



# “Verify-on-Demand” - A Practical and Scalable Approach for Broadcast Authentication in Vehicle-to-Vehicle Communication

2011-01-0584

Published  
04/12/2011

Hariharan Krishnan  
General Motors Company

Andre Weimerskirch  
escrypt Inc.

Copyright © 2011 SAE International

doi:[10.4271/2011-01-0584](https://doi.org/10.4271/2011-01-0584)

## ABSTRACT

In general for Vehicle-to-Vehicle (V2V) communication, message authentication is performed on every received wireless message by conducting verification for a valid signature, and only messages that have been successfully verified are processed further. In V2V safety communication, there are a large number of vehicles and each vehicle transmits safety messages frequently; therefore the number of received messages per second would be large. Thus authentication of each and every received message, for example based on the IEEE 1609.2 standard, is computationally very expensive and can only be carried out with expensive dedicated cryptographic hardware. An interesting observation is that most of these routine safety messages do not result in driver warnings or control actions since we expect that the safety system would be designed to provide warnings or control actions only when the threat of collision is high. If the V2V system is designed to provide too frequent warnings or control actions, then the system would be a nuisance to the driver. Therefore it is reasonable to define an approach where messages are first processed and then authenticated using verification on-demand. In this paper we describe such an approach and discuss its implementation for V2V safety system. It is shown that Verify-on-Demand (VoD) is a practical and scalable approach for broadcast authentication in V2V safety communication while conforming to the IEEE 1609.2 standard.

## INTRODUCTION

In Vehicle-to-Vehicle communication (V2V), vehicles equipped with a short range wireless transceiver and a Global Positioning System (GPS) receiver regularly exchange safety-related information including time, location, and further vehicle status data amongst neighboring vehicles [1]. The communication, in general, is done as a single-hop, periodic broadcast although multi-hop routing may also be used to extend the geographical range and region of message reception [2]. It is expected that periodic vehicle broadcast of safety information would be around 10 messages per second with an average message size about 200 bytes [3]. The required transmission range of safety messages is approximately 300 meters for V2V safety communication applications. It is expected that V2V would employ the wireless communication protocol based on IEEE 802.11p Dedicated Short Range Communications (DSRC) in the 5.9 GHz band [4], although other short range wireless protocols may also be used.

Security is a core issue for V2V safety communication [5]. In particular, vehicles need to be able to authenticate that a received message originated from a properly certified vehicle and that the message was not manipulated on its way between the sender and receiver vehicles. It is assumed that there is a Public Key Infrastructure (PKI) deployed and the messages are authenticated using digital signatures in accordance with the IEEE 1609.2 standard specification [6]. IEEE 1609.2 describes a message format of secured safety messages in a V2V network. IEEE 1609.2 suggests an API and message format for using security features based on Elliptic Curve

Digital Signature Algorithms (ECDSA) [8] and certificates, namely attaching a digital signature and a certificate, a certificate digest or a certificate chain (if a hierarchical PKI is used) with each message. While this solution is robust there are concerns regarding Over-The-Air (OTA) bandwidth overhead and run-time performance in a V2V safety application setting. Network simulations [10] suggest that a certificate once or twice per second and a digest otherwise is sufficient in order to reduce the OTA bandwidth due to certificate size.

V2V safety applications require that vehicles are able to verify a large number of messages at short delay. As the penetration of V2V vehicles increases, the number of received messages per second could become very large. Estimation for the number of messages to verify is potentially beyond 1,000 per second, whereas a delay of 10-20 ms due to security overhead is acceptable. Attaching a digital signature and a certificate to each message impose a considerable amount of OTA bandwidth overhead as well as high demands in the computing device's resources. In particular, a customized application-specific elliptic curve cryptographic processor is required to handle the computational load. Such an additional custom-specific co-processor might be commercially infeasible and hinder V2V deployment. The main requirements for a proper security protocol are efficiency, in particular low computational and OTA bandwidth overhead, as well as small latency due to security overhead and scalability. The security protocol is expected to run on embedded computer that can be found in vehicles today.

For V2V safety applications that require verification of a large number of messages per second, we look at further solutions. In general, security authentication is performed for every received wireless message by conducting verification for a valid digital signature, and only messages that have been successfully verified are processed further. However, as stated earlier, verifying digital signatures consumes a significant amount of the share of the automotive processor [7]. Thus verification of each and every received message, for example based on the IEEE 1609.2 standard, is computationally very expensive and cannot in general be carried out even with specialized hardware. An interesting observation is that, most of these periodic safety messages will not result in driver warnings since we expect that the vehicle safety system would be used to provide warnings only when the threat of collision determined by vehicle safety applications is high. Therefore, we define an approach where messages are first processed and then verified only on-demand. The solution is more efficient regarding running-time and CPU overhead and is especially suited for V2V safety applications and requires no additional security-specific computing processor.

In this paper, we first introduce the V2V safety communication system. Next, we describe the conventional Verify-and-Then-Process approach normally used for broadcast authentication in V2V safety communication. Then we describe a novel approach called Verify -on-Demand (VoD) which provides practical and scalable broadcast authentication for V2V safety communication. The details of the security implementation on a 400 MHz processor, analysis of its pros and cons will be discussed. System implementation and supporting data are used to conclude that, for V2V safety applications, 1609.2 ECDSA with VoD (i.e., verification of prioritized, application-filtered threats) achieves the desired performance.

## V2V SAFETY COMMUNICATION AND MESSAGE AUTHENTICATION

### NOMINAL V2V SAFETY COMMUNICATION SYSTEM

Figure 1 shows a simple nominal architecture of a V2V safety communication system. The Sensor Data Handler (SDH) processes Host Vehicle (HV) GPS data such as vehicle location, time, etc. and also the vehicle-bus data such as speed, acceleration, etc. The DSRC radio periodically (for e.g. 10 times per second) transmits and also receives safety broadcast data required for vehicle safety communication. Messages received from Remote Vehicles (RVs) by the DSRC Radio are then processed by the Wireless Message Handler (WMH). Safety applications and algorithms within the Threat Processing & Threat Arbitration module evaluate the collision or other safety threat level of the HV with other communicating RVs in its vicinity. If a certain vehicle safety threat threshold is exceeded, determined by the Threat Level being above a calibrated threshold, then this module issues a threat notification via the Driver Notification module, and the driver of the HV is made aware of the safety threat via appropriate driver vehicle interfaces inside the vehicle (e.g. haptic, visual, auditory warnings).

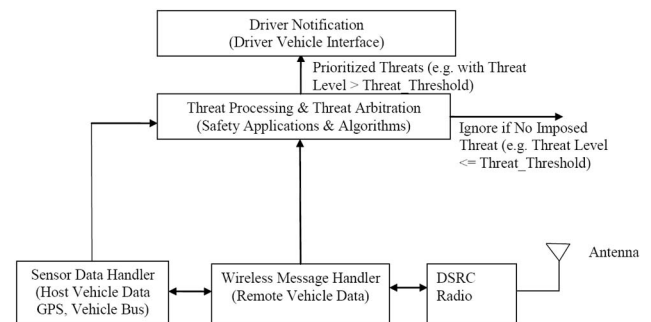


Figure 1. Nominal Architecture of V2V Communication System.

## MESSAGE BROADCAST AUTHENTICATION WITH DIGITAL SIGNATURES

In V2V, received safety messages have to be authenticated. The straightforward method of providing message broadcast authentication is to implement digital signatures. The sender signs the safety message and broadcasts the signature along with the message. Receivers can then verify the message. Before message verification, the receivers need to be able to get a hold of the sender's certificate [6, 7]. A brief description of the protocol parameters and expected performance is provided next.

### Protocol Parameters and Structure

- **H:**  $H(m)$  describes the hash of message  $m$  computed using the Secure Hash Algorithm (SHA).  $|H|$  is the hash length of  $H$ , in case of SHA-256 we have  $|H| = 32$  bytes [9].
- **Sig:**  $\text{Sig}(m, A_{SK})$  describes the signature of a message  $m$  with secret key  $A_{SK}$ . In ECDSA A-256 the signature length of  $\text{Sig}$  is  $|\text{Sig}| = 64$  bytes [8].
- **TS:** describes the 6-byte time-stamp to avoid replay attacks.
- Safety messages may include the certificate digest or certificate as part of the data packets [6]. Certificate digest in an eight byte hash of the certificate, so it is more bandwidth efficient. It is a short reference to the certificate but is not of use unless a receiver has already received and cached the certificate. Thus, one model is to transmit certificates every second and use certificate digest for messages in-between [10].
- When certificates are sent in a piggy-back fashion to form data-certificate packets, we have the following data structure:

Cert. (117 bytes)	$m$	$\text{Sig}_A(H(m)  \text{TS})$ (64 bytes)	TS (6 bytes)
----------------------	-----	---	-----------------

- Data packets structure for safety messages that include a certificate digest is as follows:

Cert. Digest (8 bytes)	$m$	$\text{Sig}_A(H(m)  \text{TS})$ (64 bytes)	TS (6 bytes)
---------------------------	-----	---	-----------------

- **Ver:**  $\text{Ver}(m, s, A_{PK})$  describes the verification process of a signature  $s$  against message  $m$  and public key  $A_{PK}$ . The result is either 'success' or 'failure'.

### Expected Performance

ECDSA-256 and SHA-256 are used to compute digital signatures [6]. The computational overhead due to hashing is

negligible for the considered message sizes. The time delay is computed as the sum of computation time at the sender and receiver side. OTA overhead per message consists of the digital signature but no additional network layer overhead since signatures are sent together with the message. As stated earlier, note that additional overhead is introduced by the certificate distribution compared to certificate digest distribution. The security overhead and expected performance measures for a 400 MHz computing platform are shown in [Table 1](#).

**Table 1. Message Authentication with Digital Signatures**

Over-the-air overhead	70 bytes per message + 8 bytes per message (certificate digest) or 117 bytes per message (certificates)
Computations for sender per message	$H(m) + \text{Sig} \approx 6$ ms
Computations for all receivers per message	$H(m) + \text{Ver} \approx 23$ ms
Maximum Signature Generations per second	$\approx 166$
Maximum Signature Verifications per second	$\approx 43$

For V2V safety communications, it is clear from [Table 1](#) that the required transmissions (e.g. 10 messages per second) can all be signed before being broadcasted without much computational complexity. However, only a small fraction of received messages may be authenticated in a 400 MHz computing platform (i.e. only from 4 RVs at the rate of 10 messages per second per vehicle). Thus message authentication is a significant and overwhelming challenge in V2V communication, which is being addressed in this paper.

## VERIFY-AND-THEN-PROCESS

As stated earlier, broadcast message authentication is of primary importance for vehicle safety communication. In particular, vehicles need to be able to authenticate that a message originated from a properly certified vehicle and that the message was not manipulated on its way between the sender and receiver vehicles. In order to accomplish the above, the message signature verification functionality may be performed at the Security Module, as shown in [Figure 2](#) with the primary aim of performing broadcast authentication

and filtering bogus messages (i.e. those messages with the correct format but invalid signature or authentication tag). The verify-and-then-process approach first verifies the signatures of all received safety messages for trustworthiness. If the signature verification is successful, then the message is processed further. Otherwise the message is a bogus message and hence discarded. There is a delay in initiating message threat processing due to time taken for verification.

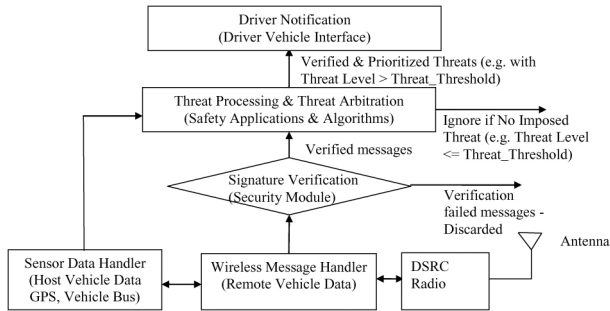


Figure 2. Verify-And-Then-Process Flow.

Thus only verified messages are processed further. If the Threat Processing & Threat Arbitration module determines that an RV message causes the safety threat level to be larger than a calibrated threshold (representing a potential threat), Driver Notification provides the needed information to the driver of the HV in the form of safety warning / notification in the most appropriate and intuitive manner. The Threat Processing & Threat Arbitration module typically works on a message-by-message basis when evaluating the safety threat level caused by an RV's V2V safety message. Driver Notification only passes a warning to the vehicle driver after evaluating a potential safety threat level. Also, refinements may be used in Driver Notification so that the driver is not repeatedly annoyed by the safety warnings or notifications, e.g. Driver Notification might decide to suppress warnings to the driver even in the case of a continuing potential threat level if an earlier warning was just provided to the driver.

From Table 1, it is quite clear that verifying digital signatures is computationally very expensive. Typical requirement of vehicle safety communication is that each vehicle broadcasts safety messages (periodically) about 10 times per second, and up to a transmission range of about 300 m. It should therefore be clear that, as the penetration of V2V vehicles increases, the number of received messages per second could be very large and would exceed 1000 messages per second. Thus verification of each and every received message, for example based on the IEEE 1609.2 standard, would consume all of the share of the automotive processor and cannot in general be carried out, even with specialized hardware, at low cost.

We therefore conclude that the verify-and-then-process approach for broadcast message authentication based on the IEEE 1609.2 standard does not provide the scalability needed

for practical automotive implementations. Novel methods for message authentication in V2V are a necessity to enable deployment in the near-future.

## VERIFY-ON-DEMAND

The verify-and-then-process approach, described in the previous section, for broadcast authentication is based on the underlying assumption that all received safety messages need to be verified before they are processed by the application layer. An interesting and powerful observation is that, most of these periodic safety messages will not result in driver warnings or control actions since we expect that the vehicle safety system would be designed to provide warnings or control actions only when the threat of a collision determined by vehicle safety applications is high. Therefore it is reasonable to define an approach where messages are first processed and then verified only on-demand. VoD is a novel approach that provides practical and scalable broadcast authentication for vehicle safety communication.

Assuming that only messages that evaluate to a safety threat level larger than a calibrated threat threshold (representing a potential threat) have an actual impact to a vehicle's safety level, it is reasonable to only verify those received safety messages that result in a safety threat level above that threshold value. Note that this approach does not affect the signature generation. All messages are still signed before being broadcasted.

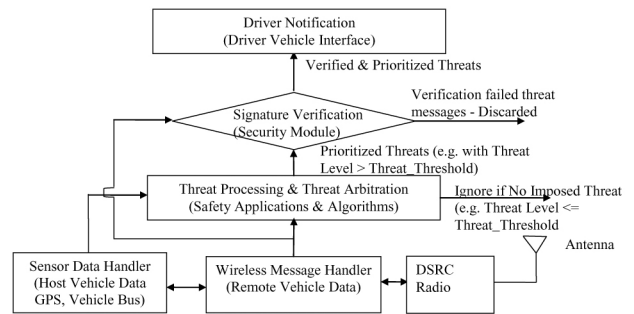


Figure 3. Verify-On-Demand Flow.

As shown in Figure 3, VoD can be implemented by introducing the signature verification functionality at the Security Module in-between the Threat Processing & Threat Arbitration and the Driver Notification modules. The Threat Processing & Threat Arbitration module evaluates the safety threat level caused by each wireless safety message received from RVs. Only for messages that evaluate to a safety threat level larger than a calibrated threshold, the Security Module initiates on-demand signature verification. Thus on-demand signature verification is required only on safety messages that result in a safety threat level that demands warnings or control actions. It waits for a verification to be completed

and, when successful, forwards prioritized threats to Driver Notification.

For the vehicle safety communication system, Threat Processing & Threat Arbitration is based on the current safety message received from remote vehicles. Current processing does not use past wireless data. Therefore for periodic messages, only the recent wireless safety message from each remote vehicle may need to be buffered to enable VoD. The life-time of the buffer can be set to the maximum processing delay expected. If there are a-periodic event-driven safety messages, then those wireless safety messages may need to be buffered as well.

Note that the security verification functionality is put in-between two application processing blocks such that separation of concerns is removed and cross-layer architecture is introduced. Therefore the implementation of this approach tends to be different than in the verify-and-then-process approach. VoD should be seen as a practical approach to broadcast authentication for vehicle safety communication since digital signature verification is computationally very expensive and there are a large number of messages in the system but only very few of those raise safety warnings or control actions during typical driving conditions. This basic principle can be used with existing security protocols and standards, such as the IEEE 1609.2, right away while the research continues into the design of other efficient authentication protocols for vehicle safety communication. The approach also allows implementation of V2V systems today on existing automotive grade (i.e. 400 MHz processor) hardware platforms, and then over time one may chose to verify more and more messages as the computational hardware platform becomes faster.

V2V safety systems should surely not be designed to raise a large number of safety notifications in a short span of time to the driver. Otherwise the driver will be annoyed by the system. If the safety system is designed with the assumption that at most 10 new messages in a given second will raise safety warnings of importance to the driver, even that will stretch the requirements for VoD. Therefore it is reasonable to expect that VoD would need to conduct at most 10 digital signature verifications per second. In comparison to the overall number of received messages, which could exceed 1,000 messages per second, this is a significant reduction of the signature verification load compared to the standard verify-and-the-process approach. Again this approach does not affect the signature generation. All safety messages are still signed before being broadcasted.

Finally, we consider the security implications of such an approach. Let us assume that an attacker has complete knowledge of all involved decision algorithms in this approach and has full control over a DSRC radio including the secret key data. The attacker's goal is to generate

malicious safety messages and sign them with valid digital signature such that there is no evidence of misbehaving. In such a case, the receiver will definitely choose the safety messages that impose a safety threat for verification and only accept the safety messages that pass verification. Such attacks need non-cryptographic methods of detection in every security approach that is employed for V2V safety communications.

We also consider denial-of-service (DoS) attacks. In general, V2V communication system can easily be overwhelmed by broadcasts of forged messages that impose a security threat and are therefore scheduled for signature verification. Thus, DoS can always easily be mounted regardless of the deployed broadcast authentication approach employed for vehicle safety communication. However, DoS attacks are easily detected by the system since verification of such messages will fail authentication. In such a situation, the system can inform the driver of a potential DoS attack and make the driver aware of such a situation.

Table 2 summarizes the pros and cons of both approaches.

**Table 2. Pros and Cons of Verify-and-then-Process and VoD**

	<i>Verify-and-then-Process</i>	<i>Verify-on-Demand (VoD)</i>
<b>Pros</b>	<ul style="list-style-type: none"> <li>No special security assumptions need to be made for the implementation.</li> <li>Clear separation of security and application layer.</li> </ul>	<ul style="list-style-type: none"> <li>Relieves the security module from its heavy load of verification.</li> <li>Allows flexible balancing of verification load.</li> <li>Stays easily compatible with future generation implementations and allows quick deployment.</li> </ul>
<b>Cons</b>	<ul style="list-style-type: none"> <li>High processing burden.</li> </ul>	<ul style="list-style-type: none"> <li>The approach introduces a cross-layer security design assumption on the application layer.</li> </ul>

## IMPLEMENTATION IN V2V TEST-BED

The Crash Avoidance Metrics Partnership-Vehicle Safety Communications 2 (CAMP-VSC2) Consortium initiated, in December 2006, a 3-year collaborative effort in the area of wireless-based safety applications under the Vehicle Safety Communications - Applications (VSC-A) Project [10]. The VSC-A project was completed in December, 2009. Under the project, a vehicle test bed (this will now be referred to as the test bed in the remaining text of this document) was developed to serve as a prototype platform for the V2V system. The test bed was used to validate system specifications and performance tests that were developed as part of the VSC-A Project. The test bed also served as a flexible platform for testing various positioning, communication, and security solutions in a real-world setting and in safe and staged crash-scenario configurations to ensure the effectiveness of the applications.

Among other things, this project also focused on security for V2V safety messages with a main focus on efficient broadcast authentication of safety messages. Security protocols were implemented to run on the On-Board Equipment (OBE), which housed a 400 MHz processor. It was concluded that, for the VSC-A safety applications, 1609.2 ECDSA with VoD (i.e., verification of prioritized, application-filtered threats) achieved the desired performance. Therefore, this is the protocol that was used for the system objective testing in the project. Objective testing confirmed that ECDSA with VoD functioned properly under all test conditions for the VSC-A safety applications.

### V2V TEST-BED

This section summarizes the test bed design and implementation. For a more detailed description, please refer to [10]. Figure 4 shows the block diagram developed for the V2V system test-bed. The following V2V safety applications were developed and implemented as part of the test-bed:

#### Emergency Electronic Brake Lights (EEBL)

The EEBL application enables an HV to broadcast a self-generated emergency brake event to surrounding RVs. Upon receiving such event information, the RV determines the relevance of the event and provides a warning to the driver, if appropriate. This application is particularly useful when the driver's line of sight is obstructed by other vehicles or bad weather conditions (e.g., fog, heavy rain).

#### Forward Collision Warning (FCW)

The FCW application is intended to warn the driver of the HV in case of an impending rear-end collision with an RV ahead in traffic in the same lane and direction of travel. FCW

is intended to help drivers in avoiding or mitigating rear-end vehicle collisions in the forward path of travel.

#### Blind Spot Warning+Lane Change Warning (BSW+LCW)

The BSW+LCW application is intended to warn the driver of the HV during a lane change attempt if the blind-spot zone into which the HV intends to switch is, or will soon be, occupied by another vehicle traveling in the same direction. Moreover, the application provides advisory information that is intended to inform the driver of the HV that a vehicle in an adjacent lane is positioned in a blind-spot zone of the HV when a lane change is not being attempted.

#### Do Not Pass Warning (DNPW)

The DNPW application is intended to warn the driver of the HV during a passing maneuver attempt when a slower moving vehicle, ahead and in the same lane, cannot be safely passed using a passing zone which is occupied by vehicles with the opposite direction of travel. In addition, the application provides advisory information that is intended to inform the driver of the HV that the passing zone is occupied when a vehicle is ahead and in the same lane and a passing maneuver is not being attempted.

#### Intersection Movement Assist (IMA)

The IMA application is intended to warn the driver of an HV when it is not safe to enter an intersection due to high collision probability with other RVs. Initially, IMA is intended to help drivers avoid or mitigate vehicle collisions at stop-sign controlled and uncontrolled intersections.

#### Control Loss Warning (CLW)

The CLW application enables an HV to broadcast a self-generated, control, loss event to surrounding RVs. Upon receiving such event information, the RV determines the relevance of the event and provides a warning to the driver, if appropriate.

The test-bed modules are composed of support and application functions. The support functions interface to external equipment and calculate data to support the V2V application modules and engineering Driver-Vehicle Interfaces (DVI)s. Since VoD is used mainly to determine the authenticity of received OTA messages, here we focus our discussion on the Wireless Message Handler (WMH) and Security Module (SM). WMH constructs and sends HV OTA messages and processes received RV OTA messages. V2V safety messages are defined in the Society of Automotive Engineers (SAE) J2735 Basic Safety Message (BSM) formats [11]. If security is enabled, WMH interfaces to the SM to generate signatures for transmitted messages and verify signatures for received messages.

Figure 4 shows the V2V test-bed with six safety applications. The application modules evaluate potential categorized safety threats based on the data and inputs from the support modules. The warning algorithm categorizes the safety output threat level of each application to be in one of the following threat states: NONE, DETECTED, INFORM or WARN. If the threat state is NONE, it implies no safety threat and so no driver notification is necessary. If the threat state is DETECTED, it implies Target Classification (TC) has determined that an RV is in a certain region of interest that resulted in the corresponding application threat processing, however, application threat processing evaluated to no safety threat and so no driver notification is necessary. If the threat state is INFORM, it implies that the application has determined a safety threat that may warrant a driver notification to caution as necessary. If the threat state is WARN, it implies that the application has determined an urgent safety threat that would warrant a driver warning and/or control action. Threat Arbitration (TA) prioritizes the concurrent threats produced by the applications. It uses the threat state of the applications as well as metrics that define crash severity for prioritization. Threat Priority (0) is the highest priority; Threat Priority (1) is the next one, and so on.

- After all the messages have been verified, write the verification results to shared memory and signal or notify TA

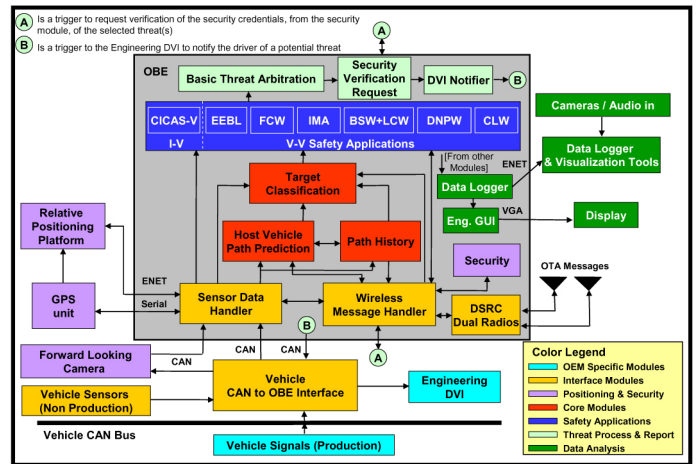


Figure 4. V2V System Test-Bed Block Diagram.

Finally, TA will only forward prioritized threats to DVI notifier (for driver warnings or control actions) only if the corresponding RV messages have successfully passed security verification.

## VOD IMPLEMENTATION

In VoD security implementation, received messages are first evaluated by applications and prioritized by TA (see Figure 4). If the output threat state of an application exceeds a predefined safety threshold (i.e. INFORM level), the signature of the received message that caused this safety alert level is verified. If the threat state does not exceed this predefined threat threshold, the message is discarded. This is shown in Figure 4 with a Security Verification Request.

Implementation details of VoD in the test-bed are provided below. Upon receiving an OTA message, WMH will:

- Decode the message using the decoding library, if the SAE J2735 message format is being used
- Parse the message (SAE J2735 format), perform validity checks, unpack, and scale the data
- Update an existing RV record or create a new record with the received data along with calculated Packet Error Rate (PER), latency, and security statistics
- Notify or signal the corresponding application process to trigger its execution
- Provide SM with the WMH assigned sequence number for the message for use in VoD security processing

When VoD security is being used, WMH will receive a signal or notification from the TA when messages must be verified (see Figure 4, Security Verification Request). Upon receiving such a request, WMH will:

- Read TA's shared memory to determine the WMH sequence number(s) of the message(s) to be verified and call SM to verify each message

We now discuss certificate queuing in conjunction with VoD implementation. If a signed OTA message is received and security is enabled, WMH will buffer the message and check the security approach. If the security approach is VoD, WMH sends a “certificate verify” request to SM if the security contents of the message contain a certificate, and sends the unverified OTA message data for further application processing. WMH provides a sequence number to be used for subsequent verify requests, and SM stores the number with the message. SM may choose one of the following approach to verify certificates: (1) Verify certificates as and when received, or (2) Store all received certificates without verifying these certificates. Only if a message is triggered for verification, then the previously stored certificate is verified. Storing received certificates is only necessary if certificates are not attached to each message. TA prioritizes the threat warnings from application modules. When VoD security authentication is being used, TA requests verification of signatures for messages that result in driver warning. Upon receiving a subsequent VoD verify request, WMH finds the message in its buffer based on the sequence number input and sends a verify request to SM. Upon receiving a response from SM, WMH provides the results to TA. TA only forwards prioritized threats that have passed security verification to DVI Notifier (for driver warnings or control actions).

## IMPLEMENTATION PERFORMANCE

IEEE 1609.2 ECDSA security protocol with verify-and-then-process and VoD were implemented on a car-PC (a standard PC running at 2.4 GHz) and on-board the WAVE Safety Unit (WSU) (a 400 MHz industry computing platform [12]). The implementation for the WSU consists of the same source code with platform-specific assembly optimized cryptographic operations. Therefore, it is possible to use the car-PC platform with its variety of development tools to develop the SM and then to cross-compile it to the WSU platform. Performance measurements of the SM running on the WSU clearly show that the IEEE 1609.2 ECDSA protocol is too resource-demanding to run in software. This also holds for the powerful car-PC. Performance numbers for the SM running on-board the WSU are presented in [Table 3](#). Note that these are actual implementation performance measures as compared to expected performance measures shown earlier in [Table 1](#).

**Table 3. Security Protocol Performance IEEE 1609.2 ECDSA**

	<b>IEEE 1609.2 ECDSA</b>
Authentication generation (crypto only on idle system)	4.9 ms (ECC-224) / 6.6 ms (ECC-256)
Authentication generation*	6.6 ms (ECC-256)
Authentication verification (crypto only on idle system)	17.8ms (ECC-224) / 26.5ms (ECC-256)
Authentication verification*	28.5 ms (ECC-256)
CPU Load for 2 WSUs at 10 messages per second: Signing / Signing + Verifying*	8% / 34%
Latency: Avg. (no channel switching,)*	36 ms
Average OTA packet size (send certificate with each 3 <sup>rd</sup> message)	115 bytes
*CPU load and latency was measured on a system that runs safety applications	

With VoD applied to ECDSA, the implementation proved that a security protocol can be efficiently implemented in software on-board of the WSU. The performance numbers per signature generation equal those of IEEE 1609.2 ECDSA. However, the CPU load of a receiving WSU is significantly lower due to the fact that only safety messages that result in a high threat level are verified. ECDSA VoD performed well with all VSC-A safety applications and was selected for the objective test procedures. Consider the verification error rate defined as the fraction of successfully verified packets over received packets that require verification. ECDSA VoD with certificates attached to each message is designed to have a zero verification error rate.

Overall the implementation strongly indicates that a security protocol can be efficiently implemented in software on board an automotive grade platform such as the WSU, if certain conditions such as advanced queuing techniques and VoD filtering are implemented.

## VOD IMPLEMENTATION PROPERTIES FOR V2V SAFETY

- Very few of the V2V safety messages have actual safety impact that will result in driver warnings or control actions since the safety system would be designed to provide warnings only when the threat of collision is high. Therefore it is reasonable to define an approach where messages are first processed and then verified only on-demand.
- VoD only verifies received messages that result in potential impact on driver safety. It is secure since each safety message that results in driver warning or control action will certainly be verified.
- Question: In a V2V system, how many concurrent driver warnings or control actions are expected to be provided in practice? The answer to this question is, likely, one, i.e. driver workload studies and considerations would suggest that, at any moment, we present an appropriate driver warning or action corresponding to the highest priority threat produced by the V2V system.
- Question: Will this answer change if we were to add many more safety applications than the one prototyped in the test-bed and shown in [Figure 4](#)? The answer to this question is, likely, No, i.e. even if we had a much larger number of safety applications in a V2V system, the system should still select the highest priority threat for driver warning at any given moment.
- Question: In a V2V system, what is the lower bound update interval when we expect that the driver warnings to change? The answer to this question is, likely, 100 ms, i.e. based on the periodic update interval of V2V safety communication, and the system process cycle time, the highest priority threat produced by the system would not change faster than 100 ms.

- Question: In a V2V system, what is the upper bound on message verification requirements for VoD? The answer to this question follows from the previous answer. With driver warnings unlikely to change faster than 100 ms, a generous upper-bound would be 10 verifications per second. With concurrent certificate verifications, we will have at most 20 ECDSA digital signature verifications per second. With prior certificate verifications, we can reduce this to at most 10 ECDSA digital signature verifications per second.
- Question: In a V2V system, what is the upper bound on message verification time delay for VoD? Answer: VoD's message verification time delay has an upper-bound of 57 ms based on the current V2V implementation on WSU (i.e. 400 Mhz processor). This includes certificate and message digital signature verification times each having an authentication verification time of 28.5 ms (see [Table 3](#)). With prior certificate verification, this delay can be reduced to 28.5 ms (see [Table 3](#)). Optimization of the algorithms and additional processor resources would significantly reduce this delay.
- The implementation is practical since safety evaluation is based only on the current safety message received. The current safety message provides all the needed remote vehicle data for safety evaluations.
- ECDSA-VoD works as long as the application has well-defined decision logic for computing threat assessment states. The implementation of VoD requires an understanding of the application's decision logic as per design, identifying the remote vehicle(s) & message(s) that were used in the decision logic, and verifying those messages that result in threat alert on-demand (as per decision logic).
- ECDSA-VoD allows customized implementations on low-cost devices. Each automotive Original Equipment Manufacturer (OEM) can optimize their ECDSA-VoD implementation to accommodate application specific demands via proper processor capability, latency reduction, and heuristics for verifications, improved security algorithm execution, etc.
- ECDSA-VoD conforms with 1609.2 standards.

## SUMMARY/CONCLUSIONS

The VoD processing method should not be seen as an alternative to efficient authentication protocols but as an orthogonal and practical approach. The basic principle can be used with existing security protocols right away (such as ECDSA) while research continues into the design of efficient authentication protocols for V2V safety communication. The design principle of verifying messages may be summarized as follows:

- If verification of all incoming messages can be done by designing an efficient authentication protocol, then we will be able to verify all incoming messages in a timely fashion.
- If verification of all incoming messages cannot be done in a timely fashion or is computationally expensive, then we can

use the VoD approach to verify only the messages that result in potential safety threats to the host vehicle and its driver.

The VoD approach results in cross layer security design and introduces security assumptions in the application layer. However, the VoD approach allows balancing of the verification load at run-time in congested situations without any further compromise on the security properties of the V2V system. The approach also allows secure implementation of V2V applications today even on a computationally weak hardware platform, and, then over time, we may chose to verify more and more messages as the computational hardware platform becomes faster. Therefore, the VoD approach is inherently compatible to future versions and current standards and allows quick deployment today.

## REFERENCES

1. Sengupta, R., Rezaei, S., Shladover, S. E., Cody, D., Dickey, S., and Krishnan, H., "Cooperative Collision Warning Systems: Concept Definition and Experimental Implementation," *Journal of Intelligent Transportation Systems*, 11(3): 143-155, 2007.
2. Bai, F., Krishnan, H., Sadekar, V., Holland, G., and Elbatt, T., "Towards Characterizing and Classifying Communication-based Automotive Applications from a Wireless Networking Perspective," *IEEE AutoNet 2006 - The 1st IEEE Workshop on Automotive Networking and Applications*, Co-located with the 49th Annual IEEE GLOBECOM Technical Conference, San Francisco, California, December, 2006.
3. Vehicle Safety Communications Project-Final Report, USDOT HS 810 591, [http://www-nrd.nhtsa.dot.gov/departments/nrd-12/pubs\\_rev.html](http://www-nrd.nhtsa.dot.gov/departments/nrd-12/pubs_rev.html), April, 2006.
4. Wireless Access in Vehicular Environment (WAVE) in Standard 802.11 Information Technology Telecommunications and Information Exchange Between Systems, Local and Metropolitan Area Networks, Specific Requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications}, IEEE 802.1 1p/D 1.0, Feb. 2006.
5. Raya, Maxim, Papadimitratos, Panos, and Hubaux, Jean-Pierre, "Securing Vehicular Communication", *Infocom '06*, April, 2006.
6. IEEE Trial-use Standard 1609.2TM-2006, WAVE - Security Services for Applications and Management Messages, 2006.
7. Raya, Maxim and Hubaux, Jean-Pierre, "The Security of Vehicular Ad Hoc Networks", *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN'05)*, pp. 11-21, 2005.

8. ANSI, "Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", ANSI X9.62, 1998.
9. NIST, Secure Hash Standard FIPS 180-2, August, 2002.
10. Vehicle Safety Communications - Applications (VSC-A) Project Final Report, Submitted to the Intelligent Transportation Systems (ITS) Joint Program Office (JPO) of the Research and Innovative Technology Administration (RITA) and the National Highway Traffic Safety Administration (NHTSA), May, 2010.
11. SAE International Surface Vehicle Standard, "Dedicated Short Range Communications (DSRC) Message Set Dictionary," SAE Standard J2735, Rev. Nov. 2009.
12. Wireless Safety Unit (WSU) Short Range Communications Module Data Sheet, Denso, June 2010.

## CONTACT INFORMATION

Dr. Hariharan Krishnan  
Staff Researcher  
Electrical & Controls Integration Laboratory GM R & D  
Center  
Mail Code: 480-106-390  
30500 Mound Road  
Warren, MI 48090-9055  
Phone: (586) 986-6966  
Fax: (586) 986 3003  
[hariharan.krishnan@gm.com](mailto:hariharan.krishnan@gm.com)

## DEFINITIONS/ABBREVIATIONS

### BSM

Basic Safety Message

### BSW

Blind Spot Warning

### CAMP

Crash Avoidance Metrics Partnership

### CLW

Control Loss Warning

### DNPW

Do-Not-Pass Warning

### DoS

Denial-of-Service

### DSRC

Dedicated Short Range Communication

### DVIN

Drive Vehicle Interface Notifier

### ECDSA

Elliptic Curve Digital Signature Algorithm

### EEBL

Emergency Electronic Brake Lights

### FCW

Forward Collision Warning

### GPS

Global Positioning System

### HV

Host Vehicle

### IMA

Intersection Movement Assist

### LCW

Lane Change Warning

### OBE

On-Board Equipment

### OEM

Original Equipment Manufacturer

### OTA

Over-the-Air

### PER

Packet Error Rate

### PKI

Public Key Infrastructure

### RV

Remote Vehicle

### SDH

Sensor Data Handler

### SHA

Secure Hash Algorithm

**SM**  
Security Module

**TA**  
Threat Arbitration

**TC**  
Target Classification

**USDOT**  
United States Department of Transportation

**V2V**  
Vehicle-to-Vehicle Communication

**VoD**  
Verify-on-Demand

**VSC**  
Vehicle Safety Communications

**WAVE**  
Wireless Access in Vehicular Environment

**WMH**  
Wireless Message Handler

---

The Engineering Meetings Board has approved this paper for publication. It has successfully completed SAE's peer review process under the supervision of the session organizer. This process requires a minimum of three (3) reviews by industry experts.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

ISSN 0148-7191

Positions and opinions advanced in this paper are those of the author(s) and not necessarily those of SAE. The author is solely responsible for the content of the paper.

**SAE Customer Service:**

Tel: 877-606-7323 (inside USA and Canada)

Tel: 724-776-4970 (outside USA)

Fax: 724-776-0790

Email: [CustomerService@sae.org](mailto:CustomerService@sae.org)

SAE Web Address: <http://www.sae.org>

Printed in USA