ABSTRAK

Teknologi *video conference* berbasis IP khususnya yang menggunakan protokol H.323 telah dikembangkan sejak lama dan saat ini siap pakai. Protokol H.323 merupakan standar yang dibuat oleh ITU-T untuk melakukan komunikasi multimedia. Pada mulanya H.323 ditujukan untuk aplikasi komunikasi multimedia yang dalam perkembangannya H.323 juga mempunyai interface ke jaringan atau protokol telekomunikasi lainnya sehingga menjadikan protokol tersebut sebuah teknologi telekomunikasi yang independent terhadap jaringan yang digunakannya. H.323 mencakup banyak protokol dan melibatkan banyak elemen, sehingga isu keamanan / *security* didalamnya menjadi cukup kompleks.

Seiring berkembangnya dunia telekomunikasi, maka muncul beberapa protokol telekomunikasi baru yang menyempurnakan sistem dari protokol H.323 seperti halnya protokol SIP. Oleh karena perkembangan dunia teknologi telekomunikasi yang pesat tersebut, maka perlu dilakukan sebuah simulasi untuk membandingkan metode keamanan pada jaringan video conference dengan menggunakan dua skenario gangguan yaitu *Insertion Attack* dan *Interception and Monitoring Attack* pada dua metode keamanan *Authentication* dan *Key switch – Diffie Hellman.*

Setelah dilakukan pemodelan jaringan dengan OPNET dan skenario gangguan kepada kedua metode keamanan tersebut, didapatkan hasil bahwa kedua metode tersebut memiliki keunggulan dan cara kerja yang berbeda, dan sistem pengamanannya berdampak kepada layanan yang dirasakan oleh pengguna jaringan dalam parameter pengukuran delay, throughput, packet loss, SMB dan SSL dengan nilai kuantitatif gangguan pada insertion attack dan interception-monitoring antara metode authentication dengan key switch adalah pada SSL berbanding 5:1, throughput berbanding 2:1, delay 0:1, dan SMB berbanding 3:14.

Kata Kunci: H.323, Video Conference, Security, Authentication, Key Switch – Diffie Hellman