Detection of Interference in Dedicated Short-Range Communications Networks

Quinn Ramsay, Hamed Noori, David G. Michelson
The University of British Columbia, Vancouver, BC, Canada V6T 1Z4

The foundation for the next generation of Intelligent Transport Systems (ITS) is being built upon several new and emerging platforms including Connected Vehicle (CV), Automated Vehicle (AV), Smart Roadway Infrastructure (SRI) and Big Data (BD) technologies and systems that use wireless communications, including 5.9 GHz Dedicated Short-Range Communications (DSRC), to facilitate the exchange of data messages and control information. Vehicle-to-Vehicle (V2V) connectivity allows equipped vehicles to share information, in real-time, with other equipped vehicles through a Basic Safety Message (BSM), enabling enhanced decision making with both safety and mobility benefits. Vehicle-to-Infrastructure (V2I) connectivity allows SRI (e.g., smart traffic signals, smart roadway signage, and smart rail grade crossings) to exchange information, e.g., Signal Phase and Timing (SPaT) information, in real-time, with equipped vehicles and mobile devices through a Generic Transfer Message (GTM). For V2I connectivity, a Basic Infrastructure Message (BIM) is being developed to enable additional safety and mobility benefits. The Society of Automotive Engineers (SAE) SAE J2735 message standard is designed to support interoperability among DSRC applications through the use of standardized message sets, data frames and data elements and supports both V2V and V2I scenarios.

As CV systems are deployed across North America, tens of millions of vehicles will be broadcasting V2V BSMs while tens of thousands of roadside units will be broadcasting V2I BIMs and variants. Along any given section of roadway, each vehicle will be "listening" for, processing, and potentially acting on the information received from these messages. Similarly, the corresponding roadside units in these sections of roadways will also be listening and processing information from these messages. For CVs to function correctly, users must be able to "trust" the messages being received. This translates into a requirement to authenticate thousands of data messages received 10 times per second and verify that they are unaltered and coming from a trusted source. This requires the application and implementation of cryptography, cybersecurity, and privacy-by-design principles and systems. While considerable resources have been devoted to developing a Security Credential Management System (SCMS) that can fill this need, the problem of ensuring the integrity of the wireless spectrum, i.e., detection and reporting of possible RF interference to regulators, has been almost completely ignored.

Here, we report on our efforts to devise a scheme for detection and reporting of RF interference in the DSRC band that will satisfy the cost and scalability requirements associated with such a large deployment. The short-range nature of DSRC networks makes it necessary for the network itself to perform the monitoring and detection function. Although some enterprise-class wireless LAN access points incorporate dedicated interference measurement receivers, we have found that this may not be necessary. Built in features of the IEEE 802.11p standard allow one to distinguish between packets that were correctly received and signals that did not result in correctly received packets. Simple logic allows one to infer whether the latter is due to congestion or interference. The principal limitation to this scheme is the sensitivity of the detection mechanism. Finally, we have determined that the SCMS proposed by the US Department of Transportation (DOT) has sufficient flexibility and capacity to relay spectrum misbehavior messages to a central authority in addition to its role in reporting bad certificates. The result fills in an important remaining gap before CV technology sees widescale deployment.