# ABSTRAK

Dhandy Wiriyadinata

Teknik Elektro

Analisis Performa Sistem Keamanan MIPv6 pada Proses Pensinyalan Menggunakan Algoritma AES dan Twofish

Teknologi *mobile* menjadi kebutuhan masyarakat modern, untuk mendukung konektivitas berlanjut, *Mobile* IPv6 menjadi solusi sekaligus penerus *Mobile* IP saat ini. Namun, aktivitas di jaringan internet membuat rentan terhadap berbagai tindakan jahat, masalah seperti keamanan informasi serta *overhead* yang tinggi menjadi perhatian komunikasi *mobile*. Untuk meningkatkan performa keamanan MIPv6, diperlukan metode enkripsi saat proses pensinyalan yang akan membangun asosiasi keamanan. IPsec menawarkan layanan keamanan di lapisan jaringan, terdapat 3 algoritma enkripsi yang disediakan saat ini, DES, 3DES, dan AES. Algoritma DES sudah tidak direkomendasikan penggunaannya berdasarkan faktor keamanan. Sementara, performa AES masih belum optimal dalam implementasi jaringan nirkabel. Penelitian ini bertujuan untuk menganalisis performa sistem keamanan dan kualitas layanan MIPv6 dengan mengimplementasikan algoritma AES dan Twofish. Algoritma Twofish merupakan kandidat yang memiliki potensi performa yang lebih baik dalam kriptografi simetris. Eksperimen menghasilkan kesimpulan bahwa performa algoritma Twofish lebih unggul berdasarkan keamanan serangan *cryptanalysis* dengan waktu *cracking* dua kali lebih lama dibandingkan AES. Dari segi kualitas layanan nilai *Throughput* Twofish memiliki kenaikan sebesar 20,05% dengan *delay* yang kecil dibandingkan AES sementara *packet loss* 0,023% pada Twofish dan 0,077% pada AES.

Kata Kunci: *Mobile* IPv6, Keamanan, IPsec, AES, Twofish

# ABSTRACT

Dhandy Wiriyadinata

Electrical Engineering

Analysis Security System Performance MIPv6 in Signaling Process

Using AES and Twofish Algorithms

Mobile technology has become a necessity for modern society, the ease that facilitates various information processes drives the growth of mobile device users. To support continuous connectivity, Mobile IPv6 technology is a solution and a successor to the current Mobile IP. However, activities on the internet are vulnerable to various malicious acts. Issues such as information security and high overhead are concern. To improve security performance of MIPv6, an encryption is needed during signaling process that will build security associations. IPsec offers security at the network layer. There are 3 encryption algorithms provided, DES, 3DES, and AES. The DES algorithm is no longer recommended based on security factors. Meanwhile, AES performance is still not optimal in the implementation of wireless networks. This study aims to analyze the performance of security system and quality of MIPv6 services by implementing AES and Twofish algorithms. Twofish algorithm has potential performance. Experiments concluded performance of Twofish algorithm is superior based on security of cryptanalysis attacks with cracking times that are twice compared to AES. In terms of service quality, Throughput of Twofish increased 20,05% with small delay compared to AES, while packet loss is 0,023% for Twofish and 0,077% for AES.

Keywords: Mobile IPv6, Security, IPsec, AES, Twofish