# Algoritma pembangkitan kunci dan enkripsi untuk perlindungan privasi pada mobile ad hoc networks = New key generation and encryption algorithms for privacy preservation in mobile ad hoc networks

Amiruddin, author



---

Abstrak

Mobile Ad Hoc Networks MANETs mendapatkan aplikasi yang luas bersamaan dengan kemajuan teknologi. Namun, MANETs beresiko karena kurangnya mekanisme keamanan. Dalam makalah ini, diusulkan algoritma baru untuk pembangkit kunci dan enkripsi untuk perlindungan privasi di MANETs. Fibonacci dimodifikasi dengan menambahkan faktor pengacak untuk menghasilkan rangkaian kunci acak dengan panjang yang sesuai yang dibutuhkan namun dengan overhead komputasi yang rendah. Sistem One Time Pad OTP dimodifikasi dengan menambahkan faktor pengacak untuk kerahasiaan data melalui enkripsi yang memenuhi uji keacakan, difusi, dan konfusi. Evaluasi algoritma yang diusulkan dilakukan dengan menggunakan Matlab dan NS-2. Hasil percobaan menunjukkan bahwa algoritma yang diusulkan menghasilkan rangkaian kunci dan Ciphertext yang acak. Melalui beberapa pengujian yaitu kecepatan, korelasi dan autokorelasi, difusi, dan konfusi, hasil simulasi menunjukkan keunggulan algoritma usulan terhadap algoritma lainnya. Sebagai bukti konsep, algoritma usulan telah disimulasikan dengan simulator jaringan.

<hr />

Mobile Ad Hoc Networks MANETs get widespread applications along with the evolving technologies. However, MANETs are at risk due to the shortage of security mechanisms. In this paper, we propose new algorithms for key generation and encryption for privacy preservation in MANETs. We modified Fibonacci sequence by adding scrambling factor to generate random key sequences with required length but incurred low computational overhead. We modified the One Time Pad OTP system by adding scrambling factor for data confidentiality through encryption which satisfies the randomness, diffusion, and confusion tests. Evaluation of the proposed algorithms was conducted using Matlab and NS 2. Experiment results showed that the proposed algorithms produced random key sequences and Ciphertexts. Through several tests i.e. speed, correlation and autocorrelation, diffusion, and confusion tests, the simulation result showed the superiority of our algorithms over the other algorithms. For the proof of concept, our algorithms have been simulated in the network simulator.