Abstract

Authentication protocols EAP MD5 and EAP TLS are security protocols that are still frequently encountered use today. This Security Protocol using the process of authentication on a wireless network using the IEEE 802.1x as the transmission medium. There are three components that use a role in the IEEE 802.1x are suplican, authenticator and authentication server. These three components will be modeled using timed automata to see the condition that occurs when an attack carried out by using the man in the middle attack and carried out additional aspects of the time in the protocol.

One form of model checking is use timed automata. Timed automata are classic finate automata that can manipulate time, developing continuously and synchronously with the absolute time [2].

This final project focuses on the modeling process authentication protocols EAP MD5 and EAP TLS using Timed Automata with the added possibility of retransmission based on the aspect of time. Once completed, the next model to be checked against an existing model based on whether the rules can be run in accordance with these rules. From the results verify the model using UPPAAL tool, it can be seen authentication protocols EAP MD5 and EAP TLS can be modeled using timed automata, and in accordance with the rules contained in the RFC protocol.

Keywords: EAP MD5, EAP TLS, Timed Automata, UPPAAL