Cyber Forensic Analysis for Operational Technology Using Graph-Based Deep Learning

Presekal, Alfan; Stefanov, Alexandru; Rajkumar, Vetrivel Subramaniam; Palensky, Peter

DOI
10.1109/SmartGridComm57358.2023.10333922

Publication date
2023

Document Version
Final published version

Published in
Proceedings of the IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)

2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) | 978-1-6654-5556-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/SmartGridComm57358.2023.10333922

Cyber Forensic Analysis for Operational Technology Using Graph-Based Deep Learning

Alfan Presekal, Alexandru Ștefanov, Vetrivel Subramaniam Rajkumar, Peter Palensky

Department of Electrical Sustainable Energy
Delft University of Technology
Delft, The Netherlands
A.Presekal@tudelft.nl

***Abstract* — The cyber attacks in Ukraine in 2015 and 2016 demonstrated the vulnerability of electrical power grids to cyber threats. They highlighted the significance of Operational Technology (OT) communication-based anomaly detection. Many anomaly detection methods are based on real-time traffic monitoring, i.e., Intrusion Detection Systems (IDS) that may produce false positives and degrade the OT communication performance. Security Operations Center (SOC) needs intelligent tools to conduct forensic analysis on generated IDS alarms and identify the attack locations. Therefore, in this paper, we propose a novel, graph-based forensic analysis method for anomaly detection in power systems using OT communication network traffic throughput. It employs a hybrid deep learning model involving Graph Convolutional Long Short-Term Memory and a Convolutional Neural Network. The proposed method aids SOC with continuous OT security monitoring and post-mortem investigations. Results indicate that the proposed method is able to pinpoint the locations of cyber attacks on power grid OT networks with an AUC score above 75%.**

Keywords— Anomaly Detection, Attack Graph, CNN, Cyber Security, Digital Forensics, Graph, GNN, LSTM, Operational Technology

I. Introduction

Cyber attacks on power systems are low-frequency, high-impact disturbances that can have a wide range of adverse consequences. The potential implications include equipment damage, load shedding, and grid instability. In the worst-case scenario, cyber attacks have the potential to cause system-wide cascading failures and a blackout. Consequently, cyber attacks on power grids pose a grave threat and have already been identified in the real world. For instance, on December 23, 2015, a cyber attack on the power grid in Ukraine resulted in a blackout that affected 225,000 customers [1]. On December 17, 2016, a more sophisticated cyber attack caused a power outage in the distribution network, causing 200 MW of load to be left unsupplied [2]. In order to accomplish their goals, the adversaries used a variety of attack strategies. These can be correlated with the seven phases of the cyber kill chain, to conduct a comprehensive evaluation of it as an advanced persistent threat. These stages include reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objectives [3]. The current techniques employed for identifying attacks on power grids are constrained in their effectiveness. The majority of these anomaly detection methods are based on power system measurements that arise after successful early attack stages of the cyber kill chain, e.g., false data injection [4]-[6]. Therefore, this points out the importance of promptly detecting attacks in their early stages by means of anomaly detection in Information Technology-Operational Technology (IT-OT) systems.

Signature-based [7], sequence-based [8], rule-based [9]-[11], and machine learning-based [12] are the four primary methods reported in the literature for detecting anomalies in power grid IT-OT communication traffic. According to recent research, there is a growing interest in machine learning-based approaches for anomaly detection, which have demonstrated superior performance [13]. Therefore, in our previous work, we proposed a near real-time anomaly detection method for OT systems using hybrid deep learning [14]. The hybrid deep learning approach incorporates Graph Neural Networks (GNN), Long Short-Term Memory (LSTM), and Convolutional Neural Networks (CNN). The deep learning model utilizes unsupervised learning techniques to acquire knowledge about the intricate patterns of OT network traffic throughput, and supervised learning methods to classify the OT traffic. This is implemented in the control center to detect cyber attacks at the early stages of the cyber kill chain by monitoring the power system OT networks using Software Defined Networking (SDN). Notwithstanding, our previous research [14] and other research on SDN in power systems is restricted by the limited adoption of SDN in the present power system [15]. However, SDN may be widely deployed in the near future.

The state-of-the-art anomaly detection methods are based on real-time traffic monitoring, i.e., Intrusion Detection Systems (IDS), that may produce false positives [16] and degrade the OT communication performance [17]. Security Operations Center (SOC) needs intelligent tools to conduct forensic analysis on generated IDS alarms and identify the attack locations. The field of digital forensics within OT systems is currently in its nascent phase when compared to its IT counterpart. OT forensic analysis may help SOC investigate IDS alarms and reduce the number of false positives from real-time detection methods. Furthermore, it may be used for in-depth security investigations without disrupting the operation of industrial control systems [18], such as power grids.

Therefore, in this paper, we propose a novel, graph-based forensic analysis method for anomaly detection in power system OT networks by utilizing the communication network traffic throughput. It employs a hybrid deep learning model involving Graph Convolutional Long Short-Term Memory (GC-LSTM) and a CNN. The proposed method aids SOC with continuous OT security monitoring and post-mortem investigations. Results indicate that the proposed method is

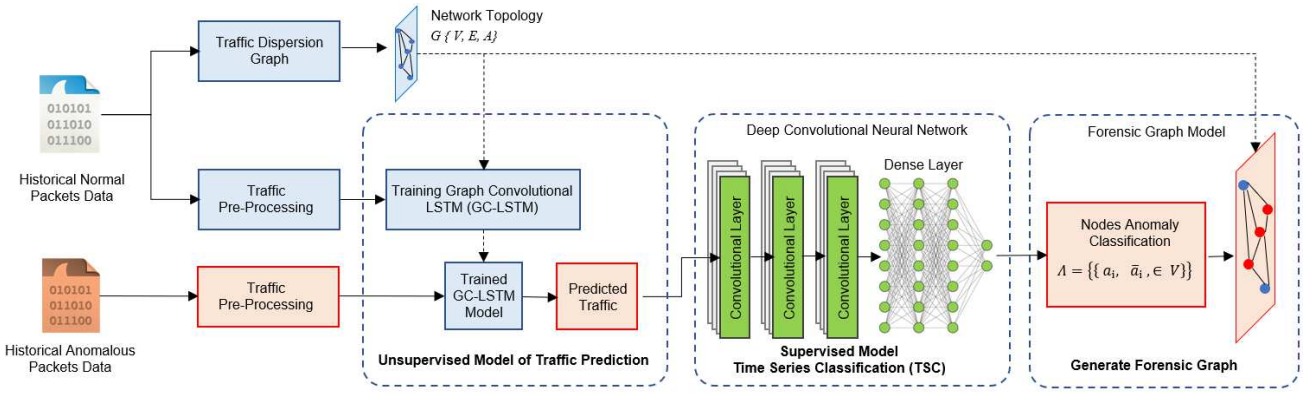

Fig. 1. Forensic graph (FGraph) model.

able to accurately pinpoint the locations of cyber attacks in the power grid OT network.

Compared to our previous research in [14], forensic OT traffic analysis also provides more flexibility. The implementation of SDN is not a prerequisite for it and can be applied to a broad range of OT communication networks, including, but not limited to, substations, control centers, and wide area networks. The forensic method allows SOC to perform in-depth post-mortem forensic investigations to avoid false positive results and minimize performance degradation of the OT communication. To summarize, the scientific contributions of this paper are as follows:

1) We propose a novel method for forensic graph-based analysis of OT traffic throughput based on packet historical data, i.e., FGraph. It is purpose-built for the detection of anomalies in OT networks by utilizing communication traffic throughput in the earlier stages of the cyber kill chain. It aids SOC in locating and identifying system-wide cyber attacks on OT networks using Traffic Dispersion Graph (TDG) and conducting post-mortem investigations through the implementation of graph-based deep learning.
2) A novel approach utilizing a hybrid deep learning model for the purpose of classifying OT network traffic throughput as either anomalous or normal. The proposed model integrates GC-LSTM and a CNN.
3) We propose FGraph Traffic Pre-Processing (TPP) with TDG to generate a forensic graph model. The graph model is used to analyze historical communication throughput between nodes. Furthermore, the time-series throughputs are classified using a hybrid deep-learning model. The classification results are used to identify anomalous nodes, which are represented in a forensic graph.

The rest of this paper is organized as follows. Section II explains the forensic graph model and anomaly detection. Section III describes the simulation result and analysis, and Section IV presents the conclusions and future work.

II. Forensic Graph Model and Anomaly Detection

This section presents the cyber attack threat model, proposed techniques for detecting anomalies, and the forensic graph model. Fig. 1 provides an overview of the methodology employed in the detection of anomalies and the subsequent creation of forensic graphs. The data collected from the network in the form of historical packets serves as input for the model. There are two processes performed using the packets, i.e., TPP and TDG. Following the pre-processing stage, GC-LSTM training takes place to produce a GC-LSTM model based on normal traffic data. This base model is subsequently utilized to predict traffic flows based on temporal and topological characteristics. The predicted traffic output is then subjected to a CNN time series classifier, which identifies the traffic flow as either normal or anomalous. As a result, the FGraph model generates a graph visualization that is predicated upon nodal classification. The following subsections provide a more thorough discussion of each stage of the method.

A. Cyber Attack Threat Model

A threat model is a systematic and organized representation of various factors and elements that have an impact on the security of an application. It helps to identify, communicate, and comprehend potential threats. An example of a power grid OT network is represented in Fig. 2. In this study, we assume that an adversary has already compromised a host located in the OT network of a substation. The adversary conducts a cyber attack on the OT network from the compromised host. This research employs the STRIDE threat model for CPS [19]. STRIDE consists of spoofing, tampering, repudiation, information disclosure, Denial of Service (DoS), and privilege elevation. In this work, we focus primarily on spoofing and DoS. A constrained threat model is used to analyze the OT communication of the power grid. The IT and OT network traffic characteristics exhibit notable distinctions. The network traffic in OT systems originates from automated processes with deterministic and homogeneous behavior [20]. In contrast, the traffic in IT systems primarily comprises of user-generated data that has a stochastic behavior. Therefore, the implementation of traffic-based anomaly detection for OT systems fundamentally differs from that of IT systems.

This research focuses on OT traffic throughput-based anomaly detection, which is capable of detecting cyber attacks that alter OT throughput relative to normal throughput levels, e.g., DoS, network reconnaissance, and spoofing attacks. In our previous work [14], a method is proposed for SDN-based real-time throughput anomaly detection. In this paper, however, we propose a method for forensic analysis of OT traffic, which does not require SDN deployment in power

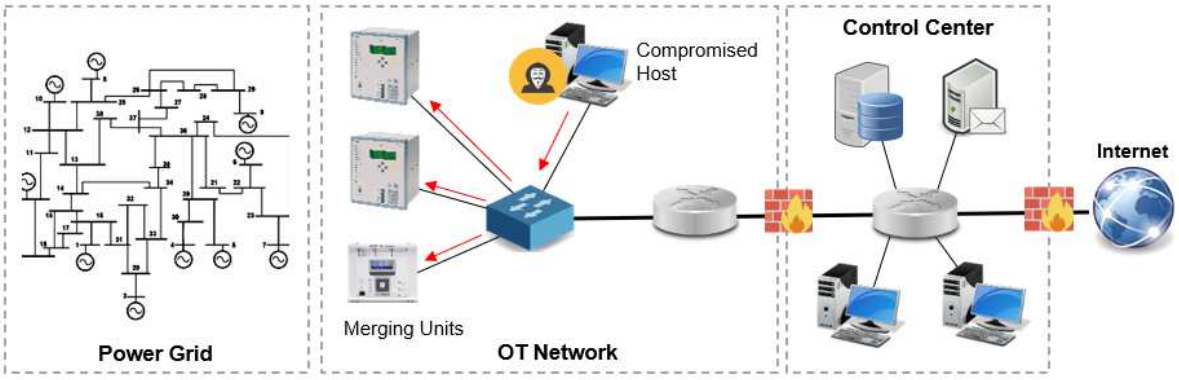

Fig. 2. OT network of a power grid

grid OT networks. The forensic analysis of traffic uses historical OT traffic data to acquire a comprehensive understanding of OT network operations, security breaches, and performance issues.

B. Traffic Pre-Processing and Traffic Dispersion Graph

Network forensics pertains to the acquisition, preservation, and scrutiny of network data with the aim of identifying unauthorized access and conducting subsequent inquiries [21]. It is a crucial component of network security, as it enables organizations to quickly detect and respond to cyber threats. Network administrators typically employ network traffic analysis tools to perform network traffic forensics, which involves capturing and analyzing traffic data in real-time or from historical traffic logs. These tools aid in detecting network anomalies, such as abnormal traffic patterns or unauthorized access attempts, that may suggest security breaches or malware infections. Wireshark, Tshark, Snort, and tcpdump are well-known software tools for network traffic analysis. These tools can capture network traffic data and provide a comprehensive analysis of the data, including the source and destination of the traffic, traffic type, and any detected anomalies or suspicious activities.

One of the methods to perform a deeper forensic analysis is through network forensic data visualization [22]. A matrix-based visualization from network forensic data was presented in [23]. The authors show the visualization summary of network data, e.g., IP addresses, ports, NetFlow payloads, entropy of source and destination IP, etc. The visualizations help to facilitate network traffic analysis and pinpoint anomalies within the network. An alternative method to visualize the network traffic data is using a TDG. The TDG is an analytical framework utilized for the purpose of observing and evaluating communication traffic. The fundamental concept behind TDG is interactions between hosts within a network [24]. Moreover, TDG employs graph structures to represent nodal information. Each individual node in a graph represents an individual host within a network. Conversely, the transmission of information among hosts is denoted by the interconnectivity of nodes, i.e., graph edges. Previously, the TDG was utilized to analyze communication network patterns. For instance, studies in [25] proposed an application of TDG for anomaly detection, based on graph information from network traffic. As shown in Fig. 1, in this research, we use TDG to generate a network graph topological representation from recorded OT traffic data.

Besides the aforementioned TDG, we also implement TPP in the model for the historical packets. This extracts information from the packets, i.e., nodes, edges, and time series traffic throughput. Algorithm 1 summarizes the pseudocode of both TDG and TPP. The input for the proposed algorithm is historical traffic packets (P) captured using Wireshark or Tshark. TDG processes the OT traffic to extract Graph information (G) from the packets, including vertices/nodes (V), edges (E), and the adjacency matrix (A). Meanwhile, TPP aims to convert the packets into time series throughput data for each node (X). The extracted graph (G) and time series throughput (X) serve as input for the subsequent forensic graph stages.

Algorithm 1: TDG and TPP Algorithm

Inputs: P: Historical communication traffic packets

Outputs: $G = \{\{V, E, A\}\}$: Graph with nodes, edges and adjacency
$\{x_1, x_2, \dots, x_v\}^t \in X$: Time series throughput data

TDG iteration for each packet p in P
for p in P **do**
  if v **not in** $G\{V\}$
    add v to V
  if e **not in** $G\{E\}$
    add e to E
end for

TPP throughput extraction iteration for each time t in T
for t **in** T **do**
  for v **in** $G\{V\}$
    $x_v^t = \sum x_v$
  end for
end for

return $G = \{\{V, E, A\}\}$ and $\{x_1, x_2, \dots, x_v\}^t \in X$

C. Graph Convolutional Long Short-Term Memory

Graph Convolutional Long Short-Term Memory (GC-LSTM) is adopted to acquire knowledge about the OT network traffic patterns. GC-LSTM employs two machine learning models, i.e., Graph Convolutional Network (GCN)

and LSTM. The GCN utilizes graph-based representations of the OT network's topological information, in conjunction with localized features derived from neighbouring communication nodes in the spatial domain. Subsequently, LSTM is employed for temporal learning by utilizing time-series data of observed OT network traffic. The integration of GCN and LSTM confers the benefit of acquiring knowledge from both, the spatial and temporal domains.

The primary input for the GC-LSTM approach is the graph structure of the OT network topology. TDG is used to derive this particular graph structure, as previously described. The Graph (G) elements are vertices/nodes (V), edges/links (E), and adjacency matrix (A). The adjacency matrix is a representation of elements denoted by Ai,j, where i and j are node index numbers. Ai,j equals 1 when two nodes are connected and 0 when they are not.

$$GCN_t^k \leftarrow (W_{gcn} \bullet \hat{A}^k) X_t \quad (1)$$

$$f_t = \sigma((W_f GCN_t^k) + (U_f h_{t-1}) + b_f) \quad (2)$$

$$i_t = \sigma((W_i GCN_t^k) + (U_i h_{t-1}) + b_i) \quad (3)$$

$$o_t = \sigma((W_o GCN_t^k) + (U_o h_{t-1}) + b_o) \quad (4)$$

$$c_t^{'} = \tanh((W_c GCN_t^k) + (U_c h_{t-1}) + b_{c'}) \quad (5)$$

$$c_t = (f_t \bullet c_{t-1}) + (i_t \bullet c_t^{'}) \quad (6)$$

$$h_t = o_t \bullet \tanh(c_t) \quad (7)$$

In (1), the GCN model is predicated on the Hadamard product multiplication ($\bullet$) of the weight matrix (W_{gcn}), adjacency matrix (A), and node features derived from the historical traffic data (X_t). The adjacency matrix is a mathematical representation that encapsulates pertinent details concerning the topology of the OT network. The modified adjacency matrix ($\hat{A}$) is obtained by adding the identity matrix (I) to the original adjacency matrix (A). The time series data set (X_t) is modelled by an equation that accounts for a specific time point (t) and the overall number of time observations (T). The node feature matrix (X) contains information about each node (x_i), where n represents the total number of nodes. The equation takes into account the exponent k, which represents the number of hops from a communication node to its neighbouring nodes, as described in [26] and [27]. Following the acquisition of spatial features through the GCN, the LSTM model is subsequently employed to examine the temporal or time-series characteristics. The functions and processes that occur within an LSTM cell are described in (2–7). The LSTM process comprises six primary sub-equations, namely the forget gate (f_t), input gate (i_t), output gate (o_t), internal cell state (c'_t), transferable cell state (c_t), and hidden state (h_t).

D. Time Series Classification and Forensic Graph Model

Time Series Classification (TSC) was implemented in [28] for anomaly detection. In this study, we propose a method for detecting anomalies in OT communication network traffic using TSC. The method employs a hybrid approach that combines both supervised and unsupervised methods for detecting anomalies in OT traffic. The utilization of unsupervised learning for time series data was implemented in [29]. Hence, an unsupervised GC-LSTM model is employed to acquire knowledge of the intricate patterns exhibited by OT network data and topology. Following this, the GC-LSTM model produces traffic predictions which serve as inputs for the TSCs.

TSC is implemented using a CNN algorithm with a multi-layer convolutional and *ReLU* activation function, as described by (8). The variables under consideration in (8) are the number of layers (l), filter size (m), weight (w), and bias (b). The CNN algorithm performs binary classification of each node as normal and anomalous. The classification is performed based on TSC from time series throughput data for each node (X). The result from the classification is then used to construct a forensic graph in the following stages.

$$y_i^l = \mathrm{Re}\,LU(\sum^{m-1} w y_{(i)}^{l-1} + b) \quad (8)$$

$$\mathrm{F}_G = \{\{f_i, \bar{f}_i, \in V\}\} \quad (9)$$

The forensic graph equation is described in (9). The FGraph is constructed based on prior knowledge regarding the topology of the OT network as well as the results of the node classifications. The FGraph (F_G) comprises two distinct components, i.e., normal nodes (f_i) and anomalous nodes ($\bar{f}_i$). The node classifications, alongside with the graph structural information, are then used to visualize the FGraph with different node colors. The node color variations help the user to pinpoint anomalous locations within the OT network topology.

III. Simulation Results and Analysis

A. Experimental Hardware-in-the-Loop Setting

Fig. 3 depicts the Hardware-in-the-Loop (HIL) configuration utilized for performing the FGraph implementation. A Real-Time Digital Simulator (RTDS) is used to model the physical power system, while IEC 61850 communication is realized between the RTDS and Intelligent Electronic Devices (IEDs) through a network switch. The IEDs comply with the IEC 61850 standard, enabling Generic Object Oriented Substation Event (GOOSE) messaging and Sampled Values (SV) for measurements. During normal operation, the RTDS sends packets to IEDs periodically. However, under cyber attack scenarios, the packet rate varies. More details on the cyber attack vector are provided in [30], [31]. Based on the co-simulation setup and cyber attack scenarios, we collect OT network traffic data for later analysis using FGraph.

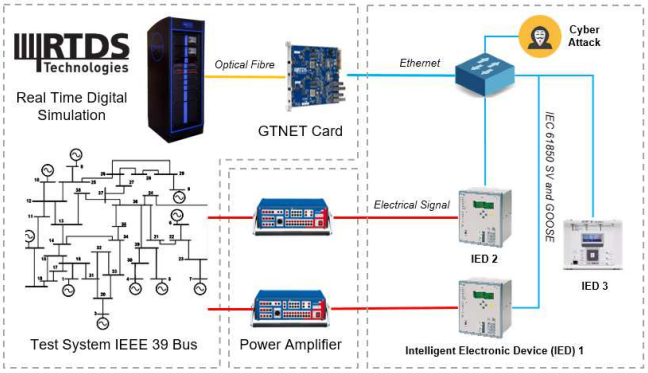

Fig. 3. Digital substation experimental setup for OT traffic generation.

B. Comparison With Open Datasets

Other than the aforementioned experimental set up, in this work, we also analyze multiple open datasets, i.e., IEC 61850 [32] and DAPT 2020 [33]. In [32], the authors provide communication data from a digital substation based on IEC 61850 standard. The dataset provides OT communication traffic data under normal, disturbance, and cyber attack scenarios. Normal data is derived from normal traffic with and without variable loading. The disturbance scenarios include busbar protection, breaker failure protection, and Under Frequency Load-Shedding (UFLS). The cyber attack scenarios cover Denial of Service, GOOSE spoofing, merging unit measurement spoofing, circuit breaker Boolean value injection, and replay attack.

In [33], the authors generate data based on normal and Advance Persistent Threat (APT) traffic for a duration of 5 days. The scenarios implement various stages of cyber attack kill chain, including vulnerability scanning, exploitation, establishing a foothold, privilege escalation, etc. The experiments incorporate red team and blue team tools, e.g., Metasploit and Snort. The NetFlow data collected from the experiment within 5 days includes source, destination, flow duration, flow bytes, etc. However, the provided NetFlow CSV data is not suitable for our proposed method of TDG and TCC. Therefore, in this work, we use the provided raw original source of packet data in *.pcap* format.

C. Network Traffic Analysis

Table 1 summarizes the network traffic data from the experimental HIL (A), IEC 61850 dataset (B) [32], and APT dataset (C) [33]. Data A and B originate from the substation models within a local network, which primarily transmits layer 2 broadcast messages using MAC addresses. Meanwhile, data C is dominated by layer 3 communication using IP addresses. Data C also indicates that the network is segregated into private and public networks. Additionally, this data has the most accumulated packet history of 5 days, with a total size of 17 GB.

Table 1: Summary of Network Traffic Data

Parameters	A	B	C
No of Nodes	85	103	786
No of Edges	198	246	821
Traffic duration	30 minutes	150 minutes	5 days
Total packet size	50 MB	100 MB	17 GB

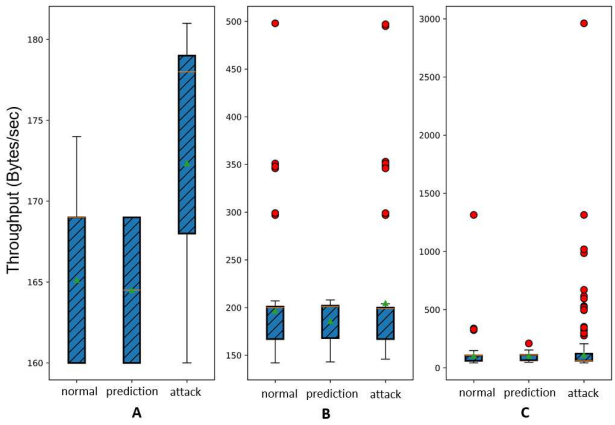

Fig. 4. Statistical comparison between normal, predicted, and attack or anomalous traffic for data A, B, and C.

All the aforementioned data is then processed using the forensic graph generation model. The GC-LSTM generates traffic predictions that serve as a normalization filter. Fig. 4 depicts a statistical comparison as box plots between normal, predicted, and attack traffic for all 3 cases. As shown in Fig. 4, normal traffic also contains outliers, indicated by red dots. These outliers can affect classification performance and result in increased false positives. Meanwhile, in the predicted traffic, the outliers are significantly reduced. Therefore, GC-LSTM helps to improve the classification accuracy of the CNN time series classifier.

D. Anomaly Detection and Forensic Graph

The anomaly detection is performed based on TSC using CNN. TSC classifies the traffic throughput as normal or anomalous. Fig. 5 shows the performance comparison for each dataset using the Receiver Operating Characteristic (ROC) curve. Dataset A provides the best result with an AUC score 0.819, followed by datasets B and C. Results for dataset C show the worst performance as the data contains more noise compared to the other two datasets. Comprehensive performance comparisons of the proposed method with the state-of-the-art methods are provided in our previous work [14].

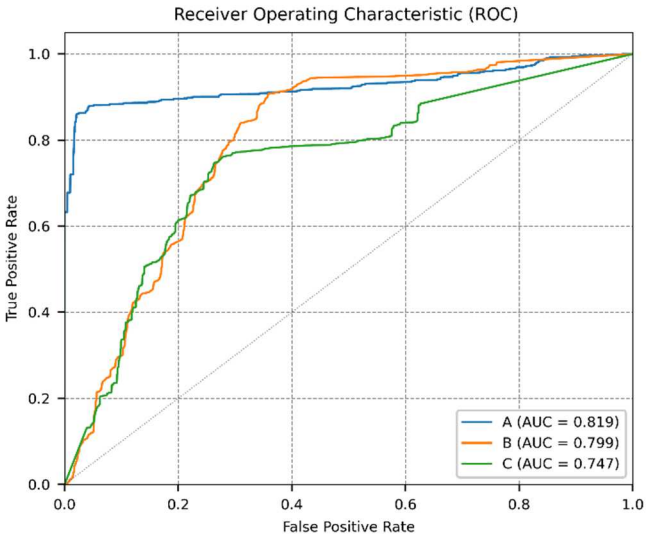

Fig. 5. ROC comparison for data A, B, and C.

Fig. 6 shows the forensic graph plot for normal and anomalous traffic. The blue node represents normal traffic, while the red one represents anomalous traffic. Fig 4. a, b, and c show the graph representation from normal traffic, while the others show the graph under attack scenarios. The cyber attack scenarios include GOOSE replay attack, reconnaissance, data manipulation, and foothold establishment. The graph comprises nodes that store data pertaining to the source and destination IP addresses or MAC addresses, as outlined in the TDG references [14], [24], and [25]. Results from the TDG show the ability to identify anomalous nodes within the network by tracing them back to their respective IP or MAC address. The operator utilizes these particular IP or MAC addresses to identify the root causes of the traffic anomaly. These IP and MAC addresses can potentially be associated with a compromised host or a host that has been targeted by an attack.

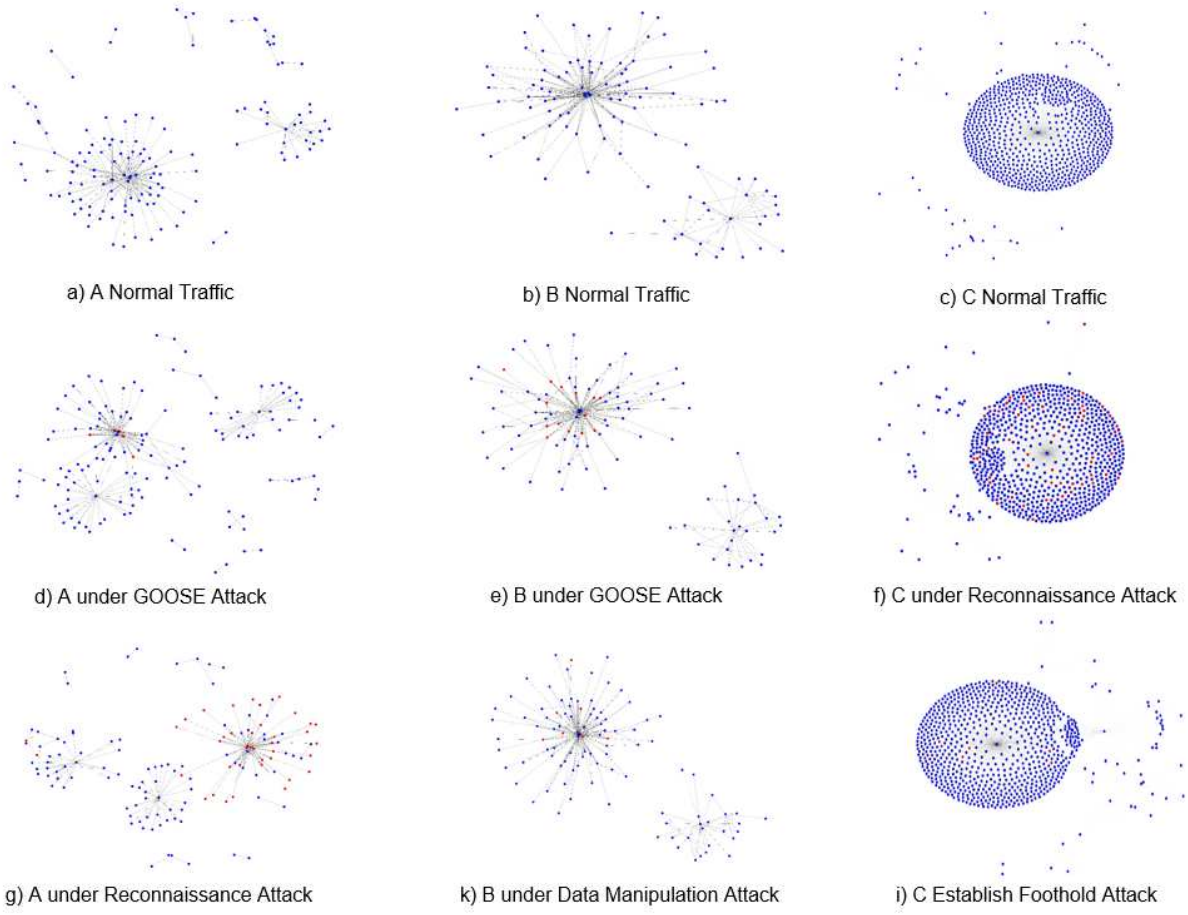

Fig. 6. Forensic graphs for normal traffic and anomalous traffic.

E. Result Analysis

Based on the conducted experiments, datasets A and B provide better anomaly detection performance, in comparison to dataset C. This is because the first two datasets contain homogenous OT traffic. Meanwhile, dataset C is IT traffic that has more heterogeneous characteristics. This characteristic is also shown in Fig. 4. Therefore, FGraph is more suitable for throughput anomaly detection in OT networks.

Compared to our previous research in [14], the performance of FGraph is lower because the FGraph input consists of packets captured with Wireshark. Other research has already identified problems related to Wireshark time inaccuracies [34], [35]. The Wireshark packet timestamp is inaccurate because it does not reflect the actual packet arrival or departure time. In particular, it is dependent on the time necessary for the kernel to process the arriving packets and access the clock. Regardless of this limitation, FGraph can serve as an alternative solution for graph-based forensic analysis in power grid OT communication networks. Although the performance is lower than [14], FGraph has more advantages due to its flexible implementation, as it does not require the deployment of SDN in the OT network. In addition, FGraph aims to avoid the degradation of the OT communication performance. Furthermore, with the recorded historical OT traffic, SOC can perform thorough analyses of the packet payloads to avoid false positives.

IV. Conclusions and Future Work

The increasing risk of cyber attacks on power grids has prompted the need for enhanced attack detection capabilities in OT systems. In this work, we proposed FGraph, a hybrid model of GC-LSTM and CNN for anomaly detection in OT communication networks for power grids. Forensic analysis on OT network traffic data aids SOC in localizing and identifying cyber attacks. GC-LSTM creates OT traffic predictions based on the spatial and temporal features of the input data. Through its predictions, the data variability and outliers are reduced. GC-LSTM enhances the anomaly detection performance of the CNN classifier. In this implementation, the detection performance is limited due to the scarcity of data for training and testing. Hence in future work, more experiments using various other datasets will be performed to improve the performance of FGraph.

Acknowledgment

This work was partially supported by Designing Systems for Informed Resilience Engineering (DeSIRE) program of the 4TU Resilience Engineering Centre, EU H2020 ERIGrid 2.0 project with Grant Agreement number 870620, and EU Horizon HVDC-WISE project with Grant Agreement number 101075424.

References

[1] D. E. Whitehead, K. Owens, D. Gammel and J. Smith, "Ukraine cyber-induced power outage: analysis and practical mitigation strategies," in

Proc. Int. Conf. for Prot. Relay Engineers, Texas, USA, Apr. 2017, pp. 1-8.

[2] M. J. Assante, R. M. Lee, and T. Conway, "ICS defense use case no. 6: modular ICS malware," *Electricity Information Sharing Center (E-ISAC) Tech. Report*, pp. 1-27, vol. 2, Aug. 2017.

[3] E. Hutchins, M. Cloppert and R. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *in Lockheed Martin Corp. Tech Report*, pp. 1-14, 2011. Accessed: May. 5, 2023. [Online]. Available: https://www.lockheedmartin.com/content/ dam/lockheed-martin/rms/ documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

[4] G. Liang, J. Zhao, F. Luo, S. R. Weller and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[5] R. Deng, G. Xiao, R. Lu, H. Liang and A. V. Vasilakos, "False data injection on state estimation in power systems attacks, impacts, and defense: a survey," *IEEE Trans. Ind. Inform.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.

[6] A. S. Musleh, G. Chen and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[7] C.W. Ten, J. Hong and C.C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 865–873, Dec. 2011.

[8] Q. Wang, X. Cai and Y Tang, "Methods of cyber-attack identification for power systems based on bilateral cyber-physical information," *Int. J. Electr. Power Energy Syst.*, vol. 125, no. 106515, pp. 1-12, Feb. 2021.

[9] R. Mitchell, and I. R. Chen, "Behavior-rule based intrusion detection systems for safety critical smart grid applications," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1254–1263, Sep. 2013.

[10] G. M. Coates, K. M. Hopkinson, S. R. Graham and S. H. Kurkowski, "Collaborative, trust-based security mechanisms for a regional utility intranet," *IEEE Trans. Power Syst.*, vol. 23, no. 3, pp. 831–844, Aug. 2008.

[11] Y. Yang *et al.*, "Intrusion detection system for network security in synchrophasor systems," in Proc. *IET Int. Conf. on Inf. and Comm. Tech.*, Beijing, China, 2013, pp. 246–252.

[12] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Trans. Neural Net. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, Aug. 2016.

[13] A. Aldweesh, A. Derham and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: a survey, taxonomy, and open issues," *Knowledge-Based Syst.*, vol. 189, no. 105124, pp. 1-19, Feb. 2020.

[14] A. Presekal, A. Ştefanov, V. S. Rajkumar and P. Palensky, "Attack Graph Model for Cyber-Physical Power Systems Using Hybrid Deep Learning," *IEEE Trans. on Smart Grid*, vol. 14, no. 5, pp. 4007-4020, Sept. 2023.

[15] A. Montazerolghaem and M. H. Yaghmaee, "Demand response application as a service: an SDN-based management framework," *IEEE Trans on Smart Grid*, vol. 13, no. 3, pp. 1952-1966, May 2022.

[16] C.Y. Ho, *et al.*, "Statistical analysis of false positives and false negatives from real traffic with intrusion detection/prevention systems," in *IEEE Communications Magazine*, vol. 50, no. 3, pp. 146-154, Mar. 2012.

[17]. Chan, H., Hammad, E. and Kundur, D., "Investigating the impact of intrusion detection system performance on communication latency and power system stability," in *Proc. of the Work. on Comm., Comp. and Con. for Res. S. E. Sys.*, Ontario, Canada, Jun. 2016, pp. 1-6.

[18] M. Cook, A. Marnerides, C. Johnson and D. Pezaros, "A Survey on Industrial Control System Digital Forensics: Challenges, Advances and Future Directions," in *IEEE Comm. Surv. & Tut.*. early access.

[19] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," *in Proc. ISGT-Europe 2017*, Turin, Italy, 2017, pp. 1-6.

[20] R. Barbosa, R. Sadre and A. Pras, "Difficulties in modeling SCADA traffic: a comparative analysis," *in Proc. Passive and Active Measure.*, Berlin, Germany, Mar. 2012, pp. 126-135.

[21] Pilli, E.S., Joshi, R.C. and Niyogi, R., 2010. Network forensic frameworks: Survey and research challenges, *Digital Investigation*, vol. 7, no. 1-2, pp.14-27.

[22] V. T. Guimarães, C. M. D. S. Freitas, R. Sadre, L. M. R. Tarouco and L. Z. Granville, "A Survey on Information Visualization for Network and Service Management," *IEEE Comm. Surv. & Tut.*, vol. 18, no. 1, pp. 285-323, Firstquarter 2016.

[23] R. Shi, M. Yang, Y. Zhao, F. Zhou, W. Huang and S. Zhang, "A Matrix-Based Visualization System for Network Traffic Forensics," *IEEE Systems Journal*, vol. 10, no. 4, pp. 1350-1360, Dec. 2016.

[24] M. Iliofotou, P. Pappu, M. Faloutsos, M. Mitzenmacher, S. Singh and G. Varghese, "Network monitoring using traffic dispersion graphs (TDGS)," in *Proc. of the 7th ACM SIGCOMM Conf. on Inter. Meas.*, San Diego, USA, Oct. 2007, pp. 315-320.

[25] D. Q. Le, T. Jeong, H. E. Roman and J. Hong, "Traffic dispersion graph based anomaly detection," in *Proc. of the 2nd Sym. on Infor. and Comm. Tech.*, Hanoi, Vietnam, Oct. 2011, pp. 36-41.

[26] Z. Cui, K. Henrickson, R. Ke and Y. Wang, "Traffic graph convolutional recurrent neural network: a deep learning framework for network-scale traffic learning and forecasting," *IEEE Trans. on Intel. Transp. Sys.*, vol. 21, no. 11, pp. 4883-4894, Nov. 2020.

[27] J. Chen, X. Wang, and X. Xu, "GC-LSTM: graph convolution embedded LSTM for dynamic link prediction," *Applied Intelligence*, pp. 1-16, Sep. 2021.

[28] H. Wu, "A survey of research on anomaly detection for time series," in *Proc. 13th Int. Compt. Conf. on Wav. Act. Med. Tech. and Inf. Proc.*, Chengdu, China, Dec. 2016, pp. 426-431.

[29] M. Längkvist, L. Karlsson and A. Loutfi, "A review of unsupervised feature learning and deep learning for time-series modelling," *Pat. Recog. Let.*, vol. 42, pp. 1-14, Jun. 2014.

[30] V. S. Rajkumar, M. Tealane, A. Ştefanov and P. Palensky, "Cyber Attacks on Protective Relays in Digital Substations and Impact Analysis," in *Proc. 8th Work. on Mod. and Simu. of Cy.-Phy. En. Sys.*, Sydney, NSW, Australia, 2020.

[31] V. S. Rajkumar, M. Tealane, A. Ştefanov, A. Presekal and P. Palensky, "Cyber Attacks on Power System Automation and Protection and Impact Analysis," in *Proc. ISGT-Europe*, The Hague, Netherlands, 2020, pp. 247-254.

[32] P. P. Biswas, H. C. Tan, Q. Zhu, Y. Li, D. Mashima and B. Chen, "A Synthesized Dataset for Cybersecurity Study of IEC 61850 based Substation," in *Proc. IEEE SmartGridComm*, Beijing, China, 2019, pp. 1-7.

[33] S. Myneni, A. Chowdhary, A. Sabur, S. Sengupta, G. Agrawal, D. Huang, et al., "DAPT 2020—Constructing a benchmark dataset for advanced persistent threats" in *Deployable Machine Learning for Security Defense*, Cham, Switzerland:Springer Int, pp. 138-163, 2020.

[34] A. F. S. Melo, J. M. Riquelme-Dominguez, F. Gonzalez-Longatt, J. L. Rueda and P. Palensky, "Sampled Values ROCOF performance methodology breakdown," in *Proc. EEEIC / I&CPS Europe*, Prague, Czech Republic, 2022, pp. 1-5.

[35] A. -C. Orgerie, P. Gonçalves, M. Imbert, J. Ridoux and D. Veitch, "Survey of Network Metrology Platforms," in *Proc. IEEE/IPSJ 12th Int. Symp. on App. and the Int.*, Izmir, Turkey, 2012, pp. 220-225.