



# Generating Realistic Cyber Security Datasets for IoT Networks with Diverse Complex Network Properties

Fouad Al Tfaily<sup>1,2</sup><sup>a</sup>, Zakariya Ghalmane<sup>1</sup><sup>b</sup>, Mortada Termos<sup>1,2</sup>, Mohamed-el-Amine Brahmia<sup>1</sup>, Ali Jaber<sup>2</sup> and Mourad Zghal<sup>1</sup>

<sup>1</sup>CESI LINEACT UR 7527, Strasbourg, France

<sup>2</sup>Computer Science Department, Faculty of Sciences, Lebanese University, Beirut, Lebanon

**Keywords:** Complex Networks, Internet of Things, Artificial Intelligence, Cyber Security, Federated Learning, Network Properties, Intrusion Detection.

**Abstract:** In the cybersecurity community, finding suitable datasets for evaluating Intrusion Detection Systems (IDS) is a challenge, particularly due to limited diversity in complex network properties. This paper proposes a dual-purpose approach that generates diverse datasets while producing efficient, compact versions that maintain detection accuracy. Our approach employs three techniques - community mixing modification, centrality-based modification, and time-based modification - each targeting specific network property adjustments while achieving significant dataset size reductions (up to 81.5%). Our approach is validated on real-world datasets, including NF-UQ-NIDS, CCD-INID-V1, and TON-IoT, demonstrating its ability to generate realistic datasets while preserving network properties, attack patterns, and structural integrity. The generated datasets exhibit diverse complex network properties, making them particularly useful for IDS technique evaluation that incorporates complex network measures. The reduced size and preserved accuracy (96.4%) make these datasets especially valuable for resource-constrained environments. Moreover, our approach facilitates the construction of homogeneous datasets required for federated learning situations where data distribution similarity across clients is essential. This contribution helps address both dataset scarcity and computational efficiency challenges while ensuring that the generated datasets retain the characteristics of real-world network traffic.

## 1 INTRODUCTION


Intrusion Detection Systems (IDS) have become critical for network security as cyber attacks against IoT devices increased over 100% in 2020-2021 Ferrag et al. (2022), demanding adaptive detection mechanisms Brahmia et al. (2022). Complex networks provide a framework for analyzing these structures through key properties: density (proportion of existing connections), transitivity (clustering tendency), and mixing parameter (inter-community connections) Ghalmane et al. (2018a, 2019a).


Network-based approaches have been successfully applied across domains, from social networks Hazimeh et al. (2018); Hamizeh et al. (2017) to IDS. Recent research showed that complex network properties are vital contributors to intrusion detection accuracy Termos et al. (2023). Termos et al. Ter-

mos et al. (2024) demonstrated through their GDLC framework that complex network features can increase detection accuracy by up to 7.7% in binary classification and 6.27% in multi-class classification, underscoring the need for datasets with diverse network characteristics.

These properties strongly influence the effectiveness of centrality measures in intrusion detection Ghalmane et al. (2019b), particularly for detecting community-based attacks. While hubs and overlapping nodes maintain network robustness Ghalmane et al. (2020, 2021). Current datasets face two critical limitations: lack of property diversity and significant computational overhead Al-Hawawreh et al. (2022).

The challenge is greater in federated learning where multiple clients train models without sharing data Ferrag et al. (2021). Federated learning, a privacy-preserving distributed learning paradigm Arbaoui et al. (2024); ARBAOUI et al. (2022), enhances computational efficiency while addressing data heterogeneity in IoT architectures Al-Hawawreh et al.

<sup>a</sup> <https://orcid.org/0009-0001-0513-1996>

<sup>b</sup> <https://orcid.org/0000-0002-2440-2886>

(2022). However, effective model training requires homogeneous data distribution across clients, which is difficult to achieve with heterogeneous real-world network data Ferrag et al. (2021).

The scarcity of diverse real-world datasets, driven by privacy concerns and operational constraints, limits the sharing of network traffic data Ferrag et al. (2022). Public datasets like CIC-IDS2017 Sharafaldin et al. (2018) and UNSW-NB15 Moustafa and Slay (2015) are available but are typically tied to specific network configurations and attack scenarios, making them unsuitable for evaluating IDS solutions in varied settings. Moreover, these datasets often lack the full range of complex network properties needed to assess advanced detection techniques.

To address these challenges, this paper introduces a novel approach that serves two critical purposes: generating diverse datasets with varying network properties to address evaluation needs, and producing more efficient, compact datasets while preserving essential characteristics. Our approach achieves significant size reductions while maintaining high detection accuracy. We accomplish this by three techniques:

- **Community Mixing Modification:** Combine high-density communities to reduce mixing parameter and enhance intra-community connections.
- **Centrality-Based Modification:** Select high-centrality nodes to increase network density and transitivity.
- **Time-Based Modification:** Utilize temporal window selection to achieve desired network properties while maintaining chronological patterns.

The remainder of this paper is structured as follows: Section 2 covers network properties and IDS datasets. Section 3 details our methodology for dataset generation techniques for diverse properties and reduced sizes. Section 4 presents experimental validation of property preservation and efficiency. Section 5 discusses conclusions and future work.

## 2 RELATED WORK

Network intrusion detection systems rely heavily on diverse datasets for development and evaluation.

As shown in Table 1, existing approaches address different IDS needs: Protocol-specific datasets like MQTTset Vaccari et al. (2020) target specific network protocols, while privacy-focused approaches such as Federated TON-IoT Moustafa et al. (2020) emphasize data confidentiality. General-purpose datasets including TON-IoT Alsaedi et al. (2020), CIC-IDS2017 Sharafaldin et al. (2018), and NF-UQ-NIDS Sarhan et al. (2022) provide varied attack scenarios but show limited network characteristic variation.

Recent synthetic data generation methods, including GAN-based techniques and topology preservation augmentation, prioritize data volume over network properties Nukavarapu et al. (2022). While GANs excel in realism, they struggle with key network properties and demand high computational resources. Topology-preserving augmentation similarly lacks diversity in structural characteristics, restricting applicability in varied network scenarios.

These approaches share a common limitation—they overlook the role of complex network properties in intrusion detection. Termos et al. (2024) showed via GDLC that features enhance detection accuracy in binary and multi-class tasks, emphasizing the need for diverse datasets. Ghalmane et al. (2018b, 2022) demonstrated that community structure, mixing parameters, and centrality measures impact attack detection, particularly for community-based attacks. These findings, validated in industrial environments Al-Hawawreh et al. (2022), highlight the need for methods that preserve structural integrity while achieving desired network properties.

This limitation is particularly apparent in federated learning scenarios, where heterogeneous environments require consistent data distributions. Current datasets struggle with data scarcity, lacking capability to generate homogeneous datasets while preserving network properties. This limitation, combined with the need for diverse properties in modern IDS approaches, motivated developing an approach for both standalone and federated learning environments.

Table 1: Characteristics of Existing Dataset Modification Approaches.

Approach	Property Control	Attack Preservation	Federated Learning Support	Scalability
Protocol-based Vaccari et al. (2020)	Limited	High	No	Medium
Feature-based Moustafa et al. (2020)	None	High	No	High
Topology-based Al-Hawawreh et al. (2022)	Partial	Medium	Partial	Medium
Community-based Ghalmane et al. (2019b)	High	Low	No	Low

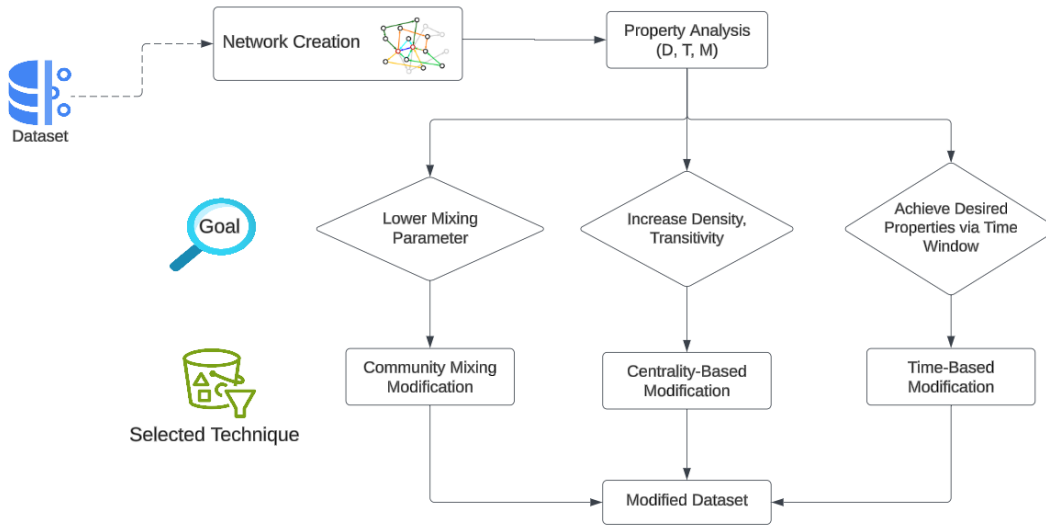


Figure 1: Proposed methodology showing technique selection based on property changes. Each path targets specific properties: lowering mixing parameter (left), increasing density and transitivity (center), or preserving properties via time window selection (right).

### 3 PROPOSED METHODOLOGY

Our methodology introduces an approach that addresses two key challenges: generating diverse network intrusion datasets and producing more efficient, compact versions while preserving detection accuracy. Our approach achieves this through a framework that varies network properties while significantly reducing dataset size. Before describing our approach in detail, we present the general framework and then detail each technique.

#### 3.1 General Methodology Overview

Our proposed approach targets three fundamental complex network properties: **density** (the ratio of actual connections to possible connections in the network), **transitivity** (the likelihood that adjacent nodes are interconnected, indicating clustering tendency), and the **mixing parameter** (the proportion of edges connecting nodes from different communities to the total edges). Our methodology follows a systematic workflow for dataset generation, illustrated in Figure 1. First, traffic records are transformed into a graph representation where nodes represent devices and edges represent connections, then fundamental network properties - Density, Transitivity, and Mixing parameter - are computed for this constructed graph. Based on these values, one of three techniques is applied to generate a synthetic dataset.

Thresholds for these properties were determined

through empirical analysis of real-world datasets to ensure realistic network characteristics. For example, Density (D) and Transitivity (T) are considered high when exceeding 0.01, and Mixing parameter (M) is considered high when exceeding 0.1. These thresholds guide the selection of communities for merging, which is performed using automated algorithms such as Infomap for community detection.

#### 3.2 Dataset Modification Techniques

The modification process takes network traffic data in standard flow format (source/Destination IP, timestamps, and associated features) as input. Each modification technique preserves the relationship between network flows and attack labels by maintaining flow-level mappings throughout the transformation process. The output retains the same format as the input data but with reduced size and modified network properties based on the applied technique. The following subsections detail each modification approach.

##### 3.2.1 Community Mixing Modification

The Community mixing modification technique primarily focuses on lowering the mixing parameter of the network. By merging high-density communities, this technique achieves two complementary effects: reduction of inter-community links and enhancement of intra-community connections. The mechanism behind this approach lies in how community merging affects network structure: when high-density commu-

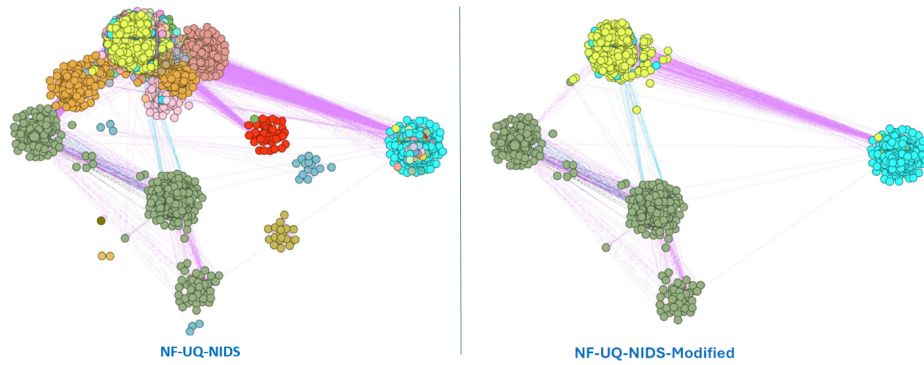


Figure 2: Network visualization of NF-UQ-NIDS before (left) and after (right) community mixing modification. Colors indicate communities, and node sizes represent degree centrality. The transformation consolidates communities and reduces inter-community connections, lowering the mixing parameter while preserving network structure.

nities are combined, edges that previously connected different communities become internal connections within the merged community.

The implementation process begins with community detection using the Infomap algorithm. For each detected community, we calculate its density as the ratio of existing connections to possible connections. Communities exceeding a density threshold of 0.01 are identified as candidates for merging. These high-density communities are then iteratively merged, and the network is reconstructed while preserving all original connections. This process continues until no further merging opportunities exist that would improve the network's mixing parameter.

### 3.2.2 Centrality-Based Modification

The centrality-based modification technique increases network density and transitivity through strategic node selection, computing eigenvector centrality for all network nodes. By keeping the top-ranked nodes based on a selected percentage threshold - for example 30% - ranked by their centrality scores, we create a more tightly connected network structure.

The implementation involves first calculating eigenvector centrality values for each node, which measures both direct and indirect influence in the network. The nodes are then sorted by their centrality scores, and the top 30% are selected as the core network components. This threshold was determined empirically to balance network density and computational efficiency, ensuring that the most influential

pathways are preserved while reducing dataset size.

### 3.2.3 Time-Based Modification

The time-based modification technique achieves desired network properties through temporal window selection. By analyzing and selecting specific time periods from the network traffic data, we identify segments where the network exhibits target values for density, transitivity, and mixing parameter. The mechanism works by evaluating how these network properties vary across different time windows - when we identify a period that matches our desired characteristics, selecting that window generates a dataset with the target network properties.

The implementation process uses a sliding window approach with a five-day interval, chosen to capture meaningful temporal patterns while maintaining computational feasibility. For each window position, we construct the corresponding network and calculate its properties—density, transitivity, and mixing parameter. Windows meeting predefined thresholds (e.g., density  $>0.01$ , transitivity  $>0.01$ , mixing parameter  $<0.1$ ) are identified, and the best matching target characteristics is selected. These thresholds were derived from analysis of real-world datasets to ensure realistic behavior. The selection process is automated, ensuring consistent application of the technique while preserving chronological integrity.

Table 2: Network property changes between original and generated datasets. Metrics include density (ratio of actual to possible connections), transitivity (clustering tendency), and mixing parameter (community separation).

Property	NF-UQ-NIDS (Original)	NF-UQ-NIDS (Generated)	CCD-INID-V1 (Original)	CCD-INID-V1 (Generated)	CIC-ToN-IoT (Original)	CIC-ToN-IoT (Generated)
Density	0.0001	0.0177	0.0071	0.0307	1.709e-05	0.0000
Transitivity	0.0001	0.0046	0.0021	0.0032	0.1440	0.1053
Mixing	0.7742	0.0085	0.1909	0.1857	0.5670	0.0026



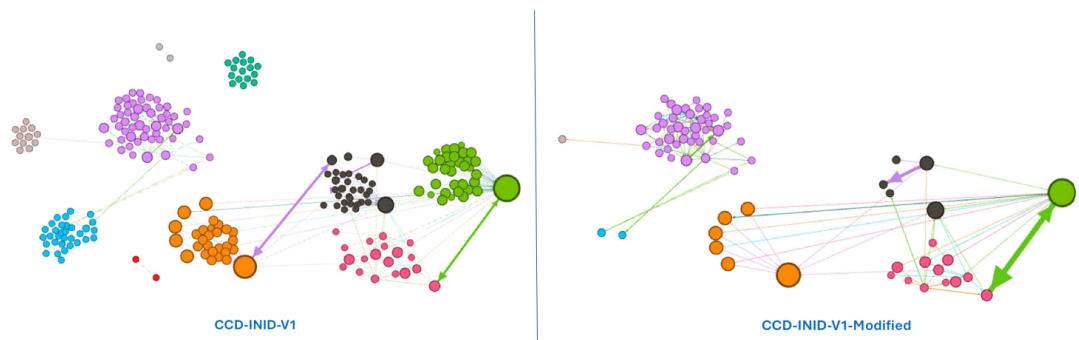


Figure 3: Network visualization of CCD-INID-V1 before (left) and after (right) centrality-based modification. Node sizes indicate eigenvector centrality, showing the selective preservation of high-centrality nodes while maintaining network structure.

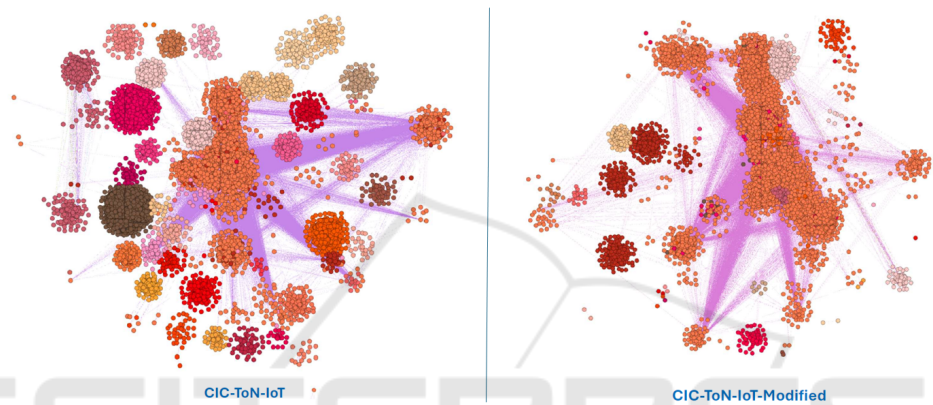


Figure 4: Network visualization of TON-IoT before (left) and after (right) time-based modification, showing preservation of temporal patterns and chronological integrity while achieving desired structural property modifications.

#### 4 RESULTS

Our proposed approach is evaluated through four complementary analyses that validate both our goals: (1) generating diverse datasets through structural transformation effectiveness and attack pattern preservation analyses, and (2) achieving computational efficiency through strong component preservation and practical deployment analyses in resource-constrained federated learning environments. The evaluation spans three representative datasets with distinct network characteristics: NF-UQ-NIDS (high mixing parameter, low density/transitivity indicat-

ing sparse connectivity), CCD-INID-V1 (moderate density, low transitivity indicating weak connectivity), and CIC-ToN-IoT (unique temporal patterns with strong community structure). The properties of these datasets are shown in Table 2, demonstrating how our techniques alter network structure while preserving essential characteristics. The modified datasets were obtained through systematic transformation: First, original datasets were transformed into graph representations. Based on initial network properties, one of three techniques was applied—for example, community mixing modification for NF-UQ-NIDS to reduce mixing parameter, and centrality-based modification

Table 3: Structural transformation summary for original and generated datasets. Metrics: records (flows), nodes (devices), edges (connections), max degree (highest connections), average path length (steps), strong components (sub-networks).

Metric	NF-UQ-NIDS (Original)	NF-UQ-NIDS (Generated)	CCD-INID-V1 (Original)	CCD-INID-V1 (Generated)	CIC-ToN-IoT (Original)	CIC-ToN-IoT (Generated)
Records	11,994,893	2,222,553	91,665	64,199	5,351,760	4,916,256
Nodes	93,645	163	229	68	143,809	66,683
Edges	468,919	468	372	140	353,604	168,185
Max Degree	5,434	106	73	67	58,037	44,363
Avg Path Length	3.950	1.950	2.8658	2.8487	2.640	2.463
Strong Comp (%)	99.99	97.5	96.81	98.11	99.99	99.97

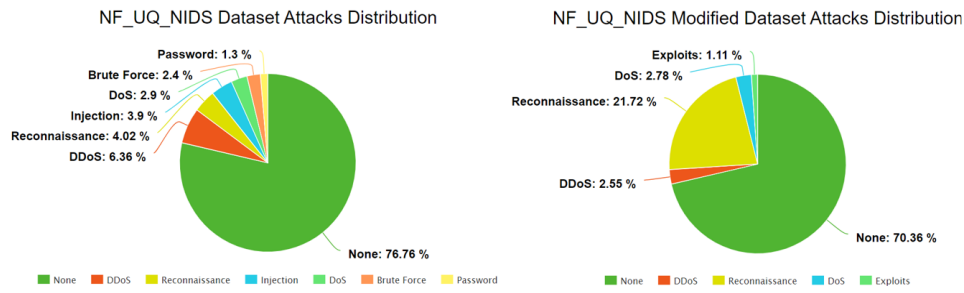


Figure 5: Attack pattern distribution in NF-UQ-NIDS before (left) and after (right) community mixing. The transformation preserves attack signatures while enhancing community structure.

for CCD-INID-V1 to increase density and transitivity. Thresholds were determined from extensive analysis of real-world datasets (density and transitivity at 0.01, mixing parameter at 0.1).

First, structural transformation effectiveness analysis demonstrates how datasets with target network properties are generated while preserving essential characteristics. For NF-UQ-NIDS, according to Table 2, high mixing parameter and low density/transitivity values indicate a sparse network with excessive inter-community connections. Following our methodology (Figure 1) we apply community mixing modification to reduce inter-community links. This transformation (Figure 2) produces consolidated communities with boundaries, reducing the mixing parameter while maintaining network structure. For CCD-INID-V1, moderate density and low transitivity values suggest a need for enhanced connectivity, hence applying centrality-based modification for higher density and transitivity through node selection. Figure 3 shows how preserving high-centrality nodes creates a balanced network structure while maintaining essential relationships. For CIC-ToN-IoT, characterized by distinct temporal patterns and high community structure, we apply time-based modification as shown in Figure 4, successfully adjusting properties while preserving chronological patterns.

The attack pattern preservation analysis validates that the generated datasets preserve key attack pat-

terns and their distributions. The NF-UQ-NIDS generated dataset preserves attack distributions benefiting from enhanced community structure's strength, shown in Figure 5. The relative proportions of normal and attack traffic patterns remain consistent, demonstrating the effectiveness of community mixing modification in maintaining attack signatures. For CCD-INID-V1, Figure 6 shows how the centrality-based modification preserves attack pattern distributions while achieving a more efficient network structure. The selective preservation of high-centrality nodes enhances the network's structural characteristics that allow Intrusion Detection Systems (IDS) to distinguish between normal and malicious traffic patterns. For CIC-ToN-IoT, Figure 7 demonstrates how temporal patterns of attacks are maintained through the time-based modification technique, with attack distributions retaining their temporal signatures while benefiting from the streamlined network topology.

The strong component preservation analysis demonstrates the robustness of the proposed approach in maintaining critical network structures. According to Table 3, the NF-UQ-NIDS generated dataset maintains 97.5% of strong components despite significant reduction in mixing parameter, indicating preserved network connectivity patterns. The CCD-INID-V1 generated dataset exhibits a 1.3% increase in strong component preservation, achieving 98.11% preservation rate while successfully increas-

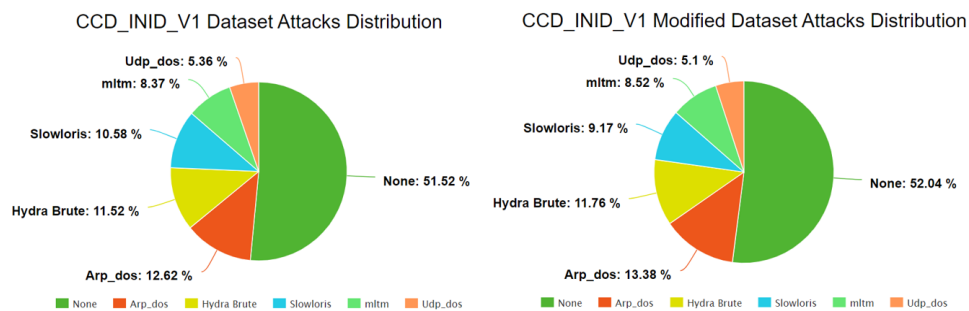


Figure 6: Attack pattern distribution in CCD-INID-V1 dataset before (left) and after (right) centrality-based modification. Showing preserved attack patterns while achieving more efficient network structure through high-centrality node selection.

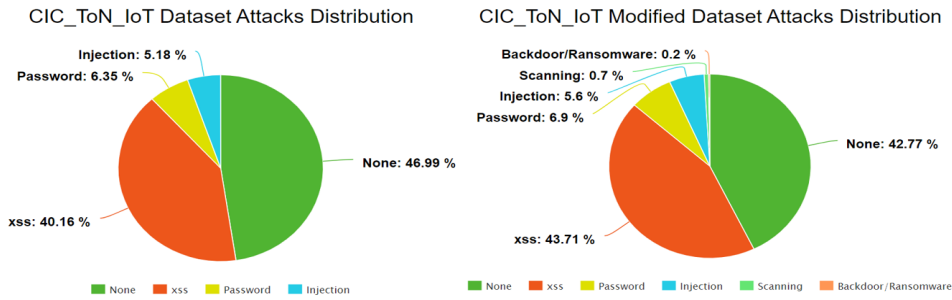


Figure 7: Attack pattern distribution in CIC-ToN-IoT dataset before (left) and after (right) time-based modification. The comparison demonstrates preserved temporal patterns while achieving desired structural modifications.

ing density and transitivity values. The CIC-ToN-IoT generated dataset demonstrates exceptional structural integrity with 99.97% of strong components preserved while achieving desired property modifications through temporal window selection. These high preservation rates validate the effectiveness of our approach in maintaining essential network relationships.

The practical deployment analysis evaluates utility in heterogeneous federated learning environments. The setup consists of four clients with varying computational constraints (RAM: 3GB-6GB, CPUs: 1-4) and different batch sizes (32-256) to reflect real-world heterogeneity. A feed-forward neural network with two hidden layers is deployed across these clients, achieving 96.4% accuracy by the third round of model aggregation. This high performance on resource-constrained devices validates the utility of the generated datasets in distributed environments, showing improved training efficiency with reduced size and maintained classification accuracy. The preservation of interpretable features through consistent components and attack distributions (Figures 5, 6, 7), coupled with successful property modifications across diverse configurations, highlights the adaptability and practical applicability of the generated datasets.

Our proposed approach effectively generates synthetic datasets with desired network properties while preserving the integrity and characteristics of the original dataset. Structural transformation, attack pattern preservation, and strong component preservation analyses demonstrate high effectiveness across multiple datasets. Further, the generated datasets prove useful in practical federated learning deployments, achieving 96.4% accuracy in heterogeneous, resource-constrained environments. Our approach reduces dataset size significantly while maintaining interpretability, and shows excellent scalability. This comprehensive evaluation confirms that the generated datasets retain important characteristics while meeting desired network properties, making them suitable for evaluating intrusion detection systems in central-

ized and federated learning environments.

## 5 CONCLUSION

This paper introduces an approach addressing critical challenges in intrusion detection evaluation: dataset scarcity and computational overhead. The techniques - Community mixing, Centrality-based, and Time-based modifications - generate datasets with network properties, achieving size reductions (up to 81.5%) maintaining detection accuracy (96.4%). This achievement makes our approach valuable for evaluation scenarios and resource-constrained environments. The approach, validated on NF-UQ-NIDS, CCD-INID-V1, and TON-IoT datasets, uses community mixing to reduce mixing parameter while increasing density, centrality-based methods to increase network density and transitivity, and time-based techniques to preserve chronological patterns.

These datasets are valuable for federated learning environments, addressing data scarcity while preserving attack patterns within 5% of originals. Going forward, future plans involve exploring semi-supervised and AI-based techniques for synthetic dataset generation accounting for network properties and attack patterns. Moreover, the approach will be further validated in federated learning environments, including generating homogeneous datasets for individual communities despite system heterogeneity.<sup>1</sup>

## REFERENCES

- Al-Hawawreh, M., Sitnikova, E., and Aboutorab, N. (2022). X-iiotid: A connectivity-agnostic and device-agnostic intrusion dataset for industrial internet of things. *IEEE Internet of Things Journal*, 9(5):3962–3977.

<sup>1</sup>The complete implementation of our approach is available at: <https://github.com/Fouad-AITfaily/IoTIDSGen>

- Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., and Anwar, A. (2020). Ton\_iot telemetry dataset: A new generation dataset of iot and iiot for data-driven intrusion detection systems. *IEEE Access*, 8.
- ARBAOUI, M., BRAHMIA, M.-E.-A., and RAHMOUN, A. (2022). Towards secure and reliable aggregation for federated learning protocols in healthcare applications. In *2022 Ninth International Conference on Software Defined Systems (SDS)*, pages 1–3.
- Arbaoui, M., Brahmia, M.-e.-A., Rahmoun, A., and Zghal, M. (2024). Federated learning survey: A multi-level taxonomy of aggregation techniques, experimental insights, and future frontiers. *ACM Transactions on Intelligent Systems and Technology*.
- Brahmia, M.-e.-A., Babouche, S., Ouchani, S., and Zghal, M. (2022). An adaptive attack prediction framework in cyber-physical systems. In *2022 Ninth International Conference on Software Defined Systems (SDS)*, pages 1–7.
- Ferrag, M. A., Friha, O., Hamouda, D., Maglaras, L., and Janicke, H. (2022). Edge-iiotset: A new comprehensive realistic cyber security dataset of iot and iiot applications for centralized and federated learning. *IEEE Access*, 10:40281–40306.
- Ferrag, M. A., Friha, O., Maglaras, L., and Janicke, H. (2021). Privacy-preserving schemes for fog-enabled iot: A comprehensive survey. *IEEE Internet of Things Journal*, 8(23):16749–16782.
- Ghalmame, Z., Brahmia, M. E. A., Zghal, M., and Cherifi, H. (2022). A stochastic approach for extracting community-based backbones. In *International Conference on Complex Networks and Their Applications*, pages 55–67. Springer International Publishing.
- Ghalmame, Z., Cherifi, C., Cherifi, H., and El Hassouni, M. (2019a). Centrality in complex networks with overlapping community structure. *Scientific reports*, 9(1):10133.
- Ghalmame, Z., Cherifi, C., Cherifi, H., and El Hassouni, M. (2020). Exploring hubs and overlapping nodes interactions in modular complex networks. *IEEE Access*, 8:79650–79683.
- Ghalmame, Z., Cherifi, C., Cherifi, H., and El Hassouni, M. (2021). Extracting modular-based backbones in weighted networks. *Information Sciences*, 576:454–474.
- Ghalmame, Z., El Hassouni, M., Cherifi, C., and Cherifi, H. (2018a). K-truss decomposition for modular centrality. In *2018 9th International Symposium on Signal, Image, Video and Communications*, pages 241–248. IEEE.
- Ghalmame, Z., El Hassouni, M., and Cherifi, H. (2018b). Betweenness centrality for networks with non-overlapping community structure. In *2018 IEEE workshop on complexity in engineering (COMPENG)*, pages 1–5. IEEE.
- Ghalmame, Z., El Hassouni, M., and Cherifi, H. (2019b). Immunization of networks with non-overlapping community structure. *Social Network Analysis and Mining*, 9:1–22.
- Hamizeh, H., Mugellini, E., Abou Khaled, O., and Cudré-Mauroux, P. (2017). Socialmatching++: A novel approach for interlinking user profiles on social networks. *Proceedings of the PROFILES@ ISWC 2017: Semantic web conferene, 22 october 2017, Vienna, Austria*.
- Hazimeh, H., Mugellini, E., Ruffieux, S., Khaled, O. A., and Cudré-Mauroux, P. (2018). Automatic embedding of social network profile links into knowledge graphs. In *Proceedings of the 9th international symposium on information and communication technology*, pages 16–23.
- Moustafa, N., Keshky, M. E., Debiez, E., and Janicke, H. (2020). Federated ton\_iot windows datasets for evaluating ai-based security applications.
- Moustafa, N. and Slay, J. (2015). Unsw-nb15: A comprehensive data set for network intrusion detection systems. In *Military Communications and Information Systems Conference*, pages 1–6.
- Nukavarapu, S., Ayyat, M., and Nadeem, T. (2022). Miragenet - towards a gan-based framework for synthetic network traffic generation. *Proceedings of IEEE GLOBECOM*, 2022:3089–3095.
- Sarhan, M., Layeghy, S., and Portmann, M. (2022). Evaluating standard feature sets towards increased generalisability and explainability of ml-based network intrusion detection. *Big Data Research*, 30:100359.
- Sharafaldin, I., Lashkari, A. H., and Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In *ICISSP*, pages 108–116.
- Termos, M., Ghalmame, Z., Fadlallah, A., Jaber, A., and Zghal, M. (2023). Intrusion detection system for iot based on complex networks and machine learning. In *2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing*, pages 471–477. IEEE.
- Termos, M., Ghalmame, Z., Fadlallah, A., Jaber, A., and Zghal, M. (2024). Gdlc: A new graph deep learning framework based on centrality measures for intrusion detection in iot networks. *Internet of Things*, 26:101214.
- Vaccari, I., Chiola, G., Aiello, M., Mongelli, M., and Cambiaso, E. (2020). Mqttset, a new dataset for machine learning techniques on mqtt. *Sensors*.