ABSTRAK

Perangkat terbatas merupakan perangkat yang menunjang pengembangan perangkat IoT. Proses komunikasi perangkat merupakan aktivitas yang terjadi pada IoT. Proses komunikasi ini dilakukan dengan protokol komunikasi. Salah satu protokol komunikasi yang digunakan adalah MQ Telemetry Transport protokol (MQTT). Protokol MQTT adalah protokol komunikasi yang ringan, cepat, dan dapat diterapkan pada perangkat terbatas. MQTT protokol menggunakan broker sebagai peladen. Namun, protokol MQTT tidak memiliki mekanisme keamanan pada pengaturan awal sehingga menimbulkan permasalahan otentikasi perangkat. Permasalahan otentikasi pada protokol MQTT diawali dengan packet sniffing untuk mendapatkan informasi sensitif dari packet komunikasi pada protokol MQTT. Permasalahan ini menyebabkan fase registrasi dan publikasi pada protokol MQTT rawan terhadap perangkat non-otentik. Mekanisme keamanan pada protokol MQTT telah dibuat sebelumnya dengan menggunakan Transport Layer Security (TLS). Namun, TLS mengkomsumsi lebih dari 100 KB memori da tidak cocok untuk consraint device. Oleh karena itu, penelitian ini mengusulkan mekanisme otentikasi yang cocok pada perangkat terbatas guna meningkatkan keamanan pada protokol MQTT. Penelitian ini mengusulkan mekanisme otentikasi yang terdiri dari pillar dinamis dan berbasis kejadian untuk protokol MQTT. Pilar dinamis bertujuan untuk memberikan properti otentikasi yang berbeda-beda pada setiap sesi guna meningkatkan keamanan otentikasi. Pilar berbasis kejadian digunakan untuk skeduling dan berpotensi mengurangi beban komputasi pada perangkat terbatas. Dari evaluasi yang dilakukan, protokol yang diajukan mampu memberikan mekanisme otentikasi pada protokol MQTT. Hasil validasi menggunakan TAMARIN PROVER menunjukkan bahwa protokol yang diajukan valid untuk ancaman packet sniffing. Protokol yang diajukan dapat diimplementasikan pada perangkat terbatas dan broker untuk melakukan mekanisme otentikasi.

Kata kunci: IoT, Otentikasi, MQTT, Perangkat Terbatas, Dinamis, Berbasis kejadian, TAMARIN PROVER