Interview

Toyota's Ken Laberteaux Talks about the Road Ahead

K. Venkatesh Prasad, *Ford Motor Company*
Steve Hodges, *Microsoft Research*
Brian Noble, *University of Michigan*

Tell us a bit about your professional interests.

I started my career working in telecommunications for about 10 years, then joined Toyota 13 years ago. My early time at Toyota was focused on wireless communications—including PHY, media access control, and security and privacy. For the past seven or eight years, I've worked on broader topics, trying to answer the question, "What should Toyota do to create a sustainable mobility society?" My current work spans questions of land use, demographics, automated driving, vehicle electrification, smart-grid development, car and ride sharing, policy analysis, and the quantified self.

Cars have been referred to as "nodes" on the Internet. How would you describe this Internet node on wheels?

I suspect the term "nodes on wheels" will be short-lived. We tend to use the name of a new technology as a verb. But over time, our awareness of the enabling technology falls away. What I used to call "video conferencing" or "Skyping," I now call "talking" or "meeting." In the same way, describing cars as "nodes on wheels" is highlighting the massive increase of data flowing to and from cars. Today, this seems novel. In the future, pervasive data will likely be normal in many facets of our life, including driving. And if cars ever become automated, we might stop using the word "driving." Then, instead of "driving to work," you'd be "going to work."

What promise do these nodes hold?

There are the things we can imagine and the things we can't yet imagine. For the former, clearly there will be dataflows addressing both the vehicle and its occupants. Data central to the car functionality includes information about safety, fuel economy, driving optimization, and firmware updates.

Technologies already exist to provide necessary levels of privacy and security, but finding the right balance between privacy, security, customer convenience, and cost remains a challenge.

Data for the occupants includes information relevant for the trip, such as traffic conditions and multimedia entertainment. Demand for such data could grow significantly in the future as driving becomes more automated.

As far as things we cannot imagine, who knows? Back when mobile phones were first connected to the Internet, who would have predicted how pervasively they would be owned—for example, pre-teens having phones? And who knew how much we would rely on them for shopping and socializing, or the countless times per day they would get our attention?

Are there any challenges you see as we progress on that promise?

Challenges but also opportunities. Let me give you three.

First of all, there are privacy and security tradeoffs. For the most part, technologies already exist to provide necessary levels of privacy and security, but finding the right balance between privacy, security, customer convenience, and cost remains a challenge. We will need to watch the technology roll out and how people use it in order to refine the solution.

As an illustrative example from the past, consider credit cards. It was clear from the start that users would provide huge amounts of personal information to the credit card companies. Despite this, we discovered that consumers found credit cards very convenient. The credit card industry had to create and implement security and privacy policies as well as cybersecurity technologies and expertise. We also saw that there were some options that could have increased the security of credit cards, which consumers rejected due to inconvenience. For example, credit cards could require the buyer to input a 20-digit pin-code at each transaction

Published by the IEEE CS ■ 1536-1268/16/$33.00 © 2016 IEEE

and change the pin-code every day. That would make credit cards more secure, but much less convenient for the users. Over time, the right balance was struck.

As an additional, more recent example, consumers today share tremendous amounts of personal data with companies like Google—for example, their interests, medical questions, the social or political causes they support, where they are considering going for vacation, and so on. But customers also find real value in what Google offers to its users in exchange for their shared search topics. Google also has created policies and technologies to safeguard customer information.

In a similar way, we as a society have to come to some consensus about security and privacy as it pertains to automotive data. There are many optimizations the car industry could provide if a driver would share certain personal information. For example, if the driver would share her intended route for a trip with her car's manufacturer, theoretically, the manufacturer could, in real time, optimize car operations during that trip, resulting in improved fuel economy and a more comfortable ride given traffic or road conditions. The car might also suggest a different route, which might further optimize car performance, or even get the driver to her destination quicker. Will a future driver see sharing that data with her car manufacturer as a good tradeoff? No one knows for certain. But if drivers want to share such information with their vehicle manufacturers, the manufacturers will need to devise secure data communication, as well as policies and procedures for the appropriate handling and use of the data once delivered. The automotive industry has already put in place many such safeguards, using both technology and policy protections, and will no doubt continue to refine its approach over time.

A second major challenge pertains to presenting the right information to the driver at the right time. As more information is collected, communicated, and analyzed, there is a risk of presenting too much information to the driver in a given moment. For example, if a new, faster route is discovered, when and how should that be shared with the driver? Should the car wait until the next time it stops for five or more seconds? Or should it present the new route sooner—such as when the car determines the mental load of the driving task is sufficiently low? In the future, large quantities of rich, compelling data might be available, making the challenge of how and when to present data to the driver an ongoing question.

A third major challenge pertains to driver distraction. As portable devices provide better, more compelling experiences, the issue of driver distraction needs to be addressed. We have seen that when the car locks out certain telematics functions or inputs, some drivers revert to their personal devices, which are indifferent to the driving situation. In such cases, some drivers resort to using a small screen on their lap instead of a larger screen near the appropriate driver's sight line. The challenge can become even larger as partial automation becomes more widely available.

INTRODUCTION

Ken Laberteaux, the senior principal scientist for the Toyota Research Institute-North America, has worked as a researcher in the automotive and telecommunication industries for 23 years. Early on at Toyota, Laberteaux worked on advanced safety systems, leveraging synergies in communication, sensing, and computation. Credited with coining the term Vanet, Laberteaux was a founder and two-year (2004 and 2005) general co-chair of the Vehicular Internetworking workshop. Before joining Toyota in 2002, Laberteaux spent 10 years as a researcher at the Tellabs Research Center, working on echo cancellation, data networking protocols, call admission control, and congestion control. While working full-time at Tellabs, Laberteaux completed his MS and PhD degrees in electrical engineering from the University of Notre Dame, focusing on adaptive control for communications. Prior to that, he received his BSE in electrical engineering from the University of Michigan, Ann Arbor.

His current research focuses on sustainable mobility systems, including US urbanization and transportation patterns, ride-sharing, demographics, grid-vehicle interactions, and vehicle electrification feasibility and optimization. Here, we talk with him about his past and present research and what challenges the automotive industry will faces in the years to come.

— K. Venkatesh Prasad, Steve Hodges, and Brian Noble, Guest Editors

You were involved in vehicular applications and internetworking technologies (Vanet) since its embryonic days, right?

Yes. In fact, I think I came up with the term "Vanet" in the fall or winter of 2003, in a meeting at UC Berkeley. Specifically, it was at the Richmond Field Station in a meeting with Raja Sengupta of UC Berkeley, Chen-Nee Chuah of UC Davis, and Dan Jiang of DaimlerChrysler. However, originally, Vanet stood for *v*ehicular *a*d hoc *net*works. It was an intentional invitation to the mobile ad hoc networking (manet) academic community, which was very strong and active. We positioned Vanet to be a subspecialty of manet.

However, at the time, the hot topics in manet were sensor networks—often creatively described as "smart dust"—and devices that operated with limited hardware resources in terms of sensing, computation, communication distances, and battery life. The situation with vehicle wireless communication was nearly the opposite. Vehicle-based

INTERVIEW

communications shared few of the severe limitations of battery, weight, or computational restrictions placed on sensor networks. Furthermore, Vanets were envisioned to be used in safety-of-life, real-time applications. The resources and performance expectations were completely different.

Since then, as the field has grown in participants, the breadth of topics has also grown. Many networks that we identified as Vanets were not ad hoc networks in a precise way that the manet community defined the term. So we broadened the name of the academic area but kept the acronym.

How did you come to work in the Vanet area?

I joined the US-based Toyota organization in 2002, at a time when a dedicated research function was being established. There were many discussions about what topics our new research group would attack.

Although I hadn't worked in wireless before joining Toyota, it seemed like a topic of growing importance at the time. The US Government had recently reserved a 75 MHz band near 5.9 GHz for dedicated short-range communications (DSRC), and the automotive community was still trying to decide precisely how the spectrum would be used. There were few standards, which were necessary to ensure vehicles from different companies could communicate. At the time, there was not even agreement on what the mix of vehicle-safety applications versus convenience/infotainment applications would be. Vanet felt like the right topic at the right time. Fortunately, my management agreed and supported this research direction.

The challenge we faced early on was, "What is the market demand for Vanet?" Vanet meant adding equipment to the car, but it was not clear who would pay for it. At the time, it was clear that significant safety benefits could be produced, but it was unclear how much benefit would exist during the transitional deployment period.

Often in the car industry, new safety technology is optional, and deployment starts in the more expensive cars. Buyers expect the purchased optional safety equipment to keep their cars safer, thus creating the incentive to pay extra. Later, once the safety benefit of the new technology is well documented, it finds its way into most new cars, through some combination of market demand and government action. However, DSRC couldn't follow this pattern, because if you purchased an optional DSRC unit for your car, you might be safer only when driving among other DSRC-equipped cars. People keep cars longer than they keep phones, tablets, computers, and the like. So, even if DSRC were mandated on every new car in year X, it would take at least 10 years after X before a clear safety benefit would be widely experienced. And if there were no government mandate, large-scale adoption would take even longer.

Once [dedicated short-range communications] becomes widespread, the possibilities of using high-quality, real-time data communication between vehicles become endless.

We argued quite a bit about the requisite adoption rate before the safety benefit would be widely acknowledged. I recall many requisite adoption rate estimates in the 60–80 percent range before improved safety would be documented.

Where is Vanet today—as a set of technologies, as a set of solutions, and as a research area?

It has taken a while, but the incremental costs of offering DSRC has dropped faster than expected, due to the falling prices of similar technologies used in other applications. Now at the end of 2015, we are close to a government mandate in the US. Some automotive companies have unilaterally announced their plan to deploy DSRC before the end of the decade. Once we cross the "Valley of Death" that challenges many new technologies, and DSRC becomes widespread, the possibilities of using high-quality, real-time data communication between vehicles—and from vehicle-to-infrastructure—become endless.

As for other Vanet technologies, usually provided over the mobile phone network, the prospects are also very exciting. Many cars come with data-enabled applications as standard equipment. During the early DSRC days, so-called cellular wireless communications were thought to be too bandlimited and too expensive to compete, a prediction that now, less than a decade later, seems silly. Wireless communication is becoming ubiquitous, and the possibilities for the car and driver are vast.

Regarding cybersecurity, what suggestions might you have for the research community interested in computing and communications related to vehicles?

We made quite a bit of progress in the last decade on this topic. I was actively involved in the security/privacy issues for DSRC. In this case, the basic technical components were already available; the issue was to stitch together the right tools that would maximize privacy while still providing the requisite security. In a paper with Jason Haas and Yih-Chun Hu ["The Impact of Key Assignment on VANET Privacy," *Security and Communication Networks*, Sept. 2009], we demonstrated the privacy limitations of a purely technical solution that still allowed the timely revocation of misbehaving nodes. This in turn encouraged an architecture in which privacy from ordinary nodes is assured technically, while privacy from the revocation authorities would be preserved using a combination of technology and

various policies. Such an architecture has been designed and received wide consensus, although work on various optimizations continues.

As for securing non-DSRC communications, again, many of the building blocks are known, but the devil is in the details. Privacy and security are often competing goals, and cost and customer convenience must also be considered.

Finally, what are your thoughts about automated driving?

These days, I spend far more time thinking about automated driving than communications. I expect it will be a transformative technology, shaping our cities, our housing and work locations, and big sections of our economy.

Not unlike DSRC, I see the real challenge to be the transitional period, when a road will be shared by cars with different levels of automation, and many with no automation at all. I feel that most of the present attention of the media, as well as many technologists, is on the final stage, where essentially all vehicles are completely automated, requiring no driver involvement after entering a destination. Although we might get there, what is far more certain—and thus, in my mind, far more pressing—is to consider a world with partial vehicle automation.

As mentioned earlier, my focus is now on much broader, societal questions related to mobility. Will partial vehicle automation technologies increase or decrease driving demand? Will it promote more urbanization or more sprawl? Will it increase or decrease traffic congestion? What about greenhouse gas emissions? These are the areas where much more work is needed, and where I will focus my work in the years to come.

Be on the Cutting Edge of Artificial Intelligence!

Publish Your Paper
in IEEE Intelligent Systems

IEEE Intelligent Systems
seeks papers on all aspects
of artificial intelligence,
focusing on the development
of the latest research into
practical, fielded applications.

For guidelines, see
www.computer.org/mc/
intelligent/author.htm.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.