

IMPROVED SECURITY ENHANCEMENT IN VEHICLE COMMUNICATION USING INTEGRATED SMART CITY INFRASTRUCTURE

Mr.R. Shanmugam

Research Scholar, Dept of Computer and Information Science, Annamalai University, Chidambaram

Dr.S.Manikandan

Assistant Professor, Dept of Computer and Information Science, Annamalai University, Chidambaram

In the rapidly evolving landscape of smart cities, the pervasive integration of Connected and Autonomous Vehicles (CAVs) via Vehicle-to-Everything (V2X) communication promises transformative advancements in transportation. However, the open and dynamic nature of V2X, coupled with wireless vulnerabilities, exposes it to significant cybersecurity threats such as jamming, spoofing, DoS, and false data injection, risking severe consequences from traffic accidents to privacy breaches. This research proposes a novel framework for robust security enhancement in vehicle communication by strategically leveraging an integrated smart city infrastructure. We meticulously analyze the current threat landscape in V2X within smart city environments. Our solution synergistically combines advanced cryptographic techniques, including Public Key Infrastructure (PKI) and Elliptic Curve Digital Signature Algorithm (ECDSA) for secure message authentication, with distributed ledger technologies (blockchain) for tamper-proof data logging and decentralized trust management. Furthermore, the framework integrates Artificial Intelligence (AI)/Machine Learning (ML) for real-time intrusion detection and predictive security. By incorporating smart city components like intelligent traffic management systems and edge computing, the proposed framework not only strengthens the overall security posture through localized decision-making and reduced latency but also significantly enhances the resilience, trustworthiness, and privacy of vehicular communication, paving the way for a more secure and efficient intelligent transportation system in future smart cities.