ABSTRACT

Vehicular Ad-hoc Network (VANET) technology is a sub-domain of the Mobile Ad-hoc Network (MANET) used in vehicles. This technology can improve driver safety because it provides communication features between vehicles. The vehicle will act as a node and supporting infrastructure. The use of this technology is vulnerable to various types of attacks such as DOS because it is still under development, increasing security for this technology will guarantee the realization of this technology. The various attacks that occur will be classified and determined which gives the heaviest impact and disrupts the performance of this technology. The use of this technology will help create digital traffic that can improve the safety and comfort of users on the road and to realize the Intelligent Transport System (ITS) to ensure a friendly environment for travel.

This research utilizes a framework for misbehavior detection (F2MD) which contains modules in the communication simulation process on VANET technology. This framework helps in detection by calculating the models, namely legacy checks and catch checks that represent vehicles according to conditions when communication on VANET technology occurs. The results of the detection will help in the process of mitigation and prevention of attacks that will occur. The results of calculations using the model used indicate an increase and are able to detect attacks with a precision of up to 90% based on the results of the calculation of recall, precision, and accuracy.

Detection results using F2MD show that the catch check model provides better detection results when it detects a denial of service (DOS) attack in a predetermined scenario. In the scenarios that have been tested show that the value of recall has increased to 0.36%, the value of precision increased by 6.7% and the value of accuracy increased by 0.17%.

Keywords : *VANET ; MANET; Node ; Communication ; DOS; ITS; framework.*

ABSTRAK

Teknologi *Vehicular Ad-hoc Network* (VANET) adalah sub-domain dari *Mobile Ad-hoc Network* (MANET) yang digunakan dalam kendaraan. Teknologi ini mampu meningkatkan keamanan pengemudi karena menyediakan fitur komunikasi antar kendaraan. Kendaraan akan bertindak sebagai simpul dan infrastruktur pendukung. Penggunaan teknologi ini rentan terhadap berbagai jenis serangan seperti DOS karena masih dalam tahap pengembangan, peningkatan keamanan untuk teknologi ini akan menjamin realisasi teknologi ini. Berbagai serangan yang terjadi akan diklasifikasikan dan ditentukan mana yang memberikan dampak terberat dan mengganggu kinerja teknologi ini. Penggunaan teknologi ini akan membantu menciptakan lalu lintas digital yang dapat meningkatkan keamanan dan kenyamanan pengguna di jalan dan untuk mewujudkan *Intelligent Transport System* (ITS) untuk memastikan lingkungan yang ramah untuk perjalanan.

Penelitian ini memanfaatkan *framework* for misbehavior detection (F2MD) yang berisi modul-modul dalam proses simulasi komunikasi pada teknologi VANET. *Framework* ini membantu dalam pendeteksian dengan melakukan perhitungan terhadap model-model yaitu *legacy check* dan *catch check* yang merepresentasikan kendaraan sesuai dengan kondisi ketika komunikasi pada teknologi VANET terjadi. Hasil dari pendeteksian tersebut akan membantu dalam proses mitigasi maupun pencegahan terhadap serangan yang akan terjadi. Hasil perhitungan menggunakan model yang digunakan menunjukkan peningkatan dan mampu mendeteksi serangan dengan ketepatan hingga 90% berdasarkan hasil dari metrik perhitungan *recall*, *precision*, dan akurasi.

Hasil deteksi menggunakan F2MD menunjukkan model *catch check* memberikan hasil deteksi yang lebih baik ketika mendeteksi serangan *denial of service* (DOS) pada skenario yang telah ditentukan. Pada skenario yang telah diujikan menunjukkan nilai *recall* mengalami peningkatan hingga 0,36%, nilai *precision* meningkat 6,7% dan nilai akurasi meningkat 0,17%.

Kata Kunci -- *VANET ; MANET; Node ; Komunikasi ; DOS ; ITS; framework.*