Hacking the Fast Lane: Security Issues with 802.11p, DSRC, and WAVE

A White Paper for Black Hat DC 2011

Rob Havelt and Bruno Oliviera

January 7, 2011

Abstract

The new 802.11p standard aims to provide reliable wireless communication for vehicular environments. The P802.11p specification defines functions and services required by Wireless Access in Vehicular Environments (WAVE) conformant stations to operate in varying environments and exchange messages either without having to join a BSS or within a BSS, and defines the WAVE signaling technique and interface functions that are controlled by the 802.11 MAC.

Wireless telecommunications and information exchange between roadside and vehicle systems present some interesting security implications. This talk will present an analysis of the 802.11p 5.9 GHz band Wireless Access in Vehicular Environments (WAVE) / Dedicated Short Range Communications (DSRC), Medium Access Control (MAC), and Physical Layer (PHY) Specifications of this protocol. We will present methods of analyzing network communications, and potential security issues in the implementation of the protocol in practical environments such as in toll road implementations, telematics systems, and other implementations.

Overview

Vehicle Ad-Hoc networks (VANET) are nothing new. The basic concept of a VANET is also fairly straightforward. Take a widely adopted and relatively low cost wireless technology (WiFi/WLA N) used to connect mobile devices together and to the Internet and add that to vehicles. Of course, if it were truly that straightforward, we would likely already have the self navigating conveyances only seen in sci-fi movies already, fuel conservation would not be an issue, nor would delays in morning or evening commutes due to traffic. If it were truly that straightforward, the nation's roadways would be among the safest and most effective way to travel. However its not exactly that easy. There are some unique challenges involved in deploying wireless networking in vehicular environments. Those challenges have been addressed in many different ways over the years.

The history of the use of radio and infrared communication for vehicle to roadside and vehicle to vehicle communication is long and storied. The concept of roadside automation, i.e. the use of communication technologies to make roadside travel safe, efficient, and friendly for the environment, was exhibited as early as the 1939 World's Fair. The General Motors exhibit "Futurama" envisioned the state of Intelligent Transportation Systems (ITS) twenty years in the future.

Later, since at least the 1960's actual radio based automation systems were developed and demonstrated. However it wasn't until the late 1990's that a total game changer happened when the Federal Communication Commission in the United States allocated a 75MHz band in the 5.9GHz range to Dedicated Short Range Communications (DSRC) technology. In 2000 the ASTM International established a working group to develop requirements for the DSRC standards. The first radio technology adopted for the DSRC range was the 802.11a wireless networking standard. Four years later a working group would be started to work on the 802.11p amendment to the standard, as well as the Wireless Access in Vehicular Environments (WAVE) standards based on the existing ASTM Vehicle Safety Communication (VSC) standard. The standards for 802.11p and multiple components of WAVE were recently ratified, and as a result, we can expect to see a proliferation of these technologies in the near future.

Services and Applications

There are many services and applications for VANET's, and they are generally classified with two categories – safety applications and non-safety/commercial.

Typical safety applications would involve:

- Assisted collision avoidance
- Forward obstacle detection and avoidance
- Lane departure warning
- Automated variable message signs
- Turn accident warning

Typical non-safety and commercial applications would involve:

- Roadway toll collection
- Traffic management
- Parking lot payment
- Traveller information support
- Freight and cargo management

WAVE standards overview

DSRC communications using 802.11p and WAVE are comprised of several standards. The following is an overview of these standards and the portions of the protocols that they govern.

Protocols	Standards		OSI Layer
WAVE PHY and MAC	IEEE 802.11p	PHY and MAC functions for an IEEE 802.11p device to function in a vehicular environment.	layer 1 and 2
Multichannel operation	IEEE 1601.4	Enhancements to the 802.11p MAC to support multichannel operation	layer 2
WAVE Networking Services	IEEE 1609.3	addressing and routing	layer 2, 3, and 4
WAVE Resource Manager	IEEE 1609.1	defines an application that allows communication from remote sites to onboard units (OBU)	N/A
WAVE Security Services	IEEE 1609.2	Secure messaging format and processing	N/A

Table 1 - WAVE Standards

Security Model

The IEEE 1609.2 standard defines a secure messaging format based on a "defence in depth" strategy. It involves a complicated public key infrastructure (PKI) with the government as the root certificate authority (CA). Due to the overall complexity and comprehensiveness of the security model, its effectiveness will depend heavily upon the implementation.

The overall security model aims to provide: Security, Anonymity, and Trust.

Security

Security services via PKI aim to provide authentication for messages (signatures), and encryption of confidential data, In order to do this, messages must be short and interactions must be fast. To achieve this for broadcast, high priority, messages a new compact certificate format and public key algorithm with short keys are used.

Trust Model

In vehicle safety applications the operator is consider un-trusted and applications should be isolated from the operator. In public safety applications, the operator is trusted. For e-Commerce applications, conventional trust models are used.

Anonymity

Things such as IP addresses, MAC Addresses, and Certificates can all be used to track and end node. Measures are put into place to anonymize and in some cases randomize these identifiers.

Protocol Analysis

In a paper published at the 6th Karlsruhe Workshop on Software Radios entitled "IEEE 802.11p Transmission Using GNURadio" Fuxjagaer et al. Show "a method to rapidly prototype a fully standard-compliant OFDM frame encoder using the GNURadio framework and the Universal Software Radio Peripheral (Version 2)."

"The encoder generates OFDM frames in digital complexbase-band representation and uses the USRP Version 2 as digital-to-analog front-end to up-convert and transmit them in the 5.9GHz band that has been allocated for dedicated short range communication (DSRC) for vehicular applications."

This is convenient for testing protocol robustness in real world applications, as well as performing security analysis. Our presentation uses the work done here to analyze some non-safety/commercial applications of the protocol.

References

"VANET: Vehicular Applications and Inter-Networking Technologies" editors Hannes Hartenson and Kenneth Laberteaux – Wiley 2010

"Vehicular Networks: From Theory to Practice" Stephan Olariu, Michele C. Weigle - Chapman & Hall/CRC Computer & Information Science Series

IEEE 802.11p Transmission Using GNURadio - P. Fuxjäger∗, A. Costantini∗†, D. Valerio∗, P. Castiglione∗, G. Zacheo∗, T. Zemen∗, F. Ricciato∗† - http://userver.ftw.at/~valerio/files/wsr10.pdf

A SECURE VANET MAC PROTOCOL FOR DSRC APPLICATIONS, Yi Qian, Kejie Lu, and Nader Moayeri - http://www.antd.nist.gov/pubs/Yi-Paper1.pdf

Standards: WAVE / DSRC / 802.11p, Dr. Michele Weigle - http://www.cs.odu.edu/~mweigle/courses/cs795-s08/lectures/5c-DSRC.pdf

Novel Issues in DSRC Communication Radios, Yasser L. Morgan - http://www.ewh.ieee.org/reg/7/canrev/cr63/IEEECanadianReview_no63.pdf

SAE International – DSRC Implementation Guide -
http://www.sae.org/standardsdev/dsrc/DSRCImplementationGuide.pdf

About Trustwave

Trustwave is the leading provider of on-demand and subscription-based information security and payment card industry compliance management solutions to businesses and government entities throughout the world. For organisations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its flagship TrustKeeper® compliance management software and other proprietary security solutions. Trustwave has helped thousands of organisations—ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers—manage compliance and secure their network infrastructure, data communications and critical information assets. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, Africa, Asia and Australia. For more information, visit https://www.trustwave.com.

About Trustwave SpiderLabs

SpiderLabs is the advanced security team within Trustwave focused on incident response, ethical hacking and application security testing for our premier clients. The team has performed hundreds of forensic investigations, thousands of ethical hacking exercises and hundreds of application security tests globally. In addition, the SpiderLabsrResearch team provides intelligence through bleeding-edge research and proof of concept tool development to enhance Trustwave's products and services. For more information, visit https://www.trustwave.com/spiderLabs.php.