ABSTRAK

Perkembangan teknologi informasi meningkatkan kebutuhan akan sistem monitoring jaringan yang mampu mendeteksi gangguan secara cepat dan memberikan informasi yang lebih kontekstual. Monitoring berbasis MikroTik umumnya masih berfokus pada pemantauan parameter dan notifikasi perubahan kondisi secara terpisah, sehingga analisis keterkaitan antar kejadian masih dilakukan secara manual. Penelitian ini mengusulkan dan mengevaluasi sistem monitoring kesehatan jaringan berbasis MikroTik dengan pendekatan *rule-based detection* dan *event correlation* untuk menghasilkan indikasi awal gangguan jaringan berdasarkan keterkaitan antar *event*.

Penelitian dilakukan pada lingkungan simulasi GNS3 menggunakan MikroTik Cloud Hosted Router (CHR). Data kesehatan jaringan berupa penggunaan CPU, memori, *delay*, *packet loss*, dan status *interface* dikumpulkan secara periodik melalui *RouterOS API*. Mekanisme *rule-based detection* digunakan untuk membentuk *event* berdasarkan nilai *threshold* dan durasi pelanggaran melalui *sliding window*, disertai mekanisme *event lifecycle* untuk memastikan konsistensi status *event*. Selanjutnya, *event correlation* digunakan untuk mengaitkan beberapa *event* yang terjadi dalam rentang waktu tertentu berdasarkan kedekatan temporal dan keterkaitan parameter. Evaluasi dilakukan menggunakan metrik *Detection Rate* (DR) dan *Mean Time to Detect* (MTTD).

Hasil penelitian menunjukkan bahwa sistem berhasil membentuk *event* gangguan dan mengaitkannya menjadi dua jenis indikasi, yaitu degradasi kualitas jaringan tanpa keterlibatan sumber daya perangkat serta degradasi kualitas jaringan akibat keterbatasan sumber daya perangkat. Berdasarkan 18 skenario insiden yang diuji, sistem memperoleh nilai *Detection Rate* sebesar 100% dan *Mean Time to Detect* sebesar 50,5 detik, di mana nilai MTTD tersebut dipengaruhi oleh durasi pelanggaran *threshold* selama 60 detik pada mekanisme *sliding window*. Hasil tersebut menunjukkan bahwa pendekatan *rule-based detection* dan *event correlation* mampu mendeteksi seluruh insiden yang diuji serta menghasilkan indikasi gangguan yang lebih terstruktur dibandingkan monitoring berbasis kejadian tunggal.

Kata Kunci: *monitoring jaringan*, MikroTik, *rule-based*, *event correlation, event lifecycle*, kesehatan jaringan.

ABSTRACT

The advancement of information technology has increased the need for network monitoring systems capable of rapidly detecting disruptions and providing more contextual information. MikroTik-based monitoring generally focuses on monitoring network parameters and notifying condition changes separately, causing the analysis of relationships between events to still be performed manually. This study proposes and evaluates a MikroTik-based network health monitoring system using rule-based detection and event correlation approaches to generate early indications of network disruptions based on the relationships among events.

The study was conducted in a GNS3 simulation environment using MikroTik Cloud Hosted Router (CHR). Network health data, including CPU usage, memory usage, delay, packet loss, and interface status, were collected periodically through the RouterOS API. The rule-based detection mechanism was used to generate events based on threshold values and violation durations using a sliding window approach, accompanied by an event lifecycle mechanism to ensure event status consistency. Furthermore, event correlation was applied to associate multiple events occurring within a specific time range based on temporal proximity and parameter relationships. The evaluation was performed using Detection Rate (DR) and Mean Time to Detect (MTTD) metrics.

The results show that the system successfully generated disruption events and correlated them into two types of indications: network quality degradation without device resource involvement and network quality degradation caused by device resource limitations. Based on 18 tested incident scenarios, the system achieved a Detection Rate of 100% and a Mean Time to Detect of 50.5 seconds, where the MTTD value was influenced by the 60-second threshold violation duration configured in the sliding window mechanism. These findings indicate that the rule-based detection and event correlation approaches were able to detect all tested incidents and provide more structured disruption indications compared to single-event-based monitoring.

.

Keywords: *network monitoring, MikroTik, rule-based, event correlation, event lifecycle, network health.*