

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

2011-01-0584

Published
04/12/2011Hariharan Krishnan
General Motors CompanyAndre 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

**Documents**

Document Sharing Hub

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).

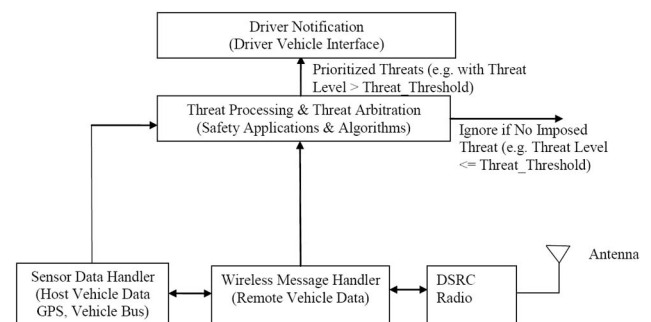


Figure 1. Nominal Architecture of V2V Communication System.

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:** $Sig(m, A_{SK})$ describes the signature of a message m with secret key A_{SK} . In ECDSA A-256 the signature length of Sig is $|Sig| = 64$ 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]. Certificates 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.	m	$Sig_A(H(m) TS)$	TS
(117 bytes)		(64 bytes)	(6 bytes)

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

Cert. Digest	m	$Sig_A(H(m) TS)$	TS
(8 bytes)		(64 bytes)	(6 bytes)

- **Ver:** $Ver(m, s, A_{PK})$ 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	$H(m) + Sig \approx 6$ ms
Computations for all receivers per message	$H(m) + Ver \approx 23$ ms
Maximum Signature Generations per second	≈ 166
Maximum Signature Verifications per second	≈ 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.

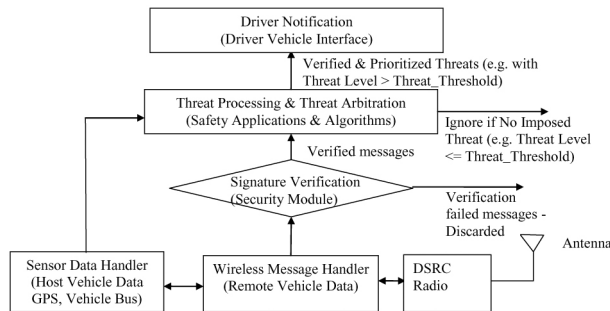


Figure 2. Verify-And-Then-Process Flow.

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.

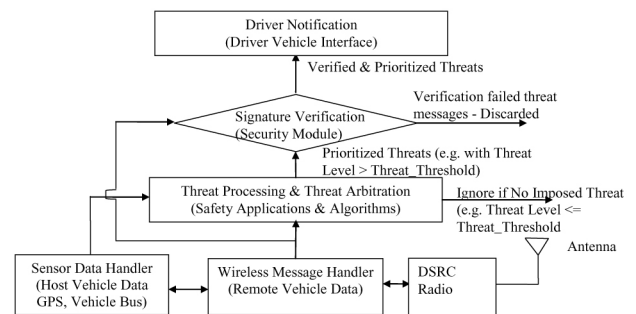


Figure 3. Verify-On-Demand Flow.

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