Dr Uday Tupakula
Senior Lecturer, School of Information and Physical Sciences
Deputy Director, Advanced Cyber Security Research Centre (ACSRC)
The University of Newcastle
Email: uday.tupakula@newcastle.edu.au
Phone: +61 2 4921 6803

1. **Are principles for a national approach to C-ITS in Australia necessary? And if so, are the draft principles, as articulated, sufficient to inform investment by industry in C-ITS?**

   It is important to have principles for the development of national approach to C-ITS. There are significant benefits with the involvement of Australian Government which can boost the investments from the industry to achieve consistency of implementation at the national level. However, it is critical that academic sector is engaged in this initiative to anticipate and analyse the impact of design and operational challenges in the C-ITS infrastructure and developing effective trustworthy solutions.

2. **Over the next 5 years, to what extent does your organisation anticipate moving into a C-ITS role or increasing its involvement in C-ITS?**

   At UoN we have Advanced Cyber Security Engineering Research Centre (ACSRC) with globally reputed research expertise in the areas of security, privacy, and trust. We have active projects in C-ITS security and have significant expertise in broad range of emerging technologies such as Cloud, SDN, NFV, MANET, 5G, Federated learning, IoT and Trust models for developing a holistic security C-ITS architecture. In particular, we are developing a C-ITS architecture which can achieve national level consistency for multi domain/cross borders scenario.

   Below we present some of the critical challenges in C-ITS that are related to our research. We strongly believe in working with different stakeholders including the Australian Government, Industry partners and wider community for achieving these goals.

3. **How might C-ITS impact other vehicle connectivity systems in Australia, including vehicle/OEM connectivity, vehicle/cloud connectivity, heavy vehicle telematics systems, mapping systems, etc?**

   Digitisation of the C-ITS offers several benefits such as greater connectivity and exchange of real-time data for efficient usage of the roads by reducing traffic congestion and improved safety by reducing traffic accidents. However, it also brings several additional challenges particularly in terms of security and privacy which can have a significant impact at National Level. Below we discuss some of these issues that need to be considered for maximising the benefits of C-ITS.
   Lack of national level master plan for C-ITS and implementation strategies will lead to significant challenges when connected vehicles cross over state boundaries with different juristridictions. This is particularly important for heavy vehicle telematics systems which are continuously crossing different state borders.
   We need to consider the legal issues, social implications and cultural aspects that are specific to Australia for the design and implementation of the national strategy for C-ITS. At the same time, we need to consider how to make use of local capabilities for supporting local employment for efficient operation and management of the C-ITS.

Advanced Driver Assistance System (ADAS) in the modern automobiles make use of various sensors to perceive the environment and make autonomous decisions for controlling the vehicles. For instance, the real-time data exchanged between the vehicles and the infrastructure can improve the efficiency of transportation systems by reducing traffic congestion and accidents. However, Autonomous Vehicles also suffer from a broad attack surface when interacting with the environment which may jeopardize traffic safety and result in serious accidents. For instance, the sensory data are susceptible to anomalies caused by various attacks and sensor malfunctions which can result in serious accidents. There is a need for techniques to differentiate legitimate data originating from trusted sources and malicious data generated by the attackers.

This is a need for techniques for validating the real time traffic related messages from V2V communications. V2V related messages can have several security, privacy and trust related issues within the domain. In particular, the fast mobility of the vehicles leads to several challenges for establishing secure V2V communication. These issues are further aggravated when V2V communications need be secured in cross domains. As the vehicles can be crossing different boundaries at high speeds, there is need for efficient techniques for cross domain authentication and handover process, continuous monitoring of the vehicles.

Although there are significant benefits for platooning of heavy vehicles, the existing techniques have prioritised safety and support real time operations at high speeds, security has not received similar priority. Several attacks have already been demonstrated by exploiting the vulnerabilities in these techniques and protocols. Also, there is need for developing security techniques for supporting specific scenarios such as toll for platooning with dynamic addition and removal of vehicles.

One of the significant challenges for modern C-ITS systems is their real-time operation in dynamically changing environments. The statistical properties of the data which the model is trying to learn can dynamically change in unforeseen ways. This requires any learning intelligent systems to be able to continuously learn and adapt to system changes.

The current technologies are mainly focussing on the safety and additional features in the AV's and C-ITS infrastructures. However, security and has not received highest priority in the design and development of AV's and C-ITS infrastructures. It is trivial for the attackers to override the safety features by exploiting the vulnerabilities in the AV's and C-ITS infrastructures. Also, the threat landscape is continuously evolving with the increase in the number of connected vehicles and there have been increasing number of cyber security attacks. In particular, there will be increasing number of remote cyber security attacks targeting different entities in the C-ITS. Compared to cyber security attacks on traditional systems, the impact of the cyber security attacks in C-ITS can be cyber physical in nature and much more devastating due the autonomous mobility feature of the connected vehicles. For instance, these attacks can lead to human causalities.

There is need for significant real time data transfers between the telematics applications in the cloud, connected vehicles and C-ITS infrastructure elements. There are several issues that need to be considered for the design and development of C-ITS.

- How to minimise the delays for real time data transfer to ensure the quality of experience?
- How to differentiate heavy vehicle telematics systems from other connected vehicles?
- How to ensure security of the data collected in C-ITS?
- How to ensure privacy of the data collected in C-ITS?
- How to automatically detect traffic incidents in C-ITS?
- How to determine that the data is received from trusted sources?

We believe that we will be able to derive maximum benefits by making use of the emerging technologies to deal with the above issues

- How to make use of emerging technologies such as SDN, NFV and 5G for improving the quality of experience and enhancing the security safety and reliability of the AV's and C-ITS infrastructure?
- How to make use of Federated Learning Techniques for ensuring the privacy?
- How to make use of above technologies for achieving consistency at National Level for cross border scenarios?

4. The draft Principles include a focus on cooperation across industry, government, the research sector, and the community: what structures would be necessary to support the development of an Australian C-ITS system?

The current testbed is suitable for operational testing of the AV's. There is need for extending the testing to enable holistic testing of the C-ITS with AV's. In particular, how to extend the testbed for the following scenarios:

- Evaluation and testing of cross border issues impacting the operation of AV's.
- Evaluation of technological aspects impacting the C-ITS. (eg. Data transfer delays, cyber security issues)
- Evaluation of static and dynamic platooning technologies

5. After the Principles, what next steps do you think would be most productive?

We must proactively consider different case scenarios for efficient and effective management of the C-ITS.

C-ITS can significantly benefit by inviting senior academics who have the relevant expertise to be part of this initiative. In particular, there is a need for establishing an advisory committee with members from Australian Government, Industry and Senior Academics to oversee different challenges technical, business and legal that can arise in developing a National Strategy with multiple domains.

There may be a need to consider the integration of other technologies and infrastructures (such as drones) into the C-ITS infrastructure for effectively dealing with the real time operational issues. For instance, for managing catastrophic events dynamically such as flooding, earthquakes and large-scale cyber security attacks targeting the C-ITS infrastructure.

Emerging technologies such as Federated Learning can be used to enhance the security in C-ITS while ensuring the privacy for the entities.

The transition to complete AV is likely to take many years. C-ITS will consists of vehicles with different levels of autonomy ranging from manual driving to complete AV. There is a need for C-ITS strategy for controlling the vehicles with different levels of autonomy. There is a need to build capability to differentiate and control vehicles with different levels of autonomy to deal with attacks on the C-ITS.