ANALISIS DAMPAK SERANGAN *DENIAL OF SERVICE* TERHADAP METRIK QOS PADA KOMUNIKASI PLC DENGAN HMI

Sifa Tsalsabila Hasyifah

21/482387/TK/53272

Diajukan kepada Departemen Teknik Nuklir dan Teknik Fisika Fakultas Teknik
Universitas Gadjah Mada pada tanggal 20 Maret 2025
untuk memenuhi sebagian persyaratan untuk memperoleh derajat
Sarjana Program Studi Teknik Fisika

INTISARI

Integrasi *Information Technology* (IT) dan *Operational Technology* (OT) dalam *Industrial Control System* (ICS) meningkatkan risiko serangan siber, seperti serangan *Denial of Service* (DoS). Serangan ini dapat mengancam kestabilan komunikasi hingga kehilangan akses terhadap peralatan fisik, namun penelitian mengenai dampaknya masih terbatas. Oleh karena itu, penelitian ini bertujuan untuk mengevaluasi dampak serangan DoS terhadap metrik *Quality of Service* (QoS), seperti *round-trip time* (RTT) dan *throughput* pada komunikasi antara *Programmable Logic Controller* (PLC) dan *Human Machine Interface* (HMI).

Penelitian ini dilakukan dengan menggunakan ICS *Testbed* yang terdiri dari PLC S7-1500 dengan HMI pada *Engineering Workstation*. Serangan DoS dilakukan dengan melakukan variasi interval dan ukuran *payload* serangan dengan teknik SYN *Flooding* menggunakan hping3. Variasi serangan diuji untuk menganalisis dampaknya terhadap RTT dan *throughput*. Selain itu, analisis dampak serangan digunakan untuk menentukan batas atas RTT dan batas bawah *throughput* sebagai indikator dalam mendeteksi serangan.

Hasil penelitian menunjukkan bahwa variasi interval dan ukuran *payload* serangan DoS memengaruhi kestabilan komunikasi. Dampak terhadap metrik QoS semakin besar seiring dengan semakin kecilnya interval dan semakin besar ukuran *payload*. Ambang batas deteksi serangan DoS ditetapkan pada nilai RTT 0,401 detik dan *throughput* 320 Bps untuk serangan yang mengganggu komunikasi, serta RTT 0,661 detik dan *throughput* 0 Bps untuk serangan dengan dampak kritis.

Kata kunci: PLC, Serangan DoS, SYN *Flooding*, RTT, *Throughput*, Batas Kendali.

Pembimbing Utama	:	Dr.-Ing. Ir. Awang Noor Indra Wardana, S.T., M.T., M.Sc., IPM.
Pembimbing Pendamping	:	Dr. Eng. Ir. Dwi Joko Suroso, S.T., M.Eng., IPP.

IMPACT ANALYSIS OF DENIAL OF SERVICE ATTACKS ON QOS METRICS IN PLC AND HMI COMMUNICATION

Sifa Tsalsabila Hasyifah

21/482387/TK/53272

Submitted to the Departement of Nuclear Engineering and Engineering Physics
Faculty of Engineering Universitas Gadjah Mada on March 20, 2025
in partial fulfillment of the requirement for the Degree of
Bachelor of Engineering in Engineering Physics

ABSTRACT

The integration of Information Technology (IT) and Operational Technology (OT) in Industrial Control Systems (ICS) increases the risk of cyberattacks, such as Denial of Service (DoS) attacks. These attacks can threaten communication stability and even lead to loss of access to physical equipment, yet research on their impact remains limited. Therefore, this study aims to evaluate the impact of DoS attacks on Quality of Service (QoS) metrics, such as round-trip time (RTT) and throughput, in communication between a Programmable Logic Controller (PLC) and a Human Machine Interface (HMI).

This research was conducted using an ICS testbed consisting of an S7-1500 PLC and an HMI on an Engineering Workstation (EWS). DoS attacks were carried out by varying the interval and payload size of SYN Flooding attacks using hping3. The variations were tested to analyze their impact on RTT and throughput. Additionally, the analysis of the attack's impact was used to determine the upper limit of RTT and the lower limit of throughput as indicators for detecting attacks.

The results show that variations in the interval and payload size of DoS attacks affect communication stability. The impact on QoS metrics increases as the interval decreases and the payload size increases. The detection thresholds for DoS attacks were set at an RTT of 0.401 seconds and a throughput of 320 Bps for attacks that disrupt communication, and an RTT of 0.661 seconds and a throughput of 0 Bps for attacks with critical impact.

Keywords: PLC, DoS Attack, SYN Flooding, RTT, Throughput, Threshold.

Supervisor : Dr.-Ing. Ir. Awang Noor Indra Wardana, S.T., M.T., M.Sc., IPM.

Co-supervisor : Dr. Eng. Ir. Dwi Joko Suroso, S.T., M.Eng., IPP.