ABSTRAK

Firman Ardiyansyah, Jurusan Teknik Elektro,Fakultas Teknik Universitas Brawijaya, Oktober 2016, *Simulasi Serangan Black Hole pada MANET (Mobile Ad Hoc Network).* Dosen Pembimbing: Ir. Wahyu Adi Priyono, M.T. dan Rusmi Ambarwati, S.T., M.T.

Abstrak— MANET *(Mobile Ad Hoc Network)* adalah kumpulan perangkat *mobile* yang digunakan untuk berkomunikasi secara nirkabel tanpa otoritas jaringan terpusat atau terstruktur. MANET memiliki beberapa karakteristik khusus seperti media yang terbuka, topologi yang dinamis, kurangnya pemantauan pusat, algoritma yang sederhana, dan tidak ada mekanisme pertahanan yang jelas. Dalam sistem jaringan yang terbuka, MANET mudah terkena berbagai jenis serangan, salah satunya adalah serangan *blackhole*. Serangan *black hole* adalah sejenis serangan *Denial of Service(DoS)* pada MANET dimana node berbahaya menyatakan kepada node sumber bahwa node tersebut memiliki rute terbaik untuk mencapai node tujuan. Masalah utama yang timbul pada saat terjadi serangan *black hole* adalah bagaimana untuk mendeteksi *black hole*, sambil menghindari sebanyak mungkin diagnosa yang salah, seperti RREP palsu. Dalam simulasi ini, mekanisme *watchdog* diintegrasikan dengan teknik *Bayesian filtering*. Mekanisme *watchdog* bertujuan memantau aktivitas node dalam jaringan untuk mendeteksi node bermasalah yang merugikan jaringan. Simulasi dilakukan menggunakan protocol routing AODV dengan dua skenario, yaitu simulasi serangan *black hole* dengan dan tanpa mekanisme *watchdog* menggunakan perangkat lunak NS-2. Hasil perbandingan performansi pada saat tidak menggunakan mekanisme *watchdog* dan dengan mekanisme watchdog diukur berdasarkan parameter *packet loss*, *delay*, dan *throughput*. nilai *packet loss* tanpa mekanisme watchdog sebesar nilai paket yang terkirim yaitu 100% untuk ukuran paket 1000 byte sementara pada saat penggunaan mekanisme *watchdog* nilai *packet loss* sebesar 0% untuk ukuran 1000 byte. Semakin kecil nilai *packet loss*, tingkat keberhasilan pencegahan serangan *black hole* dengan mekanisme *watchdog* semakin tinggi.

Kata Kunci : Serangan *Black Hole*, AODV, Mekanisme *watchdog*, NS-2.

SUMMARY

Firman Ardiyansyah Departement of Electrical Engineering, Faculty of Engineering, Universitas Brawijaya, October 2016, **Simulation of Black Hole attack in MANET (Mobile Ad Hoc Network)**, Supervisor: Ir. Wahyu Adi Priyono, M.T. and Rusmi Ambarwati, S.T., M.T.

Abstraction— MANET (Mobile Ad Hoc Network) is a collection of mobile devices that are used to communicate wirelessly without the authority of a centralized network or structured. MANET has some special characteristics such as an open media, dynamic topology, the lack of central monitoring, a simple algorithm, and no obvious defense mechanism. In the system of an open network, MANET is exposed to various types of attacks, one of which is a blackhole attack. Attacks black hole is a type of Denial of Service (DoS) on MANET where malicious nodes declare the source node that has the best route to the destination node. The main problem that arises in the event of black hole attacks is how to detect black holes, while avoiding as much as possible the wrong diagnosis, such as false RREP. In this simulation, the watchdog mechanism is integrated with Bayesian filtering techniques. Watchdog mechanism seeks to monitor the activity node in a network to detect problematic adverse node network. Simulations carried out using a routing protocol AODV with two scenarios, the simulated black hole attacks with and without using the software watchdog mechanism NS-2. Performance comparison results when not using the watchdog mechanism and the watchdog mechanisms measured by packet loss, delay, and throughput. the value of packet loss without a watchdog mechanism in the amount of packages sent 100% to the package size is 1000 bytes at a time when the use of the watchdog mechanism packet loss value of 0% for the 1000 bytes package size. The smaller the value of packet loss, the success rate of black hole attack prevention with higher watchdog mechanism.

Keywords: Black Hole Attack, AODV, watchdog mechanism, NS2.