Abstrak

Protokol authentikasi EAP MD5 dan EAP TLS adalah protokol keamanan yang masih sering dijumpai pengunaannya saat ini. Protokol Keamanan tersebut menggunakan proses authentikasi pada jaringan nirkabel dengan menggunakan IEEE 802.1x sebagai media transmisinya. Terdapat 3 komponen yang berperan pada IEEE 802.1x yaitu suplican , authenticator dan authentication server. Ketiga komponen inilah yang akan dimodelkan dengan menggunakan timed automata untuk melihat kondisi yang terjadi jika dilakukan serangan dengan menggunakan man in the middle attack dan dilakukan penambahan aspek waktu pada protokol tersebut.

Salah satu bentuk pengecekan terhadap model adalah dengan menggunakan timed automata. Timed Automata adalah finate automata klasik yang dapat memanipulasi waktu, berkembang terus menerus dan mensinkonisasikan dengan waktu mutlak[2].

Tugas akhir ini mengkhususkan diri pada proses memodelkan protokol authentikasi EAP MD5 dan EAP TLS dengan menggunakan Timed Automata dengan menambahkan kemungkinan retransmisi berdasarkan aspek waktu. Setelah model selesai maka berikutnya dilakukan pengecekan terhadap model berdasarkan aturan yang ada apakah dapat berjalan sesuai dengan aturan tersebut. Dari hasil verfikasi model tersebut dengan menggunakan alat UPPAAL maka dapat dilihat bahwasannya protokol authentikasi EAP MD5 dan EAP TLS dapat dimodelkan dengan menggunakan timed automata dan sesuai dengan aturan yang terdapat pada RFC protokol tersebut.

Kata kunci : EAP MD5, EAP TLS, Timed Automata, UPPAAL