Vehicular ad hoc Networks: Storms on the Horizon

AMELIA REGAN

Researchers and policy makers have long anticipated fully connected vehicular networks that will help prevent accidents, facilitate eco-friendly driving, and provide more accurate real-time traffic information. Today, vehicular ad hoc networks (VANETs) offer a promising way to achieve this goal. Using advances in wireless communications, computing, and vehicular technologies, VANETs rely on real-time communication not only with roadside sensors but also among vehicles and pedestrians. While there are still communication problems to solve within these complex systems, concerns about privacy, liability, and security are the chief obstacles that prevent progress towards large-scale implementation.

What are VANETs?

Computers extensively control modern passenger vehicles, from anti-lock braking systems and electronic fuel-injection, to cruise control and self-parking mechanisms. Yet, these vehicles are also an oddity in today's interconnected world; cars are unable to communicate with each other, or for the most part, with the outside world. Even when vehicles communicate with external gadgets, such as for electronic toll collection, these vehicular networks rely heavily on roadside sensors. VANETs, however, are unique in that they turn participating cars into wireless routers or nodes, allowing cars close to each other to form a network. With the addition of smart phone technology, VANETs can incorporate three different communication pathways:

- **Vehicle-to-Vehicle (V2V):** messages are transmitted between neighboring vehicles. This includes "single-hop" and "multi-hop" messaging scenarios in which vehicles communicate either directly with other vehicles or through intermediary vehicles.

- **Vehicle-to-Infrastructure (V2I):** messages are transmitted between vehicles and road-side units located on nearby arterial road intersections or highway on-ramps. ➢

Amelia Regan is Professor of Computer Science and Transportation Systems Engineering in the Bren School at the University of California, Irvine. (aregan@uci.edu).

- **Vehicle-to-Pedestrian (V2P):** messages are transmitted between vehicles and pedestrians who send and receive messages via their phones or other wireless devices.

With vehicles and pedestrians contributing to the network, VANETs are highly mobile. The more vehicles participating in the network, the more predictable speed and traffic patterns become. And because the network is created using the computers already installed in vehicles and carried by pedestrians, there are few power constraints or storage limitations.

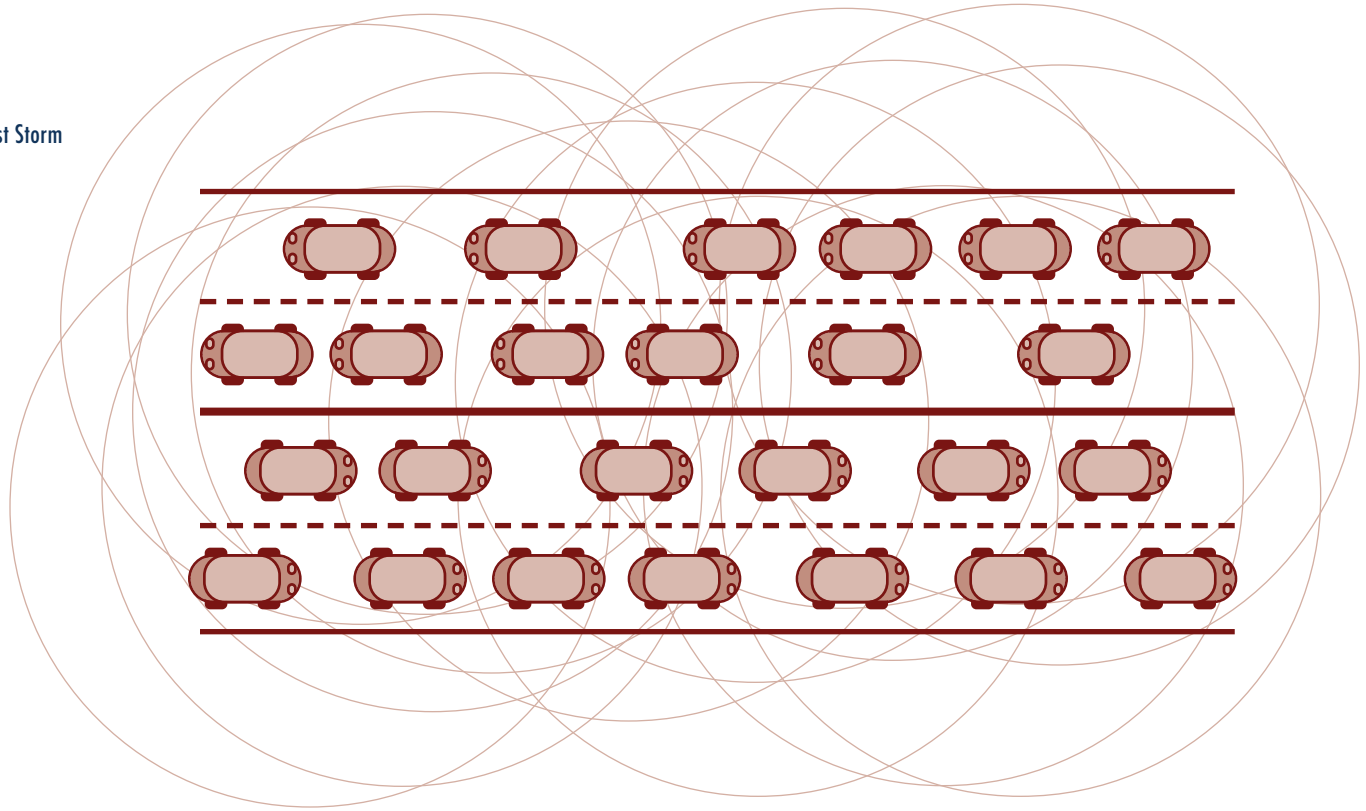
VANETS have many applications. For example, V2V and V2I systems use information on acceleration and braking behaviors of nearby vehicles to track dangers beyond a driver's line of sight, helping to prevent collisions. When vehicles communicate with each other, "platooning" is possible, allowing multiple vehicles to accelerate or brake simultaneously as one unit. Platooning reduces the distance between vehicles and aerodynamic drag, helping to improve fuel efficiency. V2P systems both improve the safety of pedestrians crossing at intersections, and facilitate carpooling and ridesharing by providing people with real-time information. A vehicular network can also provide useful information, such as route guidance, or entertainment content to passengers and drivers.

Challenges

For safety purposes, vehicles must periodically broadcast their location and speed profiles to neighboring vehicles. But when the vehicle network is highly congested, these single-hop messages may create a broadcast storm, overloading the VANET system and delaying message transmission [Figure 1].

FIGURE 1

The Broadcast Storm



Broadcast storms are worse in cities and on congested highways during rush hour. This causes problems because high communication reliability and fast dissemination of information among vehicles, pedestrians, and transportation infrastructure are essential for safety-based applications.

In addition to the communication challenges posed by broadcast storms, the success of a large-scale VANET hinges on solving the issues of privacy, liability, and security. While people may willingly share personal information on social networks, they strongly oppose its being shared without their consent. The privacy requirement, however, is in direct conflict with the need for integrity, authentication, and non-repudiation in a VANET. Many potential participants, therefore, will opt out because they do not want their location broadcast at all times to unknown parties.

Liability concerns have also delayed, and even prevented, the deployment of many VANET technologies. If the system fails and one vehicle crashes into another, who is at fault? Determining liability in a technology-induced collision involves many stakeholders, which is not a simple matter in our litigious society.

Finally, the most important issues are security and safety. VANETs require extremely fast message authentication and processing. Conversely, VANET messages must have strong protection against hacking and extremely high reliability, which significantly increases message size, and thus processing time. Therefore, as the number and speed of messages on a VANET increase, safety applications become more vulnerable to tampering.

An August 2013 *New York Times* article points out how easily automotive computers can be tampered with. Imagine that a safety message requiring immediate braking is falsely disseminated in a congested network. Forget about one vehicle crashing into another. What about dozens of vehicles crashing into each other? Hundreds? Unfortunately, the communication resources needed to ensure message integrity, sender authentication, and extremely fast dissemination are simply unavailable for safety applications at this time.

If the primary challenges related to privacy, liability, and security can be overcome, VANETs, and intelligent, connected vehicles in general, present amazing opportunities to improve transportation safety, increase traffic flows, and reduce environmental harm. ◆

This article draws on "Broadcasting Safety Information in Vehicular Networks: Issues and Approaches," published by the *IEEE Network*.

FURTHER READING

Rex Chen. 2010. "Broadcasting in Vehicular Ad Hoc Networks," PhD dissertation. University of California, Irvine.

Rex Chen, Wen-Long Jin, Amelia Regan, "Broadcasting Safety Information in Vehicular Networks: Issues and Approaches," *IEEE Network*, 24(1): 20–25.

Hannes Hartenstein and Kenneth P. Laberteaux (eds). 2010. *VANET: Vehicular Applications and Inter-Networking Technologies*, Chichester, UK: Wiley.

Kenneth Leonard. 2013. "Keeping the Promise of Connected Vehicle Technology," *TR News*, 285: 3–9.

Hossen Mustafa and Yi Zhang. 2009. *Vehicular Networks: Techniques, Standards, and Applications*, Boston: Auerbach Publications.

Nick Bilton. "Disruptions: As New Targets for Hackers, Your Car and Your House," *The New York Times*, August 11, 2013.

Di Wu. 2013. "Location Based Services in Vehicular Networks," PhD dissertation. University of California, Irvine.