INTISARI

EVALUASI *ROBUSTNESS* MODEL DETEKSI INTRUSI JARINGAN BERBASIS GRAPH NEURAL NETWORK MELALUI INJEKSI *NOISE*

Oleh

Satriawan Rasyid Purnama

21/485614/PPA/06219

Sebagian besar model deteksi intrusi jaringan beroperasi dengan asumsi bahwa data *training* dan *testing* terdistribusi secara mirip. Asumsi ini sering tidak berlaku karena lingkungan jaringan nyata memiliki tingkat dinamisitas yang tinggi dan mencakup perubahan distribusi data yang menyebabkan performa model turun. *Robustness* memastikan bahwa model tersebut tidak mudah terpengaruh oleh data yang tidak representatif atau *outlier*, sehingga evaluasi *robustness* penting bagi keandalan model deteksi intrusi jaringan untuk membantu melindungi jaringan dan sistem dengan efektif. Graph Neural Network (GNN) telah dikembangkan dalam penelitian terkini untuk deteksi intrusi jaringan, karena keunggulannya yaitu mempertimbangkan topologi aliran jaringan. Namun, evaluasi *robustness* model GNN terhadap perubahan distribusi data belum pernah dilakukan sebelumnya. Penelitian ini mengusulkan evaluasi *robustness* model deteksi intrusi jaringan berbasis GNN melalui injeksi *noise*. Tujuan dari injeksi *noise* adalah untuk mengubah nilai atribut pada data testing dan mengevaluasi bagaimana reaksi model terhadap perubahan distribusi data. Deep Neural Network (DNN) dan beberapa model berbasis *tree* juga digunakan sebagai perbandingan dalam evaluasi tersebut. Hasil eksperimen menunjukkan bahwa model GNN lebih *robust* terhadap *noise* daripada model pembandingnya. GNN hanya mengalami penurunan f1-score makro sebesar 27%, 45%, dan 10% pada dataset BoT-IoT, ToN-IoT, dan UNSW-NB15, yang merupakan penurunan terkecil dibandingkan dengan model yang memiliki penurunan terkecil di bawah GNN, yaitu sebesar 44%, 70%, dan 16%.

Kata Kunci: Deteksi Intrusi Jaringan, Evaluasi *Robustness*, Graph Neural Network, Injeksi *Noise*

ABSTRACT

EVALUATING THE ROBUSTNESS OF GRAPH NEURAL NETWORK BASED NETWORK INTRUSION DETECTION MODEL THROUGH NOISE INJECTION

By

Satriawan Rasyid Purnama

21/485614/PPA/06219

Most network intrusion detection models operate under the assumption that the training and testing data are similarly distributed. This assumption is often not true as real-world networks have high levels of dynamism and include changes in data distribution which lead to a drop in model performance. Robustness ensures that the model is not easily influenced by non-representative or outlier data. Hence, evaluating robustness is important for the reliability of the network intrusion detection model to effectively secure networks and systems. Recently, Graph Neural Networks (GNNs) have been developed for intrusion detection because of their advantage of considering the network flow topology. Evaluating the robustness of GNN models towards changes in data distribution has not been previously conducted. This study proposes to assess the robustness of GNN-based network intrusion detection models by injecting noise. The noise injection is performed by modifying the attribute values in the testing data to evaluate how the models react to changes in data distribution. Deep Neural Network (DNN) and several tree-based models are also used as comparison models. According to the experimental findings, the GNN model outperformed other models in terms of robustness against noise. The macro f1-score of the GNN model only decreased slightly by 27%, 45%, and 10% on the BoT-IoT, ToN-IoT, and UNSW-NB15 datasets, respectively. This decrease is the smallest compared to the model with the smallest decrease below GNN, which experienced a decrease of 44%, 70%, and 16%.

Keywords: Network Intrusion Detection, Robustness Evaluation, Graph Neural Network, Noise Injection