ABSTRAK

Perkembangan teknologi akses internet memasuki babak baru sejak adanya layanan akses *wireless* seperti hotspot. Dalam area ini, user dapat mengakses dengan perangkat yang mendukung teknologi *wireless*. Sejalan dengan perkembangan ini, berbagai protokol yang mendukung berbagai proses dalam teknologi ini dikembangkan dalam berbagai penelitian, proses autentikasi salah satunya, dan menghasilkan berbagai protokol, salah satunya EAP dan server autentikasi seperti RADIUS.

Walau demikian semakin meningkatnya teknologi protokol juga diimbangi dengan meningkatnya kemampuan para *attacker* dan *software* pendukungnya untuk menyerang protocol yang didesain untuk melindungi user yang terhubung pada server autentikasi.

Serangan *man-in-the-middle* adalah salah satu cara yang digunakan untuk menyadap data pribadi tersebut. Serangan ini berupa *attacker* akan berpura-pura sebagai *authenticator* (*access point*). *Robustness* sistem autentikasi berbasis EAP-MD5 pada jaringan *wireless* akan diuji dengan *formal methods* mengggunakan BAN Logic untuk membuktikan apakah serangan *man-in-the-middle* mampu mencari celah dalam protokol ini.

Kata kunci : EAP , BAN Logic , RADIUS , *Man-in-the-Middle , Formal Methods.*