Chapter 8
Safety and Security in Autonomous Traffic Systems Management With AI:
Economic Implications of Traffic Optimization in Smart Cities

Anuradha Jain
https://orcid.org/0000-0001-6996-8309
VIPS, India

ABSTRACT

Safety and security are critical pillars in managing autonomous traffic systems with AI, particularly in the context of smart cities. These systems integrate advanced technologies such as IoT, V2X communication, and machine learning to enhance traffic flow, reduce accidents, and optimize urban mobility. However, ensuring the reliability of these systems demands robust safety protocols to address challenges like mixed-traffic scenarios and unexpected system failures. Concurrently, cybersecurity measures are vital to counter threats such as hacking and data breaches that could compromise vehicle and infrastructure integrity. Economically the AI-driven traffic optimization reduces congestion, cuts fuel consumption, and improves productivity by minimizing travel delays. The shift to autonomous traffic systems fosters urban sustainability by decreasing emissions and promoting energy efficiency. While challenges remain in terms of public trust and regulatory frameworks, the economic and environmental benefits position these systems as transformative solutions for the future of urban mobility.

DOI: 10.4018/979-8-3693-9410-6.ch008

1. INTRODUCTION

These advances are leading to systems that can effectively combat contemporary transportation issues such as traffic congestion, road safety, and environmental sustainability. Safety and security provide the basis of managing autonomous traffic systems, vehicle and infrastructure operation and communication network. The efficiency with which these machines operate will minimize the burden on our cities, while at the same time the financial gains made from their operation will also have an immediate impact on our quality of life thanks to a better traffic flow and optimal resource usage (Ji, 2021).

The first aspect of safety in autonomous traffic systems is to design so that accidents cannot happen, and that risks can be managed. The technology behind autonomous vehicles (AVs) is complex, relying on advanced sensors, machine learning algorithms, and real-time data processing to make split-second decisions (Huang et al., 2021). However, ensuring safety in these systems presents problems that must be overcome, including irregularities in road conditions, human errors in mixed-traffic environments (where both human-driven and autonomous vehicles operate), and the malfunction of such systems. AI is equipped with safety measures like collision, risk, trajectory, and environmental perception to help tackle these issues. Predictive systems process vast amounts of data and use predictive modeling to forecast potential threats and corrective actions, allowing for a highly reliable means to power autonomous operations (Tang et al., 2021).

1.1 Evolution of Autonomous Traffic Systems

Along with operational security, this also applies to the security of autonomous traffic systems. These systems rely on inter-linked devices and communication networks, including Vehicle-to-Everything (V2X) communication that enables data transfer between vehicles, infrastructure, and traffic management centers. This connectivity can increase efficiency, but can also open the door for cybersecurity weaknesses. Others pose cybersecurity threats that can intercept data between the vehicle communication systems and the wider cloud network, or hacking into vehicle control systems or tampering with traffic signals, both of which can disrupt operations and create significant public safety emergencies. To secure such systems, we would need to use strong encryption algorithms, make use of blockchain tech for secure interchanges of data storage through decentralized ledgers, and AI will help scan and identifies breaches in real time. Cybersecurity protocols must be