ABSTRAK

Jaringan Oportunistik merupakan merupakan jaringan node yang terhubung secara *wireless*. Node terhubung hanya untuk sementara, dan topologi jaringan dapat berubah karena mobilitas node. Node secara oportunistik berkomunikasi satu sama lain dalam bentuk "*Store – Carry – Forward*" saat berhubungan satu sama lain. Akibat dari karakteristik node di jaringan seperti ini, maka jaringan oportunistik rentan terhadap ancaman *packet dropping* yang disebabkan oleh *malicious node*. *Malicious node* memiliki kemampuan untuk membuang sebagian atau seluruh paket yang diberikan kepadanya dengan sengaja. Hal ini mengakibatkan akan banyak paket yang tidak sampai pada tujuan selama komunikasi berlangsung dan berimbas pada dilakukannya *retransmit* paket dalam jaringan yang menyebabkan *overhead ratio* dalam jaringan menjadi terlalu tinggi dan unjuk kerja jaringan pun menurun.

Maka dari itu pada penelitian kali ini penulis mengusulkan skema deteksi *malicious node* dengan menggunakan teknik *Merkle Tree Hashing* dalam mendeteksi dan melacak keberadaan *malicious node* dan menguji keakuratan deteksi ini dengan mempertimbangkan akurasi deteksi malicious node, rasio *false negative*, dan rasio *false positif* dalam pendeteksian *malicious node*. Hasil pengujian menunjukkan deteksi *malicious node* menggunakan teknik *Merkle Tree Hashing* akurat dalam mendeteksi keberadaan *malicious node* di dalam jaringan dengan jumlah *malicious node* yang sedikit. Sementara jika jumlah *malicious node* di dalam jaringan terbilang banyak. Namun, pendeteksian menggunakan teknik *merkle tree hashing* menunjukkan rasio kesalahan pendeteksian terhadap *normal node* (rasio *false positif*) rendah ketika jumlah *malicious node* di dalam jaringan terbilang banyak. Sehingga, dibutuhkan mekanisme pendeteksian tambahan pada teknik *merkle tree hashing* untuk meningkatkan akurasi pendeteksian.

Kata Kunci : Jaringan Oportunistik, Merkle Tree Hashing, Malicious Node.

ABSTRACT

Opportunistic Network is a network of nodes that areconnected wirelessly. The nodes are connected only temporarily, and the network topology may change due to the mobility of the nodes. Nodes opportunistically communicate with each other in the form of "Store – Carry – Forward" when they relate to each other. . As a result of the characteristics of nodes in a network like this, opportunistic networks are vulnerable to packet dropping threats caused by malicious nodes. Malicious nodes have the ability to intentionally discard part or all of the packets assigned to them. This will result in many packets not reaching their destination during communication and impact on packet retransmits in the network which causes the overhead ratio in the network to be too high and network performance to decrease. Therefore in this study the authors propose a malicious node detection scheme using the Merkle Tree Hashing technique in detecting and tracking the presence of malicious nodes and testing the accuracy of this detection by considering the accuracy of detection of malicious nodes, the ratio of false negatives, and the ratio of false positives in detecting malicious nodes. . The test results show that the detection of malicious nodes using the Merkle Tree Hashing technique is accurate in detecting the presence of malicious nodes in the network with a small number of malicious nodes. Meanwhile, if the number of malicious nodes in the network is quite large. However, detection using the merkle tree hashing technique shows the ratio of detection errors to normal nodes (false positive ratio) is low when the number of malicious nodes in the network is quite large. Thus, additional detection mechanisms are needed in the merkle tree hashing technique to improve detection accuracy.

Keyword : Opportunistic Network, Merkle Tree Hashing, Malicious Node.