Connected Vehicle Challenges for the Dense Urban Environment

By Mohamad Talas, P.E., Ph.D., Robert Rausch, P.E., and Drew Van Duren

Communication technology is at the core of connecting smart city applications; the approach is to establish data communication with the roadway infrastructure, including the fixed assets and mobile devices, and then use available data to analyze the behavior of the roadway network, assess the performance of the systems in place (such as, traffic signals, message signs, speed limits), and devise ways to improve user mobility. The objective of this advanced, connected environment is to improve people’s travel experience by addressing their safety, security, and mobility. By expanding the infrastructure to include cooperative Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) data exchanges, we are able improve the safety of the motorists by reducing the frequency and severity of crashes.
Mobility is improved by using data to drive the city’s Mid-town-in Motion real-time adaptive signal timing algorithms controlling the area shown at right (Figure 1).

Based on the experiences in New York, New York, USA and elsewhere, the connected infrastructure requires the following:

- A reliable, ubiquitous data, communication network;
- A secure environment to protect the integrity and privacy of data collected;
- Mobility applications that produce tangible [measurable] results;
- Strategies to manage the network resources;
- Cost effective deployment and value engineering to ensure sustainability;
- Effective and creative outreach to incentivize end user participation and stakeholder coordination;
- Solutions to address all the use cases including their complex operating environments; and
- A mechanism to address the rapid pace of technological advancement.

In an effort to address some of the most complex use cases utilizing vehicle connectivity, the New York City Department of Transportation (NYCDOT) has undertaken a Connected Vehicle (CV) Pilot to demonstrate the benefits and challenges in deploying connected vehicle technology in a very dense environment. New York City is fortunate that it has intelligent transportation systems (ITS) infrastructure in place to support a large-scale deployment, including a ubiquitous, mega-bit wireless network (NYCWiN), approximately 13,000 advanced transportation controllers (ATC), and an advanced traffic management system. It should be noted that the New York Pilot is based solely on the use of dedicated short-range communications (DSRC) and will be using 6 of the 7 channels in the 5.9 GHz band. DSRC is the only proven technology available that could support the deployment schedule with proven, available products. After competing with other cities, New York City DOT was awarded one of three Connected Vehicle Pilot projects—which has been a learning experience for both the United States Department of Transportation (USDOT) and NYCDOT.

NYCDOT took on the challenge to deploy connected vehicle technology aimed particularly to improve travel safety and pave the way to future national deployment. During the past two years, they have employed the systems engineering process and developed a concept of operations, high-level design, and detailed design and implementation plans. Deployment planning includes installation of the field infrastructure, vehicle recruitment, vehicle installation, testing, operations, and maintenance, along with performance evaluation.

NYCDOT is now in the final stages of preparation for full-scale deployment of roadside infrastructure and equipping of vehicle fleets. Activities such as prototype testing of roughly one hundred vehicle onboard units (OBU) and twenty roadside devices (RSU) are coming to completion. Back-office software and system-level testing of connectivity are shortly to follow.

The New York Pilot Project is focused on safety applications with both V2V and V2I applications; some of the Vehicle-to-Vehicle Safety Applications include: Vehicle Turning Right in Front of Bus Warning, Forward Collision Warning, Emergency Electronic Brake Light, Blind Spot Warning, Lane Change Warning/Assist, and Intersection Movement Assist. Planned Vehicle-to-Infrastructure Safety Applications include Red Light Violation Warning, Speed Limit Compliance, Curve Speed Compliance, Work Zone Speed Compliance, and Oversize Vehicle Compliance warnings for prohibited facilities and structures.

The balance of the project’s software development activities involve data collection and performance analysis; all while striving to ensure the privacy of data collected, managing the volume of data collected, and meeting the contractual needs for performance analysis.

Figure 1. Area where Mid-town-in Motion real-time adaptive signal timing algorithms are used.
This experience has enabled the NYCDOT to face first-hand the challenges to the deployment of this technology; during the last 6 months the following challenges have been encountered:

- Updates to the standards and modifications to the device specifications.
- Deployment of the **Security Credential Management System** and changing requirements for its use; it is now being supported by a commercial entity rather than USDOT.
- Development of **Over-The-Air (OTA)** firmware updates for the OBUs using DSRC.
- Development of a central data management system.
- Development of solutions to the GPS location accuracy and positioning augmentation.
- Testing and tuning of V2V and V2I safety applications.
- Devices certifications—still in progress; this has been a learning experience for the vendors since it has taken time to stabilize the testing procedures, test equipment, and test environment.
- Development of OBU installation procedures—**without assistance from the vehicle manufacturers**—and this varies by vehicle model and year.
- Federal Communications Commission licensing—more than 1,100 licenses had to be obtained for an estimated 350 locations, including some near JFK and LaGuardia Airports—two of the City’s major airports.
- Various procurement and installation contractual management issues due to the desire for multiple vendors, the required device development, and the uncertainty of specific vehicle installation procedures.
- Development of a testing environment—for the technology, the installation, and troubleshooting the radio frequency field conditions—which have experienced interference and GPS jamming.

As NYCDOT prepares for large scale installation in early 2019, the CV team has worked through problems and developed solutions and documented those plans in agreements, specifications, and the CV deployment plan. The challenges involved with this new invocative technology and the special multifaceted and multimodal transportation network are not unique to the project. The balance of this paper will examine some of the challenges and solutions in the hope that others considering CV deployment can benefit from NYCDOT’s experiences.

**Project Design Challenges**

During phase 1 of the project, it quickly became evident that many of the essential elements for a large-scale sustainable CV deployment were missing. While the previous research and small-scale demonstration projects could sustain their operation with manual operations, and crude data collection techniques, the NYCDOT’s deployment needed to handle operations and maintenance on a larger scale. Further, the deployment needed a more automated mechanism for the collection of data to measure the performance and benefits of the system. By way of example, data retrieval would be an important consideration. The safety pilot project collected the evaluation data on flash memory microchips that required periodic access to the vehicles for retrieval; in contrast, the New York vehicles are revenue generating or commercial fleet vehicles that are expensive to “touch” because it means taking the vehicle out of service to a maintenance facility, which is not practical. The New York project needed a way to upload collected data at a minimum of once a day over a DSRC link which meant the use of more DSRC channels.

Because of the vehicle fleet size and the calendar time needed to complete the OBU installation, a way was needed to deal with over-the-air software updates as the operation of the applications was tuned, and system and software issues were solved. This led to the development of an over-the-air (OTA) firmware updating application and an OTA mechanism to “tune” the applications. With these two additional elements, it is possible to proceed with the production installation while also verifying the application software and tuning the safety and data collection applications.

Working closely with the other pilots through a series of technical roundtables, ambiguities could be resolved within the standards to make sure individual interpretations and use of the standards was consistent and that this information was passed back to the standards working groups. The New York project team has also remained active in the standards development program (SAE and National Transportation Communications for Intelligent Transportation System (ITS) Protocol (NTCIP)) such that issues were identified and brought back to the standards working groups for resolution—all to insure a sustainable, interoperable infrastructure.

Another challenge faced with the pedestrian application was the absence of DSRC operation for a Smartphone; the original
The intent of the CV pilot was to include a Smartphone based application for the visually impaired that would assist them in navigating the crosswalks of an intersection using the DSRC signal phase and timing (SPaT) and map data (MAP) information. When the chip set and phone makers would not support the use of DSRC on a Smartphone (software modifications to the chip set), the vendor, Savari, worked with the team to be able to transmit the SPaT information updates to the traffic management center (TMC) where they are combined with the MAP message content and sent to the Amazon Cloud to support a Smartphone application using cellular service. Since the NYC system is transmitting the new (2016) version of the SPaT information, the message content changes approximately 12 times per cycle (90 seconds in Manhattan) and hence, the volume of data needed by the Smartphone is reduced by more than 90 percent and it can still maintain sub-second accuracy of the signal changing times to alert the user of the signal condition and impending signal changes. Thus, the updated firmware at the traffic controllers can provide the SPaT message content to the TMC and then to the user without the need of an RSU at the intersection.

**Security Challenges of CV Deployment**

Security is a key element to the deployment of a CV infrastructure. The CV concept requires that on-board units trust data that they are receiving from the infrastructure and from other vehicles in order to identify crash threats or possible intersection stop line violations. In this section, some of the issues that are addressed by the security credential management system will be examined.

**Security and Privacy Challenges:** The interplay between safety, security, and data ownership has introduced a set of challenging issues to orchestrate; while vehicle-to-everything (V2X) deployment is principally for enhanced safety, unaddressed privacy and security concerns can impede its acceptance. New approaches and controls are needed in data management to ensure protection of individual privacy and yet provide new ways for traffic system operators and researchers to analyze traffic conditions and improve safety. For example, the new data types, sources, and consumers have complicated issues associated with data ownership, protection, and retention, including how traffic system operators and third party researchers securely obtain and make use of data. In the Connected Vehicle Pilot, unprecedented quantities of new V2X data have introduced privacy challenges such as ensuring anonymity, inability to track, and finding data management methods that make intractable the correlation of individual drivers with any raw or processed data. Before deployment, these types of challenges must be overcome to obtain and maintain agreement from all V2X stakeholders (e.g., the traffic system operators, cities, counties, fleet operators, researchers, and third party data providers/consumer) on a robust privacy posture. A consistent and acceptable legal framework is needed that addresses the privacy needs that are common as well as unique to each participating organization.

The New York project has taken steps to ensure that data collected and held at the TMC does not contain personally identifiable information (PII) and that it cannot be combined with other records such as police accident records, to potentially become PII. The potential is that the 10 Hz basic safety message (BSM) could recreate an accident scene at an intersection or elsewhere and, because of the known ending place for the vehicles, potentially identify individual drivers. Data collected is subjected to normalization, obfuscation, and aggregation for the purposes of benefit analysis—but cannot be tracked to an individual vehicle or driver.

**Servicing, connecting, and integrating V2X systems with legacy traffic infrastructure:** Significant new logical and physical points of connection emerge in the deployment of connected vehicle technology; these points of connection involve both legacy as well as new V2X equipment and data. The new V2X protocols incorporate strong cryptographic security for which some legacy equipment must be upgraded to ensure interoperability and a leveled security posture. Existing traffic signal controllers, for example, will typically require cryptographic protocol upgrades to mitigate exposure of insecure NTCIP-based protocols. These upgrades, many of which require the use of digital certificates, introduce numerous dependencies and downstream effects on existing device and system design, technology selection/adaptation, data integration, as well as system operations. Enhanced public key infrastructure (PKI) security provisioning is needed, for example, to obtain and install the cryptographic credentials that secure the triad of TMC-RSU, RSU-Signal-Controller, and Signal-Controller-TMC connectivity. This device provisioning challenges deployment organizations with the need to open new, potentially risky, internet connections through which devices are able to obtain the provisioning services. V2X deployers may need to modify existing network topologies and security controls to handle the new, internet-facing attack surfaces. New V2X devices also levy on V2X deployers new security management capabilities, for example new security monitoring techniques (device and network) as well as new tools to perform over-the-air updates of software, firmware, and device configurations in both vehicles and roadside equipment. While each new security control is requisite to mitigate security risks, attentive security design is imperative to reduce the potential for the new security controls introducing vulnerabilities in the process.

The New York project has added Datagram Transport Layer Security (DTLS) v1.2 using X.509 certificates to all NTCIP communications between and among the RSU, TMC, and ATC. This addition places new requirements on the operations and maintenance procedures at the TMC and management of the inventory of RSUs and ATCs. The system now includes a mechanism for initializing the ATC and RSU connections in the event of device
replacement. The new procedures are to guarantee trust between the field personnel and the TMC at the time of maintenance such that the TMC can re-initialize the certificates and lock down the ports on the ATC from other users. Future traffic controllers will need to include a hardware security module that will protect the cryptographic material and insure the security of the ATC.

NYC chose to add a hardware security module to the TMC systems for the purpose of signing the geometric intersection description and the traveler information message content (MAP and traffic incident management (TIM) messages). The TMC is responsible for the accuracy of the MAP and TIM information so it is only natural that the messages are signed at the TMC and authenticated at the OBU, which will then use these data. The SPaT message is signed by the RSU.

**Evolving Security Environment:** The security credential management system (SCMS) does not currently have a standard misbehavior detection and certificate revocation list distribution—both of which are essential to maintain the security of the CV infrastructures. These features are currently under development and will become available along with the supporting software utilities sometime in 2019. At that time, it will be possible to upgrade the security subsystems and download them to the OBU and modify the TMC. In the meantime, the NYC system chose to load only certificates for one week in the future to all the devices to limit attack exposure. Thus, the OBUs for NYC do not have a 3-year supply but rather must update their certificates every 7 days.

**Vehicle Installation Challenges**

Working closely with the maintenance shops, fleet owners, and OBU vendors, the NY project is developing fleet owner acceptable installation procedures for the OBU. Because of concerns over cockpit distractions, this project has opted for voice and tone alerts to the operator. This means the installation of auxiliary speakers due to being unable to connect to the vehicle’s audio systems. Again, it would be helpful if the original equipment manufacturers (OEMs) provided a means of attaching an auxiliary audio system—just as they do for their own navigation systems, but until that happens, the OBU includes an audio amplifier and provision for 2 external speakers—although the existing audio systems are unable to be muted.

Antenna installation is a “mixed bag.” Some of the fleets fully allow drilling a hole in the roof and installing the wires through removable panels. Others have opted for the use of a through the glass antenna developed by DanLaw as the preferred mounting for selected vehicle types.

Access to the vehicle’s controller area network (CAN bus) to supplement basic safety message data and enhance positioning accuracy has been a challenge. The vendors are using different approaches to meet the project requirements. One vendor connects directly to the CAN bus and is able to extract the information required for most vehicle make/model/year combinations. The other vendor has opted to purchase and supply a “gateway” box and leave the CAN bus interface to their supplier. However, as more OEMs start encrypting data on the CAN and other vehicle buses, both approaches will become more difficult for newer models. These data connections add to the complexity of the device installation and power management—and certain model vehicles do not make the information available. Keep in mind that the on-board diagnostics (OBD) II port was mandated for pollution measurements; many of the fleet vehicles already have devices connected to the OBD I port—further complicating the matter. We hope that in the near future, the OEMs will work with the standards organizations to provide a secure gateway to access the vehicle data since the deployment of aftermarket devices is critical to the widespread retrofitting of CV technology to the existing vehicle fleet.

**Data Collection**

Past CV trial and demonstrations have tended to collect every message transmitted, every message received, and ongoing trigger information for all vehicles. At the same time, the RSUs recorded and sent every BSM it heard back to the TMC for processing. The theory being that this will provide all possible data for analysis and operations optimization. However, it becomes quickly obvious that given the sheer number of vehicles on the road—such a philosophy is not practical or sustainable with a wireless network. Hence, the New York project reviewed data needed for the performance measures and focused on the concept of edge computing to foster the conversion from data to information at the edges of the system to avoid the unmanageable flow of data and processing of such data at the TMC.

Since the NYC CV pilot project was focused on deployment rather than research, only the data necessary to evaluate the safety benefits and the operational reliability of the units was collected. An analysis of the data needed for the performance and benefits analysis was performed and then a mechanism was developed which will collect only relevant data immediately before and immediately after an “incident”; an incident is defined as an alert or warning to the operator. In the case of the “control group” or before activating the alarms, the incident is considered to have occurred anyway, which provides the opportunity to analyze the operation of the safety applications prior to live activation.

Thus, based on 4 incidents per hour, the system will collect ~15 megabytes (MB) per day per vehicle, 312 gigabytes (GB) per day for all 8,000 vehicles; the number of alerts is expected to drop to closer to 4 per day once the operators recognize the presence of the system and that is only 1 MB per day as opposed to collecting all data transmitted and received which is approximately 2 terabytes (TB) per day.

Another example is the travel time data collection that is used to drive the city’s adaptive traffic management algorithms. Assuming a nominal 300-meter DSRC signal distance from the intersection, this is roughly 1,000 feet. If the intersection could hear the BSMs
for that distance both upstream and downstream, it would receive roughly 500 BSM messages from each vehicle within range—assuming it did not stop but was traveling at the progression speed; if the vehicle had to stop, the RSU would hear another 500 BSMs while the vehicle was waiting for the cross street. If the system were to record and transmit [to the TMC] every BSM it heard from each vehicle, then each vehicle would result in the transmission of between 500 and 1,000 BSMs as it traveled through each intersection. However, to compute the travel time between intersections, only a single BSM is needed when the vehicle reaches a known “zone” at the intersection. If each RSU processed the BSM data stream in real time and sent a single BSM when the vehicle entered the configured zone, then each vehicle would result in one message from the RSU to the TMC, which would receive all such messages from all of the intersections and match the vehicle ID and compute the travel time and hence average speed between the intersections. The bandwidth needed—and the central data processing needed is reduced by more than 99.8 percent and where cellular data is used, this is a significant cost savings without loss of information; the city now uses toll tag readers spaced every 10 blocks—the use of CV data improves the resolution of data without loss of fidelity and eliminates the need for the radio frequency identification readers.

This is one example of the need to consider edge computing whether it is done in the traffic controller or the RSU will depend on the products available in the future, but the CV data stream can improve data available for analysis; BSM data can be used to determine the location of diversions, incidents, queue lengths, etc. at the edge of the network and pass that information to the TMC for aggregation and management.

Summary
The New York City Connected Vehicle Pilot Deployment project has been able to focus on the actual needs and complexities of CV deployment rather than upgrading the existing ITS infrastructure. There is a considerable difference between “demonstration” projects with a few hundred vehicles and 30–40 intersections and a sustainable system with 8,000 vehicles and 400 RSUs (the original goal for the New York Project). New York City has always been a challenge for ITS deployment since the traffic management system has approximately 13,000 ATCs—all controlled over a private cellular network with multi-contractor maintenance; this is a single system with a complex traffic control network; NYC traffic control includes interval-based operation,National Electrical Manufacturers Association (NEMA) phase-ring based operation, (central based), adaptive operations, and transit signal priority. Therefore, it was only natural when the CV project started, to begin addressing the system’s scale and the project approach from the ground up such that the continued operation was both economically practical and sustainable. As the project moves forward with the installation of the OBUs, data will be collected that is necessary to track the performance of the hardware systems, the crash mitigation benefits, the accuracy of travel time data, and the user acceptance of the technology.

Mohamad Talas, P.E., PTOE, Ph.D., brings long-standing career experience in traffic engineering and continues his expertise with more than 30 years in traffic engineering and operation experience in New York City (NYC) Department of Transportation. He currently serves as the director for the NYC Department of Transportation System Engineering where he supervises the Intelligent Transportation System projects and initiatives. In the past three years, he has led the NYC Connected Vehicle Pilot Deployment project management. Dr. Talas is also an adjunct professor at New York University, Tandon School of Engineering in the Transportation Graduate Program. He earned his Ph.D. in transportation planning and engineering at NYU-Poly University, master’s degrees in transportation, planning and engineering and a master’s in electrical engineering from Fairleigh Dickinson University. He is a licensed Professional Engineer and a member of ITS America, ITE, and the Intelligent Transportation Systems Advance Transportation Controller National Standards Working Group.

Robert (Bob) Rausch, P.E. is a vice president in TransCore’s Intelligent Transportation Systems (ITS) Division with more than 48 years of experience in the design, installation, and integration of ITS, including traffic management centers and the production of hardware and software for ITS devices and systems. He has been TransCore’s technical lead for New York City’s Traffic Management Systems (12,500 traffic signals), including the centrally controlled Transit Signal Priority for the City’s Select Bus Service. He is the technical development lead for the City’s Connected Vehicle Pilot Deployment Project. He holds both a bachelor’s, and master’s degree in electrical engineering from MIT. Bob is a member of ITE.

Drew Van Duren is the technical director of IoT security at OnBoard Security, Inc., a cybersecurity company dedicated to the safe and secure deployment of transportation systems, advanced cryptography and hardware-enhanced trusted computing. He is a seasoned DoD and transportation industry security professional. Drew co-authored the book, Practical Internet of Things Security and today provides security consulting for the New York City Connected Vehicle Pilot Deployment, the world’s largest planned deployment of 10,000 connected vehicles and hundreds of smart infrastructure devices.