value of 0.0021 ms and the minimum average jitter on the 5th experiment with a value of 0.0010.

![TCP Jitter Graph](image4)

Packet Loss
The following is the result of measuring the QoS parameters of the TCP protocol packet loss based on the test scheme that has been determined in the graph above, the packet loss results from the TCP protocol obtained the maximum packet loss on the 6th experiment with a value of 0.3355% and the minimum packet loss on the 10th experiment with a value of 0.2599 ms.

![TCP Packet Loss Graph](image5)
d. Protocol UDP

Delay UDP

The following is the result of measuring the QoS parameters of the UDP protocol delay. Based on the graph of the delay results from the UDP protocol, the maximum delay in the 3rd experiment with a value of 95,600 ms, the minimum delay in the 5th and 10th experiments with a value of 2,500 ms, and the maximum average delay in the 10th experiment with a value of 4.9558 ms, and the minimum average delay on the 3rd experiment with a value of 4.6412 ms.

Jitter UDP

The following is the result of measuring the QoS parameters of the UDP protocol jitter. Based on the graph above, the jitter results of the UDP protocol obtained the maximum jitter on the 10th experiment with a value of 91.40 ms, the minimum jitter of all tests got a value of 0.0000 ms, the average maximum jitter in the 4th experiment with a value of 0.5781 ms, and the minimum average jitter in the 1st and 2nd experiments with a value of 0.0004 ms.

Packet Loss

The following is the result of measuring the QoS parameter of the UDP protocol packet loss. Based on the graph above, the packet loss results from the UDP protocol obtained the maximum packet loss on the 10th experiment with a value of 0.2559% and the minimum packet loss on the 1st experiment with a value of 0.0000%

QoS Recapitulation

By testing on each protocol with a predetermined scenario using QOS calculations (delay, jitter, and packet loss), the protocol used (ICMP, TCP, and UDP) in testing using VPN OVPN has an excellent value based on the values taken from the overall average of the number of tests of each QoS parameter. The ICMP protocol has the smallest packet loss value (0%). Still, the delay parameter (5.2 ms) is greater than the UDP protocol and smaller than the TCP protocol, and the jitter parameter gets a high value (4.68 ms). Higher than the TCP and UDP protocols. The TCP protocol has a relatively small packet loss value (0.3%) which ranks second to the ICMP protocol. The delay value is more excellent (8.48 ms) than the ICMP and UDP protocols, and the jitter parameter value is more minor (0.0013) of the ICMP protocol and more significant than the UDP protocol. While the TCP protocol itself has the highest packet loss value (0.3%) of the other two protocols, both the delay parameter (4.75 ms) and jitter (0.22 ms) have a relatively more nominal value than the other protocols.

Conclusion

The Ground Control Station security system using OPEN VPN has an excellent Quality of Service (QoS) value based on experiments using ICMP, TCP, and UDP protocols. This value is taken from the overall average number of tests for each QoS parameter; from the results of the QoS recapitulation above, UDP is more suitable for use on VPN OVPN. Then when viewed from the 4.75 ms delay and 0.22 ms jitter, the UDP protocol repositions its performance on the use of...
VPN OVPN so that this is a good recommendation for security at the Ground Control Station in the Unmanned Combat Aerial Vehicle (UCAV).

References


