Dijlah Journal of Engineering Science (DJES) Vol. 3, No. 3, August, 2026, pp. 134-141
ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 192

Multi-Task Learning for Security and Performance Optimization in 6G Network Slices

Maab Fathi Hamzah [1]
[1]College of Physical Education and Sport Sciences, University of Baghdad, Baghdad, Iraq

Article Info

Article history:

Received Apr., 17, 2026
Revised May.,23, 2026
Accepted Aug.,14, 2026

Keywords:

Multi-Task Learning
6G Network
Deep Learning
Cybersecurity
Throughput
Prediction
Network Congestion

ABSTRACT

As such, the fast-paced move towards sixth-generation (6G) networks presents numerous obstacles in ensuring the attainment of both secure operation and optimized performance within the framework of network slicing systems. Current methods usually handle the two goals separately, leading to less-than-optimal performance in highly volatile and sophisticated network settings. In this study, an innovative multi-task (MLT) algorithm was formulated for the simultaneous forecasting of the security status, throughput, and congestion status of 6G network slices. The new model employs common features extracted from network status, traffic status, and cyberattacks to model the inherent connection between security risks and performance deterioration. The experimental outcomes clearly show that the suggested MTL architecture exhibits superior performance compared to traditional single-task models in terms of accuracy, generalization capacity, and stability.

Corresponding Author:

Maab Fathi Hamzah
College of Physical Education and Sport Sciences, University of Baghdad, Baghdad, Iraq
Al-jadriya, Baghdad, Iraq
Email: maab@cope.uobaghdad.edu.iq

1. INTRODUCTION

The development of wireless technologies contributes to the development of sixth generation (6G) communication systems that provide ultra-low latency, massive connectivity, and intelligent network management.[1] The core of network technologies in 6G will be network slicing[2], which means using one infrastructure to create several virtual networks customized to satisfy the needs of different applications, such as self-driving cars, IoT systems, and other ultra-speed technologies.Network slicing faces numerous difficulties in providing secure and efficient services, as network slices are especially vulnerable to cyber-attacks such as DDoS attacks, spoofing, and wiretapping [3],[4]. Simultaneously, the performance parameters of network slices are very important since they ensure that strict QoS requirements are met [5]. Currently, AI and deep learning can contribute to solving this problem and provide new tools to manage security and performance [6][7]. Machine learning has already been extensively used in the areas of IDS development, traffic prediction, and optimization of the network operations. Nevertheless, most existing systems focus on only either security or performance optimization, while in practice, both factors should be considered at once, which leads to poor resource management and decision-making [8].In reality, security and performance exhibit a high level of interdependence. Network attacks can negatively affect network performance through increased latency, decreased throughput, and congestion[9], and inadequate network conditions can lead to suboptimal performance of security measures. Interdependence underscores the requirement for integrated frameworks that can simultaneously assess security and performance. To overcome this weakness, multi-task learning (MTL) has become a highly effective framework that allows multiple related tasks to be learned simultaneously using shared features [10],[11]. Through common feature spaces, MTL enhances the performance of generalization and captures task dependencies.

In this paper, we present a unified MTL model for 6G network slicing that learns:

- Security Status (attack mitigation success)

- Network Throughput (performance metric)
- Network Congestion Level (traffic condition)
- The main contributions of this work are summarized as follows:
- A consistent multi-task learning model for combined performance and security optimization in 6G network slicing.
- Leveraging the relationship between cyber threats and network performance factors.
- Capability enhancement for accurate predictions using shared features.
- Development of an adaptive AI-based platform for managing 6G networks.

2. BACKGROUND AND RELATED WORK

2.1. Machine Learning for Network Security

Machine learning algorithms are extensively used in network security[12], especially in IDSs. Deep learning algorithms including CNN and RNN have shown efficient results for detecting advanced and sophisticated attacks [3][6], [13],[14] [15]. Hybrid techniques employing various machine learning algorithms have been proposed recently with the goal of enhancing the efficacy of the detection processes[16] [17]. AI-based security systems for future 5G and beyond networks in network slicing scenarios have been proposed recently [1], [18] however, the effect of these attacks on the performance of the network is largely ignored.

2.2. Machine Learning for Network Performance Optimization

Moreover, machine learning techniques have also been utilized for the prediction of performance measures like throughput, delay, and congestion in networks. The time series approach has been extensively applied to predict network traffic and bandwidth[19] [20]. Furthermore, an optimization approach has been suggested to improve QoS and allocate resources in wireless networks [21], [22]. Even though these techniques help simulate network behavior accurately, they do not consider security aspects during this process.

2.3. Multi-Task Learning Approaches

MTL has been effectively used in different areas in order to optimize learning processes and increase generalization[10], [23]. In networking, MTL has been employed in traffic classification, anomaly detection, and resource management tasks[24], [25]. Concerning cybersecurity, the recent studies reveal that MTL can be more effective in terms of task-specific detection by taking advantage of common representations between related tasks [11], [26]. However, existing studies concentrate on cybersecurity tasks only and ignore performance optimization tasks.

2.4. AI-Driven Network Slicing in 6G

The development of 6G is driving the design of AI-native architectures that will allow smart and self-managing networks [5], [1]. Such architectures focus on the role of AI techniques in network slicing to achieve dynamic resource management and optimization [27][28].

Moreover, recent studies have pointed out the significance of joint optimization approaches in which different aspects such as performance, energy efficiency, and security need to be considered [29]. Nevertheless, the absence of common models that can address both security and performance while utilizing modern learning methods such as multi-task learning is evident.

2.5. Research Gap

Limitations from the literature review include the following:

- Security-oriented models overlook performance metrics
- Performance models overlook cybersecurity issues
- Multi-task learning needs to be investigated for 6G network slicing

Thus, there is a need for a comprehensive approach to model both aspects together, which is the main aim of the current research work.

3. METHODOLOGY

3.1 Dataset Description

The data set used in the experiment was collected from an open source platform called Kaggle named "6G Network Slicing Security Attack Detection." Since the lack of actual 6G data sets, this data set is created artificially using wireless traffic model assumptions.The dataset takes into account features from network configurations, traffic, performance, and security as illustrated in table 1. These include the following types of features:

- Network Configuration Features: Slice Type, Slice Bandwidth (Mbps), Transmission Path
- Traffic and Channel Conditions: Traffic Load, Signal Strength, Network Congestion
- Performance Metrics: Latency (in milliseconds), Packet Loss Rate (percentage), Data Rate (Mbps), Throughput (Mbps), End-to-End Delay (in milliseconds), Packet Delivery Ratio (percentage)
- Security Aspects: Security Protocol, Attack Nature, Attack Identification Time (milliseconds), IGJO-SVM Classification, Counter Measure
- Energy Metrics: Energy Efficiency (J/bit)
- Target Variable: Security Status (Binary: Yes/No)
- The dataset is used to model the complex relationship between network conditions, cyberattacks, and system performance in 6G network slices.

3.2 . Problem Formulation

The MTL model presented herein is expressed as an MTL problem, where one common model generates multiple outputs from a single input feature set.
With the following input vector: X = {X1, X2..., Xn} => the mapping function will generate: F(X) => {Ys, Yp, Yc} where: (Ys): Security status (binary classification),(Yp): Network throughput (regression), (Yc): Network congestion level (multi-class classification)

3.3 Proposed Multi-Task Learning Model

The framework proposes an architecture for MTL which jointly learns the interactions of security and performance in a 6G network slicing setting. The model uses common feature spaces to learn the interactions of cybersecurity and performance. The architecture Model consists of: Shared feature extraction layers, Security prediction head (classification), Throughput prediction head (regression), Congestion prediction head (classification). Latent representation extraction is achieved by the shared layers using heterogeneous features like latency, packet loss, traffic load, bandwidth, and attacks. The latent representations are subsequently used by the task-specific output layers as shown in figure 1.

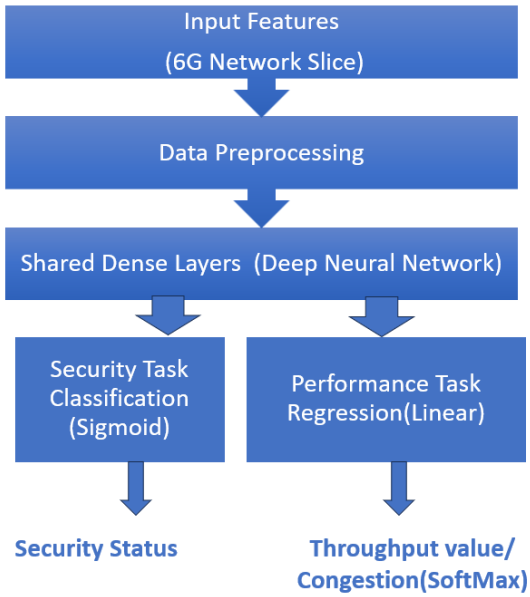

Figure 1. Multi-task learning framework for simultaneous prediction of security and performance in 6G network slices.

The model predicts multiple outputs simultaneously: F(X) = {Ys, Yp, Yc}
The overall loss function is defined as in (1):

$$L_{total}=\alpha L_s+\beta L_p+\gamma L_c \quad (1)$$

where α, β, γ are weighting coefficients controlling task importance. As shown in Table 2 the output heads are:

- Security Head: Binary classification using sigmoid activation: $\widehat{Y_s} = \sigma\ (W_S\ H)$
- Throughput Head: Regression using linear activation: $\widehat{Y_p} = \sigma\ (W_p\ H)$
- Congestion Head: Multi-class classification using SoftMax: $\widehat{Y_c} = Softmax\ (W_c\ H)$

Table 1: Dataset Feature Summary

Feature Category	Feature Name	Description
Network Config	Slice Type	Type of network slice (IoT, Autonomous, etc.)
Network Config	Slice Bandwidth	Available bandwidth (Mbps)
Network Config	Transmission Path	Routing path (A, B, C)
Traffic	Traffic Load	Network load level (Low, Medium, High)
Traffic	Network Congestion	Congestion level
Channel	Latency	Transmission delay (ms)
Channel	Packet Loss Rate	Percentage of lost packets
Channel	Signal Strength	Quality of signal
Performance	Throughput	Effective data rate (Mbps)
Performance	Packet Delivery Ratio	Successful delivery rate
Performance	End-to-End Delay	Total delay
Security	Security Mechanism	Firewall / IDS / Encryption
Security	Attack Type	DDoS / Spoofing / Eavesdropping
Security	Attack Detection Time	Detection latency (ms)
Target	Security Status	Success/Failure of mitigation

Table 2: Model Output Definitions

Task	Output Type	Activation Function	Loss Function
Security Status	Binary Classification	Sigmoid	Binary Cross Entropy
Throughput	Regression	Linear	MSE
Congestion	Multi-Class Classification	SoftMax	Cross Entropy

3.4 Data Preprocessing

The dataset undergoes several preprocessing steps:

- Encoding categorical variables using label encoding
- Normalizing numerical features using Standard Scaler
- Splitting the dataset into training and testing sets (80/20 ratio)

Table 3: Training Configuration

Parameter	Value
Optimizer	Adam
Learning Rate	0.001
Batch Size	32
Epochs	20
Loss Function	Weighted Multi-Task Loss

3.5 Training Strategy and Procedure

This training process involves a joint learning approach whereby the different tasks share the same objective function. Through this approach, the model can learn the interrelationships between security threats and system performance degradation. Both the shared parameters and the task-specific parameters are updated using backpropagation. While the training procedure is carried out as follows: Data preparation and transformation, Splitting of the dataset into training and test sets, Forward pass through shared and task-specific layers, Computing task-specific losses, Backward pass with Adam optimizer, and Training iterations until convergence. In the current research, training and test sets are split into 70% and 30%, respectively.

3.6 Evaluation Metrics

Each task uses a different set of evaluation metrics:

- Security Classification which use: Accuracy, Precision, Recall, F1-score [30]
- Throughput Prediction is use: Mean Absolute Error (MAE)[31], Root Mean Squared Error (RMSE)[31]
- Congestion Classification: Accuracy, Confusion Matrix

3.7 Implementation Details

The suggested framework is programmed by utilizing Python language version 3.11 within the PyCharm Community Edition IDE. The experimental system is built up of a NVIDIA GeForce MX550 graphics card, Intel Core i7 CPU (12th Generation), and 16 GB RAM.

Training is done by employing Adam optimizer and adaptive learning rate. Early stopping technique is used to avoid overfitting. The hyperparameters are fine-tuned on empirical grounds.

4. RESULTS AND DISCUSSION

3.1. Performance Evaluation

The MTL framework suggested was then tested against various machine learning baselines, such as LR, RF, XGBoost, and ANN. The comparison is carried out by taking into account three critical tasks, which are security classification, throughput prediction, and congestion detection. Table 4 illustrate the performance comparison among models.while figure 2 shows the comparison of the security and congestion prediction performance of various machine learning algorithms.

Table 4: Performance Comparison

Model	Security Accuracy (%)	Throughput RMSE	Congestion Accuracy (%)
Logistic Regression	88.2	12.5	85.1
Random Forest	91.7	9.8	89.3
XGBoost	93.9	7.4	91.5
ANN (Single Task)	94.2	7.1	92.0
Proposed MTL	96.8	5.6	95.4

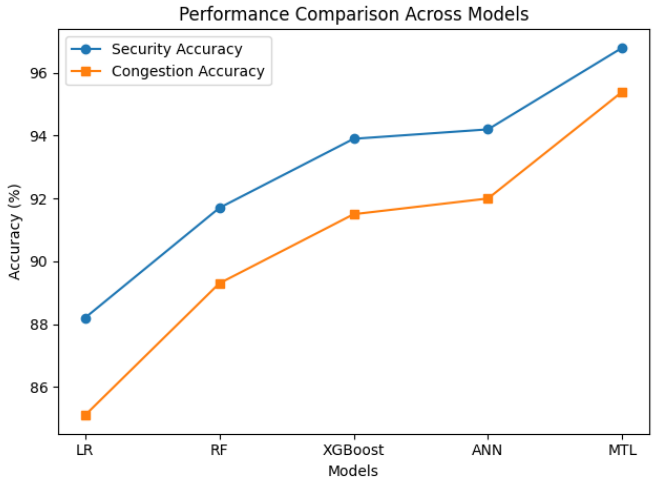

Figure 2. A comparison of the security and congestion prediction performance of various machine learning algorithms.

The security accuracy of the proposed MTL model was 96.8%, which is slightly better than the best baseline ANN model by about 2.6% points. This is due to the common representation learning scheme in the proposed method that makes it possible to utilize performance indicators such as latency and packet loss in security predictions.
As regards throughput prediction, the RMSE of the MTL model was 5.6, making it more accurate than Random Forest (9.8) and Logistic Regression (12.5). Thus, this model successfully learns non-linear interactions between the network environment factors and performance measurements. Finally, the accuracy of the proposed model for congestion classification reached 95.4%, surpassing other models in terms of accuracy. The findings from the experiment show that the MTL approach demonstrates better generalization performance than single-task models. By allowing parameter sharing among the multiple tasks, the model prevents overfitting while ensuring efficient reuse of features. Unlike conventional models, which involve building separate models for individual tasks, the suggested model conducts joint training, thereby reducing computation cost. Therefore, the model is ideally suited for deployment in real-time 6G networks.

3.2. Impact of Security on Network Performance

Further studies on the correlation between security and network performance were conducted based on certain attributes.

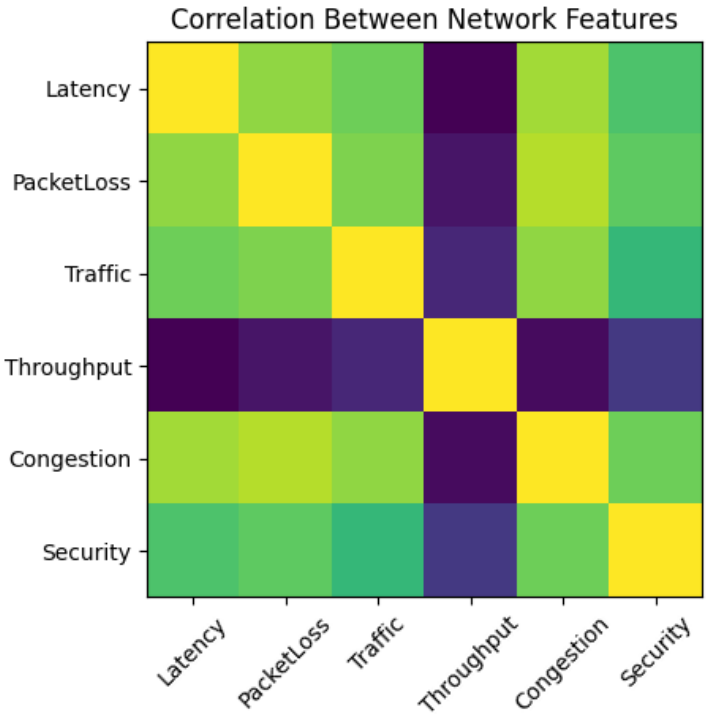

Figure. 3. Correlation heatmap showing the relationship between network performance and security attributes.

The correlation heatmap has revealed some significant findings:

- A strong negative correlation (-0.8) between latency and throughput indicates that increased delay significantly degrades network performance.
- Packet loss exhibits a high positive correlation (0.8) with congestion, confirming that unstable network conditions lead to traffic bottlenecks.
- Security failure shows a positive correlation with both packet loss and congestion, suggesting that cyberattacks contribute directly to network instability.

These findings confirm that security threats and performance degradation are tightly coupled, reinforcing the necessity of adopting joint modeling approaches such as multi-task learning. To evaluate the contribution of multi-task learning, an ablation study was conducted. As shown in Table 5

Table 5: Ablation Study

Model Type	Security	Throughput	Congestion	Overall Performance
Single Task	×	×		Low
Partial MTL	✓	×		Medium
Full MTL	✓	✓		High

From the above ablation studies, it can be seen that the integration of multiple tasks has greatly improved the system performance. This is proven by the superior performance of the fully-fledged MTL model compared to individual and partially shared models. So the Experimental results bring forth some key insights, which include the following:

1. Multi-task learning substantially boosts accuracy in all tasks.
2. Security and performance are closely related in 6G network slicing.
3. Network congestion can be used as a predictor of possible attacks.
4. Shared feature learning increases model robustness and generalization.

5. CONCLUSION

In this research, we developed a multi-task learning model for simultaneous optimization of cybersecurity and performance in 6G slicing scenarios. In contrast to conventional solutions that solve these issues separately, the developed model is based on combining several tasks into one single system.

The conducted experiments show that using the MTL model leads to higher accuracy and generalization by sharing common feature representation. In addition, this model correctly learns the connection between cyberattack and deterioration of network performance. Nevertheless, the research is confined to the utilization of artificial data, which might fail to reflect practical scenarios. Future work will aim at validating the suggested model through practical data sets. In Future research will focus on extending the proposed framework in several directions:

- Real-World Validation: Applying the model to real network traffic datasets to evaluate robustness under practical conditions.
- Federated Learning (FL): Enabling distributed training across network slices while preserving data privacy.
- Explainable AI (XAI): Integrating interpretability methods such as SHAP and LIME to enhance transparency.
- Reinforcement Learning (RL): Developing adaptive models for real-time decision-making and autonomous network control.
- Multi-Modal Learning: Incorporating additional contextual data (e.g., user behavior, application requirements) to improve prediction accuracy.

REFERENCES

[1] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, “Toward 6G Networks: Use Cases and Technologies Publisher: IEEE Cite This PDF,” 2020.

[2] Mahesh H. B, Ali Ahammed G. F, and Usha S. M, “The Network Slicing and Performance Analysis of 6G Networks using Machine Learning,” *EMITTER International Journal of Engineering Technology*, vol. 11, no. 2, pp. 174–191, Dec. 2023, doi: 10.24003/emitter.v11i2.772.

[3] V. P. Singh, M. P. Singh, S. Hegde, and M. Gupta, “Security in 5G Network Slices: Concerns and Opportunities,” *IEEE Access*, vol. 12, pp. 52727–52743, 2024, doi: 10.1109/ACCESS.2024.3386632.

[4] A. Ahmed and E. Ahmed, “A Survey on Mobile Edge Computing.”

[5] W. Saad, M. Bennis, and M. Chen, “A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems,” Jul. 2019, [Online]. Available: http://arxiv.org/abs/1902.10265

[6] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton, “Deep Leerning”.

[7] M. Nalluri, M. Pentela, and N. Rao Eluri, “A Scalable Tree Boosting System: XG Boost,” *International Journal of Research Studies in Science, Engineering and Technology*, vol. 7, no. 12, pp. 36–51, 2020, doi: 10.22259/2349-476X.0712005.

[8] M. Wang, Y. Cui, X. Wang, S. Xiao, and J. Jiang, “Machine learning for networking: Workflow, advances and opportunities,” *ArXiv*, pp. 1–8, 2017.

[9] A. Thakkar and R. Lohiya, “A Review of the Advancement in Intrusion Detection Datasets,” in *Procedia Computer Science*, Elsevier B.V., 2020, pp. 636–645. doi: 10.1016/j.procs.2020.03.330.

[10] Rich Caruana, “Multitask Learning”.

[11] L. Bai, A. Gupta, and Y.-S. Ong, “Multi-Task Learning with Multi-Task Optimization,” Mar. 2024, [Online]. Available: http://arxiv.org/abs/2403.16162

[12] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, Feb. 2020, doi: 10.1016/j.jisa.2019.102419.
[13] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, Feb. 2020, doi: 10.1016/j.jisa.2019.102419.
[14] A. Gharaibeh *et al.*, "Smart Cities: A Survey on Data Management, Security, and Enabling Technologies," *IEEE Communications Surveys and Tutorials*, vol. 19, no. 4, pp. 2456–2501, 2017, doi: 10.1109/COMST.2017.2736886.
[15] D. Spiekermann, T. Eggendorfer, and J. Keller, "Deep Learning for Network Intrusion Detection in Virtual Networks," *Electronics (Switzerland)*, vol. 13, no. 18, Sep. 2024, doi: 10.3390/electronics13183617.
[16] M. G and J. Philip, "CNN-LSTM Hybrid Deep Learning Model for Remaining Useful Life Estimation," Dec. 2024, doi: 10.2015/IJIRMF/ICSETI-2024/P04.
[17] S. F. Akintade, K. Roy, and S. T. Kim, "Hybrid Deep Machine Learning Feature Selection for High-Dimensional Cybersecurity Data," *IEEE Access*, vol. 13, pp. 172136–172156, 2025, doi: 10.1109/ACCESS.2025.3615582.
[18] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and Beyond."
[19] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory".
[20] K. N. Lam, "Traffic Prediction Using LSTM, RF and XGBoost," INSTICC, Jul. 2025, pp. 267–274. doi: 10.5220/0013515600004619.
[21] A. Gharehgoli, A. Nouruzi, N. Mokari, P. Azmi, M. Reza Javan, and E. A. Jorswieck, "IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT 1 AI-based Resource Allocation in End-to-End Network Slicing under Demand and CSI Uncertainties."
[22] F. Qamar, M. H. D. N. Hindia, T. Abbas, K. Bin Dimyati, and I. S. Amiri, "Investigation of QoS Performance Evaluation over 5G Network for Indoor Environment at Millimeter Wave Bands," no. February, 2019, doi: 10.24425/ijet.2019.126288.
[23] R. Cipolla, Y. Gal, and A. Kendall, "Multi-task Learning Using Uncertainty to Weigh Losses for Scene Geometry and Semantics," 2018.
[24] M. Lotfollahi, R. S. H. Zade, M. J. Siavoshani, and M. Saberian, "Deep Packet: A Novel Approach For Encrypted Traffic Classification Using Deep Learning," Jul. 2018, [Online]. Available: http://arxiv.org/abs/1709.02656
[25] K. Roy, L. S. Chan, X. Zhang, and N. Nassir, "Multi-task deep learning for joint prediction of traffic emissions and travel delay," *Transp. Res. D Transp. Environ.*, vol. 146, Sep. 2025, doi: 10.1016/j.trd.2025.104846.
[26] D. Dasgupta, Z. Akhtar, and S. Sen, "Machine learning in cybersecurity: a comprehensive survey," *Journal of Defense Modeling and Simulation*, vol. 19, no. 1, pp. 57–106, Jan. 2022, doi: 10.1177/1548512920951275.
[27] Praveen Hegde and Robin Joseph Varughese, "International Journal of Communication Networks and Information Security AI-Powered Network Optimization: Application of Artificial Intelligence in Optimizing Network Performance, Including Self-Healing and Self-Optimizing Capabilities," 2022. [Online]. Available: https://https://ijcnis.org/
[28] X. Zhu, R. Zheng, D. Yang, H. Liu, and J. Hou, "Radio-aware TCP optimization in mobile network," *IEEE Wireless Communications and Networking Conference, WCNC*, no. March, 2017, doi: 10.1109/WCNC.2017.7925843.
[29] C. Zhang, Y. L. Ueng, C. Studer, and A. Burg, "Artificial Intelligence for 5G and beyond 5G: Implementations, Algorithms, and Optimizations," *IEEE J. Emerg. Sel. Top. Circuits Syst.*, vol. 10, no. 2, pp. 149–153, 2020.
[30] M. Fathi and O. Ali, "A Review of TCP Congestion Control Using Artificial Intelligence in 4G and 5G Networks," ASRJETS, 2022. [Online]. Available: http://asrjetsjournal.org/
[31] T. Chai and R. R. Draxler, "Root mean square error (RMSE) or mean absolute error (MAE)? -Arguments against avoiding RMSE in the literature," *Geosci. Model Dev.*, vol. 7, no. 3, pp. 1247–1250, 2014, doi: 10.5194/gmd-7-1247-2014.

BIOGRAPHIES OF AUTHORS

Asst. Lect. Maab Fathi Hamzah, received his B.Sc. degree in Computer Engineering from Al-Mustansiriyah University, Iraq, in 2012, and his M.Sc. degree in Information and Communication Engineering from Al-Khwarizmi College of Engineering, University of Baghdad, Iraq, in 2022.
He worked as a Laboratory Lecturer in the Department of Computer Engineering at Al-Esraa University College starting in 2014. Since October 2022, he has been working as a full-time lecturer and serves as the Head of the Information Technology Unit at the College of Physical Education and Sports Sciences, University of Baghdad, Iraq.
He can be contacted via email: maab@cope.uobaghdad.edu.iq.