Comparison of Content Between "A New D-MAGIC: Dynamic Model for Cybersecurity Attack Detection using GNNs into Clustering" to "Real-Time Network Security: Integrating ANN and Dynamic Graph-Based Clustering"

This document outlines the additional content included in this that was not present in "A New D-MAGIC: Dynamic Model for Cybersecurity Attack Detection using GNNs into Clustering". The comparison highlights new methodology, more experiments and a more detailed explanation.

The previous paper was submitted to **2025 IEEE International Conference on Communications (ICC): SAC Machine Learning for Communications and Networking Track** on Nov. 7, 2024.

1. **Introduction of SAGA Algorithm**
    a. The new algorithm, SAGA (Sophisticated Anomaly detection with GNN into ANN), builds upon D-MAGIC by incorporating Approximate Nearest Neighbor (ANN) analysis to enhance anomaly detection capabilities.

    b. SAGA introduces a hybrid approach that detects both clustered anomalies and isolated outliers, which clustering alone might fail to classify. This method extends the detection scope and improves identification of subtle or emerging threats.

2. **More Experiments with the Algorithm (D-MAGIC)**
    a. This paper includes experiments with different flow parameter (F) window sizes, such as F=1000,2000,4000, providing a more comprehensive evaluation of how the detection window size impacts anomaly detection performance.

    b. These variations in F offer insights into the trade-offs between computational efficiency and detection accuracy in real-time anomaly detection scenarios

3. **Expansion of Existing Sections**
    a. **Related Work:** Expanded to include more articles and contextual background, providing a broader discussion of existing methods in anomaly detection and their limitations compared to the proposed methods.

    b. **Methodology:** Enhanced descriptions of both D-MAGIC and SAGA, with detailed explanations of their mechanisms, including tripartite graph representation, GCN embedding, and the integration of ANN.

    c. **Results Section:** Now includes comparative analysis of the two algorithms (D-MAGIC and SAGA), highlighting their respective strengths on CIC-IDS-2017 and CSE-CIC-IDS-2018 datasets. For example: D-MAGIC excels on dense datasets, while SAGA achieves higher accuracy for sparse anomalies.

4. **Addition of Detailed Tables to the Results Section**
    In the previous article, only a single table was included to summarize accuracy for each attack type in D-MAGIC (for both CIC-IDS-2017 and CSE-CIC-IDS-2018). The updated article includes significantly more detailed tables:
    a. **Performance Metrics for F=1000,2000,400 on D-MAGIC (CIC-IDS-2018):**
        i. Tables present F1-score, precision, recall, and accuracy for each attack type.
        ii. These tables provide insights into how detection performance varies with different window sizes.

b. **Performance Metrics Breakdown for F=1000,2000,4000 on D-MAGIC (CIC-IDS-2018):**
    i. Tables include false positive rate (FPR) and true positive rate (TPR) for each attack type.
    ii. Breakdown enables detailed evaluation of detection quality for individual attacks.
c. **Performance Metrics for F=1000,2000,4000 on D-MAGIC (CIC-IDS-2017):**
    i. Similar to the CIC-IDS-2018 tables, these show F1-score, precision, recall, and accuracy for each attack type.
    ii. Highlights performance trends across different window sizes.
d. **Performance Metrics for F=4000 on SAGA (CIC-IDS-2018):**
    i. A single table summarizing F1-score, precision, recall, and accuracy for each attack type under the SAGA algorithm.
    ii. Demonstrates the unique strengths of SAGA in detecting isolated and emerging threats.
e. **Performance Metrics Breakdown for F=4000 on SAGA (CIC-IDS-2018):**
    i. Includes FPR and TPR for each attack type, complementing the general performance metrics table.
    ii. Highlights the specific advantages of the SAGA algorithm in anomaly detection.

These additional tables provide a granular and detailed evaluation of the algorithms' performance, offering a clearer understanding of their strengths and limitations under various configurations.

This structured approach in the current article strengthens its contributions and provides a clearer understanding of the proposed solutions' adaptability and efficacy in varying conditions.