Need for Accelerating Policy, Standards, and Governance for VANET Implementation

Paul M. Brown

Old Dominion University

Intelligent Transportation Systems (ITS) have been developed to make the transportation system more efficient, safe, and sustainable. The US Department of Transportation (DOT) opens an article *How Connected Vehicles Work* by expressing, "In 2018, more than 37,000 people were killed needlessly in traffic crashes. In addition to the devastating human toll and suffering from motor vehicle crashes, the American taxpayer supports more than $140 billion per year in costs for emergency response, fatalities, injuries, and property damage related costs." (transportation.gov). Evidently there is urgent need to implement a solution to mitigate the loss of life and economic burdens of current vehicle transportation. ITS involves the use of modern technologies to improve transportation services and infrastructure. One of the key components of ITS is Vehicular Ad-Hoc Networks (VANETs), which enables vehicles to communicate with each other and with infrastructure. VANETs offer significant potential to enhance safety, reduce congestion, and improve fuel efficiency. National Institute of Standards and Technology's published work, *Design Secure and Application-Oriented VANET,* states "the main benefit […] is in active safety systems, which target to increase safety of passengers by exchanging warning messages between vehicles." (Qian & Moayeri). However, the implementation of VANETs poses challenges related to policy, standards, and governance. This document will explore the needs for policy, standards, and governance in future intelligent transportation systems, such as in VANET implementation in the US.

Policy is an essential component of any ITS system, including VANETs. Policy can be developed at the national, state, or local level. ITS Joint Program Office (JPO) "was established to coordinate intermodal policy in the implementation of the ITS program, originally termed the Intelligent Vehicle Highway System (IVHS) program." (highways.dot.gov). The primary goal of

policy development in VANET implementation is to ensure that the technology is used efficiently and safely. Policies can address issues related to security, privacy, liability, and ethical concerns. Security is a critical concern in VANET implementation. The communication between vehicles and infrastructure should be secure to prevent unauthorized access and protect against cyber-attacks. Policies should be developed to ensure that the communication channels are secure and that appropriate encryption methods are used. Privacy is another concern related to VANET implementation. The communication between vehicles and infrastructure should not violate the privacy of individuals. Policies should be developed to ensure that personal data is protected and that the collection, storage, and sharing of data comply with privacy regulations. Liability is a critical issue in VANET implementation. Policies should be developed to establish clear liability rules in case of accidents caused using VANETs. It is essential to determine who is responsible for the accidents and the compensation for the victims. Ethical concerns also need to be addressed in VANET implementation. Policies should be developed to ensure that the use of VANETs does not violate ethical principles. For example, the use of VANETs should not discriminate against certain groups of people or lead to social exclusion.

Standards are essential for the interoperability and compatibility of VANETs. In October 2018 an article titled *A Review on VANET Routing Protocols and Wireless Standards* expresses "…due to the non deterministic mobility behavior and high velocity of automobiles, the topology is unpredictable." (Singh, et al.). This represents a great need for attention in the area of standards. Standards define the protocols, procedures, and communication formats used by vehicles and infrastructure. Standards are developed by organizations such as the Institute of Electrical and Electronics Engineers (IEEE), the National Institute for Standards in Technology (NIST), and the Society of Automotive Engineers (SAE). The development of standards is

necessary to ensure that VANETs can communicate with each other and with infrastructure seamlessly. Standards can also help reduce the complexity of VANETs and make them easier to deploy. Standards can address issues related to communication protocols, security, privacy, and interoperability. Communication protocols are critical for VANETs, and standards should be developed to define the communication protocols used by vehicles and infrastructure. The communication protocols should ensure that data is transmitted securely, efficiently, and reliably. Security is an essential concern in VANETs. Standards should be developed to ensure that the communication channels are secure and that appropriate encryption methods are used. Standards should also address issues related to authentication and authorization. Standards should also be developed for privacy to ensure that personal data is protected and that the collection, storage, and sharing of data comply with privacy regulations. Standards should define the procedures for obtaining consent and the handling of personal data. Interoperability is also an essential consideration in VANETs. Standards should be developed to ensure that VANETs can communicate with each other and with infrastructure seamlessly. Interoperability standards can address issues related to communication protocols, data formats, and network topology.

Governance refers to the rules, processes, and structures that govern the use of VANETs. This is another essential component to VANETs. The Transportation Research Board released a 2019 policy snapshot highlighting that “Stakeholders need to debate, discuss, and analyze how transportation can evolve to meet growing and evolving needs and adapt to changes in society, technology, the environment, and public policy.” (nap.nationalacademies.org). Governance can address issues related to funding, infrastructure deployment, and data management. Funding is a critical concern in VANET deployment. Governance should be developed to ensure that adequate funding is available for the deployment of VANET infrastructure. Funding can come

from the government, private sector, or a combination of both. Governance should also define the criteria for funding allocation and the monitoring of fund usage. Infrastructure deployment is another concern related to VANET deployment. Governance should be developed to ensure that VANET infrastructure is deployed efficiently and effectively. Governance should define the procedures for site selection, installation, and maintenance of VANET infrastructure. Governance should also address issues related to the ownership and management of VANET infrastructure. Data management is also a critical consideration in VANET deployment. Governance should be developed to ensure that data is managed effectively and responsibly. Governance should define the procedures for data collection, storage, sharing, and analysis. Governance should also address issues related to data ownership, security, and privacy.

The US Department of Transportation (DOT) has been working on the implementation of VANETs since 2001. The DOT has developed several initiatives to promote the deployment of VANETs, such as the Vehicle Infrastructure Integration (VII) program and the Connected Vehicle (CV) program. The VII program aimed to develop the infrastructure necessary for the deployment of VANETs. The program developed standards for communication protocols, data formats, and network topology. The program also deployed infrastructure, such as roadside units and on-board units, to enable communication between vehicles and infrastructure. However, the VII program faced several challenges, such as funding constraints, lack of coordination between stakeholders, and technological barriers.

The CV program aimed to build on the achievements of the VII program and promote the deployment of VANETs. The program developed standards for communication protocols, security, privacy, and interoperability. The program also deployed infrastructure, such as roadside units, to enable communication between vehicles and infrastructure. The CV program

included a research program to evaluate the effectiveness of VANETs in improving safety, reducing congestion, and enhancing mobility. The CV program faced several challenges, such as regulatory barriers, privacy concerns, and technological limitations. The program also faced opposition from some stakeholders, such as privacy advocates and car manufacturers. To address these challenges, the DOT developed policies, standards, and governance structures. The DOT developed policies to ensure that the deployment of VANETs complies with regulations related to security, privacy, and liability. The DOT also developed standards to ensure that VANETs can communicate with each other and with infrastructure seamlessly. The DOT also developed governance structures to ensure that VANETs are deployed properly.

Vehicular Ad-Hoc Networks offer significant potential to enhance safety, reduce congestion, and improve fuel efficiency in intelligent transportation systems. However, the implementation of VANETs poses challenges related to policy, standards, and governance. Policy development is essential to ensure that the technology is used efficiently and safely. Standards are necessary for the interoperability and compatibility of VANETs. Governance is essential for the effective and efficient deployment of VANETs. The US Department of Transportation's initiatives to promote the deployment of VANETs have faced several challenges, but policies, standards, and governance structures have been developed to address these challenges.

Future research should focus on addressing the challenges related to policy, standards, and governance. For example, policymakers should develop regulations that balance the need for data privacy and security with the benefits of data sharing in VANETs. Standards organizations should continue to develop protocols that ensure the interoperability and compatibility of

VANETs across different manufacturers and technologies. Governance structures should be developed to ensure that the deployment of VANETs is efficient, effective, and equitable.

Another area of research that should be explored is the integration of VANETs with other emerging technologies, such as 5G networks, artificial intelligence, and autonomous vehicles. The integration of these technologies has the potential to revolutionize the transportation industry, but it also poses challenges related to policy, standards, and governance. For example, the deployment of autonomous vehicles requires regulations that address liability, safety, and cybersecurity. The integration of 5G networks with VANETs requires protocols that ensure the secure and efficient exchange of data between vehicles and infrastructure. The integration of artificial intelligence with VANETs requires ethical and transparent policies for data collection and analysis.

In conclusion, the implementation of VANETs in intelligent transportation systems requires the development of policies, standards, and governance structures that address the challenges related to data privacy, security, interoperability, and efficiency. The US Department of Transportation's initiatives to promote the deployment of VANETs have provided a valuable roadmap for other countries and organizations that are interested in implementing this technology. However, future research should focus on evaluating the effectiveness of VANETs in improving transportation services and infrastructure, as well as addressing the challenges related to the integration of VANETs with other emerging technologies. Ultimately, the success of VANETs will depend on the collaboration and cooperation of policymakers, standards organizations, and stakeholders in the transportation industry.

Furthermore, it is important to note that the deployment of VANETs will not happen overnight. It will require significant investments in infrastructure, research, and development. Governments

and private sector organizations will need to work together to ensure that the necessary resources are allocated to support the deployment of VANETs.

In addition, there will be challenges related to the adoption of VANETs by consumers. For example, consumers may be concerned about data privacy and security when sharing their location and other information with VANETs. Therefore, it will be important to develop policies and standards that address these concerns and ensure that consumers have control over their data.

Moreover, the deployment of VANETs will require significant changes in the way that transportation infrastructure is designed and operated. For example, infrastructure will need to be equipped with sensors and communication devices to enable communication with vehicles. Roadway design will need to consider the requirements of VANETs, such as the need for reliable communication and accurate location information. These changes will require collaboration between transportation engineers, policymakers, and standards organizations.

Another challenge related to the deployment of VANETs is the potential for cybersecurity threats. VANETs will be a target for cybercriminals, who may attempt to disrupt communication or steal sensitive information. Therefore, it will be important to develop policies and standards that address cybersecurity threats and ensure that VANETs are secure and resilient.

Finally, it is important to note that the deployment of VANETs will not be a panacea for all transportation problems. While VANETs have the potential to improve safety, reduce congestion, and enhance mobility, they will not be able to solve all transportation problems. Therefore, it will be important to develop a comprehensive approach to transportation planning that considers the potential benefits and limitations of VANETs, as well as other emerging technologies.

In conclusion, the deployment of VANETs in intelligent transportation systems offers significant potential to improve safety, reduce congestion, and enhance mobility. However, the deployment of VANETs poses significant challenges related to policy, standards, and governance. Governments, private sector organizations, and standards organizations will need to work together to develop policies and standards that address these challenges and ensure that VANETs are deployed efficiently, effectively, and securely. Moreover, the deployment of VANETs will require significant investments in infrastructure, research, and development. It will also require collaboration between transportation engineers, policymakers, and standards organizations. Finally, it is important to note that the deployment of VANETs will not be a panacea for all transportation problems and will need to be integrated with other emerging technologies and transportation planning approaches. To address the challenges related to policy, standards, and governance in the deployment of VANETs, it is important to identify the key stakeholders and their roles. The stakeholders in the deployment of VANETs include government agencies, private sector organizations, standards organizations, consumers, and transportation professionals.

Government agencies play a critical role in the deployment of VANETs. They are responsible for developing policies and regulations that promote the deployment of VANETs, as well as for funding research and development. In the US, the Department of Transportation has been leading the efforts to promote the deployment of VANETs, through initiatives such as the Connected Vehicle Pilot Deployment Program. However, other government agencies, such as the Federal Communications Commission, also play an important role in regulating the use of the wireless spectrum, which is essential for the operation of VANETs.

Private sector organizations also play a critical role in the deployment of VANETs. These organizations are responsible for developing and manufacturing the technologies that enable the operation of VANETs, such as communication devices and sensors. Private sector organizations also play an important role in developing standards and protocols that ensure the interoperability and compatibility of VANETs across different manufacturers and technologies. Moreover, private sector organizations are also responsible for developing business models that support the deployment of VANETs, such as subscription-based services and advertising-based revenue models.

Standards organizations play a critical role in the deployment of VANETs. These organizations are responsible for developing the protocols and standards that ensure the interoperability and compatibility of VANETs across different manufacturers and technologies. Standards organizations also play an important role in developing guidelines and best practices for the deployment of VANETs, such as those related to cybersecurity and data privacy. In the US, the IEEE Standards Association has been leading the efforts to develop standards for VANETs, through initiatives such as the IEEE 1609 series of standards.

Consumers also play an important role in the deployment of VANETs. They are the end-users of the technology and their adoption of VANETs will be critical to the success of the technology. Therefore, it is important to develop policies and standards that address their concerns related to data privacy and security, as well as to ensure that they have control over their data. Moreover, it is important to educate consumers about the potential benefits of VANETs and how they can improve safety, reduce congestion, and enhance mobility.

Transportation professionals also play a critical role in the deployment of VANETs. They are responsible for designing and operating the transportation infrastructure that supports the

deployment of VANETs, such as roadways and traffic management systems. Moreover, transportation professionals also play an important role in developing transportation planning approaches that take into account the potential benefits and limitations of VANETs, as well as other emerging technologies.

To ensure the success of VANETs, it is important for these stakeholders to collaborate and work together to address the challenges related to policy, standards, and governance. For example, government agencies can work with private sector organizations to develop policies and regulations that promote the deployment of VANETs while also addressing the concerns of consumers related to data privacy and security. Standards organizations can work with private sector organizations to develop protocols and standards that ensure the interoperability and compatibility of VANETs across different manufacturers and technologies. Transportation professionals can work with government agencies and private sector organizations to design and operate the transportation infrastructure that supports the deployment of VANETs.

In conclusion, the deployment of VANETs in intelligent transportation systems offers significant potential to improve safety, reduce congestion, and enhance mobility. However, the deployment of VANETs poses significant challenges related to policy, standards, and governance. To address these challenges, it is important for key stakeholders to collaborate and work together to develop policies, standards, and governance structures that promote the deployment of VANETs while addressing the concerns of consumers related to data privacy and security. This collaboration can enable the development of a comprehensive framework that supports the deployment of VANETs, while ensuring the interoperability, reliability, and security of the technology.

One area where policy, standards, and governance are particularly critical is in the development of cybersecurity guidelines and best practices for VANETs. The security of VANETs is essential

to ensure the safety and privacy of the users and prevent potential malicious activities that may occur. As VANETs involve the transmission of sensitive data, such as vehicle locations, speeds, and driving patterns, they are vulnerable to a range of cyber threats, including data theft, hacking, and cyber-attacks.

Therefore, it is important to develop cybersecurity guidelines and best practices that can address the potential vulnerabilities and threats that may arise in the deployment of VANETs. These guidelines and best practices can provide a framework for ensuring the security of VANETs, including measures to prevent unauthorized access to the network, encrypt sensitive data, and ensure the authenticity and integrity of the messages transmitted through the network. Additionally, these guidelines and best practices can also outline the procedures for managing security incidents and responding to potential cyber threats, including the identification of the incident, the analysis of the impact, and the mitigation of the consequences.

To develop effective cybersecurity guidelines and best practices for VANETs, it is important to involve all key stakeholders, including government agencies, private sector organizations, standards organizations, consumers, and transportation professionals. This collaboration can enable the development of a comprehensive and coordinated approach that addresses the needs and concerns of all stakeholders. Additionally, this collaboration can also ensure the alignment of the cybersecurity guidelines and best practices with other policy, standards, and governance frameworks that are relevant to VANETs, such as those related to data privacy and safety regulations.

Another critical area where policy, standards, and governance are essential in the deployment of VANETs is in the development of a framework for data management and sharing. VANETs generate a vast amount of data that can be used to improve transportation planning,

enhance traffic management, and enable new services and applications. However, this data also poses significant challenges related to data privacy, security, and ownership.

Therefore, it is important to develop a framework for data management and sharing that addresses these challenges and ensures the responsible and ethical use of data generated by VANETs. This framework should outline the procedures and protocols for collecting, processing, storing, and sharing data, as well as the guidelines for data privacy and security. Additionally, this framework should also define the roles and responsibilities of the stakeholders involved in data management and sharing, including government agencies, private sector organizations, standards organizations, consumers, and transportation professionals.

To develop an effective framework for data management and sharing, it is important to involve all key stakeholders and ensure their participation in the decision-making process. This collaboration can enable the development of a comprehensive and coordinated approach that addresses the needs and concerns of all stakeholders, while also enabling the responsible and ethical use of data generated by VANETs. Additionally, this collaboration can also ensure the alignment of the data management and sharing framework with other policy, standards, and governance frameworks that are relevant to VANETs, such as those related to data privacy and ownership regulations.

In conclusion, the deployment of VANETs in intelligent transportation systems offers significant potential to improve safety, reduce congestion, and enhance mobility. However, the deployment of VANETs also poses significant challenges related to policy, standards, and governance. To address these challenges, it is important for key stakeholders to collaborate and work together to develop policies, standards, and governance structures that promote the deployment of VANETs while also addressing the concerns of consumers related to data privacy

and security. Additionally, it is also essential to develop frameworks for cybersecurity, data management, and sharing that ensure the responsible and ethical use of data generated by VANETs, while also ensuring the interoperability, reliability, and security of the technology. Effective policy, standards, and governance structures can play a crucial role in ensuring the successful deployment of VANETs in the US and other countries around the world. These structures can provide a clear framework for the development, deployment, and management of VANETs, while also ensuring that the technology meets the needs and expectations of all stakeholders.

Overall, the deployment of VANETs in intelligent transportation systems is an exciting development that offers significant potential to improve safety, reduce congestion, and enhance mobility. However, it is essential to address the challenges related to policy, standards, and governance to ensure the responsible and ethical use of the technology and enable its full potential to be realized. By collaborating and working together, key stakeholders can develop the policies, standards, and governance structures that are necessary to promote the deployment of VANETs while addressing the concerns of consumers related to data privacy and security.

References:

Babulal, Kanojia Sindhuben. (2019). Review Paper on VANET and the Challenges. 16. 228-232.

How connected vehicles work. U.S. Department of Transportation. (n.d.). Retrieved April 21, 2023, from https://www.transportation.gov/research-and-technology/how-connected-vehicles-work

Shetty, S.R. and Manjaiah, D.H. (2021) *A comprehensive study of security attack on VANET*, *SpringerLink*. Springer Singapore. Available at: https://link.springer.com/chapter/10.1007/978-981-16-2937-2_25 (Accessed: April 21, 2023).

Smith, E. (n.d.). *The future of Intelligent Transportation Systems (ITS): Applying lessons learned from 30 years of Innovation*. The Future of Intelligent Transportation Systems (ITS): Applying Lessons Learned From 30 Years of Innovation | FHWA. Retrieved April 21, 2023, from https://highways.dot.gov/public-roads/spring-2022/03

Xiao, L., Zhuang, W., Zhou, S., & Chen, C. (2019). *Learning-based Vanet communication and security techniques*. Springer International Publishing.

Yeferny, Taoufik & Hamad, Sofian. (2021). Vehicular Ad-hoc Networks: Architecture, Applications and Challenges.