INTISARI

Analisis Perbandingan Kinerja Protokol MQTT dan AMQP pada Pengiriman Pesan Peringatan dari Sensor NIDS berdasarkan Serangan Jaringan

Oleh

Hariyo Prasetyo
21/476218/PPA/06157

Penelitian ini bertujuan membandingkan kinerja protokol MQTT dan AMQP dalam pengiriman data dari sensor *Network Intrusion Detection System* (NIDS) ke *defense center* saat terjadi serangan jaringan yang beragam. Metode pengumpulan data dilakukan melalui observasi eksperimental menggunakan aplikasi *Tcpdump* dan *Wireshark* untuk menganalisis lalu lintas jaringan antara sensor dan *defense center* dengan protokol AMQP dan MQTT secara bergantian. Parameter yang diukur meliputi *throughput*, *delay*, dan *packet loss*.

Hasil penelitian menunjukkan bahwa MQTT memiliki *throughput* lebih rendah daripada AMQP. Pada semua skenario uji, *throughput* tertinggi terjadi saat serangan *DoS Land Attack*, dengan rata-rata MQTT sebesar 13,57 Kbps dan AMQP sebesar 18,18 Kbps. MQTT juga memiliki *delay* yang lebih rendah, terutama pada interval kedatangan pesan yang pendek. Pada serangan SSH *Brute Force*, rata-rata *delay* tertinggi untuk MQTT adalah 4,35 ms, sedangkan AMQP terjadi pada serangan *DoS SYN Flood* dengan nilai 21,49 ms. Tidak ditemukan *packet loss* pada kedua protokol dalam semua kondisi uji, menunjukkan kemampuan baik dalam menjaga integritas pesan dan menghindari kehilangan paket.

Analisis statistik menggunakan uji *Mann-Whitney* menunjukkan adanya perbedaan signifikan antara MQTT dan AMQP dalam *throughput* dan *delay*. Berdasarkan hasil penelitian, protokol MQTT direkomendasikan untuk pengiriman pesan peringatan dari sensor NIDS dalam membangun sistem NIDS yang handal. MQTT mampu merespons serangan atau ancaman dengan cepat dan efektif tanpa kelebihan beban pada jaringan. Rekomendasi ini didasarkan pada analisis komprehensif kinerja kedua protokol dan hasil statistik yang mendukung perbedaan signifikan antara keduanya.

Kata Kunci: MQTT, AMQP, *NIDS, throughput, delay, packet loss, Mann-Whitney.*

ABSTRACT

Comparative Analysis of MQTT and AMQP Protocol Performance in Delivering Network Alert Messages from NIDS Sensor Based on Network Attacks

Oleh

Hariyo Prasetyo
21/476218/PPA/06157

This research aims to compare the performance of MQTT and AMQP protocols in delivering data from Network Intrusion Detection System (NIDS) sensors to the defense center during various network attack scenarios. The data collection method involves experimental observation using tcpdump and Wireshark application to analyze the network traffic between the sensors and defense center using both AMQP and MQTT protocols alternately. The measured parameters include throughput, delay, and packet loss.

The research findings indicate that MQTT has lower throughput compared to AMQP. In all test scenarios, the highest throughput occurred during DoS Land Attack, with an average of 13.57 Kbps for MQTT and 18.18 Kbps for AMQP. MQTT also exhibited lower delay, especially for short message arrival intervals. During SSH Brute Force attacks, the highest average delay for MQTT was 4.35 ms, while for AMQP it occurred during DoS SYN Flood with a value of 21.49 ms. No packet loss was observed for both protocols in all test conditions, demonstrating their ability to maintain message integrity and avoid packet loss.

Statistical analysis using the Mann-Whitney test revealed significant differences between MQTT and AMQP in terms of throughput and delay. Based on the research results, MQTT protocol is recommended for delivering alert messages from NIDS sensors in building a reliable NIDS system. MQTT can effectively and promptly respond to attacks or threats without experiencing network overload. This recommendation is based on a comprehensive analysis of the performance of both protocols and supported by statistically significant differences between them.

Keywords: MQTT, AMQP, NIDS, throughput, delay, packet loss, Mann-Whitney.