Secure Anonymous Broadcasting in Vehicular Networks

Christine Laurendeau and Michel Barbeau
School of Computer Science, Carleton University
1125 Colonel By Drive, Ottawa, ON Canada K1S 5B6
Tel: 613-520-2600; Fax: 613-520-4334
E-mail: {claurend,barbeau}@scs.carleton.ca

Abstract

Vehicular networks face a typical quandary in their requirement for communications that are at once secure and private. While the messages broadcast between vehicles and between vehicles and the supporting infrastructure must be authentic and non repudiable, they must also ensure the vehicle driver's anonymity. The Dedicated Short Range Communications (DSRC) framework's Wireless Access in Vehicular Environments (WAVE) application development architecture mandates the use of Public Key Infrastructure (PKI) mechanisms for securing messages, consequently compromising the driver's expectation of privacy. In this paper, we propose a WAVE-based protocol for the secure and anonymous propagation of vehicle safety broadcast messages. A hybrid key infrastructure approach is put forth which combines the use of a shared network authorization key for devices that require anonymity and PKI for devices that do not.

1 Introduction

Identity-based mechanisms are common for restricting network resource access to authorized parties, as well as for providing the means of detecting and revoking attackers. Public Key Infrastructure (PKI) systems stand out as a prime example where in addition to ensuring message integrity and confidentiality, unique digital certificates identify their possessor(s) to other parties. Balancing network security requirements with participant need for anonymity is a challenging endeavor, and vehicular networks are no exception.

The Dedicated Short Range Communications (DSRC) Wireless Access in Vehicular Environments (WAVE) architecture [17] proposes an infrastructure for communications between vehicles and between vehicles and the associated infrastructure to support applications aimed at maximizing vehicular traffic safety and driver convenience. In order to secure vehicular communications, WAVE mandates the use of PKI mechanisms, where service application messages are encrypted and vehicle safety messages are digitally signed. Unfortunately in the latter case, the use of digital signatures entails the transmission of the sender's unique certificate, thus providing the means for other devices, authorized or unauthorized, to potentially track a particular vehicle and its driver over a period of time and space. Given that individual privacy is a highly prized commodity and that the lack of it may be exploited in unexpected fashion (e.g. judicial proceedings, business rivalry, health insurance denials), WAVE's vulnerability to location tracking may hinder the wide-spread adoption of this potentially life-saving technology. In [19], we conducted a threat analysis of the WAVE architecture in order to assess the most important risks. Location tracking was identified as a critical threat.

In this paper, we introduce the Secure Anonymous Broadcasting (SAB) protocol for the secure and anonymous transmission of vehicle safety broadcast messages. A hybrid key infrastructure is described, employing both symmetric and asymmetric mechanisms. Through the use of a shared network authorization key supplemented with an encrypted sender identifier, the privacy of devices requiring anonymity is protected and the means for authorities to identify a sending device in case of an attack is retained. Devices which can be identified, for example infrastructure units and public safety vehicles such as ambulances and police cars, maintain the use of digital signatures to uphold their status as the more trusted devices. We assess SAB's security by revisiting the previously identified threats to WAVE and ensuring that the risk associated with location tracking is reduced, while no other risk is increased.

Section 2 provides an overview of existing mechanisms to provide anonymity. Section 3 outlines vehicular application requirements and corresponding WAVE specifications. Section 4 describes the SAB protocol. Section 5 provides an analysis comparing SAB to WAVE. Section 6 concludes the paper.

2 Related Work

Various means of anonymizing network traffic have been proposed in the literature and may be categorized as infrastructure-based, cryptography-based or protocol-based.

Infrastructure-based Anonymity. Specialized network servers known as *anonymizers* are used to hide a sender's identity from potential eavesdroppers, for example in the *onion routing* protocol introduced by Syverson *et al.* [24] and in the *Crowds* web transaction anonymizer scheme proposed by Reiter and Rubin [22]. Beresford and Stajano [3] adapt the anonymizer concept to the domain of pervasive computing by introducing common *mix zones* in which users change pseudonyms, so that observers cannot match a user identity departing the zone to its identity upon entry. Spatio-temporal cloaking and its related concept, *k-anonymity*, are suggested by Gruteser and Grunwald [14], as well as Gedik and Liu [12], to provide a means to protect a user's identity from Location-Based Service (LBS) providers. By aggregating the requests bound for a given LBS provider until one user is indistinguishable from $k-1$ other users, either with respect to physical location or the timing of the request, an anonymity server can protect a user's precise identity and location. However, the inherent necessity for all messages to be routed through middleware make infrastructure-based anonymity measures infeasible for vehicular networks, given the requirement for low latency and scalability, as well as the need for precise vehicle locations to be available for many applications.

Cryptography-based Anonymity. One mechanism for rendering PKI anonymous is outlined by Zhang *et al.* [26]. It allows a Certificate Authority (CA) to issue multiple anonymous certificates based on an original one, so that any message signed with an anonymous certificate can be traced back to the original certificate owner by the CA. The additional certificates act as pseudonyms for the owner and can be changed periodically to retain anonymity. However, as with any alias, they can become trackable over time unless frequently changed, and an algorithm for managing suitable switching intervals is lacking, as are the means for certificate revocation. Group signatures, on the other hand, were pioneered by Chaum and van Heyst [10] to allow a message to be signed by any member of a pre-defined group with the member's private key, while allowing a recipient to verify the signature with a shared group public key. In this manner, no recipient or eavesdropper can know which private key was used to generate the signature, except for a group manager who can "open" a signature if necessary to trace it to the original signing private key. Unfortunately, some group member revocation schemes, such as the one advanced by Bresson and Stern [5], require generating signatures of proportional size to the number of group members. In a vehicular network encompassing millions of vehicles, this is unscalable. Others, such as the scheme suggested by Ateniese *et al.* [2], require a group manager to reissue and disseminate new group certificates to the remaining members for every revocation. Boneh *et al.*'s scheme using a fixed signature size [4] requires every remaining group member to calculate a new private key and group public key based on the exhaustive list of revoked members each time a member is revoked. The means for such a list to be effectively disseminated to remaining group members, in a reliable and scalable fashion, is not explored and represents an important obstacle to the success of such a list-based revocation scheme. Overall, group signatures appear to be better suited to smaller, more manageable groups than vehicular networks.

Protocol-based Anonymity. A number of PKI-based protocols have been suggested for introducing anonymity in Vehicular Ad Hoc Networks (VANETs). In [21], Raya and Hubaux suggest that each vehicle be equipped with a set of pre-loaded certificates and that the vehicle periodically switch to a new one in order to maintain anonymity. However, it is unclear how rogue device repudiation and revocation could be successfully implemented. In the event that a rogue device is identified and directed to destroy its compromised certificate, mechanisms must be put in place to ensure compliance. Another pitfall in this approach concerns its scalability. Sufficient numbers of certificates must be issued for each vehicle to maintain anonymity over a significant period of time. As a result, the size of the certificate database to be searched by a CA in order to match a compromised certificate to its owner's identity is daunting. In [23], Sampigethaya *et al.* outline a scheme where vehicles are organized into groups, and only group leaders broadcast messages while the remaining members maintain silence in order to promote anonymity. However, given the high volume of messages required for vehicle safety applications, silent periods are not suitable for broadcast messages.

3 Vehicular Network Model

The CAMP Vehicle Safety Communications Consortium (VSCC) of automakers has identified a set of essential vehicle safety applications [8], including collision avoidance warnings, driver assistance (merging, lane changes, platooning) and traffic information (traffic jams, road closures, work zones) applications. While information dissemination applications may be initiated by infrastructure devices, multihop inter-vehicle communications are necessary to ensure propagation to vehicles beyond the infrastructure range. Many types of applications require periodic broadcast messages from each vehicle in order to gather their coordinates, velocity and bearing. These applications place limits on

message delivery latency, which in turn is affected by message size. The size of safety messages is expected not to exceed 100 bytes.

With WAVE, vehicles are equipped with On-Board Units (OBUs), and infrastructure devices are known as Road-Side Units (RSUs). Along with RSUs, Public Safety OBUs (PSOBUs) constitute a trusted class of devices and may include police cars, ambulances, fire trucks and possibly city buses. Two types of vehicular applications have been identified: *transaction applications*, which allow OBUs (via RSUs) access to remote service providers hosting a variety of information services such as navigation information systems and location finders; and *broadcast applications*, which typically convey vehicle safety information.

The WAVE security standard [16] outlines the PKI mechanisms for securing both transaction and broadcast messages. Given that *transaction messages* typically contain personal information and that their delivery latency is not subject to stringent conditions, they are secured through symmetric encryption using the Advanced Encryption Standard in CCM mode (AES-CCM) [18] with a random key. This key is in turn encrypted with the receiver's public key using the asymmetric encryption algorithm Elliptic Curve Integrated Encryption Scheme (ECIES) [9]. *Broadcast messages*, on the other hand, convey information that is at once directed for public consumption and bounded by strict latency limits. As a result, they are not encrypted but rather sent in the clear and digitally signed by the sender with the Elliptic Curve Digital Signature Algorithm (ECDSA) [1] as a means of non-repudiation. In this manner, sending WAVE devices are held accountable for the messages they transmit, and a perpetrator can be identified should an attack occur.

The encryption of transaction messages, whether signed or not, effectively hides the sender's identity. Consequently, there are few, if any, privacy concerns with transaction messages. Broadcast messages, however, pose a unique problem in that the sender's certificate, which is transmitted with every message for the receiver's verification, renders the sending vehicle trackable by an attacker. In addition, broadcast messages are predicted to contain at least 250 bytes, of which 125 bytes represent the signer's certificate [16], in the best case scenario. A *certificate chain* of up to five certificates (consisting of the message signer's certificate, the certificate signer's certificate, and so on) may also be included. This results in a message size of nearly 750 bytes, and considerable computational effort is required for validating each certificate in the chain for every received message. It is clear that broad-spectrum PKI, as applied to every type of device in the network, expands the message size and processing time beyond the expected vehicular application requirements to the detriment of bandwidth usage and message latency.

4 SAB Protocol

The Secure Anonymous Broadcasting (SAB) protocol offers an approach for anonymizing broadcast messages in a secure fashion. It proposes a hybrid key infrastructure which differentiates between the privacy requirements of different types of vehicular network devices. The use of PKI is limited to the devices which must remain identifiable and which carry the onus of trust. An alternate scheme is introduced for devices which should remain anonymous.

The protocol description makes use of the BAN logic notation [7]. Encryption of message M using symmetric key K is represented as $\{M\}_K$. Asymmetric encryption public and private key pairs take the form $\{K, K^{-1}\}$, where K is the public key and K^{-1} the private one. Therefore, if device A's public/private key pair is denoted as $\{A, A^{-1}\}$ and the device communicates message M to device B, the encrypted message takes the form $\{M\}_B$ where M is encrypted with B's public key. A digitally signed message is represented as $\{M\}_{A^{-1}}$ where M is signed with A's private key. As well, we denote the output of cryptographic hash functions, such as HMAC, over message M using key K as $H_K(M)$.

4.1 Hybrid Key Infrastructure

RSUs and PSOBUs, as *trusted devices*, occupy a unique position of trust in a vehicular network, and as such cannot remain anonymous. As a result, they retain the use of PKI digital signatures on the broadcast messages they originate.

On the other hand, OBUs such as vehicles owned by private citizens and commercial organizations have a right to preserve their location privacy. They can remain anonymous, as long as they may be held accountable for the authenticity of the messages they originate, and a device can be repudiated in case of an attack. We propose that *anonymous devices* be provided with a shared network authorization key AK known to all authorized members of the network. The AK grants the privilege of sending broadcast messages. Each broadcast message M includes a HMAC digest, computed using AK by the sender and denoted as $H_{AK}(M)$.

In order to enable the revocation of rogues, an identifier for the sending device is included with each broadcast message. To maintain anonymity, this identifier must remain illegible for all devices other than a trusted authority responsible for revocation, such as a CA. Device A includes the following *OBU identifier* with each broadcast message:

$$\{Id_A, H_{SK_A}(Id_A|H_{AK}(M))\}_{CA}$$

A unique identifier, such as an *Electronic License Plate* [15] and denoted by Id_A, is associated with each device and can be traced back to the device's logical identity by the CA.

This identifier and a copy of the message digest $H_{AK}(M)$ are concatenated and further hashed with a secret key SK_A known only to the sending device A and the CA. This measure prevents an attacker from masquerading as another device or replaying another device's identifier from a previous message. The resulting hash output and Id_A are encrypted with the CA's public key so that the sending device's identity is kept secret from all devices but the CA, which is tasked with revoking rogue devices. Semantically secure encryption, which means that a plaintext encrypted multiple times with the same key will produce different ciphertexts [13], ensures that every identifier generated by one device, even for the same message, is different.

4.2 Key Management

Transportation authorities are typically established at the state or provincial level of government. In our model, the task of managing network authorization keys and transaction message digital certificates remains with the same agencies, using multiple server-based CAs communicating with each other over the infrastructure network. The contiguous area R encompassed by the vehicular network is partitioned into a set of n distinct regions or *jurisdictions*, such that $R = \{R_1, R_2, ..., R_n\}$, where $R_i \cap R_j = \emptyset$ for all $1 \leq i, j \leq n$ and $i \neq j$. Jurisdictions may map to a state or province, or to a county or municipality. A local CA, denoted as CA_ℓ where $\ell \in R$, is assigned to each jurisdiction. Because the use of a global network authorization key is unscalable, every CA_ℓ manages a local authorization key AK_ℓ which is valid only in jurisdiction ℓ. Each device is assigned to a home CA, denoted as CA_h with $h \in R$, which stores its certificate information.

Enrolment. In order to propagate vehicle safety broadcast messages, trusted devices require a digital certificate, and anonymous devices need a network authorization key. While certificates are obtained manually through transportation authorities, the authorization key is requested and renewed automatically. Each anonymous device A is assigned a unique identifier Id_A by its CA_h, as well as a secret key SK_A known only to the device and its CA_h. The Id_A serves to identify broadcast message senders to their CA_h, and the secret key SK_A is used to prove this identity.

Renewal and Jurisdiction Handoff. Whenever the local authorization key AK_ℓ expires, device A must petition the CA_ℓ for a new authorization key AK'_ℓ using a transaction message. Similarly, if A enters a new jurisdiction ℓ', it must forward its request to the new local $CA_{\ell'}$ to obtain its authorization key $AK_{\ell'}$. In either case, the local CA obtains authorization from A's home CA_h before complying to ensure that A is still authorized to broadcast. A set of concurrent network authorization keys is used to ensure that key renewal requests are staggered in order not to overwhelm the network upon authorization key expiry. It should be noted that authorization key renewals depend on the device being within RSU range. For this reason, there must be a built-in tolerance in remote areas for broadcast messages hashed with expired authorization keys. As well, an optimal network authorization key renewal interval must be devised which maximizes protection against attacks while minimizing the associated overhead.

Revocation. Certificate revocation for trusted devices is implemented through Certificate Revocation Lists (CRLs), as currently mandated by WAVE. While CRLs are of questionable scalability when relied upon for revocation of all devices, the restriction of their use to trusted devices can greatly alleviate the size of these lists. Additionally, since trusted devices are either fixed or typically have their mobility patterns restricted to one or a few adjoining jurisdictions, the required frequency and scope of CRL distribution is naturally limited. Network authorization key revocation is achieved primarily through expiry and renewal, with only authorized devices in good standing allowed access to the renewed key. In the event that an attack is detected and device A must be revoked, the CA_ℓ receives the attack message and decrypts the associated OBU identifier. It then forwards both the message and identifier to the device's CA_h for revocation. The CA_h retrieves the SK_A associated with Id_A and computes the hash value of Id_A concatenated with the message digest. If this value matches the one in the decrypted OBU identifier, then the sending device is identified as A, flagged in CA_h's database as a rogue and denied further access to network authorization keys in all jurisdictions. If the hash values don't match, then either a masquerading attack has been detected where another device's identifier has been appropriated, or a replay attack has occurred using a different message. In this situation, alternate means of rogue attribution must be employed.

4.3 Safety Message Broadcast

A trusted device S transmitting a broadcast message M signs it with its private key S^{-1} and transmits:

$$\{M, S, \{M\}_{S^{-1}}\}$$

The recipient verifies the signature using the unsigned message, S's public key and the signature. If the signature verifies and the public key certificate is deemed valid, then the message is processed. Otherwise, it is discarded.

An anonymous device A proves its authorization to transmit a broadcast message M by hashing it with the network authorization key to produce a message digest $H_{AK}(M)$. It then transmits the message, the message digest, its CA_h identifier and its OBU identifier as described in Section 4.1:

$$\{M, H_{AK}(M), CA_h, OBUid\}$$

where

$$OBUid = \{Id_A, H_{SK_A}(Id_A|H_{AK}(M))\}_{CA_\ell}$$

Each recipient verifies that the message digest was generated with the valid AK. If it was, the recipient processes the message. Otherwise, the message is forwarded as an alert to the local CA.

5 SAB Analysis

We gauge the security of the SAB protocol in terms of its effect on the risks uncovered in the WAVE threat analysis [19]. We compare the performance of SAB with WAVE in terms of broadcast message size and cryptographic operation execution time required for sending and receiving broadcast messages.

5.1 Threat Analysis

The European Telecommunications Standards Institute (ETSI) threat analysis methodology [11] assigns a risk value of critical, major or minor to a threat, based on its likelihood of occurrence and its impact on a user or a system. In turn, the likelihood of a threat being carried out is assessed in terms of the potential motivation on the part of an attacker and technical difficulties, such as security mechanisms, that must be overcome in mounting an attack. A low impact threat where an attacker motivation is low or where the technical difficulties are considerable is ranked as minor. A threat with a moderate motivation and solvable technical difficulties is assessed as major if it has a medium impact, or critical if its impact is high. A threat with a high or medium impact and with high or moderate motivation and little technical difficulty is ranked as critical. Of the threats to WAVE identified in [19], four are affected by the proposed SAB protocol: location tracking (which is a critical threat), masquerading, replay and false broadcast messages (minor threats).

Location Tracking. In adopting a shared network authorization key to prove device membership in a vehicular network, SAB provides devices with anonymity since no visible identifier is associated with each device. Anonymous non-repudiation is further ensured with an identifier encrypted with the CA's public key so that no other device can identify a message's sender. While the attacker motivation and the impact on the user associated with this threat are still ranked as high, the strong technical difficulties introduced by SAB for location tracking downgrade this risk to a minor threat.

Masquerading. The technical difficulties encountered by an attacker attempting to attribute a false message to another device's identifier are considerable. Given that identifiers are transmitted in encrypted form and are only known to the sending device and its home CA, an attacker cannot knowingly target a given identifier but may generate random identifiers and happen upon a valid one by chance. In this case, however, the attacker also needs the secret key known only to the device associated with the identifier and its home CA in order to generate a valid hash value of the identifier and message digest. As a result of these difficulties, the masquerading threat remains a minor one.

Replay. As with the masquerading attack, an attacker attempting to replay another device's identifier with a new message would fail, since the CA would detect that a different message digest is referenced in the encrypted OBU identifier. An attempt to replay a previously valid message with its genuine identifier faces a limited window of opportunity, given that the network authorization key changes frequently and a stale message is likely to have been hashed with an expired key. With the strong technical difficulties in carrying out a replay attack, the threat remains a minor one.

False Broadcast Messages. False messages aimed at providing devices with erroneous information are countered in WAVE by having senders use valid digital certificates to sign each message. In SAB, messages are hashed with a network authorization key. With both protocols, the sender's authorization to broadcast a message is verified by every recipient. It is at least as difficult for an attacker to fraudulently obtain an authorization key as a digital certificate. SAB authorization keys have short lifetimes which curtail an attacker's window of opportunity. Devices petitioning for authorization key renewal are verified dynamically at their home CA to ensure that they are still authorized members of the vehicular network. On the other hand, WAVE digital certificates are assumed to be valid until they appear on CRLs, which may be outdated and suffer from scalable distribution issues.

Devices operated by outsiders to the vehicular network do not possess valid credentials, such as a digital certificate. As a result, they cannot sign messages in WAVE nor obtain authorization keys in SAB. The risk of outsider attacks is therefore minor, given the technical hurdles. However, three types of false message insider attacks must be contemplated:

- Attacks with invalid credentials
- Attacks with valid but unauthorized credentials
- Attacks with valid and authorized credentials

In WAVE, messages generated by rogue insiders possessing invalid credentials, such as a falsified or expired digital certificate, either have their signature unverifiable or their certificate included in a CRL. The SAB device without valid credentials is unable to obtain an authorization key, and the messages hashed without this key can be detected. This type of attack poses only a minor threat.

Rogue insiders may obtain valid credentials which they are unauthorized to possess, for example stolen digital cer-

tificates not yet reported as such, or certificates otherwise fraudulently obtained. In this case, the credentials are only temporarily valid and become invalid as soon as the fraud is detected. Once this happens, the stolen certificate is placed on a CRL and distributed in WAVE, and it is flagged as a rogue in SAB so that its possessor cannot obtain further authorization keys. The short window of opportunity for this type of attack renders it a minor risk.

When a rogue insider possesses valid and authorized credentials, verifiable digital signatures can be generated in WAVE, and authorization keys can be obtained in SAB. The only current countermeasure for this case is the finite lifetime of the digital certificate itself and the presumed difficulty for the attacker to continue to obtain valid authorized certificates, despite engaging in false message attacks. The means to detect such attacks and counter them effectively remains an open issue. Further, this type of attack may be complicated by the perpetrator attempting to avoid revocation by improperly formatting the OBU identifier included in the attack message, or by including a false identifier. To counter this attempt at evasion, the role of the CA can be augmented to include intermittent monitoring of the OBU identifiers of broadcast messages. This practice may provide a rudimentary means to flag the presence of a rogue insider by the invalid OBU identifier on the messages it transmits. The possibility of such detection may therefore prove to be an additional deterrent to the generation of false messages in SAB, given that WAVE provides no mechanism to detect rogue insiders with valid authorized credentials.

5.2 Message Size

The components of WAVE and SAB messages are broken down and compared in Table 1. The message depicted represents a 32-byte payload corresponding to a *position report* message that devices are periodically required to transmit. It conveys the device's coordinates, velocity and bearing. The payload is encapsulated in a WAVE unsigned message data structure [16], for a total of 67 bytes. Table 1 depicts the WAVE message transmitted, including the unsigned message (67 bytes), the signer's certificate (125 bytes, although a certificate chain may be included of up to five certificates) and the digital signature (64 bytes), for a total over 256 bytes.

The corresponding 67-byte message in SAB would also be transmitted, just as with WAVE, but with a HMAC digest of the message (20 bytes), the sender's home CA identifier (2 bytes), and an OBU identifier consisting of the sender's unique identifier (8 bytes) and the hashed value of the identifier and message digest (20 bytes), as outlined in Section 4.1. The ECIES encryption of the OBU identifier adds a significant amount of overhead, depending on the elliptic curve chosen. Tests were conducted using the Crypto++ cryptographic functions library [25] with two of the elliptic curves specified by NIST [20]. Regardless of the size of the plaintext, the P-224 elliptic curve adds 77 bytes of overhead, and the P-256 curve adds 85 bytes. Table 1 assumes the use of the P-224 curve. As a result, the total message size for SAB is 194 bytes.

Although SAB broadcast messages also fall short of the required 100 bytes, the total overhead included in each broadcast message, i.e. the message size minus the payload, is 127 bytes with SAB, compared to a minimum of 189 with WAVE. SAB thus provides an improvement of at least 33% over WAVE messages in terms of bandwidth consumption and associated latency. SAB has an additional advantage over WAVE in that without the use of a certificate chain, the message overhead size is fixed.

Table 1. Position Report Size (bytes)

Data Structure	WAVE	SAB
Unsigned Message	67	67
Certificate Chain	125 – 625	N/A
Signature	64	N/A
HMAC	N/A	20
CA identifier	N/A	2
OBU Identifier	N/A	28
Encryption Overhead	N/A	77
Total	$>$ **256**	**194**

5.3 Cryptographic Operations

We examine the computational cost of cryptographic operations required for sending and receiving SAB broadcast messages compared to WAVE messages. WAVE mandates the use of ECDSA for signature generation and verification based on the NIST elliptic curves P-224 or P-256 and ECIES for encryption.

Benchmark tests were conducted using the Crypto++ library on a Pentium 1.60 GHz processor, with the parameter values for the P-224 and P-256 curves as specified by NIST [20]. A message base of one thousand 67-byte messages was constructed, and each message was signed and its signature subsequently verified using the ECDSA algorithm for both the P-224 and P-256 curves. Further, 1000 28-byte identifiers were encrypted with the ECIES algorithm using the same elliptic curves.

In addition to the standard implementation of the cryptographic operations, Crypto++ allows for the use of a precomputed table of powers of fixed bases in order to speed up exponentiation. Since WAVE devices are not expected to be highly constrained in terms of memory, the use of pre-computed information appears to be a favorable option given its positive effect on performance. However, it

was noted during the benchmark tests that the use of pre-computation had a negative impact on the variance of the results. Since our goal is to compare the cryptographic operation cost between two protocols and not to identify the conditions for optimal performance, we illustrate the results obtained without the use of pre-computation because of the significant reduction in variability. It should be noted, however, that measures for performance improvement may be achieved through the use of pre-computed tables, or through optimizations such as those outlined by Brown *et al.* [6]. Table 2 illustrates the comparison results.

Table 2. Cryptographic Operation Execution Time (in ms)

Sending Device				
	WAVE		**SAB**	
	P-224	**P-256**	**P-224**	**P-256**
Sign	15.73	18.53	N/A	N/A
Encrypt	N/A	N/A	31.05	36.56
HMAC	N/A	N/A	0	0
Total	**15.73**	**18.53**	**31.05**	**36.56**
Receiving Device				
	WAVE		**SAB**	
	P-224	**P-256**		
Verify	$31.08 * 2$	$42.08 * 2$	N/A	
HMAC	N/A	N/A	0	
Total	**62.16**	**84.16**	**0**	

For the sending device, WAVE requires only a signature to be generated. On average, this can be accomplished with the P-224 curve in 15.73 ms and with P-256 in 18.53 ms. In contrast, SAB requires the sending device to generate a HMAC message digest, as well as an encryption of the OBU identifier. Since our tests revealed that HMACs can be generated on one kilobyte of data in 17 μs, we deemed the HMAC operation cost to be negligible in comparison to the other operations measured in milliseconds. The ECIES encryption of 28-byte OBU identifiers took 31.05 ms on average with the P-224 curve and 36.56 ms with P-256. Overall, a sending device takes roughly twice as long to process an outgoing message with SAB than with WAVE.

Upon receiving a message, WAVE devices must verify at least two signatures, one on the message and one on the sender's certificate. If a certificate chain is included, then every certificate in the chain must be verified, for a total of up to six signature verifications. With the P-224 curve, two verifications averaged 62.16 ms, while with the P-256 curve, they took 84.16 ms. By comparison, SAB only requires a hash value to be generated and compared against the corresponding received value, although if concurrent network authorization keys are used to stagger key renewals, several hash operations may be required. Decryption of the OBU identifier by the CA is required only in the event that the sender is a suspected rogue and not as a matter of course. As a result, the computational cost in SAB receiving devices is negligible.

The most frequently transmitted broadcast messages are likely to be position reports. In a given time period, a device receives as many position reports as it has neighbors n, while it only sends one. The cost of sending and receiving messages with WAVE is represented by two constants, s and r respectively. The cost of sending a SAB message is twice the one in WAVE ($2s$), while its receiving cost is null. SAB is the better solution if the computational performance in sending one message (s for WAVE and $2s$ for SAB) and receiving as many messages as there are neighbors ($n * r$ for WAVE and 0 for SAB) is more efficient in SAB than in WAVE:

$$\begin{array}{rcl} \textbf{SAB} & & \textbf{WAVE} \\ n*0+1*2s & < & n*r+1*s \\ s & < & nr \\ \frac{s}{r} & < & n \end{array}$$

Since we know from our tests that $s < r$, we know that $\frac{s}{r} < 1$. As a result, SAB is more efficient if $n \geq 1$, where a device has at least one other device in range. So in very sparse traffic, if a device has no neighbors, WAVE's transmission performance is better. If, however, the device has one or more neighbors necessitating signature verifications on several messages, which is the more likely scenario especially in urban settings, SAB is computationally superior. In general, given the open nature of the wireless medium, nodes inherently receive more messages than they send.

6 Conclusion

In this paper, we introduced the SAB protocol for the anonymous broadcasting of vehicle safety application messages. We described a hybrid key infrastructure combining PKI for trusted devices and a shared network authorization key for devices requiring anonymity. The non-repudiation property was retained for anonymous devices with the inclusion in the message of a unique sender identifier encrypted for access by the revoking authority and anonymous for other devices.

We compared SAB with the existing DSRC-based WAVE protocol along three separate metrics. We established that SAB effectively addresses the location tracking threat without increasing the comparative vulnerability of vehicular devices to other threats such as masquerading, replay attacks and false broadcast messages. We showed that

SAB achieves a 33% reduction in overhead for broadcast messages over the WAVE protocol. We also demonstrated that SAB employs fewer computationally expensive cryptographic operations overall, most notably in the case where a device has at least one other device within range.

Although both WAVE and SAB protect the vehicular network against outsiders and some types of rogue insider attacks, few mechanisms exist in either protocol for the detection of false messages and rogue devices using valid credentials. These shortcomings need to be addressed to ensure the integrity of the vehicle safety messages broadcast in vehicular networks.

Acknowledgements

The authors gratefully acknowledge the financial support received for this research from the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Automobile of the 21st Century (AUTO21) Network of Centres of Excellence (NCE).

References

[1] American National Standards Institute. Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA). ANSI Standard, X9.62-2005, 2005.

[2] G. Ateniese, D. Song, and G. Tsudik. Quasi-Efficient Revocation of Group Signatures. In *Proceedings of the Sixth International Conference on Financial Crytography*, 2002.

[3] A. R. Beresford and F. Stajano. Location Privacy in Pervasive Computing. In *IEEE Pervasive Computing*, volume 2, pages 46–55, January–March 2003.

[4] D. Boneh, X. Boyen, and H. Shacham. Short Group Signatures. In *Proceedings of the 24th Annual International Cryptography Conference*. Lecture Notes in Computer Science, Springer Berlin / Heidelberg, Volume 3152, 2004.

[5] E. Bresson and J. Stern. Efficient Revocation in Group Signatures. In *Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptosystems*. Lecture Notes in Computer Science, Springer Berlin / Heidelberg, Volume 1992, 2000.

[6] M. Brown, D. Hankerson, J. Lopez, and A. Menezes. Software Implementation of the NIST Elliptic Curves Over Prime Fields. In *Proceedings of the RSA Conference (CT-RSA)*. Lecture Notes in Computer Science, Springer Berlin / Heidelberg, Volume 2020, 2001.

[7] M. Burrows, M. Abadi, and R. Needham. A Logic of Authentication. In *ACM Transactions on Computer Systems*, volume 8, pages 18–36, February 1990.

[8] CAMP Vehicle Safety Communications Consortium. Vehicle Safety Communications Project Task 3 Final Report. National Highway Traffic Safety Administration, U.S. Department of Transportation, DOT HS 809 859, 2005.

[9] Certicom Research. Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography, Version 1.0, 2000.

[10] D. Chaum and E. van Heyst. Group Signatures. In *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. Lecture Notes in Computer Science, Springer Berlin / Heidelberg, Volume 547, 1991.

[11] ETSI. Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis. Technical Specification ETSI TS 102 165-1 V4.1.1, 2003.

[12] B. Gedik and L. Liu. Location Privacy in Mobile Systems: A Personalized Anonymization Model. In *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems*, 2005.

[13] S. Goldwasser and S. Micali. Probabilistic Encryption. In *Journal of Computer and System Sciences*, volume 28, pages 270–299, 1984.

[14] M. Gruteser and D. Grunwald. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In *Proceedings of the First International Conference on Mobile Systems, Applications and Services*, 2003.

[15] J.-P. Hubaux, S. Capkun, and J. Luo. The security and privacy of smart vehicles. In *IEEE Security and Privacy*, pages 49–55, May/June 2004.

[16] IEEE Intelligent Transportation Systems Committee. IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages. IEEE Std 1609.2-2006, July 2006.

[17] IEEE Vehicular Technology Society. 5.9 GHz Dedicated Short Range Communications (DSRC) - Overview.

[18] Internet Engineering Task Force. IETF Request for Comments: 3565, Use of Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS). IETF RFC 3565, 2003.

[19] C. Laurendeau and M. Barbeau. Threats to Security in DSRC/WAVE. In *Proceedings of the 5th International Conference on Ad Hoc Networks and Wireless (ADHOC-NOW)*. Lecture Notes in Computer Science, Springer Berlin / Heidelberg, Volume 4104, 2006.

[20] National Institute of Standards and Technology. Digital Signature Standard (DSS). Federal Information Processing Standards Publication, FIPS 186-2, 2000.

[21] M. Raya and J.-P. Hubaux. The Security of Vehicular Ad Hoc Networks. In *Proceedings of the Third ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2005.

[22] M. K. Reiter and A. D. Rubin. Anonymous Web Transactions With Crowds. In *Communications of the ACM*, volume 42, pages 32–48, February 1999.

[23] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki. CARAVAN: Providing Location Privacy for VANET. In *Proceedings of the Conference on Embedded Security in Cars (ESCAR)*, 2005.

[24] P. Syverson, D. Goldschlag, and M. Reed. Anonymous Connections and Onion Routing. In *Proceedings of the IEEE Symposium on Security and Privacy*, 1997.

[25] Wei Dai. Crypto++ Library 5.4.

[26] N. Zhang, Q. Shi, and M. Merabti. Anonymous Public-Key Certificates for Anonymous and Fair Document Exchange. In *IEE Proceedings – Communications*, volume 147, pages 345–350, December 2000.