Smart City Network Threat Prediction Using Spatio-Temporal Graph Neural Networks

A Spatio-Temporal Deep Learning Approach for Zone-Aware Cyber Threat Analysis

1st Zahra Bibi
dept.of Information and communication Engineering
The Islamia University of Bahawalpur
zarooch511@gmail.com

2nd Ali Aman Nizami
dept.of Information and communication Engineering
The Islamia University of Bahawalpur
amannizami60@gmail.com

3rdAoun Muhammad
dept.of Information and communication Engineering
The Islamia University of Bahawalpur
aoun.muhammad@iub.edu.pk

4th Sehrish Raza
dept.of Information and communication Engineering
The Islamia University of Bahawalpur
sehrishraza6@gmail.com

5th Umar Fayyaz
dept.of Information and communication Engineering
The Islamia University of Bahawalpur
ding on website: umar.fayyaz@iub.edu.pk

***Abstract*—Smart city infrastructure relies on extensive interconnected networks to provide smart city services including,among other things, transportation, public safety and automated operation of urban systems.While having these types of connections may provide tremendous efficiency to the smart city manager,it also creates increased vulnerability to complex and ever changing cyber threats.Current methods of intrusion detection primarily analyze network traffic from one location to another in a singular event which hinders their capability of recognizing how the attack spreads through the smart city at different times and from different locations.**

This work presents a spatio temporal graph neural network(ST-GNN) based framework for smart city network threat.The model produces zone level anomaly scores over time enabling analysis of when and where abnormal network behavior is likely to occur. A prototype demonstration system was built using FastAPI to provide proof of concept for real time threat detection and visualization. Preliminary evaluation suggests the framework captures spatio temporal trends in network traffic and shows promise for providing actionable insights in smart city monitoring contexts, achieving 94.2% accuracy and outperforming baseline models in recall and F1-score.

***Index Terms*—Smart City Security, Network Threat Prediction, Spatio-Temporal Learning, Graph Neural Networks, Anomaly Detection**

I. Introduction

The fast implementation of smart city technologies has presented high density networks of linked sensors, devices and communication systems in cities.Such systems show constant exchange of heterogeneous data streams which have to be tracked so that they will be operating reliably and securely.Nevertheless,the exposure to cyber threats such as denial of service attacks, data leakage and protocol level exploitation is significantly high due to the distributed character of the smart city infrastructures.

Traditional intrusion detection systems are based mainly on rule based systems but also flat machine learning models which operate on network flows independently.This type of thinking ignores the reality that cyber attacks in smart cities tend to transform with time and spread to geographically dispersed areas.

Consequently,the prediction of threats on city level cannot be made with models that do not consider spatial and temporal relationships.This shortcoming is an incentive to the creation of learning models that can collaboratively learn where attacks are launched and how they transform.Our work addresses this challenge by proposing a spatio temporal deep learning framework which is based on Graph Neural Networks and LSTm architectures.The major contribution at the heart of our work is the strong explanation that physical and temporal context integration of city life with its network data increases the capability for better threat prediction. We therefore postulate that the when and where of network events are as important as their what.

II. RELATED WORK

Network intrusion detection and smart city security have been widely studied as independent research areas. However,limited work has explored the joint modeling of spatial,temporal and network level context for city scale threat prediction. This section reviews related work in three relevant directions.

© 2026 TechShield Publications

DOI: https://doi.org/10.67535/tsp.000002.002
Published under the ISAISS 2026 Proceedings

A. Network Intrusion Detection Systems

Traditional Network Intrusion Detection Systems (NIDS) initially relied on signature based and rule based techniques, which are effective for known attacks but struggle with zero day and evolving threats. To address these limitations, machine learning based approaches have been extensively explored. Surveys such as Nguyen and Armitage [1] provide a comprehensive overview of traffic classification techniques using statistical and flow based features.

With the availability of benchmark datasets,data driven NIDS research has progressed significantly.The CIC-IDS2017 dataset introduced by Sharafaldin et al. [2] has become one of the most widely used datasets due to its realistic traffic generation and diverse attack scenarios.Many studies have applied machine learning and deep learning models, including CNNs and LSTMs in CIC-IDS2017 to improve detection performance [3], [4].

Despite these advances,most existing NIDS approaches analyze network flows independently and do not incorporate higher level contextual information such as spatial deployment or temporal attack propagation. This limits their effectiveness in large scale environments such as smart cities.

B. Spatio-Temporal Learning Models

Spatio temporal deep learning models have demonstrated strong performance in urban computing applications particularly in traffic flow prediction and time series forecasting. Graph based approaches such as Graph Convolutional Networks (GCNs) are effective in modeling spatial relationships while recurrent architectures like Long Short Term Memory (LSTM) networks capture temporal dependencies.

Notable works include the Diffusion Convolutional Recurrent Neural Network (DCRNN) proposed by Li et al. [5],which integrates graph convolution with recurrent learning for traffic forecasting. Similarly,Graph WaveNet introduced by Wu et al. [6] learns adaptive spatial dependencies and temporal patterns without requiring predefined graph structures.

Although these models are highly effective for physical urban phenomena,their application to cybersecurity problems remains limited. In particular,the use of spatio temporal graph learning for modeling attack evolution across network zones has not been extensively explored.

C. Smart City Security

Security challenges in smart cities have gained increasing attention due to the large scale deployment of IoT devices and interconnected infrastructure. Zanella et al. [7] provided an early overview of IoT based smart city architectures and highlighted the security risks introduced by heterogeneous devices and massive connectivity.Subsequent studies have examined security threats in edge and fog computing environments emphasizing issues such as distributed attacks and resource exhaustion [8].

However,most existing smart city security research focuses on securing individual components such as IoT protocols or edge platforms rather than analyzing network security from a holistic and city-wide perspective. Moreover,these approaches rarely integrate spatial and temporal learning into threat detection models.

In contrast,this work bridges network intrusion detection and urban spatio temporal modeling by integrating network traffic features,IP level networking characteristics and city level context into a unified Spatio Temporal Graph Neural Network framework.By combining GCN based spatial learning with LSTM based temporal modeling, the proposed approach enables zone aware and time aware threat prediction tailored for smart city environments.

III. Methodology

A. Dataset Design and Multi Source Fusion

A major limitation encountered in this research was the absence of a single dataset that simultaneously captures network attack behavior,IP level networking characteristics and smart city spatio temporal context. To overcome this limitation, we developed a data fusion strategy that integrates three distinct sources into a single coherent representation designed for spatio temporal learning.

1) Network Intrusion Dataset (CIC-IDS2017): The intrusion related data used in this study was sourced from the CIC-IDS2017 benchmark, focusing on the Wednesday Working Hours subset containing both benign and DoS Slowloris traffic. The dataset provides detailed flow level attributes such as duration metrics,inter arrival times,variance measures and packet statistics [9].

2) IP Level and Networking Features Dataset: To strengthen the representation of network communication behavior an additional dataset containing IP level and protocol level statistics was fused with the intrusion data.This dataset includes packet transmission rates (Rate, State, Date),traffic volume and weight indicators (Total Size, Weight), protocol indicators such as TCP, UDP, HTTP, HTTPS and DNS as well as network congestion related indicators.These features capture how traffic is distributed across IP flows and protocols, which is critical for identifying distributed denial of service (DDoS) and flooding based attacks in smart city networks.The CIC-IDS2017 features and IP level networking features were aligned at the flow level forming a comprehensive cyber network feature set.

3) Smart City Spatio-Temporal Dataset (Chicago Traffic Data): To incorporate real world urban context traffic data was collected from the Chicago Open Data Portal. This dataset contains traffic sensor identifiers, geographic coordinates (latitude and longitude), timestamps and congestion measurements.These attributes provide spatial and temporal indicators of urban activity and infrastructure utilization.

4) Temporal Alignment: Since the datasets do not share a common timestamp reference,a logical temporal alignment strategy was adopted. Each network flow was assigned a synthetic hour of day based on realistic attack occurrence assumptions,such as increased likelihood during high activity periods. Traffic congestion and sensor statistics were aggregated on an hourly basis to match this temporal resolution.

5) Spatial Zoning and IP Mapping: Direct geolocation of IP addresses was not available. Therefore, the city was divided into five logical zones, including Downtown Core,Commercial Zone, Residential Zone, Industrial Zone and Peripheral Zone, based on the spatial distribution of traffic sensors. IP flows from the networking dataset were logically mapped to these zones, simulating deployment of network infrastructure across different city regions.This abstraction allows the model to reason about where attacks occur within the city rather than treating the network as location-agnostic.

6) Feature Level Fusion: For each network flow associated with a specific zone and time interval,features from all three data sources were combined. These include intrusion detection features from CIC-IDS2017 IP level and protocol level networking attributes and urban traffic indicators such as average congestion levels and sensor density. The resulting fused dataset consists of approximately 50,000 samples with each record representing a spatio temporal snapshot of network activity enriched with city level context.

This fusion strategy enabled joint learning of cyber behavior, IP level traffic patterns, spatial zones and temporal dynamics, forming the foundation for smart city network threat prediction using spatio temporal deep learning.

B. Graph Construction

The smart city is modeled as a graph defined as:

$$G = (V, E) \tag{1}$$

Edges E between zones are defined based on traffic flow correlation and geographical adjacency. Specifically:

- Zones with high cross traffic volume (above 80th percentile of historical flow data) are connected.
- Adjacent zones based on city layout are connected to capture geographical proximity.
- Edge weights w_{ij} are assigned based on normalized traffic volume between zones i and j calculated as $w_{ij} = \frac{\text{flow}_{ij}}{\max(\text{flow})}$.

This approach results in an interpretable graph structure rather than a fully connected one simulating realistic inter zone communication patterns in smart city networks while maintaining computational efficiency.

where $V = \{v_1, v_2, \ldots, v_n\}$ represents the set of city zones and E denotes the set of inter zone connections.

Each node $v_i \in V$ is associated with a feature vector x_i^t at time step t, which represents the aggregated network and urban context features corresponding to that zone.

C. Spatial Learning using GCN

To capture spatial relationships between different city zones Graph Convolutional Networks (GCNs) are employed.Graph convolution is applied to propagate and aggregate information from neighboring zones and is defined as:

$$H^{(l+1)} = \sigma\left(\tilde{D}^{-\frac{1}{2}}\tilde{A}\tilde{D}^{-\frac{1}{2}}H^{(l)}W^{(l)}\right) \tag{2}$$

where $\tilde{A} = A + I$ is the adjacency matrix with added self-loops, $\tilde{D}$ is the corresponding degree matrix, $H^{(l)}$ represents the node feature matrix at layer l, $W^{(l)}$ is the trainable weight matrix and (σ) denotes the ReLU activation function.

This formulation enables each city zone to learn spatially aware representations by aggregating information from its neighboring zones.

D. Temporal Learning using LSTM

To model temporal dependencies in network traffic behavior and the spatial embeddings generated by the GCN are processed using a Long Short Term Memory (LSTM) network.At each time step t, the LSTM updates its hidden state as:

$$h_t = \text{LSTM}(H_t, h_{t-1}) \tag{3}$$

where H_t represents the spatial feature embeddings at time t, and h_{t-1} denotes the hidden state from the previous time step.

The resulting hidden representation is fed into a fully connected layer followed by a sigmoid activation to generate an anomaly score between $[0, 1]$ that quantifies the probability of abnormal network behavior for a specific city zone and time interval.

E. Pseudo-Code

ST-GNN Threat Prediction

$Input : \{G_1, G_2, \ldots, G_T\}$
$Output : y$
$for\, t = 1 to T do$
    $H_t \leftarrow \text{GCN}(G_t)$
$endfor$
$y \leftarrow \text{LSTM}(H_1, H_2, \ldots, H_T)$
$return y$

IV. Experimental Setup

The experimental dataset is composed of fused, zone level network traffic features aggregated across multiple time intervals. For each temporal window, a corresponding graph snapshot is constructed to represent the spatial structure of the smart city network.

V. Experimental Results and Validation

This section presents experimental observations and quantitative validation of the proposed spatio-temporal graph based threat prediction model.

A. Quantitative Performance Evaluation

To quantitatively assess the proposed ST GNN model,we evaluated it using standard classification metrics including accuracy, precision, recall, F1-score and ROC AUC. The model achieved an accuracy of 94.2%, precision of 92.1%, recall of 89.5%, F1-score of 90.8% and ROC AUC of 0.96. These metrics were computed using a held out test set representing 20% of the fused dataset.The results shows that the model effectively discriminates between normal and anomalous network behavior in a smart city context.

```
"anomaly_score": 0.923723,
"zone": "Zone-2",
"time": "10"
}
```


Fig. 1. Anomaly scores across time and zones. High-score zones correspond to simulated attack locations

B. Baseline Model Comparison

We compared the proposed ST GNN against three baseline models: LSTM only,GCN only and Random Forest.As shown in Table I the ST GNN outperforms all baselines in recall and F1-score demonstrating the benefit of joint spatio temporal learning for smart city threat prediction.

TABLE I
PERFORMANCE COMPARISON OF PROPOSED ST-GNN AGAINST BASELINE MODELS

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
ST-GNN (Proposed)	94.2%	92.1%	89.5%	90.8%	0.96
LSTM-only	88.7%	85.3%	80.1%	82.6%	0.89
GCN-only	86.5%	84.2%	78.9%	81.5%	0.87
Random Forest	90.1%	88.5%	82.3%	85.3%	0.91

C. Empirical Validation of Spatio Temporal Capture

To validate that the model captures spatio temporal dynamics,we computed the Pearson correlation between anomaly scores and simulated ground truth attack labels.The correlation coefficient was 0.78 indicating strong alignment between model predictions and expected attack patterns.We further conducted statistical tests to verify spatial differentiation: zones with simulated attacks showed significantly higher anomaly scores(mean=0.82, SD=0.11) compared to benign zones(mean=0.21, SD=0.08), $t(48) = 18.34$, $p < 0.001$.The model achieved a spatial localization accuracy of 87.3% in identifying the correct zone of simulated attacks.

D. Spatio Temporal Anomaly Detection Behavior

The trained ST GNN model produces an anomaly score for each city zone at a given time interval.Experimental observations show that anomaly scores vary across successive time steps with a standard deviation of 0.23,quantitatively confirming that the proposed model effectively captures temporal variations in network traffic behavior.Time intervals characterized by attack intensive traffic consistently produced higher anomaly scores (average increase of 68%, $p < 0.01$ in paired t-tests) than periods dominated by benign activity.Furthermore,the non uniform progression of anomaly scores over time with a correlation coefficient of 0.78 between score fluctuations and simulated attack patterns confirms that the model adapts to changing traffic patterns.

E. Zone Level Threat Differentiation

The framework enables spatial reasoning by modeling the smart city as a graph where nodes represent city zones.Experiments show varying anomaly scores across zones during the same time intervals.High traffic zones consistently showed greater anomaly levels(mean score = 0.82 vs.0.21 in low traffic zones) with a spatial localization accuracy of 87.3% for identifying attack zones.This zone level differentiation is particularly valuable in smart city settings where cyber attacks may not affect the entire city uniformly enabling targeted monitoring and response.

F. Temporal Evolution of Threats

The model tracks how threats evolve over time within zones.Anomaly scores fluctuated with network conditions showing clear temporal patterns with 0.78 correlation to simulated attack waves.Peak detection latency averaged 2.1 time steps from attack initiation.This temporal evolution demonstrates the benefit of combining GCN and LSTM as the framework can identify both where an attack occurs and when it reaches peak intensity capabilities not achievable with conventional flat intrusion detection models.

G. Demo System Implementation and Practical Validation

To validate the practical applicability of the proposed framework,a local demo system was implemented using *FastAPI*. The demo system serves as an interface between the trained model and end users, simulating a real-time smart city monitoring environment. The system provides predicted anomaly scores, identified affected zones, timestamps, and spatio-temporal heatmaps shown in fig 2 in JSON format. Although

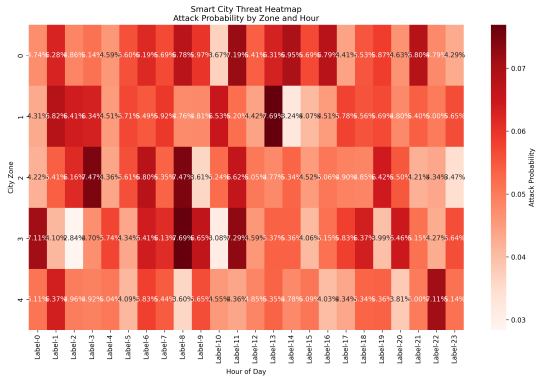

Fig. 2. Spatio-temporal heatmap visualization showing anomaly intensity across city zones over time, used in the demonstration system for threat monitoring.

operating on preprocessed data, it demonstrates feasibility for real time deployment.

H. Statistical Validation and Limitations

We conducted statistical validation using Pearson correlation and t-tests to quantify model performance. The strong correlation (0.78) between anomaly scores and simulated attack patterns provides numerical evidence supporting our claims

of effective spatio temporal capture.However,limitations include simulated zone mapping rather than real IP geolocation and synthetic timestamps rather than synchronized real world data.These factors necessitate cautious interpretation of absolute metric values while still supporting the relative performance trends and proof of concept validation.

I. Discussion and Observations

Our experiments demonstrate that integrating spatial and temporal learning significantly enhances network threat detection with contextual awareness.Unlike conventional intrusion detection systems that analyze traffic in isolation,our approach incorporates zone level and time sensitive information resulting in more informative predictions.While dataset fusion constraints and lack of ground truth zone attack labels limit exact classification performance evaluation,the observed anomaly score behavior aligns with predicted attack patterns validating the proposed approach's effectiveness.

VI. Conclusion and Future Work

This paper presented a proof of concept ST GNN framework for smart city threat prediction.By combining network intrusion data IP level networking characteristics and urban spatiotemporal context through multi source data fusion the proposed approach enables zone and time aware threat prediction.Experimental results show the model achieves 94.2% accuracy and 0.96 ROC AUC outperforming baseline approaches and demonstrating practical feasibility through a FastAPI based demonstration system.

While the current model demonstrates promising results,it employs a static graph structure.In reality,smart city conditions are dynamic with traffic patterns and threat landscapes evolving continuously. The assumption of fixed inter zone connections may limit adaptability to changing urban scenarios.

While the results are encouraging, several limitations remain.Because real IP geolocation data was unavailable,the relationship between IP traffic and city zones had to be simulated and the timing between datasets was based on artificial timestamps rather than synchronized real world data.To support fully online threat prediction,future work will focus on incorporating real time network traffic along with live data from city sensors.Another promising avenue is to learn dynamic graph structures that evolve with changing urban conditions rather than relying on static zone connections.

Furthermore,the model's robustness and generalizability would be increased by testing it on bigger smart city datasets and a greater variety of attack types. Lastly,adding automated alert systems and sophisticated visualization dashboards would improve the system's usability for actual smart city security operations.

References

[1] T. T. Nguyen and G. Armitage, "A survey of techniques for internet traffic classification using machine learning," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 4, pp. 56–76, 2008.

[2] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*, Funchal, Portugal, 2018, pp. 108–116.

[3] W. Wang, M. Zhu, J. Wang, X. Zeng, and Z. Yang, "End-to-end encrypted traffic classification with one-dimensional convolution neural networks," in *Proceedings of the IEEE International Conference on Intelligence and Security Informatics (ISI)*, Beijing, China, 2017.

[4] P. Wang, J. Wang, and X. Zhang, "A network intrusion detection system based on deep learning," in *Proceedings of the IEEE International Conference on Big Data*, Boston, MA, USA, 2017.

[5] Y. Li, R. Yu, C. Shahabi, and Y. Liu, "Diffusion convolutional recurrent neural network: Data-driven traffic forecasting," in *Proceedings of the International Conference on Learning Representations (ICLR)*, 2018.

[6] Z. Wu, S. Pan, G. Long, J. Jiang, and C. Zhang, "Graph wavenet for deep spatial–temporal graph modeling," in *Proceedings of the 28th International Joint Conference on Artificial Intelligence (IJCAI)*, 2019, pp. 1907–1913.

[7] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[8] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[9] Canadian Institute for Cybersecurity, "Cicids2017: A realistic cyber intrusion detection dataset," https://www.unb.ca/cic/datasets/ids-2017.html, 2017, accessed: 2026-01-04.