A Secure V2X Connected Vehicle Transponder System for Vehicle Prioritization

Pino Porciello, Kevin Henry

ESCRYPT, Waterloo, Ontario, Canada

Abstract

V2X is an essential enabler for safer roads and future autonomous vehicle technology, but also enables applications to help improve the movement of traffic, with one promising application being V2X-based signal prioritization to help improve the movement of public transit, emergency vehicles, and freight. V2X can enable roadside infrastructure to automatically recognize the unique properties of a vehicle and take optimal action. In the case of an intersection, the solution can adjust the signal timing (extend or force a green light) depending on the vehicle's priority, reducing the vehicle's travel time and fuel consumption.

The primary challenges to public transit priority, emergency vehicle pre-emption, and integrating freight priority, are numerous. There are no common, secure and jointly managed vehicle identification and role systems; each department has different solutions that rely on non-standardized radio communication systems, and the infrastructure which controls lights has no means of communicating obstacles to connected vehicles and no means of receiving desired route information to enable priority. V2X and the cyber security mechanisms behind V2X, namely the Security Credential Management System (SCMS), can help overcome the present challenges.

This paper presents a secure V2X vehicle transponder system for a vehicle prioritization demonstration that illustrates the potential use of V2X technology in vehicle prioritization applications. This project also starts to build the foundation for ITS safety applications by creating a system that can securely communicate to non-connected entities, including pedestrians and cyclists, and communicate signal and phase information to autonomous and connected vehicles.

Keywords:

Security, V2X, Vehicle Prioritization

1 Introduction

V2X is an essential enabler for safer roads and future autonomous vehicle technology, but also enables applications to help improve the movement of traffic, with one promising application being V2X-based signal prioritization to help improve the movement of public transit, emergency vehicles, and freight. V2X can enable roadside infrastructure to automatically recognize the unique properties of a vehicle and take optimal action. In the case of an intersection, the solution can adjust the signal timing (extend or force a green light) depending on the vehicle's priority, reducing the vehicle's travel time and fuel consumption. Large freight vehicles can expend a considerable amount of fuel when accelerating from a complete stop, so properly applied signal prioritization could result in substantial fuel savings, thereby easing the environmental impact of large vehicles.

The primary challenges to public transit priority, emergency vehicle pre-emption, and integrating freight priority, are numerous. There is no common, secure and jointly managed vehicle identification and role systems, each department has different solutions that rely on non-standardized radio communication systems, and the infrastructure which controls lights has no means of communicating obstacles to connected vehicles and no means of receiving desired route information to enable priority. V2X and the cyber security mechanisms behind V2X, namely the Security Credential Management System (SCMS), can help overcome these challenges.

Vehicle prioritization has direct applications to the following:

- Public Transit: One of the ways cities can reduce traffic congestion is to minimize demand through the use of public transit. Public transit plays a large role in congestion reduction because it can carry more people through the same roadway than personal vehicles. However, citizens are less likely to use public transit when travel times are long or unpredictable. Cities with successful transit systems have developed the concept of transit priority, enabling buses and transit vehicles to gain back lost travel time from stops through priority flow via traffic light control on city streets. However, transit priority systems are very expensive because they are single-purpose and require unique integrations with traffic controllers.
- Emergency Vehicles: Emergency vehicle preemption is a common technique used by cities to reduce travel time. However, it can expose cities to legal liability if an emergency vehicle triggers a light change that results in an injury. To mitigate this, more advanced and prohibitively expensive emergency systems integrate routing information with priority rather than preemption, allowing the EMS route to be cleared in advance of the vehicle. In addition, the drivers of EMS vehicles often are not aware if there are pedestrians in a crosswalk as they

approach at speed. There are no mature systems today that enable connected vehicles to see non-connected objects (including people) in a crosswalk.

- Freight: Cities, especially those in proximity to international borders and ports of entry, need to move freight through their roadways in an efficient manner and this topic is a high priority and challenge in traffic management practice. Very few cities have freight priority solutions and very few industries have the ability to both monitor freight and enable city infrastructure to route freight.

Having single-purpose transit, EMS, and freight systems increases the cost to cities and creates challenges for traffic engineers. Such systems often have proprietary security designs, which can introduce security threats because the system is not open for review by experts. The cost is high because each single-purpose system requires its own hardware, routing, servers, identity and security systems and management. These systems are typically based on closed standards, therefore they cannot share information with one another or with incompatible systems in other cities. Furthermore, traffic engineers then need to optimize for the two or more independent systems that interrupt already-taxed traffic management centers.

2 V2X Introduction

Direct vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication (collectively referred to as V2X) enables vehicles to communicate with the low latency and high integrity needed to enable collision avoidance and driving assistance applications. The United States Department of Transportation (USDOT) has predicted that this technology can reduce or eliminate up to 80% of non-alcohol related collisions. [1]

In order to function safely, V2X needs a security infrastructure to ensure the trustworthiness of of every communicated message. Specifically, the source of each message needs to be trusted and the message content must be protected from outside interference or modification. In order to create the required environment of trust, the security specification requires digital signatures to protect the integrity of the message content and certificates to validate the authenticity of the sender.

In addition, in order for the information in V2X to be useful, it must be sent in a standard format. Interoperability of the message content and security credentials ensures the ability for different devices within V2X to communicate with each other in a reliable and timely manner. Systems sourced, manufactured, and installed by various OEMs and aftermarket retailers must adhere to the same standard, otherwise the usefulness of V2X will be diminished.

The Security Credential Management System (SCMS) is an infrastructure that has been designed specifically to enable V2X capabilities. [3] This underlying infrastructure provides secure, reliable, two-way authenticated messages between vehicles and roadside equipment and enables interoperability amongst the different vendors and components of the V2X system. The SCMS establishes trusted relationships so that vehicles can check the validity of information received from other vehicles and equipment. The SCMS design is built on Elliptic Curve Cryptography (ECC) technology and best practices along with novel extensions that support privacy and large-scale deployment. The many benefits of V2X are dependent on the successful implementation and operation of the SCMS platform [4].

2.1 The Security Credential Management System (SCMS) for V2X

The SCMS is a large-scale Public Key Infrastructure (PKI) with several novel enhancements intended to specifically support connected vehicles and roadside equipment. The system issues *credentials* which allow communicating devices to trust only authorized sources. The security technology is built around ECC, a highly efficient public key algorithm that can operate at high speed on embedded processors and enables small digital signatures. It takes advantage of implicit certificates, a method of further enhancing the small size of ECC signatures and reducing the overall size of, and the overhead required, to handle the digital certificates that must be transmitted and stored by vehicles and roadside equipment. This feature is used extensively to support privacy by issuing thousands of unique certificates to every vehicle. The SCMS design supports a distributed architecture which allows separation of roles so that automobile manufacturers (OEMs), fleet owners, and Intelligent Transport System (ITS) managers can operate independently while sharing a common root of trust. The goal of the system is to ensure that all vehicles and roadside equipment can reliably exchange authenticated messages even when they are managed by different organizations which do not have existing formal relationships.

Figure 1 demonstrates the proposed entities within the SCMS and maps the typical communication patterns between them. The roles of each entity are described briefly below.

Policy & Technical Management

In the SCMS, these components manage the overall system. Policy updates are published in a standard format, certified by the Policy Generator, and made available to all participants. High-level controlling entities called Electors are established in order to facilitate Root Management.

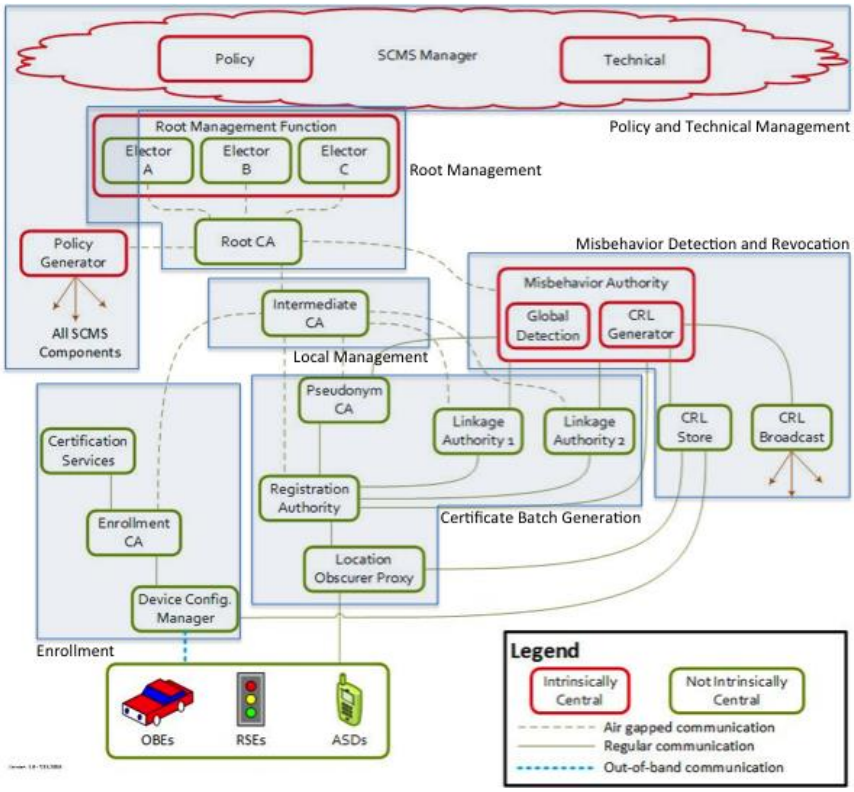

Figure 1. Annotated SCMS Architecture Diagram.

Root Management

Establishes the system-wide root of trust, the Root CA. The Electors endorse the Root CA and provide a mechanism for adding or removing Root CAs from the system. The system can have a single Root CA or multiple Root CAs.

Local Management

The Root CA is kept offline and is typically only brought online to certify Intermediate CAs (ICAs), which in turn certify the other components in the system.

Enrollment

The enrollment process takes place before the end-entity starts operation. It involves initial bootstrapping of the end-entity at the OEM, where an out-of-band communication channel is established between the end-entity and the Device Configuration Manager (DCM) in a secure environment during manufacture. The DCM acts as an interface between the end-entity and the Enrollment CA (ECA) and ensures that only authorized devices are able to submit an enrollment request. The enrollment certificate serves as an end-entity's "entry ticket" to request pseudonym certificates. Enrollment certificates can be blacklisted to prevent the request of pseudonym certificates at a Registration Authority (RA).

Pseudonym Issuing

The process of generating pseudonym certificates for the end-entities (EEs) is distributed across four components. This is done so that no single entity knows which pseudonym certificates end up with a specific vehicle; hence SCMS provides privacy protection against insider as well as outsider attacks. The entities involved in generating pseudonym certificates are as follows:

- Registration Authority (RA): Receives the certificate requests from EEs and forwards them to the Pseudonym CA after expanding the individual request per EE into thousands of requests and shuffling them across multiple EEs. These requests are combined with inputs from Linkage Authorities. The RA knows the enrollment information associated with an EE, and can reconstruct batches of certificates, but cannot see the individual certificates because they are encrypted directly to the EE.
- Pseudonym CA (PCA): The actual issuing CA which collects the information to be inserted in the certificates, signs and encrypts them, but without being able to trace them to a particular EE. The PCA sees all pseudonym certificates, but does not know which belong to any given batch, or know which vehicle is requesting them.
- Linkage Authorities (LA): These components generate linkage values to be included in the EE certificates and sends these linkage values encrypted to the PCA. The LAs do not learn which certificates contain which linkage values. The origin (seed) of these linkage values is only revealed in the case of misbehavior of an EE; this is done by including the seed in a Certificate Revocation List (CRL). Both LAs must cooperate in order to link certificates together. Revealing the seed linkage value, revokes all the pseudonym certificates of the misbehaving EE.
- Location Obscurer Proxy (LOP): As a final privacy-protecting measure, an EE's physical location is obscured to the RA by connecting via a proxy.

Misbehavior Detection

Receives reports of anomalous behavior, identifies bad actors, cooperates with the Linkage Authorities, and creates and distributes CRLs. If both LAs reveal the linkage seeds used to generate a batch of certificates (only at the request of the Misbehavior Authority), then they can be published in a CRL, thereby revoking the entire batch of pseudonyms.

End-Entity

An End-Entity (EE) may be On-Board Equipment (OBE) on the vehicle or Roadside Equipment (RSE). In general, OBEs are issued batches of pseudonyms so that they can rotate through them for privacy reasons, while RSEs are issued individual short-lived single-purpose pseudonyms, as privacy is generally not necessary for RSEs.

3 Vehicle Prioritization Solution

A secure V2X connected vehicle transponder system for vehicle prioritization has been developed to coordinate transit signal priority, emergency vehicle preemption, and freight priority. It consists of connected infrastructure and connected vehicle integration, which includes a V2X SCMS security certificate management for public transit, emergency, and freight vehicles. This system also starts to build the foundation for ITS safety applications by creating a system that can securely communicate with non-connected objects, including pedestrian and cyclist presence, and signal and phase information to autonomous and connected vehicles.

The developed solution is a collection of V2X components that can be used to demonstrate a secure and connected vehicle prioritization application across both Dedicated Short-Range Communications (DSRC) and cellular technology. As transit, emergency, and freight vehicles approach an intersection, the solution will enable the roadside infrastructure to automatically recognize the unique properties of the vehicle and take optimal action. In the case of an intersection, the solution can adjust the signal timing (extending or force a green light) depending on the vehicle's priority, reducing the vehicle's travel time, or preventing it from having to stop. The developed solution will necessitate the installation of equipment in freight, emergency, and public transportation vehicles with DSRC radios and telematics devices. Each intersection that requires Emergency Vehicle Preemption (EVP), Transit Service Priority (TSP), and/or freight priority will need to be equipped with additional hardware.

The solution will use a V2X service to issue security certificates to vehicles and infrastructure to enable secure messaging among independent components. This security architecture will protect the solution from abuse by making sure that the system is capable of assigning new roles and permissions to vehicles, validating certificates, and managing certificate revocation (e.g. when the certificates are retired or compromised). The security architecture is used to establish and manage trust and data security. This will also allow the deployed system to eliminate silos between applications, city departments and municipalities, facilitating the exchange of trusted data.

4 Vehicle Prioritization Demonstration Project

The overall objective of the vehicle prioritization demonstration project is to deploy, test, and demonstrate a complete, commercializable solution that cities can utilize for their transit, emergency, and freight vehicle prioritization requirements. The demonstration project will implement and deploy a commercial-ready secured and trusted V2X connected vehicle

transponder system that enables and demonstrates vehicle priority, preemption, and bi-directional communications. The demonstration will include: three levels of prioritization programmed into a connected vehicle security certificate with corresponding infrastructure services; the ability to issue, modify, and revoke security certificates; and the ability for the infrastructure to communicate traffic signal status and pedestrian presence to connected vehicles.

The demonstration project will show basic V2X applications running on real infrastructure and vehicles with operational security infrastructure. This will include signal status, as well as basic emergency vehicle preemption. The technology will be integrated into test vehicles to demonstrate prioritization as well as the ability for the intersection to notify the vehicle regarding the traffic signal status (green/yellow/red). The demonstration will also show how cellular data containing freight and emergency vehicle route information can coordinate with an intersection controller to enable green light priority as the test vehicle approaches the intersection.

The demonstration will take place using a small number of proof-of-concept integrated vehicles and intersections, which will serve as demonstration to unlock commercialization opportunities with municipalities and connected vehicle manufacturers and fleets. The project will integrate three technologies (DSRC, cellular, and infrastructure) to implement bi-directional communication for vehicle priority and safety applications. The resulting cross-technology system will enable demonstration vehicles to traverse a connected city corridor and utilize DSRC and cellular to trigger green light priority that responds to the position and route of the vehicles.

The following summarizes the components of the overall solution planned for demonstration:

a. Basic security and communication
   I. Demonstration of basic security infrastructure
   II. Demonstration of technology agnostic to DSRC or cellular
   III. Demonstration of simple non-secure pre-emption (DSRC and cellular)
   IV. Demonstration of certificate based, authorized pre-emption (DSRC and cellular)
   V. Demonstration of certificate revocation (Intersection)
   VI. Demonstration of intersection to send signal and phase information to vehicle (Green / Yellow / Red and pedestrian crosswalk status)
   VII. Demonstration of practical workflow for secure module replacement
b. Emergency vehicle preemption, freight priority, transit priority
   I. Demonstration of cellular transmission of vehicle route to infrastructure (cellular features)
   II. Demonstration of simple freight priority (DSRC and cellular)

III. Demonstration of specialized routing based on freight classification (DSRC and cellular)
IV. Demonstration of pre-authorized cargo-based freight priority (cellular)

C. Green extension and safety
I. Demonstration of pedestrian and bicycle presence data sharing from infrastructure to connected vehicles (Pedestrian Safety Messages)
II. Demonstration of infrastructure to force or extend green lights based on incoming preemptive or priority vehicles

5 References

[1] William Whyte, André Weimerskirch, Virendra Kumar, and Thorsten Hehn, "A security credential management system for V2V communications", IEEE Vehicular Networking Conference, 2013.

[2] Iteris, Inc. (2016) Connected Vehicle Reference Implementation Architecture. [Online]. http://www.iteris.com/cvria/

[3] J. Wang et al., "Vehicle-to-vehicle communications: Readiness of V2V technology for application", National Highway Traffic Safety Administration, Washington, DC, DOT HS 812 014, 2014.

[4] DSRC Technical Committee, "Dedicated Short Range Communications (DSRC) Message Set Dictionary Support Page", SAE International, Standard J2735_201603, 2016.