ABSTRAK

Pendeteksian *malicious* node menjadi hal yang cukup sulit pada jaringan DTN. Hal ini disebabkan komunikasi pengiriman pesan yang bersifat *intermittent*, *delay* yang panjang, dan *end-to-end path* tidak selalu ada. Salah satu *malicious* node yang ada di jaringan DTN adalah serangan *blackhole*. Node *blackhole* akan membuang semua pesan yang diterima sekalipun ia masih memiliki *buffer* dan memanfaatkan node lain untuk menyembunyikan perilaku nakalnya (*Colluding Blackhole*). Dalam penelitian ini, penulis memanfaatkan metode yang ada di *machine learning* untuk melakukan pendeteksian *blackhole*, yaitu *Fuzzy Decision Tree (FDT)*. Penulis akan mengumpulkan data perilaku setiap node yang melakukan pengiriman pesan di jaringan, dan kemudian membangun sebuah model untuk mengklasifikasi data tersebut berdasarkan kelas normal atau *blackhole* dengan batas yang tidak tegas, serta membandingkan hasil evaluasi model tesebut dengan beberapa variasi serangan.

Kata kunci: *Blackhole attack, fuzzy decision tree, delay tolerant network*

ABSTRACT

Detecting malicious nodes becomes quite difficult on a DTN network. This is due to intermittent message delivery communications, long delays, and the end-to-end path is not always available. One of the malicious nodes in the DTN network is a blackhole attack. The blackhole node will discard all received messages even if it still has a buffer and use other nodes to hide its naughty behavior (Colluding Blackhole). In this study, the authors use the existing method in machine learning to perform blackhole detection, namely Fuzzy Decision Tree (FDT). The author will collect data on the behavior of each node that sends messages on the network, and then build a model to classify the data based on normal or blackhole classes with unclear boundaries, and compare the results of the evaluation of the model with several variations of attacks.

Keywords: Blackhole attack, fuzzy decision tree, delay tolerant network