Security Implications of the Transition from IEEE 802.11p to Cellular (C-V2X / 5G/6G) in Intelligent Transportation Systems (ITS) – A risk analysis

Supervisors: Badis HAMMI and Nesrine KAÂNICHE

Context and motivation:

The rollout of Connected and Autonomous Vehicles (CAVs) increasingly relies on vehicular communications as a core enabler of Cooperative ITS (C-ITS) services (safety messages, cooperative perception, platooning, traffic management). Historically, these services have depended on IEEE 802.11p-based stacks (DSRC / ITS-G5), which provide localized, low-latency V2X exchanges with well-understood threat models. The migration toward Cellular V2X (C-V2X) and 5G (and future 6G) architectures promises greater range, native support for edge computing (MEC), network slicing, and high throughput. However, this architectural shift also expands the attack surface (network cores, radio access, cloud/edge infrastructure, operator domains) and changes fundamental assumptions about trust, latency, and privacy. A systemic, evidence-based risk analysis is therefore required to understand how threat models, vulnerabilities, and mitigation strategies must evolve to preserve safety, privacy, and integrity in next-generation ITS.

Objective:

Produce a rigorous, systemic analysis of security and privacy implications arising from the transition from IEEE 802.11p to cellular V2X and 5G/6G technologies in ITS. The study will (1) compare threat landscapes and vulnerability surfaces across legacy and cellular architectures, (2) identify new attack vectors introduced by cellularization and edge/cloud integration, (3) evaluate certificate management and revocation practices at scale, and (iv) propose practical mitigation strategies, architectures, and testing artifacts to harden future deployments.

Core research questions:

1. How do the threat models for 802.11p and C-V2X/5G differ in practice (radio layer, link layer, network/core, edge/cloud)?
2. Which vulnerability classes become more (or less) critical when ITS migrates to cellular infrastructures (e.g., SIM/USIM compromises, network slicing isolation failures, MEC compromise, signalling storms)?
3. How do certificate management, authentication, and revocation scale and perform under cellular paradigms, and which gaps exist relative to safety requirements?
4. Which network-level attacks materially affect vehicular safety and privacy?

Methodology:

1. State-of-the-art review: systematic literature survey and standards analysis (802.11p, ITS-G5, C-V2X, 3GPP releases, MEC, network slicing, security frameworks).
2. Formalized threat modeling: develop comparative attack trees and data-flow analyses for representative ITS services under both paradigms.
3. Attack surface and vulnerability inventory: enumerate assets, interfaces, and likely adversarial capabilities; map to CVE/CWE classes and to safety impacts.

Deliverables:

1. Comprehensive comparative risk assessment report.
2. Attack catalog and reproducible testbed artifacts (emulated scenarios, scripts, Docker images) for community use.
3. Quantitative measurements of attack impact on safety-critical KPIs.
4. Proposed mitigations, configuration guidelines, and a brief for standardization bodies.