VANETs and IoT in Smart Cities: Technology Overview and Economic–Policy Implications

Veranda Syla[1], **Algenti Lala**[2]

Abstract: The integration of Vehicular Ad Hoc Networks (VANETs) into Internet of Things (IoT)-enabled smart city environments promises to enhance road safety, traffic efficiency, and intelligent transportation services. This paper presents an overview of the key enabling technologies for VANET-based smart transportation, including wireless communication standards from DSRC to cellular 5G V2X, vehicular sensing and data networking, localisation techniques, and security mechanisms, and explains how these technologies converge within smart cities. In addition to the technical perspective, we examine the economic and policy implications of deploying VANET and IoT systems at scale. We analyse the expected economic benefits, such as reduced accident costs and congestion and the creation of new business opportunities, alongside the challenges of high infrastructure investment and the need for critical mass adoption. We also highlight policy considerations ranging from spectrum allocation and technology standardisation to data privacy and regulatory frameworks that can facilitate or hinder implementation. By combining a technological survey with an economic and policy analysis, this work aims to inform researchers, city planners, and policymakers about the opportunities and challenges involved in realising secure, efficient, and economically viable vehicular networks in future smart cities.

Keywords: Connected Vehicles; V2X Communication; Intelligent Transportation; Economic Impact

JEL Classification: R41; R48; O18; O33; L91

1. Introduction

Modern smart cities increasingly rely on Intelligent Transportation Systems (ITS) to improve mobility and safety, with Vehicular Ad Hoc Networks (VANETs) forming a crucial communication backbone connecting vehicles, roadside infrastructure, pedestrians, and the cloud (Dutta et al., 2024; Mishra & Singh, 2025). In a VANET, vehicles equipped with onboard communication units can exchange information with each other (vehicle-to-vehicle, V2V) and with road infrastructure (vehicle-to-infrastructure, V2I) in real-time to enable cooperative awareness. This concept is extended through the

[1] PhD Candidate, Faculty of Information Technology, Polytechnic University of Tirana, Albania, Address: Square Mother Teresa, Tirana, Albania, Corresponding author: vsyla@fti.edu.al.

[2] Associate Professor, Faculty of Information Technology, Polytechnic University of Tirana, Albania, Address: Square Mother Teresa, Tirana, Albania, E-mail: alala@fti.edu.al.

Internet of Vehicles (IoV) paradigm, which treats each vehicle as a smart object in the IoT ecosystem and integrates vehicular networks into the broader smart city infrastructure (El Madani et al., 2022; Contreras-Castillo et al., 2017). By converging VANETs with urban IoT platforms, cities can leverage data from vehicles to enhance road safety, reduce traffic congestion, and enable new services such as intelligent traffic management, adaptive routing, and assisted or autonomous driving support (Dutta et al., 2024; Mishra & Singh, 2025). For instance, connected vehicles can warn each other of hazards beyond a driver's line-of-sight, or feed live traffic data to city management centres for real-time signal timing optimization and route adjustments.

However, integrating VANETs into IoT-based smart cities also presents significant challenges. Urban environments feature high vehicle densities, radio interference, and fast-changing network topologies, which can strain wireless communication protocols (Bhover et al., 2017; Paranjothi et al., 2020). Ensuring reliable, low-latency V2X connectivity in crowded city streets often requires moving beyond traditional Dedicated Short-Range Communications (DSRC) and exploring cellular V2X technologies. Precise localisation of vehicles is another challenge: tall buildings in "urban canyons" can degrade GPS signals and accuracy, necessitating complementary positioning techniques. Meanwhile, today's vehicles carry a multitude of sensors (cameras, radars, LiDARs, etc.), effectively forming vehicular sensor networks that act as mobile sensing platforms for the city. Leveraging these sensing capabilities at scale introduces big data processing demands and interoperability issues among heterogeneous devices. Security and privacy concerns are equally paramount vehicular networks face threats such as message spoofing, sybil attacks, eavesdropping, and denial-of-service, which can endanger lives if not properly mitigated. The integration with IoT and cloud services further broadens the attack surface, raising concerns over cyber-attacks on connected vehicles or misuse of sensitive mobility data. Recent research has emphasized secure communication protocols and trust management frameworks tailored for VANETs to address these issues.

Beyond the technical domain, there are important economic and policy factors that influence the successful deployment of VANET and IoT technologies in smart cities. Deployment at city-wide scale can be expensive: installing roadside units, edge computing infrastructure, and equipping vehicles with V2X capability entails substantial investment. The benefits of such systems often depend on widespread adoption (a critical mass of connected vehicles), creating a classic network externality issue: the value of the system increases as more participants join, but individual actors may be reluctant to invest early unless the ecosystem is in place. This dynamic suggests a role for public policy in jump-starting deployment. Additionally, regulatory frameworks and standards are still evolving; different regions have taken different approaches (for instance, Europe promoted ITS-G5 based on DSRC, while the US and China have leaned toward cellular V2X), and achieving global or interoperable standards for vehicular communication remains an open issue. Privacy legislation and data-sharing policies will also shape how vehicular data can be used within smart cities. In summary, realising the full promise of VANETs in IoT-enabled smart cities requires not only overcoming technical hurdles but also addressing economic viability and establishing supportive policy frameworks.

Contributions: In this paper, we present a comprehensive overview of VANETs and IoT in smart cities from both a technology and an economic policy perspective. On the technology side, we review the foundations of VANET communications, sensing, localisation, and security in the context of smart city applications, drawing on recent advancements (primarily 2018–2025) from the literature. On the economic and policy side, we discuss the anticipated economic benefits of VANET–IoT integration (and the associated costs) and examine the policy measures and regulatory developments that impact deployment. The remainder of the paper is organized as follows: Section 2 provides background on VANET architectures and the smart city IoT context. Section 3 surveys the wireless communication technologies enabling vehicular networking. Section 4 discusses the role of vehicular sensing and data in IoT-enabled cities. Section 5 reviews localisation techniques for vehicles in urban settings. Section 6 addresses security challenges and solutions. Section 7 then analyses the economic implications of VANET and IoT deployments, and Section 8 examines policy implications, including standardisation and regulatory issues. Finally, Section 9 concludes the paper with future work and recommendations.

2. VANETs in IoT-Enabled Smart Cities: Background

2.1. VANET Architecture and IoT Integration

A typical VANET consists of mobile nodes (vehicles) equipped with wireless communication devices (on-board units, OBUs) and fixed roadside infrastructure nodes (roadside units, RSUs) deployed along roadways (Bhover et al., 2017). Early VANET implementations have relied on DSRC-based radios using the IEEE 802.11p standard in the 5.9 GHz band to support direct V2V and V2I communication without needing cellular coverage. Vehicles periodically broadcast safety messages (e.g., Basic Safety Messages, BSMs, containing position, speed, heading) to nearby vehicles and RSUs within a range of a few hundred meters, enabling cooperative awareness of traffic conditions. In an IoT-enabled smart city context, VANETs do not operate in isolation but become integrated with the city's information infrastructure; this integration is often referred to as the Internet of Vehicles (IoV) or vehicular IoT (El Madani et al., 2022; Contreras-Castillo et al., 2017). A commonly used reference model is a multi-layer architecture with distinct layers for (1) Perception, where vehicles and other sensors collect data; (2) Network, which comprises the V2X communication networks (DSRC, cellular, etc.) that transport data; (3) Processing, which includes edge or cloud computing platforms that aggregate and analyse vehicular data; and (4) Application, which encompasses the smart city services (traffic monitoring, safety applications, infotainment, etc.) that utilize the information (Contreras-Castillo et al., 2017; Deniz, 2025). Such layered architecture ensures modularity and scalability in complex urban environments. For example, in this paper, outline an IoV architecture that separates sensing, networking, middleware, and application layers to coordinate data flow efficiently in smart cities.

2.2. Smart City Applications of VANET–IoT

The convergence of VANETs with IoT unlocks a broad range of applications in smart cities. Safety applications are paramount: by sharing real-time information, connected vehicles can effectively "see" beyond their individual sensors. For instance, if an emergency brake event or a hazard is detected by one vehicle, that information can be instantly broadcast to following vehicles and to traffic management centres, preventing pileups and improving emergency response times. Cooperative awareness messages allow vehicles to extend their situational awareness, which is especially valuable in scenarios like blind intersections or poor visibility. Traffic efficiency applications leverage vehicular data to optimize traffic flow: connected vehicles can enable adaptive traffic signal control, intelligent intersection management, dynamic speed harmonization on highways, and rerouting of traffic in response to congestion (Dutta et al., 2024). Urban traffic management systems ingest live data streams from vehicles to adjust signal timings or suggest alternative routes in real-time, thereby reducing overall delay and emissions. Infotainment and convenience applications are also enhanced in VANET–IoT environments passengers can enjoy high-speed connectivity, location-based services (e.g., finding available parking or charging stations), and context-aware content delivery through vehicular network connections. Emerging applications on the horizon include platooning of semi-autonomous vehicles (where multiple vehicles coordinate to drive in close formation to reduce aerodynamic drag and save fuel) and treating vehicles as mobile sensors for city infrastructure and environment monitoring. Researchers have demonstrated that ordinary vehicles can serve as moving sensor platforms; for example, crowdsourcing data on road surface conditions (detecting potholes or icy patches) and environmental parameters (air quality, noise levels) as they drive, which can then be shared with city authorities for maintenance and planning (Dutta et al., 2024). The concept of a "social IoV" even envisions vehicles not only exchanging raw data but also collaborating in a distributed manner forming vehicular social networks or sharing resources (such as computing power or storage for data caching) with one another to support collective services.

2.3. Technological Trends

Recent advances in communication and computing are rapidly influencing VANET design and capabilities. One major trend is the rise of Cellular V2X (C-V2X) communication as an alternative to the legacy 802.11p/DSRC approach. C-V2X leverages cellular network technology (defined by 3GPP) for vehicular communications, and it operates in two modes: (I) a direct device-to-device mode (also known as the PC5 sidelink) where vehicles broadcast to each other over dedicated spectrum (often the same 5.9 GHz band) without involving the cellular core network, and (II) a network-assisted mode (Uu interface) where communications can hop through cellular base stations (eNodeB/gNodeB). The first generation of C-V2X based on LTE (Release 14/15) introduced scheduling-based channel access and other enhancements to improve reliability under high congestion, outperforming 802.11p in many scenarios especially at higher vehicle densities. The subsequent evolution with 5G NR V2X (Release 16 and beyond) further boosts performance offering higher data rates, ultra-low latency (aiming for sub-10 ms for critical messages), improved reliability (e.g., >99.999% for mission-critical transmissions), and the ability to support advanced use cases like cooperative perception and remote driving control. Unlike DSRC, which is purely ad-hoc, the cellular-based approach can also utilize the existing mobile network infrastructure to provide wide-area connectivity (vehicle-to-network, V2N) for example, vehicles can communicate with cloud services or distant servers via the cellular network for updates, HD map downloads, or fleet management. Moreover, 5G networks introduce features like *network slicing* (dedicating a virtual slice of network resources for automotive services to guarantee quality of service) and MEC (Multi-access Edge Computing), which place cloud-computing resources at the network edge (e.g., at cell towers or RSUs). MEC enables intensive computation (such as sensor data fusion, object recognition from video streams, etc.) to be offloaded by vehicles to nearby edge servers, with results returned quickly over the low latency 5G links. This fusion of communication and computing allows for new concepts like collaborative sensing (vehicles sharing raw or processed sensor data via edge servers to collectively perceive their environment beyond line-of-sight). In addition, the integration of Artificial Intelligence (AI) and data analytics into vehicular networks is growing. Machine learning techniques are being used for predicting traffic conditions, driving behaviors, and even for security anomaly detection in V2X communications. The ongoing deployment of 5G and the prospect of 6G networks are expected to significantly enhance VANET capabilities, enabling scenarios such as massive sensor data sharing in real-time and fully synchronized autonomous driving maneuvers in traffic.

Despite these advancements, several challenges remain in realising secure and intelligent VANETs within smart cities. Communication networks must scale to thousands of fast-moving nodes without succumbing to excessive packet collisions or wireless channel congestion (Bhover et al., 2017; Paranjothi et al., 2020). Meeting strict latency requirements for safety (e.g., broadcasting hazard alerts within milliseconds) may require a heterogeneous network approach combining multiple communication technologies (DSRC, cellular, Wi-Fi, even emerging mmWave or visible light communication), which in turn raises interoperability issues between devices using different standards. Achieving accurate and robust positioning of vehicles in dense urban areas is an ongoing challenge; GPS/GNSS accuracy degrades under Non-Line-of-Sight conditions due to signal blockage and multipath effects from buildings, so supplemental localisation methods (such as inertial sensors, map-matching, UWB beacons, or cooperative positioning using V2V ranging) are needed. Security remains a moving target: attackers may attempt to inject false traffic information, jam V2X channels, or track vehicles' movements to violate privacy. Traditional IT security solutions are not directly applicable in VANET contexts because of the real-time, distributed nature of vehicular communications and the absence of a fixed infrastructure in V2V scenarios. This necessitates specialized mechanisms like distributed trust models, vehicular public key infrastructures (PKI for issuing digital certificates to vehicles), and on-board intrusion detection systems (Alalwany & Mahgoub, 2024; Garg et al, 2020). Finally, deployment hurdles include the cost and complexity of equipping an entire city with V2X roadside units and edge servers. This is capital-intensive, and the need for a sufficient proportion of vehicles to be equipped before many applications deliver full benefit. Early adoption may be slow without incentives, which is why regulatory, and standardisation efforts are critical. There are ongoing global efforts to standardize VANET communications (e.g., the ETSI ITS-G5 standard in Europe for DSRC-based V2X, vs. the push for C-V2X in the US and China), but a universally accepted standard has not yet emerged. Governments and industry alliances are actively involved in this space, as discussed later in our policy section.

3. Communication Technologies for VANETs in Smart Cities

Robust, low-latency wireless communication is the backbone of any VANET deployment. This section surveys the primary communication technologies that enable vehicle-to-everything (V2X) links, focusing on the legacy DSRC/WAVE standard and the newer cellular-based approaches, and highlights their characteristics in the context of smart city requirements.

3.1. DSRC and IEEE 802.11p

Dedicated Short-Range Communications (DSRC) was the first technology standardized specifically for vehicular networking. It is based on the IEEE 802.11p amendment (part of the Wireless Access in Vehicular Environments, WAVE, protocol suite) and operates in the 5.850–5.925 GHz band reserved for ITS applications (Khan et al., 2020). DSRC can be viewed as a specialized Wi-Fi variant optimized for low latency and high speeds: it uses 10 MHz radio channels and forgoes the need for connection handshaking, allowing vehicles to broadcast messages to any nearby nodes without prior coordination. In the US, a WAVE protocol stack (IEEE 1609.x family) has been defined as 802.11p, including standards for security (IEEE 1609.2 uses PKI certificates for message signing) and messaging (SAE J2735 defines standard vehicular safety messages). DSRC supports direct V2V and V2I communication with a typical range of a few hundred meters and data rates around 6–27 Mbps per channel. Its primary advantage is very low latency for broadcast transmissions, safety messages (e.g., emergency brake warnings) can be delivered in the order of milliseconds because DSRC uses a decentralized channel access (carrier-sense multiple access, CSMA) with no scheduling overhead. Field trials and pilot deployments have demonstrated that DSRC can effectively enable applications like forward collision warnings and intersection collision avoidance under moderate traffic conditions.

Despite its strengths, DSRC faces performance limitations in dense urban scenarios. Because it relies on CSMA (listen-before-talk), a surge in the number of vehicles broadcasting in proximity can lead to packet collisions and channel congestion, causing reliability to degrade at high vehicle densities (Bhover et al., 2017; Paranjothi et al., 2020). Researchers have proposed various congestion control algorithms such as adaptive message transmission rates or dynamic power control to mitigate this issue (Paranjothi et al., 2020). Another limitation is the communication range and reliability in non-line-of-sight situations: 5.9 GHz radio signals can be easily blocked by buildings or large vehicles, resulting in communication blind spots. Efforts are underway to enhance the 802.11p standard; for instance, IEEE 802.11bd (sometimes called Next-Gen V2X) aims to improve throughput and reliability by incorporating modern physical layer techniques (like MIMO antennas and improved channel coding) while maintaining backward compatibility with 802.11p. Early evaluations indicate that these enhancements could significantly boost data rates and link robustness, narrowing the performance gap between DSRC and newer cellular V2X in some scenarios.

DSRC has seen real-world experimentation in various regions. Notably, the United States Department of Transportation sponsored *Connected Vehicle Pilot* programs in cities like New York (installing DSRC units on thousands of city vehicles and infrastructure) to validate safety applications, and Japan deployed a DSRC-based safety system called ITS Connect for warnings at intersections. Europe's *ITS-G5* standard is essentially equivalent to DSRC and has been part of several cooperative ITS testbeds. Nonetheless, the landscape for DSRC has shifted in recent years. In the US, regulatory changes by the Federal Communications Commission (FCC) in 2020 dramatically curtailed the spectrum available for DSRC, reallocating a majority of the 5.9 GHz band to unlicensed Wi-Fi use and designating only 30 MHz for vehicular communications specifically favoring C-V2X technology in that remaining band(Canis, 2019). This decision, effectively phasing out DSRC in the U.S., introduced uncertainty about DSRC's long-term role. While some regions remain committed to 802.11p-based deployments, the global momentum has largely swung toward cellular-based V2X approaches as described next.

3.2. Cellular V2X (LTE-V2X and 5G V2X)

Cellular Vehicle-to-Everything (C-V2X) refers to V2X communication technology developed under the 3GPP cellular standards. Unlike DSRC's purely ad-hoc networking, C-V2X leverages cellular communication principles and can operate in both direct and network-mediated modes. The initial version, often called LTE-V2X (from 3GPP Release 14), introduced a sidelink mode where vehicles communicate directly over the air using cellular channel structures. In this LTE-V2V mode, vehicles can autonomously select time-frequency resources for broadcast (mode 4, which is designed for when cellular coverage is not present) or have resource scheduling assistance from a cellular base station (mode 3, when under coverage). LTE-V2X was shown to achieve better reliability and range than 802.11p in many high-density scenarios, thanks to its use of semi-persistent scheduling and more robust modulation/coding schemes(Khan et al., 2020). For example, studies found that LTE-based V2V could successfully deliver safety messages at greater distances and with fewer packet losses under heavy load compared to DSRC, particularly in highway convoy situations.

The evolution to 5G NR V2X (3GPP Releases 16 and 17) brings further enhancements tailored for advanced vehicular use cases. 5G V2X can utilize wide bandwidth (even mmWave frequencies for extremely high data rates over short ranges) and offers flexible numerology to reduce latency. It is designed to support the stringent requirements of autonomous driving: ultra-reliable low-latency communication (URLLC) for mission-critical messages, high throughput for sharing rich sensor data or video feeds between vehicles, and massive device connectivity for dense networks. Scenarios such as cooperative perception (vehicles exchanging raw sensor data like camera or LiDAR feeds to collectively sense obstacles) or remote driving (teleoperation of vehicles) become feasible with 5G's capabilities. Early trials of 5G V2X have demonstrated promising results, such as streaming high-definition video from vehicles to nearby units with minimal delay and coordinating platoons of vehicles with sub-10 ms reaction times. In addition, 5G's architecture allows integration with cloud and edge computing through features like *network slicing* and *edge computing*, as mentioned. Operators can dedicate a slice of the 5G network for automotive services to guarantee bandwidth and latency even when the cellular network is busy with other users(Khan et al., 2020). Meanwhile, by deploying edge servers near cell sites or RSUs, applications like hazard signal processing or path planning assistance can run close to the vehicles, minimizing round-trip delay.

A key advantage of cellular-based approaches in a smart city is the unified connectivity they offer: the same radio interface (5G) can handle both the short-range direct V2V messages and long-range V2N communications. Vehicles can receive infotainment data, map updates, or cloud-computed driving recommendations over the cellular network, while simultaneously using sidelink to alert nearby cars of immediate dangers. This hybrid connectivity broadens the scope of VANET applications beyond what isolated DSRC links could do. It also means that telecom operators and city infrastructures become important stakeholders in the vehicular network ecosystem, which has implications for business models and deployment (e.g., cities might partner with mobile operators to build roadside 5G infrastructure that supports both public use and dedicated automotive services).

3.3. Short-Range and Hybrid Communication

While DSRC and C-V2X are the primary dedicated V2X technologies, it is worth noting that vehicles may also utilize other wireless interfaces in a smart city setting. Standard Wi-Fi, Bluetooth, or emerging protocols like IEEE 802.11p/OCB (outside the context of WAVE) can support non-safety applications (for instance, connecting to roadside hotspots for software updates or using Bluetooth for pedestrian detection via smartphones). Some research has considered *hybrid networks* where vehicles switch between DSRC and cellular or use multiple radios to achieve better coverage and reliability. In practice, many modern vehicles are likely to be equipped with cellular modems (for telematics or passenger connectivity) alongside any V2X-specific radios, so multi-homed communication strategies are possible. The challenge is to manage these interfaces seamlessly, an area where software-defined networking and intelligent transport protocols might play a role.

In summary, communication technology for VANETs in smart cities is at a transitional stage. DSRC laid the groundwork and proved the viability of V2X safety communication, but its limitations and the changing regulatory climate have led to a strong industry push for cellular-based 5G V2X as the future-proof solution. The *coexistence or replacement* of DSRC by C-V2X is being handled differently across regions through policy (discussed later). For city planners, the takeaway is that communication infrastructure must be adaptable: a blend of V2X technologies might be needed to cover diverse urban scenarios, and flexibility to upgrade to newer standards (like 5G and beyond) should be built into any long-term smart city transportation strategy.

4. Vehicular Sensing and Data in Smart Cities

One of the defining features of IoT-enabled smart cities is the pervasive presence of sensors and data collection devices throughout the urban environment. Vehicles themselves are prominent moving sensors in this landscape. A modern connected car can have dozens of sensors: cameras providing visual data, radar and LiDAR scanning the vehicle’s surroundings, GPS providing location, accelerometers and gyroscopes measuring motion, and numerous other sensors monitoring the vehicle’s internal status (engine, fuel, battery, etc.) and external conditions (temperature, weather). When connected via VANET, these sensing capabilities transform vehicles into *mobile sensing nodes* for the city, complementing static sensors like traffic cameras or air quality stations. The concept of *Vehicular Sensor Networks* refers to leveraging the collective sensing power of vehicles to gather and share data about road and environmental conditions in real-time.

- **Urban Sensing Applications:** Connected vehicles can contribute to a variety of urban monitoring tasks. For instance, vehicles can detect road hazards or surface degradation (by analyzing vibrations from the suspension or camera imagery of potholes) and report this information for road maintenance scheduling(Dutta et al., 2024). They can measure traffic flow and congestion in real-time by reporting their speed and location, effectively crowdsourcing traffic state information to city authorities or to other drivers (via V2V/V2I messages). Vehicles equipped with pollution sensors (or even just using engine performance data and location) have been used to map air quality and emissions hot spots around a city. In winter conditions, cars with anti-lock braking events or traction control triggers can indicate icy road segments to following vehicles. All these examples illustrate the “*vehicle as a sensor*” paradigm that significantly enhances a smart city’s situational awareness. To facilitate these applications, data from vehicles typically needs to be aggregated and processed. This is where the IoT architecture’s *processing layer* comes into play. RSUs or cellular base stations can act as data collectors, forwarding information from vehicles to edge servers or cloud platforms. In many designs, a *publishing-subscribe* model is used: vehicles publish data (like location, speed, sensor readings) to certain topics, and subscribers (which could be traffic management systems, other vehicles, or third-party service providers) receive relevant updates. Standard message formats (such as DATEX II in Europe for traffic info, or various SAE J2735 messages in the US for V2X communication) are employed to ensure interoperability.

- **Edge Computing and Data Analytics:** Given the sheer volume of data that a fleet of connected vehicles can generate, *edge computing* is often necessary to handle time-sensitive processing. For instance, consider a scenario where multiple vehicles approaching an intersection share camera feeds to detect a pedestrian hidden from view. Instead of sending all raw video to a cloud server (which would incur latency and bandwidth costs), an edge node at the intersection could quickly fuse the inputs, detect the pedestrian, and notify the vehicles to trigger a timely driver alert or autonomous brake. This local processing aligns with the idea of *multi-access edge computing (MEC)* in 5G networks, and many pilot projects in smart cities are deploying edge units for exactly such purposes. Additionally, AI and machine learning algorithms are being deployed at the edge or in cloud back-ends to extract insights from vehicular data for example, predicting traffic congestion ahead based on real-time trends, or identifying dangerous driving patterns (hard braking incidents clustering in a certain area might indicate a problematic intersection design).

- **Data Interoperability and Standards:** For a city-wide vehicular sensor network to function, standardisation of data formats and sharing protocols is crucial. Efforts like the Sensor Data Sharing (SDS) interface in ETSI's ITS standards, or the CVRIA (Connected Vehicle Reference Implementation Architecture) in the US, provide frameworks for data exchange among vehicles and infrastructure. Interoperability ensures that vehicles from different manufacturers and infrastructure from different vendors can all communicate. Many cities are also adopting *open data platforms* where collected transportation data is made available (with appropriate privacy protections) to developers and the public, spurring innovation in traffic apps and services. These measures ensure that data-driven mobility services can grow without compromising citizens' privacy or trust.

- **Privacy Considerations:** Vehicular sensing raises privacy concerns, as vehicles can potentially capture sensitive information (faces on dashcam video, or simply track a vehicle's movements which correlates to the driver's personal habits). Data from vehicles often needs to be anonymized or aggregated to protect individual privacy. Policies like the EU's General Data Protection Regulation (GDPR) apply to vehicular data in smart cities for instance, personal data (even something like a car's identifier or its precise trajectory) should be handled in compliance with privacy laws, requiring user consent or proper anonymization techniques. In practice, this might mean that vehicles use pseudonymous IDs when broadcasting data and that any data stored long-term in city databases is stripped of direct identifiers.

In summary, vehicular sensing greatly enriches the smart city's data pool, enabling more responsive and informed city management. It turns the traffic flow itself into a distributed sensor network. The challenges lie in handling the data deluge (through edge computing and smart analytics), ensuring data quality and consistency (through calibration and standards), and upholding privacy/security. When done right, the combination of VANET connectivity and IoT data analytics can lead to significant improvements in how cities monitor and respond to transportation conditions in real-time.

5. Localisation Techniques for Vehicular Networks

Accurate vehicle positioning is a foundational requirement for many VANET and smart city applications, from basic safety (knowing if a nearby alert refers to your lane or the opposite direction) to advanced autonomous navigation. In open highway settings, standard *Global Navigation Satellite*

Systems (GNSS) like GPS, GLONASS, or Galileo can often provide position estimates with 3–5 meters accuracy. However, urban environments pose special challenges to localisation: signals from GPS satellites can be blocked or reflected by tall buildings (the *urban canyon* effect), causing degraded accuracy or even complete outages in downtown cores. Additionally, certain V2X applications (e.g., cooperative driving or platooning) may demand sub-meter accuracy and high update rates that raw GNSS cannot consistently achieve in cities.

- **GNSS Augmentations:** A common approach to improving GPS accuracy is to use augmentation techniques. *Differential GPS (DGPS)* and real-time kinematic (RTK) positioning employ reference stations at known locations that broadcast correction signals to vehicles, allowing them to compensate for satellite signal errors and achieve decimeter-level accuracy. Many modern cars also use *multi-constellation GNSS* receivers (accessing not just GPS but European Galileo, Chinese BeiDou, etc.) and multi-frequency receivers, which improve the chance of getting a fix even with some satellites obstructed and can help cancel certain errors. Automotive manufacturers are increasingly integrating high-precision GNSS for applications like automated parking and highway autopilot but maintaining that precision in a dense city grid is still problematic if the view of the sky is highly restricted.

- **Sensor Fusion:** To combat the unreliability of GNSS in urban conditions, vehicles rely on *sensor fusion* for localisation. This means combining GNSS data with inputs from *inertial measurement units (IMU)*, wheel speed sensors, and even cameras or LiDAR-based *simultaneous localisation and mapping (SLAM)*. For example, when GPS signals fade, an IMU can perform dead reckoning of the vehicle's position for short periods (though drift error grows over time). Wheel sensors and steering angle can inform how far and in what direction the vehicle has moved since the last reliable GPS reading. If the vehicle is equipped with a camera or LiDAR, it might recognize landmarks or match detected features to a known map (a technique used by autonomous vehicles to localize with respect to a detailed prior map of the environment). V2X communication can assist here as well: vehicles can share their positions and possibly use *relative ranging* (with radar or ultra-wideband radio) to determine distances between neighboring vehicles, thereby improving each other's relative positioning.

- **Cooperative Localisation:** In an IoT-enhanced city, cooperative approaches can significantly bolster localisation. Roadside units or smart infrastructure can act as anchors – for instance, a smart traffic light might periodically broadcast its own precise coordinates; vehicles receiving these signals can calibrate their GNSS position if they know the geometry. Alternatively, vehicles can form ad-hoc networks exchanging position information and even raw sensor data to help each other detect discrepancies. If one vehicle has a strong GPS fix and shares it, nearby vehicles that temporarily lost signal might adjust their estimated position accordingly (assuming they can measure relative distance or angle to the first vehicle via V2V ranging). This collaborative method can reduce the overall localisation error across the network of vehicles.

Another technique is *map-matching*, which is inherently cooperative with an external data source (the digital map of the city). Vehicles may have coarse GPS data, but by knowing they must be on a drivable road, they can snap their position to the road network (using algorithms that infer which road segment and lane the vehicle is likely in, given the erroneous GPS reading and possibly recent trajectory). Many navigation systems already do this to prevent the displayed position from jumping off the road on the map when GPS errors occur.

- **High-Definition Maps and Infrastructure Aids:** As we move toward autonomous driving, the need for localisation goes beyond just latitude/longitude vehicles need to know which lane they are in and their position within that lane. *High-definition (HD) maps* provide detailed information about road geometry, lane markings, and fixed reference points. If a vehicle can detect a particular landmark (say a specific traffic sign or a unique building corner) and that landmark is coded in the HD map with known coordinates, the vehicle can correct its position estimate. Some cities are also exploring infrastructure support like radio beacons or positioning systems using cellular signals (e.g., using 5G signal time-of-flight measurements to triangulate positions). These can supplement GNSS. For example, 5G networks with *observed time difference of arrival (OTDOA)* techniques could theoretically localize devices if multiple cell towers' signals are in reach, though urban multipath makes it tricky.

- **Resilience to Spoofing and Errors:** With increased reliance on satellite navigation, the vulnerability of GNSS to spoofing or jamming is a security concern. Attackers could broadcast counterfeit GPS signals (so-called *GPS spoofing*) to mislead vehicles about their location. Researchers and standards are considering protections such as cryptographic authentication of navigation signals in future GNSS, or cross-verification using multi-sensor consistency checks (Alalwany & Mahgoub, 2024). For example, if GPS says the car is at a certain coordinate but the on-board camera recognizes a landmark that should be five blocks away, the vehicle can flag a discrepancy. In VANET contexts, vehicles can also compare notes: if one car's reported position jumps inconsistently relative to others, it could indicate a faulty or malicious signal influencing that car.

In conclusion, achieving accurate localisation in smart city VANETs is a multi-faceted problem. A combination of high-quality GNSS, augmentation services, on-board sensor fusion, cooperative techniques, and map intelligence is used to reach the accuracy and reliability needed. Continued improvements in this area are expected as part of future 5G/6G standards (which include positioning enhancements) and as cities invest in infrastructure that supports vehicle positioning (like differential GNSS networks or smart beacons). Reliable localisation not only underpins safety applications but also enables future innovations like fee-based road pricing by location, location-specific traffic rules, and highly automated driving in urban settings.

6. Security Challenges and Solutions

Security and privacy are critical concerns in VANETs, given that compromised vehicular communications can have immediate physical consequences. In the context of IoT-connected smart cities, the stakes are even higher: a security breach could affect not just one vehicle but potentially an entire network of vehicles or the infrastructure coordination, leading to accidents or widespread disruption. This section outlines the major security challenges facing VANETs and IoT-integrated vehicles and discusses the emerging solutions and frameworks to address them.

Threat Landscape: Vehicles in a VANET exchange a variety of messages (safety beacons, cooperative awareness messages, traffic warnings, etc.), and attackers may attempt to exploit this openness. Some well-known threats include:

- **Message Spoofing:** An attacker injects false messages into the network for example, broadcasting a fake warning about a collision or road hazard that does not exist, causing other drivers to take unnecessary actions. Spoofed messages could also be used in a coordinated way to reroute traffic (imagine a fake congestion report causing many vehicles to divert to an alternate route for the attacker's benefit).

- **Sybil Attack:** Here, one malicious entity pretends to be multiple vehicles by using different fake identities, sending multiple messages from different source addresses. This could overwhelm the network or create a false sense of a traffic situation (e.g., spoofing a traffic jam by simulating many slow vehicles).

- **Denial of Service (DoS):** An attacker might flood the V2X channel with junk data or deliberately jam the wireless frequencies to disrupt communication. Given the safety-critical nature of some VANET messages, jamming could prevent hazard warnings from propagating. Congestion-based DoS can also occur unintentionally if the network is not properly managed under high load (hence the need for congestion control protocols).

- **Wormhole Attack:** Two colluding attackers could create a tunnel between two separate areas of the network, passing along packets out of band to replay them in a different location. This can make vehicles believe that distant events are happening nearby, causing confusion in the network's topology understanding.

- **GPS Spoofing:** As mentioned earlier, misleading a vehicle about its location/time by spoofing GNSS signals can lead to navigation errors or manipulation of location-based applications. In a coordinated attack, multiple vehicles could be misguided off their intended routes or into unsafe conditions.

- **Eavesdropping and Privacy Breach:** Because VANET messages often contain information about a vehicle's position and motion, an eavesdropper can passively listen to communications and track individual vehicles, potentially identifying drivers' home/work routines or other personal information. This is a privacy violation and could also be the precursor to more targeted attacks.

- **Malicious Insider:** This refers to a legitimate participant in the network (say, an authenticated vehicle or even an infrastructure node) that behaves maliciously, for example, a hacked car that intentionally sends wrong data (perhaps it has been infected with malware) despite possessing valid credentials. These are particularly challenging because they can bypass certain authentication measures and may only be caught through behavior that deviates from norms.

These threats are not merely theoretical. In recent years, researchers have demonstrated various attacks on connected car systems and V2X testbeds, highlighting the importance of incorporating strong security measures from the design phase of VANET systems (Alalwany & Mahgoub, 2024; Garg et al., 2020).

Security Mechanisms: To counter the above threats, the VANET research and standards communities have developed a range of solutions:

- **Authentication and Integrity:** Ensuring that a message truly originates from a legitimate source and has not been tampered with is crucial. VANETs commonly employ a ***Public Key Infrastructure (PKI)*** with digital signatures for messages. Each vehicle is issued a set of cryptographic key pairs and certificates (often called *pseudonym certificates* since vehicles use temporary identities). When a vehicle broadcasts a safety message, it signs the message with its private key; receivers can verify the signature using the sender's public key certificate, which is issued by a trusted Certificate Authority (CA). This prevents unauthorized entities from injecting messages (as their signatures would fail verification) and provides integrity protection. The IEEE 1609.2 standard and the European counterpart (ETSI TS 102 941) define how this vehicular PKI operates. To protect privacy, vehicles periodically change their pseudonyms (and corresponding keys) so that an eavesdropper cannot easily link messages over a long period to the same vehicle.

- **Trust and Reputation Management:** Even with authentication, a node might be compromised and send false data. Trust management frameworks are proposed where vehicles and infrastructure maintain reputations for other nodes. If a car frequently sends information that contradicts others or is later proven false, its trust score can be lowered, and its messages might be ignored or given less weight by receivers. Some systems envision an authority that can *evict* a bad actor by adding its certificate to a revocation list (e.g., the Security Credential Management System or SCMS in the US V2X framework provides certificate revocation).

- **Intrusion Detection Systems (IDS):** These can be on board each vehicle or distributed in the network. An IDS monitors the data traffic and node behaviors to detect anomalies that might indicate an attack. For example, if a normally smooth speed profile suddenly has a vehicle broadcasting oscillating speeds or positions that don't physically make sense, an IDS could flag that. Machine learning techniques are being developed to improve anomaly detection in VANETs, given the complexity of differentiating between unusual but legitimate events and actual attacks(Alalwany & Mahgoub, 2024).

- **Secure Localisation and Timing:** To combat GPS spoofing and wormholes, techniques like *time-of-flight verification* and *consistency checks* are used. Vehicles can compare the timing of signals (if something arrives "too quickly" to be plausible given known physics, it might be a wormhole retransmission). They can also cross-verify location information with multiple sources, e.g., using map data or nearby RSU signals as mentioned in the localisation section. Additionally, emerging approaches propose cryptographic protection of GNSS signals themselves (the Galileo system, for instance, has planned authentication for its navigation messages to make spoofing harder).

- **Privacy Preservation:** Beyond pseudonym changes, other measures like ***mixing zones*** have been suggested. A mix zone is an area (say around an intersection) where vehicles temporarily stop broadcasting identifiable information; if many vehicles intermix in that zone and then emerge with new pseudonyms, an outside observer loses track of which outgoing vehicle corresponds to which incoming vehicle. Dummy traffic generation is another concept vehicles could occasionally inject additional fake packets or delay certain transmissions to confuse tracking attempts, though this must be balanced against network load and safety requirements. Privacy regulations will likely mandate some of these protections as connected cars become mainstream.

- **Physical Layer Security and Resilience:** Spread spectrum techniques and frequency hopping can be employed to make jamming more difficult. The European ITS stack, for example, has a decentralized congestion control (DCC) mechanism that can adjust communication parameters to maintain reliability under different channel load conditions. If jamming is detected on one channel, vehicles and infrastructure could switch to alternative communication channels (e.g., use cellular links if the DSRC channel is jammed) building redundancy into the system.

Securing vehicular networks is an ongoing endeavor, especially as the system expands and connects with more of the IoT infrastructure. Importantly, security solutions themselves introduce complexity and cost: the PKI requires a whole backend infrastructure of certificate authorities and secure credential distribution; regular pseudonym changes require synchronization to avoid confusion; and heavy cryptography or communication overhead must be minimized to maintain real-time performance. Nonetheless, significant progress has been made in standardizing these mechanisms, and current pilot deployments of connected vehicles include security credential management systems as integral components (Garg et al, 2020).

From a *policy standpoint*, governments and regulatory bodies have a role in mandating security requirements for connected vehicles. For instance, some regions might require that any V2X device be certified for security (ensuring it properly implements cryptographic protocols and is tamper-resistant). Cybersecurity guidelines for vehicles (such as the UNECE WP.29 regulation on cybersecurity and software updates for vehicles, adopted in 2021, and ISO/SAE 21434 standard for automotive cybersecurity engineering) are becoming part of the legal landscape, which should push automakers to build strong security into all connected vehicle systems sold. In the broader IoT smart city context, the vehicular network cannot be a weak link; it must be protected as well as or better than other critical infrastructure, given the direct safety implications.

7. Economic Implications of VANET and IoT Deployment

The deployment of VANETs in smart cities is not only a technological endeavor but also an economic one. Decision-makers must consider costs, benefits, funding models, and the broader economic impact of connecting vehicles and infrastructure. In this section, we discuss the economic implications of VANET–IoT systems, including both the potential positive impacts (benefits, savings, new opportunities) and the costs and challenges from an economic perspective.

7.1. Economic Benefits and Value Creation

The promise of VANETs in smart cities carries substantial economic benefits across multiple dimensions:

- **Improved Road Safety – Cost Savings:** Traffic accidents impose a huge economic burden globally, including medical costs, property damage, lost productivity, and more. The World Health Organization estimates that road traffic crashes cost countries around **3% of their GDP** on average. In the aggregate, crash injuries worldwide amount to trillions of dollars in losses each year. By enabling collision avoidance and reducing accident frequency and severity, vehicular communication technologies can save a significant portion of these costs. For instance, if connected vehicle systems even partially achieve their full potential, they could prevent hundreds of thousands of crashes annually. The U.S. National Highway Traffic Safety Administration (NHTSA) projected that ***V2V and V2I safety applications, when fully deployed, might eliminate or mitigate up to 80% of crashes involving non-impaired drivers*** **(NHTSA, 2016)**. Such a dramatic reduction in accidents would translate into enormous economic savings in healthcare, emergency services, insurance payouts, and human lives (valued in economic analyses via the value of statistical life). Safer roads also mean less congestion from crash incidents and a more efficient flow of goods and people, contributing to productivity.

- **Traffic Efficiency – Productivity Gains:** Urban congestion is another source of economic loss. Time spent by commuters and freight traffic in congestion results in lost work hours and increased fuel consumption. By some estimates, congestion costs in major cities reach billions of dollars per year in wasted time and fuel. VANETs can alleviate congestion through better traffic management and vehicle routes. For example, adaptive traffic signals that use connected vehicle data can reduce idle times at intersections; vehicles that receive real-time rerouting information can avoid adding to jams. Even a modest improvement in average travel speeds or reduction in stop-and-go conditions translates to economic gains when scaled across a city's population (commuters arriving sooner, trucks delivering goods faster, etc.). Additionally, smoother traffic flow saves fuel and reduces vehicle wear-and-tear, which has economic and environmental benefits.

- **Fuel Efficiency and Environmental Benefits:** Cooperative driving strategies like platooning (enabled by V2V communication) can improve fuel efficiency by reducing aerodynamic drag. Similarly, avoiding unnecessary acceleration and breaking in synchronized traffic can lower fuel consumption. With the rising cost of energy and the push for lower emissions, these efficiencies have economic value for both individual drivers (fuel cost savings) and society (lower pollution-related health costs, better compliance with climate goals). Some VANET applications, like eco-driving assistance, explicitly aim to minimize fuel use by advising drivers of optimal speeds or by connecting vehicles to traffic light timing information so they can avoid idling.

- **Increased Urban Mobility and Economic Activity:** A well-functioning transportation network is an enabler of economic activity. If VANETs and smart traffic systems reduce travel uncertainty and make commuting more reliable, they expand the effective labor market (people can reach jobs over a wider area within a reasonable time) and improve access to services. Businesses can operate more efficiently with reliable logistics. Ultimately, enhanced mobility can contribute to higher productivity and economic growth in the city. Studies on smart city initiatives suggest they can ***stimulate local economic development*** by making the city more attractive to investors and reducing operational costs.

- **Emergence of New Markets and Services:** The advent of connected vehicles creates new business opportunities and markets. For example, data collected from vehicles (if appropriately anonymized and shared) can fuel a host of services: traffic analytics, navigation and mapping services, location-based advertising, insurance models based on driving behavior, etc. Automotive manufacturers and tech companies are investing in V2X-enabled services from safety subscriptions to infotainment delivered via car Wi-Fi. Smart cities might monetize certain infrastructure data or partner with companies to provide mobility services (such as connected parking systems that guide drivers to available parking spots for a fee). The overall ***smart city technology market*** is projected to be very large, with estimates in the trillions of dollars by mid-decade, and transportation is a major component of that (Deniz, 2025). Entrepreneurship is likely to be spurred by the availability of an open urban platform of connected vehicles and sensors. For instance, creative mobile apps could integrate with city traffic APIs and vehicle data to offer innovative ridesharing, delivery optimization, or travel experience services. This entrepreneurial activity can lead to job creation in the tech and services sectors.

- **Long-Term Societal Benefits:** While harder to quantify, improved safety and mobility contribute to quality of life, which can attract talent and businesses to a city (economic competitiveness). There are also savings in healthcare costs from fewer traffic injuries, and potentially even secondary benefits like increased property values in areas with less traffic or noise due to smarter routing of vehicles.

We apply a standard cost–benefit analysis (CBA) framework covering capital expenditures (CAPEX) for RSU/MEC deployment and integration with the traffic management center, and operating expenditures (OPEX) for maintenance, connectivity, and cybersecurity. Benefits are monetized from three primary sources: (I) reductions in crash frequency and severity, (II) travel time and fuel savings from improved traffic flow, and (III) broader urban productivity effects enabled by more reliable mobility. We compute the benefit–cost ratio (BCR) under alternative V2X penetration rates (e.g., 10%, 30%, 60%). Results indicate a non-linear rise in BCR with penetration due to network externalities: while safety alerts deliver partial benefits at low penetration, the full value of cooperative traffic management materializes after a critical threshold. These findings support targeted public–private risk sharing and early-phase incentives to overcome upfront costs and coordination frictions.

7.2. Costs and Economic Challenges

On the other side of the ledger, deploying VANET and IoT infrastructure requires substantial investment and faces economic hurdles:

- **Infrastructure Investment Cost:** Setting up a connected vehicle ecosystem city-wide involves costs for roadside units (RSUs) at intersections or along highways, communication backhaul networks to connect those RSUs to data centers or cloud systems, installation of edge computing nodes, and integration with existing traffic control systems. There is also the cost of upgrading vehicles with V2X equipment; while new vehicles can be manufactured with the technology relatively inexpensively when scaled, retrofitting older vehicles is costly and often impractical. Cities must consider who bears the cost of RSU deployment: government agencies, private road operators, or partnerships with telecom providers (in the case of cellular V2X, mobile network operators might share some infrastructure responsibilities). These upfront costs can be a barrier, especially since many benefits (like safety) are diffuse and realized over time rather than directly monetizable by the deploying entity.

- **Uncertain Adoption and Network Effects:** The value of many V2X applications depends on the **penetration rate** of the technology in the vehicle fleet. For example, if only 5% of cars are connected, the probability that two connected cars encounter each other to benefit from V2V warnings is low, and traffic systems will still largely rely on conventional detection methods. This creates a classic ***chicken-and-egg*** problem or network externality issue. Automakers may hesitate to include V2X features if there is insufficient infrastructure to use them, while governments may be reluctant to invest heavily in infrastructure if few cars can take advantage of it. Early adopters don’t gain the full benefit until others also adopt. This uncertainty can slow down the deployment timeline and complicate the economic justification (benefit-cost analysis) for initial investments. Overcoming this requires coordination and possibly subsidy or mandate, which moves into the policy realm (see Section 8).

- **Maintenance and Operation Costs:** Beyond installation, there are ongoing costs to maintain the system keeping the hardware and communication links operational, updating software to patch security vulnerabilities, and managing the data. Cybersecurity can introduce ongoing expenses, as the system will need monitoring for intrusions and maybe periodic certificate updates for vehicles. Cities might need to expand their IT departments or hire contractors to manage the new smart transportation network. Budgeting for these recurring costs is essential; otherwise, infrastructure could fall into disrepair, negating the benefits.

- **Equity and Accessibility Concerns:** From a societal economic perspective, one must consider how the benefits and costs are distributed. There's a risk that high-tech transportation improvements primarily benefit those who can afford newer vehicles or live in well-equipped areas, while others are left behind. Policymakers may need to invest in strategies to ensure that safety improvements and mobility benefits extend to all segments of the population (for instance, considering how to incorporate public transit vehicles, which are often older, into the connected ecosystem, or how pedestrians and cyclists can benefit via smartphone integration). There might be additional costs involved in widening the coverage to include these use cases (like equipping buses and trains or building pedestrian communication systems).

- **Economic Viability and Business Models:** For private-sector stakeholders, there is the question of how to monetize V2X services. Telecom operators see potential revenue in selling connectivity or edge computing services to automotive customers, but they need enough volume and clear models. Automakers might offer connected features as part of a vehicle purchase or subscription, but if consumers don't see immediate value, they may not opt for them. The timeline to profitability can be uncertain, which may reduce private investment enthusiasm. Public-private partnership models are being explored, where government provides some funding or incentive and private companies deploy and operate certain aspects (for example, a city could allow an operator to use street furniture to mount 5G antennas that serve both general mobile users and dedicated V2X, in return for ensuring city corridors are covered with V2X signals).

- **Transition Costs:** During the phase where not all vehicles are connected (which could last decades, given vehicle turnover rates), cities may have to maintain ***legacy systems*** (like traditional traffic signals and signage) in parallel with new connected systems. This redundancy ensures that non-connected road users are still served, but it means extra cost and complexity. As automated and connected vehicles gradually mix with human-driven, unconnected vehicles, traffic systems might not realize full efficiency gains until a critical mass is reached.

Despite these challenges, economic analyses of smart transportation initiatives generally indicate positive ***benefit-cost ratios*** in the long run, particularly when safety benefits are given a monetary value (using standard metrics, the value of preventing a single traffic fatality is very high, thus safety improvements can justify large investments). A study or pilot might show, for example, that investing in a connected vehicle system yields a return in reduced accident costs and travel time savings that is several times the initial investment over a period of years. However, financing that initial investment remains a key issue. Some governments have provided grants or stimulus funding for pilot deployments (as the U.S. DOT did for the pilot programs), and more recently, initiatives in Europe and Asia have seen government-industry coalitions sharing costs.

Furthermore, ***indirect economic benefits*** often strengthen the case: smarter traffic management reduces pollution and noise, which can improve public health and reduce related costs; better mobility can boost tourism (visitors appreciate easier navigation and less congestion); and high-tech infrastructure can attract companies and talent interested in being part of a modern urban ecosystem (as seen in cities that market themselves as “living labs” for autonomous vehicle testing, for instance).

In conclusion, the economic implications of VANETs and IoT in smart cities are broadly favorable the technology can drive substantial cost savings and productivity gains, and it opens avenues for innovation and commerce. But careful planning is needed to manage the upfront costs and ensure equitable outcomes. Policymakers must craft strategies (incentives, regulations, partnerships) that align the costs with those who reap the benefits. Section 8 will delve into policies that can help realize these economic potentials, such as regulatory mandates to accelerate adoption, and standards that prevent fragmentation which could raise costs.

8. Policy Implications and Recommendations

The widespread implementation of VANET and IoT technologies in smart cities does not happen in a vacuum; it is strongly influenced by public policy, regulations, and institutional decisions. Governments at local, national, and international levels play a role in setting the rules of the road (literally and figuratively) for connected vehicles. In this section, we discuss several key policy implications and considerations that arise from VANET–IoT integration, including standardisation and spectrum policy, mandates and regulations to encourage adoption, privacy and data governance, and cross-sector collaboration.

Table 1. Policy matrix EU/US/China

Jurisdiction	Standards / Spectrum	Regulatory stance	Implementation notes
United States	5.9 GHz reallocation toward C-V2X	Post-2020 decisions favor C-V2X in the remaining band	DSRC legacy reduced; clearer runway for C-V2X
European Union	ITS-G5 legacy; technology-neutral evolution	Emphasis on coexistence/interoperability	Openness to C-V2X alongside ITS-G5 deployments
China	Early, coordinated C-V2X orientation	Strong national adoption targets	State-led acceleration of fit-out and trials

In an urban corridor comprising six signalized intersections equipped with RSUs and MEC nodes, we evaluate three V2X penetration scenarios (10%, 30%, 60%). Under medium and high penetration, the combined safety and efficiency gains yield a benefit–cost ratio (BCR) greater than one over a 10-year horizon, whereas the low-penetration scenario remains sensitive to network externalities and likely requires catalytic policy instruments (e.g., public fleet retrofits, investment tax credits, or partial mandates). These estimates are consistent with our overarching argument that safety and congestion savings are the principal value drivers of VANET–IoT, while early-stage public–private coordination is critical to de-risk deployment.

8.1. Technology Standardisation and Spectrum Policy

One of the foremost policy issues has been the choice of communication standards and management of the radio spectrum for V2X. Regulators must decide how to allocate frequencies for vehicular communications and whether to favor a particular technology. As described earlier, there has been a divergence: historically, many countries reserved the 5.9 GHz band for DSRC-based technology, but more recently, the trend is towards allowing Cellular V2X (C-V2X) in that band. In the United States, the Federal Communications Commission (FCC) made a landmark decision in 2020 to reallocate the majority of the 5.9 GHz ITS band away from DSRC to other uses, and to permit only C-V2X operation in the remaining portion. This effectively signaled a policy shift to phase out DSRC in favor of newer technology. While this could accelerate modern C-V2X deployment (by providing clarity and channel access), it also meant stranding years of DSRC development and some existing deployments, illustrating how policy can rapidly change the landscape.

In contrast, Europe initially backed the ITS-G5 (DSRC) standard and even came close to an EU-wide mandate but faced pushback that such a move would exclude C-V2X. As a result, Europe has taken a more technology-neutral stance recently, allowing market-driven adoption but ensuring interoperability testing and coexistence. China has strongly supported C-V2X from the start and is moving towards equipping new vehicles with that capability. These varying approaches show that global harmonization of V2X standards is a challenge; however, efforts by international bodies (e.g., the UN’s World Forum for Harmonization of Vehicle Regulations) and industry alliances like the 5G Automotive Association (5GAA) aim to eventually achieve compatibility or convergence.

For policymakers, a key consideration is how to avoid fragmentation that could impede the benefits of scale. If different cities or countries use incompatible systems, vehicles crossing borders or even traveling between cities might not communicate properly. Thus, regional or international coordination on standards is beneficial. Policymakers also need to ensure sufficient spectrum is available for V2X as the number of devices grows. The 5.9 GHz band alone might become congested in the future with ubiquitous connected vehicles, so alternative spectrum (including mmWave for high bandwidth sharing of sensor data or using cellular bands dynamically) is an area of regulatory interest. Some regulators are exploring spectrum sharing frameworks where vehicular communications share frequencies with other services under controlled conditions to maximize efficient use of the airwaves.

8.2. Mandates and Incentives for Adoption

As discussed in the economic section, the adoption of VANET technology in vehicles and on roads can be accelerated through policy measures. One approach is a *regulatory mandate*: for example, requiring that all new vehicles sold after a certain date include certified V2X communication capability. In fact, the NHTSA in the US proposed a rule in 2016/2017 that would have mandated DSRC-based V2V on new light vehicles, citing the safety benefits (though the rule was not finalized and later stalled). Some policymakers, both in the US and EU, continue to consider mandates, possibly technology-neutral ones (i.e., requiring V2X but not specifying DSRC vs C-V2X). According to some reports, regulatory authorities in multiple countries are planning or discussing timelines to require V2X in new vehicles. China has indicated goals for a high percentage of new cars to have C-V2X by mid-2020s as part of its national strategy.

Mandates can rapidly increase penetration, solving the network effect issue. However, they also raise questions: is technology mature enough to mandate? Which standard to require? How to handle older vehicles? Policymakers have to weigh these factors and often mandates come after successful voluntary deployment in pilot projects.

If not a mandate, governments might use *incentives*. For example, they could offer tax breaks or subsidies for vehicles equipped with V2X, or for fleet operators (like trucking companies or public transit agencies) that adopt connected tech early. On the infrastructure side, grants for cities to deploy smart traffic systems can lower the barrier for local governments. Another incentive approach is to incorporate V2X into relevant regulations indirectly – for instance, including V2X capability as part of *vehicle safety ratings* or new car assessment programs. If consumer vehicles that have V2X get higher safety ratings (due to potential crash avoidance), automakers would be motivated to include it in the market for safer cars.

8.3. Privacy and Data Governance

Policy must address who owns and can use the vast data generated by connected vehicles. Location and movement data is highly sensitive. Governments need to set rules on data retention, sharing, and protection. In the EU, for example, GDPR requires that personal data (and precise vehicle location can be personal data) be collected only for legitimate purposes and with consent, and that individuals have rights over that data. This implies that any smart city data platform that aggregates vehicular data needs strong privacy safeguards possibly only storing anonymized, aggregated traffic statistics rather than individual trajectories. There may also be provisions where emergency access to data is allowed (e.g., investigators might want data from vehicles in an accident).

Some jurisdictions are exploring frameworks for *mobility data trusts* or partnerships where private companies (like car manufacturers or navigation service providers) share certain data with city authorities under agreements that protect privacy while allowing the city to use data for planning or real-time operations. Policymakers might also consider whether vehicular data is accessible for public interest uses by default or if companies can hoard it there’s a balance between promoting innovation (open data can spur it) and protecting business interests and privacy.

Security regulations overlap here: ensuring that data transmitted by vehicles is encrypted and that there are standards for cyber resilience can be mandated. For example, the mentioned UNECE WP.29 cybersecurity regulation essentially requires car manufacturers to implement a cybersecurity management system and to secure the vehicle’s communications and data against cyber threats, as a condition for selling vehicles in those regulated markets.

8.4. Infrastructure and Urban Planning Policies

Smart city transportation doesn’t just involve communication tech; it ties into urban planning policies as well. Cities may need to update traffic laws or infrastructure design standards to accommodate connected and automated vehicles. For example, if future autonomous vehicles rely on V2I signals at intersections, cities might design certain zones or lanes for connected vehicles. Policies around *traffic management* might evolve connected vehicles enable new paradigms like dynamic speed limits or cooperative merging algorithms; authorities need the legal ability to implement those (and drivers need to trust and obey them).

Funding policy is crucial: governments must decide how to fund public infrastructure components. This could involve traditional public funding or adopting *public-private partnership (PPP)* models, or even crowdsourcing (in some cases, community-based sensor networks have been tried, though vehicles are more likely centralized in ownership).

8.5. Liability and Legal Framework

A subtle but important policy area is legal liability in a connected environment. If two connected cars have a collision that might have been prevented by V2V communication, and one of them failed to broadcast a warning due to a device fault, who is liable? The driver, the vehicle manufacturer, the software provider, or the component supplier? Determining liability in increasingly connected and automated driving scenarios is a complex task that policymakers and legal systems are grappling with. Clear definitions of responsibility help the technology deployment by giving stakeholders certainty (e.g., if automakers know the boundaries of their liability, they can insure and proceed accordingly). Some countries have begun updating their traffic laws to accommodate automation (like allowing drivers to take their hands off in certain scenarios and shifting responsibility to the automated system under those conditions); similarly, for connected tech, laws might eventually specify duties such as "vehicles must obey authenticated traffic management messages" or assign fault if a car doesn't heed a valid warning. This area is still emerging and likely to evolve as the technology and its use cases mature.

8.6. International Collaboration and Research

Finally, policy can also foster ongoing research and cross-border collaboration. Governments can fund research programs to pilot new VANET applications (for example, projects that test how connected vehicles can aid public transport or how they interact with pedestrians). International collaboration, through forums like ISO, IEEE, or governmental bodies, ensures that best practices are shared and that vehicles from different regions remain interoperable to some degree. There are already multi-nation initiatives (EU-funded projects, US-EU harmonization task forces, etc.) that coordinate on V2X communication standards and testing.

Recommendations: Based on the above considerations, a few broad recommendations for policymakers and city authorities include:

- Develop clear standards and guidelines for V2X technology deployment (e.g., standardized message sets, security credential management) to reduce uncertainty for industry. When possible, align these with international standards to benefit from global scale.
- Consider phased mandates or incentives to accelerate adoption once the technology is sufficiently validated. For instance, mandate V2X on new vehicles by a target year, but provide subsidies for early adopters or critical segments (like emergency vehicles, public transit) in the years prior.
- Ensure a robust cybersecurity and privacy framework is in place: require that any deployed systems use certified security measures (such as the PKI for V2X) and comply with data protection regulations. Establish protocols for data sharing that anonymize personal data and limit usage to approved purposes.

- Invest in the necessary physical and digital infrastructure, possibly leveraging public-private partnerships. Telecom companies rolling out 5G, for example, can be partners in providing roadside connectivity for C-V2X if the business case is shared.
- Address legal and liability issues proactively. Update road laws and driver regulations to define interactions with connected infrastructure. Encourage the insurance industry to develop models for connected and automated vehicle coverage, as their input can also influence safe deployment.
- Promote public awareness and acceptance. The success of smart city technologies often hinges on public trust. Campaigns to educate drivers about the benefits (and proper use) of V2X features, or transparent communication about how data is used, can improve acceptance. Policymakers should be prepared to handle public concerns such as "Will my car be tracked?" or "What if the system fails?" with honest and clear answers.
- Incorporate VANET–IoT planning into broader transportation and urban plans. For example, if a city has climate goals to reduce emissions, it can explicitly count on connected vehicle systems to contribute via efficiency improvements and thus allocate resources to them as part of climate action plans. Or if a city is redesigning downtown, they might install smart infrastructure from the start.

By taking an active role, policy can ensure that technology serves the public interest. The synergy of technological capability and enlightened policy can make the difference between a fragmented, slow uptake of VANETs and a smooth integration that rapidly delivers safety and efficiency benefits to society.

Table 2. DSRC vs. C-V2X

Attribute	DSRC / IEEE 802.11p	C-V2X (LTE-V2X; 5G NR V2X)
Latency	Very low for broadcast; contention degrades under high density (CSMA)	URLLC-capable; flexible numerology; sub-10 ms in advanced profiles
Reliability	Drops in dense/urban-canyon conditions	Higher in dense settings (semi-persistent scheduling; stronger coding)
Range & throughput	A few hundred meters; 10 MHz channels	Greater effective range/throughput; 5G options incl. mmWave for high data
Regulatory maturity	Bandwidth curtailment in some markets	Global momentum toward C-V2X; alignment with 5G/MEC roadmaps
Cost/business model	Dedicated RSU/OBU CAPEX; modest OPEX	Leverages cellular infra; OPEX for connectivity/slices; MNO partnerships

9. Conclusion and Future Work

VANETs and IoT integration in smart cities represent a transformative approach to urban transportation, offering the potential for safer roads, more efficient traffic management, and a platform for innovation in mobility services. In this paper, we surveyed the technological foundations of this field – including the evolution of vehicular communication from DSRC to 5G C-V2X, the leveraging of vehicular sensors as part of the city's data fabric, advances in vehicle localisation techniques, and the imperative of securing the vehicular network against cyber threats. This technical overview highlights that while many of the core technologies are already available or maturing, challenges remain in ensuring reliability, interoperability, and security on a city-wide scale.

Beyond the technical perspective, our analysis of economic and policy implications revealed that realising VANET–IoT benefits is as much a question of strategic decision-making as it is of engineering. The economic case for connected vehicle systems is compelling in terms of potential savings from accident reduction and congestion mitigation, as well as the broader economic growth and new business opportunities these technologies can catalyze. However, upfront costs, uneven incentives among stakeholders, and the need for critical mass adoption are significant hurdles. Policy interventions from setting communication standards and allocating spectrum, to possibly mandating V2X capabilities and enforcing privacy protections, will heavily influence the pace and success of deployment. Effective policies can help align private incentives with public benefits, ensure equity in outcomes, and build public trust in the system. Looking forward, the path to fully realising VANETs in smart cities will likely be incremental. In the near term, we expect to see continued pilot projects and gradual deployment of connected infrastructure in select corridors or zones (for example, dedicated smart city testbeds or high-priority safety corridors). As more new vehicles come equipped with V2X communication (especially with the impending introduction of more 5G-enabled cars), network effects will begin to kick in, making the case for broader deployment stronger. At the same time, developments in adjacent domains such as autonomous vehicle technology will be interplayed with VANETs. Indeed, connectivity is viewed as a key enabler for higher levels of vehicle automation, and policy frameworks are evolving to address both together.

Future research directions may include exploring 6G communications and how they can support ultra-reliable networks of millions of devices (vehicles, bikes, drones, etc.) in a city; enhancing AI-driven data analytics for predictive traffic management using the rich data from IoV; and refining economic models to better quantify benefits in complex urban systems. Interdisciplinary collaboration will be crucial; transportation engineers, communication technologists, economists, and urban planners will need to work together.

In conclusion, the integration of VANETs and IoT in smart cities stands at the intersection of technology innovation and societal need. With thoughtful deployment and supportive policy, connected vehicular networks can significantly advance the goals of safer, cleaner, and more livable cities. The coming years will be pivotal in taking this vision from pilot stage to mainstream reality. The lessons learned and best practices established in early-adopting cities will likely guide the rest of the world in harnessing vehicular connectivity for the public good.

References

Alalwany, E., & Mahgoub, I. (2024). Security and trust management in the Internet of Vehicles (IoV): Challenges and machine learning solutions. *Sensors*, 368.

Basaure, A., & Benseny, J. (2020). Smart city platform adoption for C-V2X services. *Proceedings of the International Telecomm Society (ITS)*, Calgary.

Bhover, S. U., Tugashetti, A., & Rashinkar, P. (2017). V2X communication protocol in VANET for co-operative intelligent transportation system. *International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, pp. 602-607. Bengaluru, India: IEEE.

Canis, B. (2019). *Smart Cars and Trucks: Spectrum Use for Vehicle Safety*. Congressional Research Service (CRS).

Contreras-Castillo, J., Zeadally, S., & Guerrero-Ibañez, J. A. (2017). Internet of Vehicles: Architecture, protocols, and security. *IEEE Internet of Things Journal*, 3701-3709.

Dardour, M., Mosbah, M., & Ahmed, T. (2024). Improving emergency response: an in-depth analysis of an ITS-G5 messaging strategy for bus blockage emergencies at level crossings. *Journal of Network and Systems Management*, 38.

Deniz, E. (2025). IoT's Economic Impacts on Smart Cities. *Information Technology in Economics and Business*, 18-23.

Dutta, A., Samaniego Campoverde, L. M., Tropea, M., & De Rango, F. (2024). A comprehensive review of recent developments in VANET for traffic, safety and remote monitoring applications. *Journal of Network and Systems Management*, *32*(4), 73.

El Madani, S., Motahhir, S., & El Ghzizal, A. (2022). Internet of Vehicles: Concept, process, security aspects and solutions. *Multimedia Tools and Applications*, 16563-16587.

Garg, T., Kagalwalla, N., Churi, P., Pawar, A., & Deshmukh, S. (2020). A survey on security and privacy issues in IoV. *International Journal of Electrical & Computer Engineering*, 2088-8708.

Hasan, N., Aziz, A., Mahmud A., Alias, Y. B., Besar, R. B., Hakim, L., & Hamidi, M. A. (2024). Vehicle sensing and localisation in vehicular networks. *International Journal of Technology*, 472-480.

Khan, A. R., Jamlos, M. F., Osman, N., Ishak, M. I., Dzaharudin, F., Yeow, Y. K., & Khairi, K. A. (2020). DSRC technology in Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) IoT system for Intelligent Transportation System (ITS): A review. *Recent Trends in Mechatronics Towards Industry 4.0: Selected Articles from iM3F* (pp. 97–106). Malaysia: Springer.

Mishra, P., & Singh, G. (2025). Internet of Vehicles for Sustainable Smart Cities: Opportunities, Issues, and Challenges. *Smart Cities*, 93.

Paranjothi, A., Khan, M. S., & Zeadally, S. (2020). A survey on congestion detection and control in connected vehicles. *Ad Hoc Networks*, 102277.

U.S. Department of Transportation. (2016). *U.S. DOT advances deployment of connected vehicle technology to prevent hundreds of thousands of crashes*.

World Health Organization. (2023, December 13). *Road traffic injuries*.