Artificial Intelligence in Networking Research in the Arab World

BASEM SHIHADA*, Computer, Electrical and Mathematical Sciences and Engineering Division, King Abdullah University of Science and Technology, Kingdom of Saudi Arabia

MOHAMED ABDALLAH, Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Qatar

The rapid evolution of networking technologies, driven by Artificial Intelligence (AI) and Machine Learning (ML), is reshaping the landscape of digital connectivity across the Arab world. As the region undergoes a notable digital transformation, fueled by the adoption of edge and cloud computing, 5/6G, and the Internet of Things, AI and ML applications are being leveraged to optimize network performance, enhance security, and ensure scalability. This paper shows a sample of the contribution of the Arab world in the integration of AI/ML in modernizing networks, focusing on two key areas: intelligent wireless connectivity including non-terrestrial network integration and intelligent and secure systems. The paper also addresses challenges, including the need for skilled professionals, regulatory frameworks, and data availability for training AI/ML models. Overall, this work showcases the Arab world's growing influence in networking research, offering solutions with the potential for transformative economic and technological impact.

Additional Key Words and Phrases: Artificial Intelligence, Arab World, Non-Terrestrial Networks, IoT, Smart Grids

ACM Reference Format:
Basem Shihada and Mohamed Abdallah. 2025. Artificial Intelligence in Networking Research in the Arab World. In *Proceedings of (CACM Arab World Special Section)*. ACM, New York, NY, USA, 6 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

The past decade has witnessed exponential growth in wireless networks, accompanied by increasing demands for higher data speeds and broader connectivity [1]. As user expectations rise, the existing network infrastructure faces significant challenges related to resource limitations, connectivity quality, and spectrum congestion. These issues have led to performance degradation and have necessitated innovative solutions to ensure sustainable network growth.

In response to these challenges, the Arab world has quickly emerged in the networking research, with efforts focused on building intelligent, sustainable networks that integrate advanced AI and ML techniques [2]. These technologies play a pivotal role in optimizing network operations, automating management tasks, and enabling smarter, more efficient communication systems. Research institutions and telecommunications companies in many Arab countries are at the forefront of these advancements, collaborating with academia to develop cutting-edge solutions.

This paper aims to provide a sample of the current state of networking research in the Arab world, emphasizing on the following two primary areas: intelligent wireless connectivity including non-terrestrial network integration

Authors' Contact Information: Basem Shihada, basem.shihada@kaust.edu.sa, Computer, Electrical and Mathematical Sciences and Engineering Division, King Abdullah University of Science and Technology, Thuwal, Kingdom of Saudi Arabia; Mohamed Abdallah, Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar, moabdallah@hbku.edu.qa.

and intelligent and secure systems. The discussion will highlight the region's contributions to these fields. It will also address the challenges that must be overcome to fully realize the potential of AI and ML in modern networking.

2 Intelligent Wireless Connectivity

The deployment of 5G of mobile cellular networks represents a significant leap forward in communication technology, offering enhanced features in terms of coverage, capacity, and data speeds. However, as network demands continue to grow, 5G must address the challenges of providing reliable connectivity in underserved areas while managing the increasing data load in densely populated regions. A pivotal solution to these challenges involves the integration of AI and ML techniques in next generation 6G networks, which enable networks to dynamically optimize resources and improve service quality [3].

2.1 Intelligent 5 and 6G Networks

In the context of 6G, AI and ML technologies are leveraged to manage network resources more intelligently by automating processes such as dynamic spectrum allocation, traffic load balancing, and predictive maintenance [3]. These capabilities are essential for maintaining the quality of service (QoS) in environments where data demand fluctuates rapidly, such as urban centers and large-scale events. Researchers in the Arab world have made several contributions to this area, particularly in the development of ML algorithms that predict network traffic patterns and adapt network configurations in real-time. For instance, researchers in [4] proposed dual attention-based federated learning (FL) models to perform traffic prediction in heterogeneous terrestrial networks accurately, ensuring optimal data routing and enhancing the overall efficiency of the network. Another notable contribution in [5] is the development of the Deep Reinforcement learning (DRL)-based Radio Access Technology (RAT) called DeepRAT, which is a hierarchical multi-agent DRL-based solution for jointly optimizing RATs assignment and dynamic resource allocation in heterogeneous networks. This work was done in collaboration with Ooredoo, which is a local Qatari telecommunication company, where dataset was collected to understand the network behavior. The DeepRAT framework has demonstrated superior performance compared to existing heuristic approaches, maximizing downlink sum-rate and adapting effectively to dynamic network changes such as edge device mobility.

2.2 Intelligent Integration of Non-Terrestrial Networks

To extend the connectivity to remote and underserved regions, the use of non-terrestrial networks (NTNs), such as satellites and UAVs, is becoming increasingly important. The new generation of Low Earth Orbit (LEO) satellites plays a critical role in providing high-capacity, low-latency communications that complement terrestrial networks. Researchers have explored methods for optimizing traffic offloading between integrated satellite and terrestrial networks, aiming to relieve congestion on terrestrial backhauls. The proposed approaches involve offloading Ultra-Reliable Low-Latency Communication traffic to terrestrial networks while routing Enhanced Mobile Broadband traffic through satellites to meet diverse latency and data rate requirements [6].

Further, advancements in UAV-based communication have led to innovative solutions for network coverage in urban environments. The "Learn-As-You-Fly" algorithm in [7], dynamically adjusts UAV positions and associations with ground users to maximize network performance. This algorithm utilizes reinforcement learning techniques to adapt to changing traffic conditions, providing a flexible and efficient means of managing data traffic [7]. In [8], researchers proposed a Dynamic Digital Twin Edge Air-Ground Network (D2TEAGN) for 6G-enabled industrial Internet of Things (IoT) that integrates UAVs, edge computing, and digital twin technology to optimize resource allocation and task offloading. The problem was mapped into a Markov Decision Process and then solved using a customized DDPG algorithm. The D2TEAGN framework reduces energy consumption by up to 27% compared to baseline methods by jointly optimizing UAV trajectory, device association, and edge resources while respecting delay and energy constraints.

3 Intelligent and Secure Systems

In the age of IoT, networks should not only act as flowing pipes but instead should stand as an intelligent communication system that helps in analyzing and optimizing traffic. In this section, we highlight the relevant, intelligent IoT work that provides higher reliability, performance, and, most importantly, security of IoT over today's IP network.

3.1 Intelligent IoT Traffic Management

IoT networks face unique traffic patterns characterized by frequent, variable, and often unpredictable data transmissions. To address these challenges, researchers have developed intelligent traffic management systems that utilize AI/ML to enhance the QoS. For instance, efforts in the region have led to the creation of a smart IoT QoS system, known as SDN-based Application-aware Dynamic IoT QoS (SADIQ), which dynamically adjusts network parameters based on the specific requirements of IoT applications [9]. This system has significantly improved error rates in applications such as weather monitoring and smart parking, with reductions in temperature reporting errors and incorrect parking status detection by up to 45x and 30x, respectively. By observing the spatial and temporal correlations in IoT traffic, researchers have developed a traffic prediction at the edge using the Federated Meta-Learning approach. Such intelligent data handling ensures that critical information is prioritized while reducing network congestion and minimizing data loss and thus, increase network reliability and performance [9].

3.2 Intelligent and Secure Decentralized IoT Architectures

The traditional centralized approach to IoT network management presents challenges in terms of scalability, latency, and security, especially as the number of connected devices continues to grow. To overcome these limitations, a shift towards decentralized and automated IoT architectures is essential. Researchers in the Arab world have proposed edge-centric IoT models based on blockchain technology, which provide a more scalable and secure framework for managing IoT data. An example of this approach is the development of a blockchain-based system called Synopsis, which utilizes Byzantine fault tolerance consensus protocols to facilitate secure and efficient data exchange in IoT networks [10]. This system has achieved substantial improvements, including a reduction in memory footprint from megabytes to a few kilobytes and a decrease in message complexity and commitment delay by 85% and 99.4%, respectively.

Security remains a significant concern for IoT networks, given the ever-increasing number of cyber threats and vulnerabilities. To address these risks, researchers have turned to AI/ML techniques capable of detecting and mitigating potential threats in real-time, thereby enhancing the overall resilience of IoT systems. In this context, FL emerges as a powerful approach that enables secure, scalable, and resource-efficient AI-driven IoT solutions. These benefits are realized through techniques, which collectively optimize the learning performance as well as the resource consumption considering both data and resource heterogeneity. For example, in order to handle statistical heterogeneity and varying resource constraints, client selection and hierarchical FL frameworks have been proposed, reducing energy consumption while sustaining robust model performance [11]. Specifically, clustered FL (CFL) [11] further enhances convergence and scalability by grouping clients with similar data distributions, outperforming traditional FL solutions in complex IoT settings. Real-world IoT deployments often entail large volumes of unlabeled data, limited resources, and latency constraints, prompting additional refinements to FL-based methods. In this context, combining FL and CFL with semi-supervised learning (SSL) has effectively leveraged unlabeled data at the network edge, boosting global model accuracy while minimizing communication and computation overheads. Extending this synergy, integrating CFL and SSL [12] has demonstrated improvements in model accuracy and reduced energy usage by employing specialized models and judicious client scheduling strategies. These multifaceted FL-based strategies, including CFL and SSL integrations, have collectively improved data handling, resource allocation, and scalability in decentralized IoT environments. Consequently, IoT deployments can become more intelligent and resilient, as these methods enable robust collaboration among diverse devices while preserving privacy and optimizing resource usage.

Despite FL's intrinsic privacy advantages, the technology remains susceptible to adversarial threats such as poisoning and evasion attacks that compromise global model reliability [13]. To strengthen security, the authors implement DRL-based solutions that facilitate reputation mechanisms capable of detecting and mitigating malicious participants. The DRL agent continuously assesses the behavior of IoT devices during the FL process, assigning reputation scores based on their contributions and reliability [13]. Devices exhibiting anomalous behavior receive lower scores, reducing their influence on the global model and thereby enhancing the overall robustness of the FL system. Beyond DRL-based solutions, the framework incorporates divergence-based detection methods to identify adversarial activities. These methods effectively safeguard IoT applications against potential threats by analyzing the differences between benign and malicious model updates. This dual-layered approach ensures that both known and emerging adversarial behaviors are promptly detected and addressed, maintaining the integrity of the FL process.

3.3 Intelligent and Secure Smart Grids

Smart grids represent a critical component of next-generation IoT ecosystems, bridging energy distribution, metering, and consumer demand through sophisticated communication infrastructures. However, these infrastructures remain highly susceptible to cybersecurity vulnerabilities and adversarial ML attacks. Researchers have conducted extensive work to protect smart grid communication protocols against these evolving threats, focusing on collaborative frameworks, anomaly detection, and resilient system design. A key solution proposed is FedPot, an FL–based framework for improving the security of Advanced Metering Infrastructure. FedPot enables small-scale power suppliers (SPSs) to deploy honeypots and securely share data with traditional power retailers, ensuring both data privacy and enhanced detection of malicious activities. This framework incorporates a quality-aware FL mechanism that integrates a data quality measure into an enhanced FedAvg algorithm. Additionally, FedPot introduces a fair and transparent incentive mechanism to reward SPSs based on the quality and usefulness of their shared data, thereby promoting active collaboration. Simulation results validate FedPot's capacity to strengthen security frameworks for smart grids while maintaining fairness in reward distribution [14]. Also researchers have developed a dual-layered defense strategy against cyber and adversarial ML attacks within the IEC 60870-5-104 protocol. This approach combines conventional cybersecurity measures with adversarial training, reinforcing known defenses to address protocol vulnerabilities and utilizing adversarial examples to train intrusion detection systems for enhanced robustness. Such a layered strategy mitigates risks from both traditional cyber threats and sophisticated adversarial behaviors, ensuring reliable grid operations [15]. Lastly, electricity theft remains a major concern in smart grid systems, where adversaries manipulate meter readings to inflate energy injection. To counter this, a fine-tuned recurrent neural network model conducts time-series analyses of meter data and incorporates additional features such as daily and monthly consumption patterns. Experimental results demonstrate robust detection of theft scenarios, even under minimal data perturbations. These cutting-edge security mechanisms, ranging from collaborative federated approaches to sophisticated anomaly detection, collectively form a comprehensive defensive framework for safeguarding smart grid networks [16].

4 Discussion

The integration of AI and ML in networking is rapidly advancing the capabilities of modern communication systems, with notable research being conducted to address key challenges in wireless connectivity, IoT systems, and next-generation networks. The research landscape is characterized by a strong emphasis on developing intelligent algorithms for network optimization, predictive maintenance, and enhanced security.

Arab researchers have demonstrated the potential of AI/ML to optimize various aspects of network management, from traffic prediction and resource allocation to advanced security measures. These innovations have enhanced the performance of existing 5G networks and laid the groundwork for 6G, where intelligent communication will be central to the network's operation. The focus on integrating non-terrestrial communication systems, such as satellites, UAVs, and none-terrestrial platforms, exemplifies a forward-looking approach to achieving comprehensive global connectivity. A key aspect of the 6G vision is to provide more personalized, human-centric communication experiences. This approach extends beyond mere connectivity to consider user expectations for privacy, accessibility, and seamless interaction. The development of human-centric mobile communication frameworks aims to deliver services that adapt to user needs, offering secure and context-aware connectivity across various applications. In this context, researchers have proposed frameworks that integrate AI-driven data analytics to deliver adaptive services, such as real-time language translation, health monitoring, and augmented reality applications [17]. By prioritizing user-centric features, 6G networks can enhance the quality of life and drive innovation across sectors such as healthcare, education, and entertainment [17].

Despite these advancements, challenges remain in scaling AI/ML solutions for broader adoption. Key issues include the need for skilled professionals who can develop and maintain complex AI-driven systems, as well as the establishment of robust regulatory frameworks that support innovation while ensuring data security and privacy. Additionally, the availability and quality of data for training AI models continue to be a barrier, requiring collaborative efforts between academia, industry, and governments to facilitate data sharing and develop regional data ecosystems.

The decentralized architecture trend, especially in IoT networks, reflects a paradigm shift away from traditional centralized models toward more resilient and scalable frameworks. The use of blockchain and AI for secure, distributed network management indicates a commitment to addressing the scalability and security issues inherent in large-scale IoT deployments. However, these approaches must also contend with the increased complexity of decentralized systems and the need for efficient consensus mechanisms.

5 Conclusion

The Arab world is leveraging AI and ML to optimize existing networks, advance IoT, and pioneer 6G technologies. Integrating NTNs and adaptive communication solutions addresses current challenges while preparing for future demands. Overcoming workforce, regulatory, and data hurdles is crucial for maximizing these advancements. By fostering innovation and viewing networks as intelligent ecosystems, the research work in the region has the potential to contribute to the global networking advancements and drive digital and economic progress.

References

[1] Shuping Dang, Osama Amin, Basem Shihada, and Mohamed-Slim Alouini. What should 6G be? *Nature Electronics*, 3(1):20–29, 2020.

[2] Basem Shihada, Tamer Elbatt, Ahmed Eltawil, Mohammad Mansour, Essaid Sabir, Slim Rekhis, and Sanaa Sharafeddine. Networking research for the arab world: from regional initiatives to potential global impact. *Commun. ACM*, 64(4):114–119, March 2021.

[3] Sahar Ammar, Chun Pong Lau, and Basem Shihada. An in-depth survey on virtualization technologies in 6g integrated terrestrial and non-terrestrial networks. *IEEE Open Journal of the Communications Society*, 5:3690–3734, 2024.

[4] Chuanting Zhang, Shuping Dang, Basem Shihada, and Mohamed-Slim Alouini. Dual attention-based federated learning for wireless traffic prediction. In *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*, pages 1–10, 2021.

[5] Abdulmalik Alwarafy, Bekir Sait Çiftler, Mohamed Abdallah, Mounir Hamdi, and Naofal Al-Dhahir. Hierarchical multi-agent drl-based framework for joint multi-rat assignment and dynamic resource allocation in next-generation hetnets. *IEEE Transactions on Network Science and Engineering*, 9(4):2481–2494, 2022.

[6] Wiem Abderrahim, Osama Amin, and Basem Shihada. How to leverage high altitude platforms in green computing? *IEEE Communications Magazine*, 61(7):134–140, 2023.

[7] Hajar El Hammouti, Mustapha Benjillali, Basem Shihada, and Mohamed-Slim Alouini. Learn-as-you-fly: A distributed algorithm for joint 3d placement and user association in multi-uavs networks. *IEEE Transactions on Wireless Communications*, 18(12):5831–5844, 2019.

[8] Muhammet Hevesli, Abegaz Mohammed Seid, Aiman Erbad, and Mohamed Abdallah. Task offloading optimization in digital twin assisted mec-enabled air–ground iiot 6g networks. *IEEE Transactions on Vehicular Technology*, 73(11):17527–17542, 2024.

[9] Enas Ahmad, Maha Alaslani, Fahad R. Dogar, and Basem Shihada. Location-aware, context-driven qos for iot applications. *IEEE Systems Journal*, 14(1):232–243, 2020.

[10] Maha Alaslani, Sonali Suri, Basem Shihada, and Faisal Nawab. Synopsis: a scalable byzantine distributed ledger for iot networks. In *2024 6th International Conference on Blockchain Computing and Applications (BCCA)*, pages 30–38, 2024.

[11] Moqbel Hamood, Abdullatif Albaseer, Mohamed Abdallah, Ala Al-Fuqaha, and Amr Mohamed. Optimized federated multitask learning in mobile edge networks: A hybrid client selection and model aggregation approach. *IEEE Transactions on Vehicular Technology*, 73(11):17613–17629, 2024.

[12] Moqbel Hamood, Abdullatif Albaseer, Mohamed Abdallah, and Ala Al-Fuqaha. Efficient data labeling and optimal device scheduling in hwns using clustered federated semi-supervised learning. *IEEE Transactions on Communications*, pages 1–1, 2024.

[13] Noora Mohammed Al-Maslamani, Bekir Sait Ciftler, Mohamed Abdallah, and Mohamed M. E. A. Mahmoud. Toward secure federated learning for iot using drl-enabled reputation mechanism. *IEEE Internet of Things Journal*, 9(21):21971–21983, 2022.

[14] Abdullatif Albaseer, Nima Abdi, Mohamed Abdallah, Marwa Qaraqe, and Saif Al-Kuwari. Fedpot: A quality-aware collaborative and incentivized honeypot-based detector for smart grid networks. *IEEE Transactions on Network and Service Management*, 21(4):4844–4860, 2024.

[15] Hadir Teryak, Abdullatif Albaseer, Mohamed Abdallah, Saif Al-Kuwari, and Marwa Qaraqe. Double-edged defense: Thwarting cyber attacks and adversarial machine learning in iec 60870-5-104 smart grids. *IEEE Open Journal of the Industrial Electronics Society*, 4:629–642, 2023.

[16] Maymouna Ez Eddin, Abdullatif Albaseer, Mohamed Abdallah, Sertac Bayhan, Marwa K. Qaraqe, Saif Al-Kuwari, and Haitham Abu-Rub. Fine-tuned rnn-based detector for electricity theft attacks in smart grid generation domain. *IEEE Open Journal of the Industrial Electronics Society*, 3:733–750, 2022.

[17] Luyao Yang, Osama Amin, and Basem Shihada. Intelligent wearable systems: Opportunities and challenges in health and sports. *ACM Comput. Surv.*, 56(7), April 2024.

Received 1 February 2025; revised TBD 2025; accepted TBD 2025