A Cross-layer Approach to Privacy-preserving Authentication in WAVE-enabled VANETs

Subir Biswas, *Student Member, IEEE,* Jelena Mišić, *Senior Member, IEEE*

Abstract

We present an anonymous authentication and verification scheme for WAVE-based vehicular ad hoc networks (VANETs). Our contribution includes vehicular message authentication, as well as an efficient prioritized verification strategy for periodic road-safety messages. A variation of elliptic curve digital signature algorithm (ECDSA) is used in combination with the identity-based (ID-based) signature where current position information of a vehicle is utilized as the ID of the corresponding vehicle. This waives the need of a third-party public key certificate for message authentication in VANETs. A VANET authentication requires verification of the signature of the received message. A high density road-traffic condition poses a challenge for authentication of vehicular messages since required verification time is often much longer than the average inter-arrival time. An adaptive verification strategy uses cross-layer features of WAVE-based VANETs and information relevance for verifying the received safety-messages. Messages of each traffic class are verified following the corresponding verification priority. The verification probability depends on VANET's MAC-layer priorities and the application relevance of individual safety messages. Performance analysis and simulation results have shown that our approach is secure, privacy preserving, scalable, and resource-efficient.

Index Terms

ECDSA; Authentication; ID-based signature; IEEE 802.11p, EDCA; and Access Categories;

I. Introduction

Authentication is an essential requirement for a reliable vehicular ad hoc network. VANET allows on-board units (OBUs) of vehicles on road to deliver safety- and/or other application messages to the neighboring vehicles for providing assistance on safe driving, road-safety, drivers' comfort etc. However, a received traffic message from a VANET entity may contain harmful contents that can jeopardize the integrity of the VANET. Therefore, a VANET message should be authenticated upon reception.

Subir Biswas is with the Department of Computer Science, University of Manitoba, Winnipeg, MB R3T 2N2, Canada. e-mail: bigstan@cs.umaitoba.ca

Jelena Mišić is with the Department of Computer Science, Ryerson University, Toronto, ON M5B 2K3, Canada. email: jmisic@scs.ryerson.ca

In order to mitigate the trust issues in vehicular communications, an obvious choice is to deploy an appropriate signature scheme (e.g. [1], [2]) for authenticating received messages. Yet, an ordinary signature scheme reveals the actual identity of a signer which is undesirable as far as privacy is concerned. Nevertheless, unconditional privacy may impair the prospect of vehicular communications since an anonymous entity could deliberately transmit some false and misleading messages to its neighbors. Therefore, a VANET entity should be accountable to the corresponding authority in case of a critical event or dispute on road (e.g. a collision, or traffic congestion).

Proposed security services (1609.2 [3]) for IEEE Wireless Access in Vehicular Communications (WAVE) have incorporated Elliptic Curve Digital Signature Algorithm (ECDSA) protocol for VANET authentications. ECDSA is Elliptic Curve Cryptosystem (ECC)-based implementation of the commonly used digital signature algorithm (DSA [4]). ECC provides the same security level as the other discrete logarithm approaches, while the size of the required ECC credentials are much smaller than that of the discrete logarithm systems. The WAVE security services adopt ECDSA-based message authentication for vehicular communications. Two standard elliptic curves namely P-224 and P-256 have been suggested for general purpose message authentications, and certificate authentications in VANETs [5].

A VANET entity is required to transmit periodic safety messages containing its current coordinates, speed, acceleration etc. to the neighboring devices. The typical interval for safety message broadcasts ranges from 100 ms to 300 ms. An authentication scheme has to be incorporated in order to provide reliability and trust for the delivered safety information. Received messages are verified by the receiving entity to ensure the message integrity, and authenticity of sender's identity. Unfortunately signature verification incurs a cryptographic processing delay at the verifier's end. Although the verification delay for ECDSA is in the order of milliseconds, with hundreds of vehicles in a dense traffic scenario, an OBU would receive an enormous amount of periodic messages per unit time causing a bottleneck to the authentication process at the receiver end.

If OBUs are configured to broadcast their periodic messages every 100 ms, under a heavy traffic scenario, many of the safety messages would either be discarded due to the constrained buffer size of the verification process, or accepted without any verification. Therefore in busy traffic hours, a receiver of vehicular messages would either risk a fatal road-traffic consequence, or it would reject a significant portion of received messages without authenticating when its maximum verification capacity is reached.

The current WAVE standards do not include an efficient anonymous authentication scheme for vehicular messages, or even an intelligent authentication strategy which can efficiently verify from a massive number of vehicular safety/application messages.

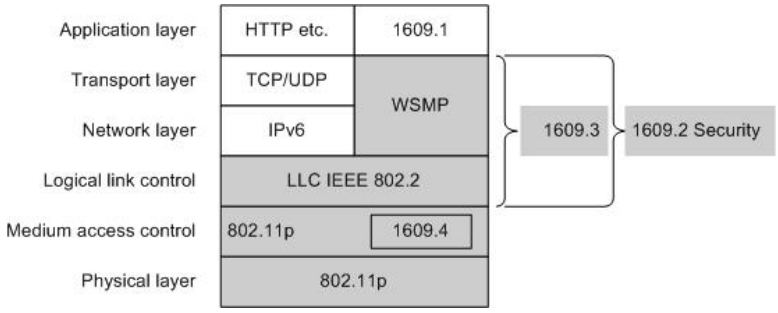


Fig. 1. Protocol stack of a WAVE-based VANET. Shaded layers are used in our scheme.

A number of different signature schemes have been suggested to incorporate anonymous authentication for vehicular communications. We can roughly categorize them into two different types: *anonymous certificate-based approaches*, and *group signature-based approaches*. These approaches are impractical and/or inappropriate for a large scale VANET implementation as they are either inefficient, or established on some infeasible mathematical assumptions.

In this paper, we present a WAVE-based cross-layer scheme of privacy-preserving and conditional authentication for signing and verifying vehicular safety application messages. We develop a variant of ECDSA mechanism incorporating an ID-based authentication scheme [6], [7] where the current position of the signer and each individual receiver will be used as the corresponding identity parameter for anonymous signature generation and verification. Unlike most other existing ideas of anonymous authentication, this scheme does not need a trusted third-party certificate, or any strong mathematical assumption-based signature procedures.

We assume that application priorities are mapped into the Enhanced Distributed Channel Access (EDCA) traffic classes. The probability of successful delivery of message broadcasts depends on the WAVE's EDCA traffic class and the traffic load so that the receiver can scale message verification rates according to MAC priorities and traffic congestion. For message verification in a dense traffic scenario, received messages are chronologically ordered according to their relevance. The verification mechanism considers MAC-layer priorities along with the current traffic intensity to derive an adaptive verification probability for received messages.

Shaded area in Figure 1 indicates the protocols involved in our authentication scheme. Our scheme involves Security ([3]), Networking with WSMP ([8]), IEEE 802.11p MAC and PHY ([9],[10]) layers to generate the signature, to transmit signed periodic safety messages, and for the verification of received messages. VANET entities use WSMP packets for broadcasting periodic traffic-safety messages while the message delivery and verification procedures of received messages rely on the EDCA mechanism of IEEE 802.11p MAC.

We organize the rest of the paper as follows. The literature review is given in Section II. Sections III, and IV contain anticipated attack/adversary model, and the design goals respectively.

The anonymous user-authentication scheme is illustrated and discussed in Section V. A brief introduction to WAVE EDCA mechanism is given in VI. The prioritized message verification is described and analyzed in Section VII. Performance of the related networking issues have been discussed in Section VIII while Section IX concludes the paper.

II. Related Work

In this section, we provide a brief summary of recent literature revealing the related ideas of anonymous authentication and different verification strategies for vehicular communications. For the convenience of our discussion, we divide the section into following three subsections.

A. Anonymous Certificate-based Authentication

A vehicular authentication scheme has been proposed in [11] where each OBU would be preloaded with a massive amount of short-lived anonymous certificates. These certificates can be transferred to the vehicle's OBU during the registration, or renewal of the registration of the vehicle. Used certificates are time-specified; hence in most cases, a lot more certificates are to be stored in an OBU than they are actually used by a user. Since each vehicle contains a large number of anonymous certificates, in case of any traffic dispute, a rigorous effort would be needed to find out the actual identity of the signer of a specific message transmission. Also, as the time goes by, revocation of a user's certificate pool becomes harder since the size of the revocation list grows at a severe rate.

Another solution is proposed in [12] which addresses the issue of revocation in anonymous certificate approaches. A bilinear pairing based technique [13], along with one-way hash functions keep the size of the revocation list linear with the number of revoked OBUs in VANET. In this approach, an OBU updates the trusted third party certificates by re-signing them with corresponding RSU-keys. However, this scheme requires RSUs at regular intervals of VANET-enabled roads and highways. Secondly, since RSUs are installed at the roadside locations without due surveillance and physical protection, they are vulnerable to compromise attack. Therefore, implementation of such scheme would be expensive and yet prone to malicious attacks.

A solution presented in [14] resolves the issue of RSU compromise attack while it requires multiple handshaking between OBU and RSU for vehicular authentication. Like the scheme in [12], this approach also requires an uninterrupted coverage of RSUs in the VANET which is impractical from the implementation point of view.

An anonymous authentication approach presented in [15] combines the PKI-based authentication and TESLA [16] protocol for VANETs. A sender's first message is signed and verified using a PKI-based signature along with a trusted third party certificate. If the first message from a sender is authenticated, the subsequent messages are simply verified at the receiving entity by

comparing the message authentication code (MAC) using the TESLA procedure. This scheme requires a receiving OBU to save all the third party certificates from the neighboring vehicles in its memory for a long period of time.

A discrete logarithm and hash based solution to VANET authentication has been proposed in [17]. The used discrete logarithm based signature scheme requires larger keys (at least 512 bits long), for signature generation and verification. Therefore, this approach requires resources with high computation capability, and it performs slower than an elliptic curve based system (ECC) with similar security strength.

B. Group Signature-based Authentication

A group-signature scheme allows a member OBU to sign a message on behalf of the group. The signing member remains anonymous in the group, but a group manager can determine the actual identity of the signer in case of a dispute.

An ID-based signature [18], as well as a group signature scheme [19] are combined in [15] to provide anonymous authentication in VANETs. OBUs are preloaded with a single group-public-key, and individual private keys. A bilinear-pairing based short group-signature is used by an OBU to sign a message. An RSU on the other hand, uses an ID-based approach to sign RSU beacons. Location information of an RSU is used as the public key in RSU's ID-based signature which can be verified by an OBU using its own location information.

Message linkable group signature (MLGS) for anonymous authentication in VANETs has been proposed in [20]. Sybil attacks in VANETs can be thwarted with this approach as the actual identity of the sender is detected if it signs a message more than once. This scheme relies on bilinear-pairing groups, and a cryptographic primitive called threshold cryptography [21], where an adaptive algorithm enables a receiver to trust a message only if the message is endorsed by at least a predefined number of anonymous vehicles.

In [22], a hybrid approach allows a VANET group member to sign its self-generated pseudonyms which are transmitted along with signed messages. Each OBU is pre-loaded with a unique group signing key and a common group public key. Self-generated pseudonyms are certified using its group signing key, while the message is signed by the corresponding private key for the used pseudonym. When received, a self-certificate is verified using the group public key while the signed message is verified by the authenticated sender public key. Apparently, a message verification in this approach consumes additional network bandwidth since each transmission from a sender contains a signature on the message as well as on a pseudonym.

C. Signature Verification Policies

The problem of authenticating huge number of signed messages in a given time has been addressed in two major ways: random verification, and aggregated (batch) verification of messages.

1) Random verification: In a random verification scheme, received messages are randomly selected for verification by a receiving entity. The idea has been incorporated for VANET in [11] to obtain scalability in signature verification process.

A random verification mechanism for group signature-based anonymous authentication in VANETs has been proposed in [23] showed that for up to $n = 1000$ nodes in a VANET, 95% of broadcast messages are authenticated if each OBU randomly verifies just 3 messages per n messages received. Several other VANET authentication schemes (e.g. [24], [25]) adopted this technique for its network scalability and simplicity.

A resource-aware verification scheme for VANET messages has been presented in [26] where the physical distance between sender and receiver is considered as the basis of prioritizing received messages. Received messages from the nearest vehicles are to be authenticated immediately, while rest of the messages would be chosen for verification in a random manner within the resource budget. However, in a sparse traffic scenario where the average distance between two vehicles is large, this approach becomes an ordinary random verification scheme.

2) Batch verification: A batch verification technique in VANET allows verification of all received messages simultaneously. Most batch-verification schemes proposed for VANETs use a costly bilinear pairing-based verification technique [27], [28]. A fast batch verification mechanism has been presented in [29] using ECDSA authentication scheme.

A batch verification mechanism is an efficient way of ensuring the trust of multiple messages received in a unit time. Nevertheless, implementation of this approach depends on the underlying mechanism of the signature protocol.

III. Attack Model and Vulnerabilities

We assume that our communication channel is not secure, and participating OBUs are not trustworthy. Major attacks and malicious behavior of an adversary anticipated on an anonymous authentication scheme in VANET environment are listed below.

A. Message Forging

An adversary may attempt to forge a message by altering the original contents of a valid message from a legitimate OBU. It may also try to produce a valid signature on the altered message payload. Required secret credentials of the target node are either derived by guessing, or stolen from a legitimate OBU as OBUs are not equipped with tamper-resistant hardware.

B. OBU Compromise and Repudiation

An adversary may compromise an OBU to obtain its secret credentials which are used for generating valid signatures. Also, a compromised node may deliberately send false and harmful messages, and later deny its involvement in signing any such messages. Denial of responsibility of such kind from an adversary is called repudiation attack.

C. Message replaying and tunneling

An attacker may collect and store a signed emergency message from a particular traffic area, and attempt to deliver it at a later time when the original message is invalid. Similarly, an attacker may collude with another attacker from a different area. A colluding attacker may tunnel the legitimate emergency messages from a specific traffic area to a different area where the message content is irrelevant for the given traffic. This unnecessary replaying of legitimate emergency or safety- messages would create confusion among the VANET users in the new area.

D. Linking of Signatures

Signature linking refers to a situation when an attacker or an eavesdropper successfully distinguishes an anonymous entity within a group by linking some of its signatures. Back to back periodic messages might contain similar information in the message payload from a particular OBU. An adversary may attempt to use two or more consecutive signed messages from a node to identify the signer based on the received contents.

In a group signature-based approach, each vehicle belongs to a group which allows 'group-anonymous message signature [23] for vehicular authentications. However, if the ratio of the number of OBUs and the number of groups in a specific scenario is not high enough, the user-anonymity of the VANET is compromised.

E. Random Verification Attack

This attack is a consequence of the vulnerability induced by a random verification policy. Success of a random verification approach is highly reliant on traffic density or the number of participants in the VANET; and therefore, un-sustaining. A harmful message may get through the authentication process without verification to jeopardize the safety of the traffic system. In a dense traffic condition, it is quite unlikely that all received messages would be authenticated. Knowing that a verifier would randomly verify received messages, an adversary may take advantage of this situation by injecting a large number of harmful messages in each authentication cycle. This attack may bring fatal traffic consequences for a VANET-based traffic system. We define this attack as *random verification attack* in VANETs.

Hence, a realtime system like VANET must not risk an abuse by deploying the ordinary random verification approach which might allow a harmful message from a malicious VANET entity.

F. False signature attack on Batch Verifications

Signatures can be aggregated in batches for batch verifications. However, the whole batch would be dropped or rejected even if there is just one false signature in the batch.

An improved mechanism of batch verification [27] can isolate all false signatures in a batch. Upon detection of false signature in a batch, the verification algorithm divides the batch recursively, and follows a binary authentication tree (BAT) down to its leaves where individual signatures are associated. Nonetheless, this approach is effective only under normal situations when there are few false signatures in a batch.

A collusion of multiple attackers could make this approach unscalable in a high density traffic scenario since a verifier would require longer time to isolate individual malicious messages than the message inter-arrival time. This may eventually turn up as a denial of service (DoS) attack if all receivers in a VANET fail to process subsequent batches of signatures due to resource unavailability.

IV. Design Goals

In order to mitigate the anticipated attacks and vulnerabilities in VANETs, we introduce the following design goals based on our attack model and anticipated vulnerabilities on an anonymous authentication scheme for VANET.

A. A third-party trusted authority

We suggest a third-party trusted authority called central authority (CA) which would be responsible for generating and storing secrets, and signature credentials of OBUs and RSUs. It should be able to resolve any identity dispute on traffic incidents upon request from an appropriate authority (e.g. Police, Court, Dept. of Transportation etc.). The CA is secured and protected against all sorts of physical attacks and adversarial compromises.

B. Privacy-preserving ID of OBUs

In order to provide anonymous authentication through signed messages in a VANET, it is essential to have multiple entities (i.e. OBUs) in the network with an identical name so that individual nodes may not be recognizable from the sender information of the delivered messages. Therefore, for privacy-preserving authentication in a VANET, each participating OBU in a given

area must have a common identifier. Assuming that each OBU is equipped with a GPS device, the common geographical area of participating OBUs can be used as the privacy-preserving identifier for individual OBUs. Identity information of an OBU is determined from the most significant bits of GPS coordinates so that all OBUs within the communication range of each other can have the same identity information.

C. Privacy-preserving authentication for VANETs

- An adversary should not be able to associate a unique identifier with an OBU in a particular VANET. However, the third-party trusted authority or CA must be able to distinguish an OBU based on some unique credential used by the OBU during its signature generation process. Retrieving the actual identity of an OBU could be essential during resolving a traffic dispute that involves VANET communications. Therefore, a unique primary secret has to be associated with an individual node in a VANET.
- An OBU must have the proof of its association with the third-party CA, as well as the specific vehicle type, and the OBU itself. Hence, a secondary delegation key for each entity in VANET should be generated at the CA involving the third-party system, vehicle type identifier, and the OBU's primary unique secret.
- An adversary may obtain the secondary unique key (delegation key) by compromising an OBU from a stolen vehicle. This may encourage an adversary to launch false or harmful message delivery attacks using the compromised key. In that case, the responsibility of such malicious act would go to the original user of the compromised OBU of the stolen vehicle. Thus, the activation of signature generation process should be protected by a user-password at the OBU.
- An adversary should not be able to successfully tunnel a legitimate signed message of a valid OBU to deliver it in a different area within the same time frame or at a different time. Therefore, a signing OBU must associate its current area (GPS location) information, as well as the current timestamp of the message during the signature generation process. A verifying node should also utilize its own area identifier and current time frame during the verification of a received message.

D. Limitations of Bilinear Pairing

Most existing anonymous authentication approaches (e.g. [12], [14], [15], [20]) and signature verification schemes for VANET use bilinear pairing as the foundation of their cryptographic primitives for VANET authentication and verification. When computation time and complexity are concerned, bilinear pairing operations are quite expensive compared to other alternative

primitives in cryptography. Bilinear pairing-based approaches of cryptographic primitives have been criticized in [30] since most typical and frequently made pairing assumptions are impractical and not feasible to comply with.

E. Priority-based verification of VANET safety messages

Efficient authentication of periodic safety messages is a challenge in VANETs with dense traffic conditions. Verifying all individual signatures in such conditions would create a bottleneck at each of the receivers.

Although we can not completely avoid a random verification attack (as indicated in Section III-E), we can effectively reduce the impact of such misbehavior by introducing verification priorities among received messages. High priority messages would be more frequently verified than the low priority ones. Also, high-priority application messages must be less vulnerable to a random verification attack.

Therefore, application priority should be mapped into priority scheme of lower protocol layers (e.g. in Medium Access Control (MAC) traffic classes). This mapping should be beneficial for achieving the quality of service (QoS) differentiation among messages and protection against MAC-layer's denial of service (DoS) attacks [31]. Messages with high MAC priority have smaller delay and lower drop probability which enhance their chances of being verified at the receiving end.

V. Anonymous User-authentication in VANETs

In our authentication model, each vehicle is registered at the local transportation department which works as the central authority for providing the security and privacy to VANETs. Privacy credentials are securely preloaded into a vehicle's OBU during the registration or yearly renewal time.

A. Definitions

Definition 1. *A finite field $\mathbb{F}_p$ is a finite set of p elements along with addition and multiplication operations on $\mathbb{F}$. The number of elements is denoted as the order of the finite field. There exists a finite field of order q if and only if q is a prime power, and on the other hand, if q is a prime power, then there exists only one finite field of order q denoted by $\mathbb{F}_q$.*

Definition 2. *An Elliptic Curve E over a finite field $\mathbb{F}_p$ is defined in the form of the following equation:*

$$y^2 = x^3 + ax + b, \tag{1}$$

where a prime $p > 3$; $a, b \in F_p$, *and* $4a^3 + 27b^2 \not\equiv 0 (mod\ p)$. *The set of elements of the Elliptic Curve* $E(\mathbb{F}_p)$ *consists of the points* (x, y) *where* $x \in \mathbb{F}_p$ *and* $y \in \mathbb{F}_p$. *A point at infinity* $\boldsymbol{O}$ *together with the set of points* $E(\mathbb{F}_p)$ *identifies an elliptic curve.*

Note that the addition, multiplication, and inversion operations on an elliptic curve points are different from ordinary binary operations. Please refer to [2] for the detailed description of the mentioned operations.

1) ECDSA Domain Parameters: The domain parameters of Elliptic Curve Digital Signature Algorithm (ECDSA) require an Elliptic Curve E over a finite field of size q, and a base point $G \in (\mathbb{F}_q)$. Value q is chosen as a prime power p^t where p is a prime number, and t is a positive integer. We choose, $t = 1$, thus $p = q$. Also, as indicated in Equation (1), two field elements a and b are chosen, where, $a, b \in (\mathbb{F}_q)$. All these parameters could be shared by the entities or by some specific user depending upon the ECDSA configuration.

2) ECDSA Summary: A signer of message m follows the steps:

i. *Key Pair Generation:* Select a random number $d \in_R \mathbb{Z}_q^*$ to compute $Q = dG$; where G is a base point of the elliptic curve $E(\mathbb{F}_p)$.

ii. *Signature Generation:* The signer computes $(x_1, y_1) = kG$; where k is a random number and $1 \leq k \leq q$. The signer then computes $r = x_1 mod\ q$ and $s = k^{-1}(SHA1(m) + dr) mod\ q$; where if $r = 0$ or $s = 0$, the signer aborts the current operation and restarts the procedure. (r, s) represents the signature for message m.

iii. *Verification:* A verifier first checks if r and s are in the interval $[1, q - 1]$. It then does the following computations: $w = s^{-1} mod\ q$
$u_1 = SHA1(m) w\ mod\ q$
$u_2 = rw\ mod\ q$
$X = u_1 G + u_2 Q$
If $x \neq \boldsymbol{O}$ and $v = r$, the verifier accepts the signature, otherwise the delivered message is rejected.

B. Notations

Table I contains the list of notations that are used throughout the illustration of our scheme.

C. Description

We derive following four functional steps of our scheme based on the modification of the original ECDSA mechanism.

TABLE I
NOTATIONS

Component	Description
CA	Trusted central authority
Q	master public key
q	a large random prime number
x	master secret; $1 < x < q$
G	a base point over $E(\mathbb{F}_p)$
x_p	session parameter
k_i	primary secret associated to user i
$H_1(.), H_2(.)$	hash functions; $H_1(.), H_2(.) : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$
loc_p	area identifier of a user during session p
k_p	hash outcome of current area identifier and time
m	a message to be signed and delivered
t	a timestamp

1) Key Initialization Module:

i. CA chooses the system secret x, where $1 < x < q$; and computes

$$Q = xG \tag{2}$$

ii. CA associates a random primary secret k_i (Where, $1 < k_i < q$) with each individual OBU_i of a particular type. And, the vehicle type identifier R_i is calculated as:

$$R_i = k_i G \tag{3}$$

Suppose, $i, i+1, i+2, ..., i+N-1$ are registered vehicles; CA computes the group identifier $R_i = k_i \ (modq)G = k_{i+1} \ (modq)G = k_{i+2} \ (modq)G = ... = k_{i+N-1} \ (modq)G$.

iii. Hash function $H_1(.)$ is used for computing $h_i = H_1(R_i)$.

iv. CA derives a unique partial delegation key (secondary key) for each vehicle i from the the master secret x using the corresponding primary secret k_i, and h_i values as indicated below.

$$s_i = (1 + xh_i k_i^{-1}) mod \ q \tag{4}$$

$$s_{u_i} = s_i \oplus Password \tag{5}$$

Derived user secret s_{u_i} is securely copied to the corresponding OBU_i's disk-space.

2) Pre-processing: In the beginning of OBU activation, a user enters his password which is then XOR-ed with the saved secret s_{u_i} to reproduce the actual delegation secret s_i.

A deliverable message– whether a periodic safety message, or an emergency event message such as a road-traffic accident notification is associated with the current system time, and the vehicle's position. Session parameters are obtained by the signer and a verifier entity (OBU

and/or RSU) using the corresponding area information and current system time. The steps are given as:

i. The signing vehicle determines k_p for the message m.

$$k_p = H_2(loc_p || t) \tag{6}$$

The value of loc_p is rounded up by taking only few most significant bits of the GPS co-ordinates so that OBUs in the communication range of each-other would have the same loc_p.

ii. It then computes the session parameter x_p as

$$(x_p, y_p) = k_p R_i mod\ q \tag{7}$$

3) Signature Generation:

i. Once the session parameter x_p is generated for the message m, OBU signs the message as shown by the following ECDSA formula:

$$s_{p,i} = k_p^{-1}(H_1(m) + s_i x_p) mod\ q \tag{8}$$

ii. The signature payload and the message are combined as $(m||R_i||s_{p,i})$ to be delivered to the neighboring vehicles (OBUs) and RSUs within the communication range of the OBU.

4) Verification: For a receiver OBU or RSU, it is important to verify the the source identity, as well as the integrity of the received message. The received signature components are used in the verification process as illustrated below.

i. A receiving entity computes k_p from its own area information and the current timestamp using the relationship given in Equation (6).
ii. Equation (7) is used to obtain (x_p, y_p) values by the verifier.
iii. The verifier entity computes h_i by following the relation $h_i = H_1(R_i)$.
iv. Finally, if the following relationship holds, the signature is verified as a valid one.

$$(x_p, y_p) = (H_1(m)R_i + x_p(R_i + h_i Q))s_{p,i}^{-1} mod\ q \tag{9}$$

D. Security Analysis

Security of this scheme depends on the associated difficulty of solving the elliptic curve discrete logarithm problem. Following malicious behaviors and challenges are among the most anticipated ones in our anonymous authentication scheme:

1) Signature Forging: Generation of a signature by OBU_i involves the corresponding secret key s_i. As given in Equation (4), secret s_i is computed by CA using the system secret x, individual secret k_i, and h_i.

The system public key Q is known to all OBUs in a VANET. However, an adversary can not successfully determine the value of x from the knowledge of Q (= xG) due to the intractability of elliptic curve discrete logarithm problem.

On the other hand, k_i is a secret corresponding to the OBU_i, which is randomly generated and stored only within the CA. The hash value h_i is computed using k_i and G as given in $R_i = k_iG$ and $h_i = H_1(R_i)$. Therefore, an adversary would not be able to derive a valid signature on a message using OBU_i's k_i, h_i, and the system secret x.

2) Replaying Old/Expired Messages: Assume that an adversary attempts to replay and old and expired message m' in the VANET. The session parameter x'_p has been generated by the original sender using Equation (6) and (7) as shown in $k'_p = H_2(loc_p||t')$ and $(x'_p, y'_p) = k'_pR_i mod\ q$ where t' is the timestamp used by the original signer of the message. If t' is an old/expired timestamp, the current session parameter x_p generated by verifying nodes would be different from x'_p which would discard the signed m' as an invalid message. Therefore, repeating an old and expired signature would not pass the verification process at the receiver OBU/RSU.

3) Message Tunneling: Let, loc_p'' be the area identifier of a verifier. A session parameter would be generated at the verifier's end as $k_p'' = H_2(loc_p''||t)$ and $(x_p'', y_p'') = k_p''R_i mod\ q$. However, if the position of the original sender of the message is outside the communication range of the receiver, $loc_p'' \neq loc_p$ (where loc_p is is the position of the original signer). Therefore, the received session parameter x_p would be different from the receiver's session parameter x_p'', and hence signature verification of the message would be unsuccessful in a different area than the area of the original signer of the message.

An adversary is unable to forge a signature in this scheme. Also, an old message from an OBU would not pass the verification process, and since the area information is embedded with each signature; the verification process of the received message would be unsuccessful if it is delivered at an area outside the communication range of the original sender.

4) Non-repudiation: In order to generate a message signature, a signer requires a unique secret key s_i, as well as session parameters k_p and x_p as shown in Equation (6) and (7) respectively. Nevertheless, a valid signature can not be produced without the unique secret s_i of a node, which is generated by the CA from the master secret key x as given in Equation (4). Calculation of the system secret x involves solving an elliptic curve discrete-logarithm problem. Thus, if a signature is successfully verified by a receiver, the message must have been signed only by the sender with the corresponding unique secret s_i. As a result, once a message is signed and delivered, the sender OBU can not deny the signature for the sent message.

TABLE II
COMPARISON AMONG VANET AUTHENTICATION SCHEMES

Authentication Scheme	Signature size (Bytes)
WAVE 1609.2 [3]	182
Lu et al. [14]	189
GSIS. [15]	201
Wu et al. [20]	137
Hybrid [22] (un-optimized)	298
Our scheme (160-bit EC)	40
Our scheme (NIST P-224)	56
Our scheme (NIST P-256)	64

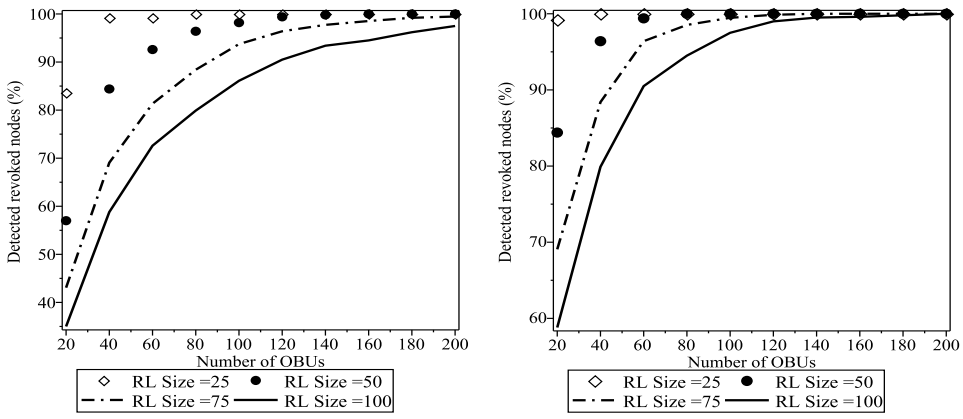
5) OBU Compromise: An attacker may compromise an OBU_i to obtain its unique secret credential s_i using which an adversary may sign false and malicious messages later on. However, an OBU_i does not store the unique secret key s_i in its memory (since it is generated and stored only at the CA). As indicated in Section V-C1, the corresponding user-password is XOR-ed with the unique secret key s_i, while the outcome s_{u_i} is stored in the memory of OBU_i. In order to activate the OBU_i, the corresponding user-password is entered which is XOR-ed with the s_{u_i} to reproduce the unique secret s_i for signing messages.

Hence, in order to obtain the original value of s_i, an attacker must know the corresponding user-password. Therefore, a compromise in our scheme would not let an adversary find the unique delegation secret s_i.

6) Signature Linking: An OBU may sign identical payloads in subsequent time-frames. A timestamp t is used for generation of a session parameter x_p (refer to Equation (7)) during the signature preprocessing phase. The timestamp t is valid until 100 ms from the signature generation time. It ensures the change of signature contents in different time frames even if the message resembles to a previously sent expired message. An adversary attempting to link two or more subsequent signatures may not be successful as the signature contents change every time due to the change of the timestamp.

E. Overhead

For a 160-bit elliptic curve, the size of $s_{p,i}$ is 40 bytes. The current security standards for VANET [3] suggest two different types of NIST [5] curves— P-224 and P-256 which have signature size of 56 bytes, and 64 bytes respectively. While P-224 is used for safety message broadcasts, P-256 is generally used for certificate generation and delivery. Note that we do not need any public key certificate in our scheme. Table II gives a comparison of signature overheads from other VANET message-authentication approaches.



(a) $\alpha = 2$ (b) $\alpha = 4$

Fig. 2. Randomizing the revocation process among OBUs for different RL sizes.

F. Identity Dispute and Revocation

On an identity dispute, CA may use the tainted vehicle's type-id and generate signatures using each individual secret s_i with the same type-id. If the alleged signature is a valid one, and the time, area information are accurate; it would match with one of the generated signatures by CA. Secret credentials of the matched signature are used to identify the tainted OBU.

When CA revokes an entity (say, OBU_i), it appends the corresponding secret s_i to the revocation list and sends an update to all suspected traffic locations through RSUs. Using the revoked s_i, an OBU can internally derive a new signature on each received message. If a received signature matches the derived one, verifying OBU identifies the sender as a revoked entity, and alerts the neighborhood.

Instead of checking through the complete revocation list, a random checking policy would enable an OBU or RSU randomly verify α number of entries from the revocation list. Figure 2 indicates the proportion of the detected revoked OBUs for different sizes of revocation lists. Revoked OBUs in a VANET have higher chances of being detected if the revocation list is smaller. Also, a higher α value ensures the detection of revoked entities by comparatively less number of users. Obviously, the more the neighboring OBUs are the greater the proportion of revoked nodes to be spotted in a VANET.

VI. EDCA Preliminaries

IEEE's Dedicated Short Range Communications or DSRC (IEEE 802.11p) [10] operates on a 75 MHz radio spectrum dedicated to a control channel (CCH), and 6 service channels (SCHs) in the range of 5.8/5.9 GHz.

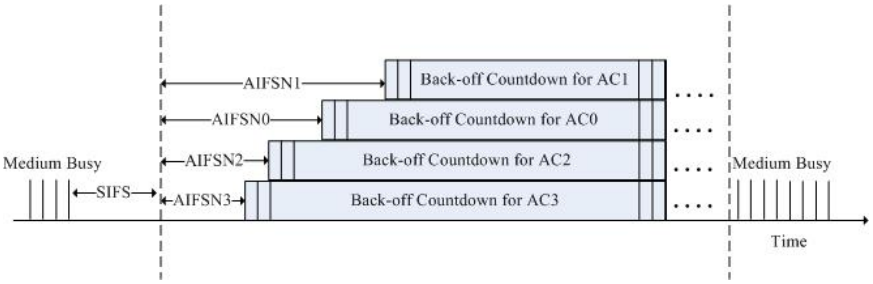


Fig. 3. IEEE 802.11p's EDCA mechanism

TABLE III
EDCA Parameters used in CCH(values taken from [9]).

ACI	AC	CWmin	CWmax	AIFSN
3	voice	3	7	2
2	video	3	7	3
0	best effort	7	15	6
1	background	15	511	9

The concept of user priority in DSRC has been borrowed from the IEEE 802.11e enhanced distributed channel access (EDCA) mechanism to induce the prioritized access for data transmission on each DSRC channel. Access over each channel can be performed using four access categories (AC_γ; $\gamma = 0..3$) as shown in Table III. Priority of AC_γ is regulated with two channel access parameters, namely the Arbitration Inter-Frame Space ($AIFS_\gamma$), and Contention Window (CW_γ). Unlike a unicast operation, WAVE broadcast using AC_γ uses only $CWmin_\gamma$ value to construct the backoff period.

We provide a brief outline on EDCA mechanism here with the help of Figure 3.

When the medium is idle, before transmitting a data frame, a station waits for $AIFS_\gamma = SIFS + AIFSN_\gamma \times t_{slot}$ where t_{slot} is the duration of one time slot ($t_{slot} = 16\mu sec$), and $AIFSN_\gamma$ is determined by the priority class γ.

If the medium becomes busy during $AIFS_\gamma$ period, the sender needs to wait for the end of busy period. As soon as the medium becomes idle, the sender restarts the $AIFS_\gamma$ waiting process before being able to perform any action.

When there is a frame to broadcast, the sender selects a random number between 0 and CWmin and counts down after every time slot while medium is idle. If the medium becomes busy, the station has to wait again for $AIFS_\gamma$ before being able to decrement the backoff counter. The sender can broadcast the packet only when the backoff counter reaches the value of 0. Broadcast packets are not acknowledged in EDCA. So in case of a packet collision, packet will be dropped.

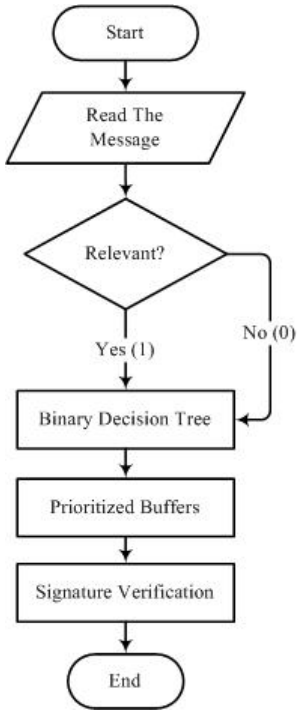


Fig. 4. Block diagram of our verification scheme.

VII. Priority-based verification of VANET safety messages

A. The Framework

Since vehicles in close proximity have similar safety features and attributes in their periodic messages, a portion of all received messages at a particular time would give a fair idea about the contemporary traffic condition in a VANET. In this scheme, an OBU prioritizes all received messages based on the relevance of some important physical attributes of a vehicle along with their EDCA classes.

A general framework of our scheme is given in Figure 4. We consider three different pieces of primary safety information– position, acceleration and speed to be extracted from all received messages. The collected information are fed into the corresponding Bloom Filters of the receiving entity. Individual Bloom Filters are deployed in each verifier entity in order to keep record of the most recent traffic safety updates. A primary overview of Bloom Filters is illustrated in our previous work [32].

An OBU periodically updates its own road-safety attributes (e.g. location, acceleration, speed etc.) into the corresponding Bloom Filters. Recent entries of road-safety information of the vehicle remain in the Bloom Filter's bit array until the Bloom Filter is reset.

Each Bloom Filter individually checks the corresponding part of the received payload, and compares it against the existing entries within the bit array. A perfect binary decision tree [33] as given in Figure 5 assigns each received message with a relevance score. The relevance score

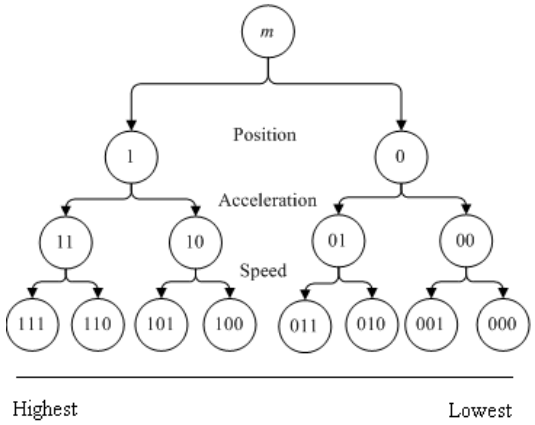


Fig. 5. Binary tree for relevance scores.

is determined based on the received message's similarity to the recent history of periodic safety information of the receiving entity.

1) Relevance Score from the Binary Tree: The root of the tree represents a received message m while the other subsequent parent nodes indicate the responses from the associated Bloom Filters at each level. Every tree level corresponds to an individual attribute of a safety message.

Up on reception, a periodic safety message's data payload is passed to the designated Bloom Filters where each filter checks for the specific part of the safety information. If a newly received message component *with an acceptable tolerance ([34])* matches an existing entry (i.e. any recent entry of the vehicle itself) in the corresponding Bloom Filter, it returns a 1. Otherwise, it returns a 0.

At each level of the tree, a left child of a parent node represents the corresponding relevance of safety information, and is given a value of 1. On the other hand, a right child of a parent node indicates the non-relevance of an associated safety attribute, and is given a value of 0. Assigned binary values from parent nodes are passed to the corresponding child nodes to determine the relevance score by concatenating the bits in order. Each received message in a receiving VANET entity is tagged with a relevance score defined by the leaves of the decision tree.

Messages tagged at the left most leaf are the most relevant ones (with relevance score 7) as the relevance score of the tagged messages tend to get lower as we move along from left to right at the bottom of the tree.

2) Prioritized Buffering of Messages: As shown in Figure 6, an OBU temporarily stores all received messages into four buffers according to their EDCA access categories. Each buffer contains corresponding access category messages arranged in the decreasing order of their relevance scores. The size of a buffer is determined by the maximum number of messages that can be verified within the time frame called $maxDuration[AC_\gamma]$ (for $\gamma = 0..3$). The verification probability

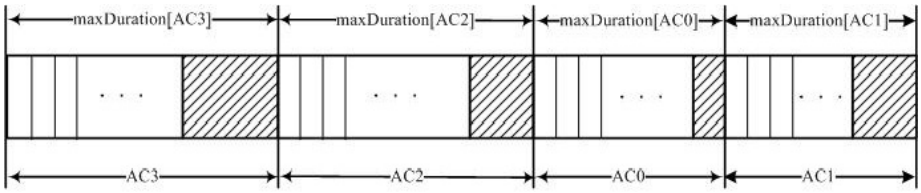


Fig. 6. Prioritized scheduling of message verification. Shaded area represents unused time-slots in a buffer.

(p_{v_γ}), and the time frame *maxDuration*[AC_γ] of a particular access category are proportional to the successful delivery ratio of the corresponding AC_γ messages.

Verifications of buffered messages are done in a round robin fashion over the message buffers in order of their priorities. The length of the round robin cycle should be shorter (say, 100 ms) than the maximum buffering time (say, 300ms) of un-authenticated messages.

If the total number of received safety messages in a round robin cycle exceeds the receiver's verification capacity, highest priority messages from across the prioritized buffers would be verified in each cycle.

B. Cross-layered Approach to Verification

VANET periodic safety messages use broadcast communications over the IEEE 1609.4 [9] MAC protocol which incorporates EDCA mechanism for prioritizing among the four traffic classes.

1) Back-off Time and Verification Probability: The WAVE EDCA mechanism ensures that a packet with the higher priority access class gets the preference to a packet from a lower priority access class during the transmission. Thus, lower access category packets in a VANET experience a higher packet drop rate than that of the higher access category packets. Packets drop in VANET communications due to the EDCA priorities of MAC layer transmissions, and the traffic intensity within the access class.

Apparently, the probability of successful packet delivery on a particular access category could be used as the basis of determining the verification probability of received messages. However, since broadcast messages are not acknowledged in EDCA, neither a sender nor a receiver of a message is aware of the collision leading to a packet drop event in the medium. Therefore, successful packet delivery ratio can not be used by a WAVE device to estimate the verification probability of received messages.

Nevertheless, the required back-off time for transmitting a packet also depends on: a) the MAC priority, and b) congestion within the traffic class just like a packet drop event in VANET. Hence, an alternative measure could be to use the back-off time of a message transmission to determine the verification probability of the prioritized buffers.

The correlation between the drop probability and the back-off time for a single message transmission over a particular access category is given as:

$$Corr(p_{d_\gamma}, BK_\gamma) = \frac{cov(p_{d_\gamma}, BK_\gamma)}{var(p_{d_\gamma}).var(BK_\gamma)} \tag{10}$$

for $\gamma = 0..3$, where the covariance $cov(p_{d_\gamma}, BK_\gamma) = \mathbf{E}(p_{d_\gamma} \times BK_\gamma) - \mathbf{E}(p_{d_\gamma}) \times \mathbf{E}(BK_\gamma)$; and $var(p_{d_\gamma})$, $var(BK_\gamma)$ are the variances of the drop probability p_{d_γ} and average back-off time for a message transmission BK_γ respectively. We further discuss the packet drop probability and back-off time in Section VIII.

We use the back-off time for a packet transmission in order to derive the verification probability of a particular access class in VANET.

$$p_{v_\gamma} = \left(1 - \frac{BK_\gamma^\omega}{\sum_{z=0}^{3} BK_z^\omega}\right) \times \frac{1}{\delta - 1} \tag{11}$$

where BK_γ is the average back-off time for a message delivery over AC_γ, δ is the number of ACs in use by OBUs in VANET, ω is a scaling factor which provides a weight value to the verification probability of an individual access category.

An OBU can estimate its average back-off delay for all access categories while transmitting different priority data frames. If an OBU does not have any data to transmit from a particular access category, it can still measure the back-off time by transmitting a zero payload probing packet over the specific access class. Authentication primitives for the probing packet are not required as it would be ignored by all nodes upon reception.

2) Adaptive Scheduling of Message Buffers for Verification: When a buffer for a particular access category messages is fully or partially empty, the verifier application chronologically verifies the buffered messages (if there is any) before switching to the next buffer. Unused verification time from each individual buffer is distributed among all the access classes following the ratio of their successful message delivery. The maxDuration[AC_γ] (where $\gamma = 0..3$) values are updated at the end of the verification of each access category buffer. This ensures the fairness in distribution of the unused time among the buffered messages. Algorithm 1 illustrates the procedure of scheduling the message buffers for prioritized verification of received messages.

3) Stabilizing the Bloom Filters: Frequent updates from the neighboring vehicles would contribute to the rapid growth of the number of elements in a Bloom Filter's bit array, affecting the performance of the filter with false positive errors since the size of a Bloom Filter is constant. A large size Bloom Filter may resolve the problem to some extent, but it aggravates the false positive rate for some of the elements in the bit array [35].

A *stable* Bloom Filter [36] stores only the most recent elements in the bit array with the requirement of extra spaces to save the history for each element of the bit array. Since there is no way to separate the most recent elements from the old ones in an ordinary Bloom Filter,

Algorithm 1 Adaptive scheduling of message verification.

DEFINE AC {AC3,AC2,AC0,AC1}
while (TRUE) **do**
  AC ← AC3;
  bufferCount ← 4;
  while (bufferCount>0) **do**
    bufferCount−−;
    if (buffer[AC]! =null)AND(elapsedTime[AC]<maxDuration[AC]) **then**
      VERIFY messages from the beginning of buffer[AC];
    else if (buffer[AC]==null) **then**
      $excessTime[AC] \leftarrow maxDuration[AC] - elapsedTime[AC]$;
      for $index = 0$ to 3 **do**
        $maxDuration[AC_{index}] \leftarrow maxDuration[AC_{index}] + \frac{p_{v_{index}} \times excessTime[AC]}{\sum_{z=0}^{3} p_{v_z}}$;
      end for
      AC ← NEXT AC;
    else if (elapsedTime[AC]>=maxDuration[AC]) **then**
      AC ← NEXT AC;
    end if
  end while
end while

we must clear the *aged* Bloom Filter, and re-load it with fresh elements at a regular interval in order to restrict the error probability to a fixed level.

In a traffic scenario of N vehicles in the communication range of a verifier entity, let us assume that the refresh interval of a Bloom Filter is I seconds, and the periodic transmission rate is f messages per second. Then, elements inserted into each Bloom Filter before resetting is computed as, $n_{bf} = N \times I \times f$.

The relationship between the total number of elements n_{bf}, and the Bloom Filter size M for an optimal use with a predefined error probability of P_{error} is given as, $n_{bf} \approx M \times \frac{(ln\,2)^2}{|ln\,P_{error}|}$; [35].

Combining these two above relationships, we get:

$$I \approx \frac{M}{N \times f} \times \frac{(ln\,2)^2}{|ln\,P_{error}|}. \tag{12}$$

Therefore, the refresh interval of a Bloom Filter depends on the number of total data entries, as well as the error probability of the corresponding Bloom Filter.

C. Mitigating vulnerabilities

Our approach allows safety message authentication according to the relevance score of received messages in the individual access category. Received messages from closer OBUs get higher verification opportunity than others and messages from distant OBUs are less likely to be chosen for the verification. Since a message with higher relevance score is relatively close, and hence more important to the verifier, an attacker would be spotted easily by the verifying entity.

VIII. Performance Evaluation

A. Network Simulation Setup

We developed a WAVE-based simulator with four MAC priorities to investigate our authentication and verification scheme using the network simulator ns-2.34. To the best of our knowledge, this is the first simulator to implement VANET's periodic message broadcast with MAC-layer's EDCA access categories.

We consider a simple urban vehicular traffic scenario in a $1500m \times 100m$ bidirectional road with 2 lanes in each direction. Vehicles' speed vary following a Gausian distribution with mean of 60 km/hr and standard deviation of 5 km/hr. An RSU is installed at the roadside while different number of OBUs are mounted with moving vehicles on road. We allow the RSU and OBUs to broadcast a WSMP packet every 100 ms for simulating OBU's basic safety messages and RSU's periodic service announcements, respectively. RSU transmits its periodic messages over the highest access category AC3 while equal number of OBUs broadcast their periodic safety messages over each access category.

Times of the initial message broadcast for individual OBUs and the RSU have been selected from a uniform distribution over 100 ms period. We run each experiment for 90 seconds following a 10 seconds warm up period. Each experiment has been conducted 10 times using different seeds, while individual results are averaged for the final outcome.

We implemented the EDCA mechanism over IEEE Std 802.11p MAC and PHY provided by ns-2.34's IEEE 802.11Ext package given in [37]. EDCA parameters as shown in III have been configured for four access categories. We assume that each VANET entity operates only on the control channel (CCH) with a specific priority class. Other MAC and PHY parameters used in our simulation are listed in Table IV. Payloads for the ordinary WSM broadcast is set to 254 Bytes as indicated in the WAVE Standard (see C.6 of [3]). Since our authentication scheme does not require any third party certificates, the payload size in our scheme is reduced to 128 Bytes.

TABLE IV
SIMULATION PARAMETERS FOR MAC AND PHY

Parameters	Values
Radio Range	500m
Data Rate	6Mbps
Slot Time	16μs
SIFS	32μs
Bandwidth	10MHz
Frequency	5.89GHz
Propagation Model	TwoRayGround

B. Packet Drop Probability and Backoff Delay

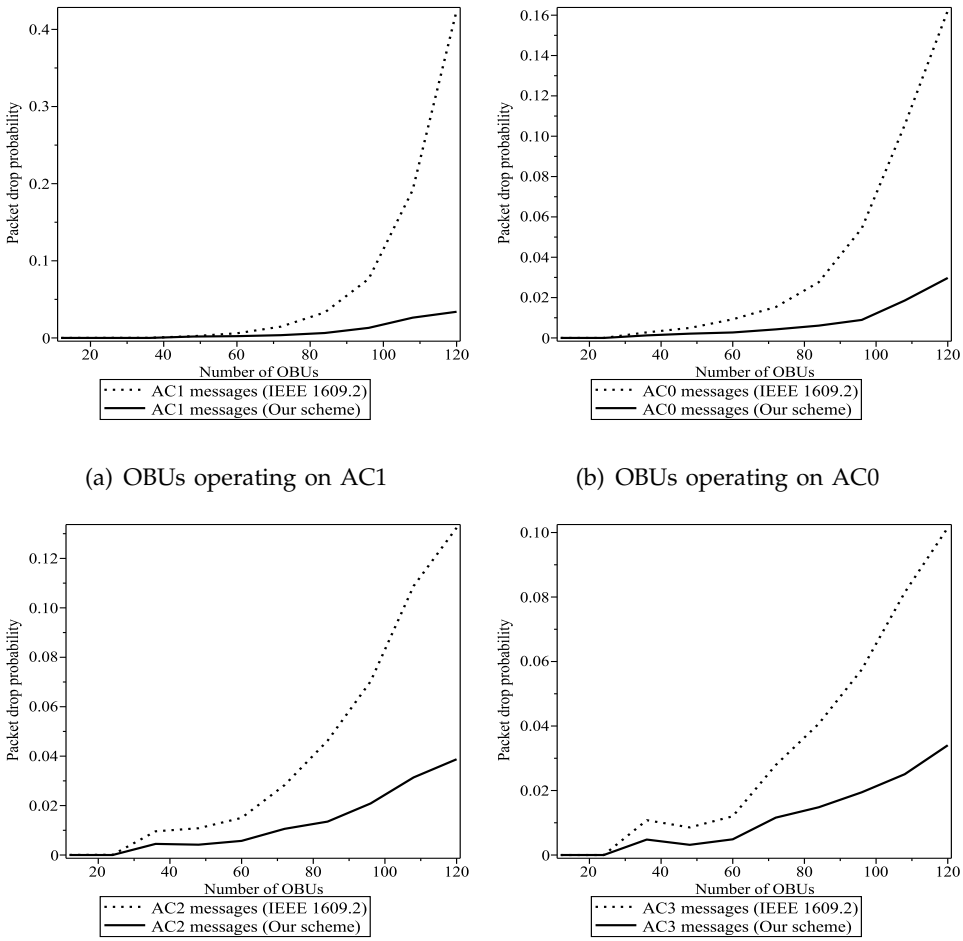
Packet delivery in a wireless network is impaired due to the excessive offered load, and inherent noise of the medium. Figure 7 illustrates the affect of different access categories on OBUs' periodic transmissions in terms of the probability of failed delivery of broadcast messages. The probability of packet drop climbs as the number of OBUs increases. Exclusion of the trusted third-party certificate with each OBU message implies reduced payload size in our authentication scheme, which results in a lower packet drop rate compared to the IEEE Std 1609.2-based authentication in VANETs.

Unlike an OBU's periodic transmission, an RSU includes a trusted third-party certificate with every individual broadcast. However, this inclusion does not significantly affect the vehicular communications as the number of OBU messages is much higher than that of RSU's.

Figure 8 presents the average back-off period measured for each individual transmission using IEEE Std 1609.2-based authentication and our approach respectively. The back-off time in EDCA depends on the AIFSN value, as well as the CW size of the corresponding access category. Therefore, higher access class messages have low back-off time, and vice versa. Our authentication scheme is lighter than the conventional ECDSA scheme used in IEEE Std 1609.2, and hence it incurs reduced back-off delay compared to the ECDSA-based approach. This would accelerate the message authentication process in a high-speed road-traffic condition of VANET.

C. Prioritized Verification Probability

Table V shows strong correlations (over 95%) between the message drop probability (Figure 7) and the average back-off time to transmit a message (Figure 8) for each access category with IEEE Std 1609.2- and our authentication scheme. This would allow an OBU to utilize its average back-off time as the basis of determining the verification priority of a particular access class using Equation (11). The verification probabilities of received messages for different access categories are presented in Figure 9. The verification probability of each access class is determined



(a) OBUs operating on AC1

(b) OBUs operating on AC0

(c) OBUs operating on AC2

(d) OBUs operating on AC3

Fig. 7. Drop probability of periodic safety messages for OBUs over different access categories

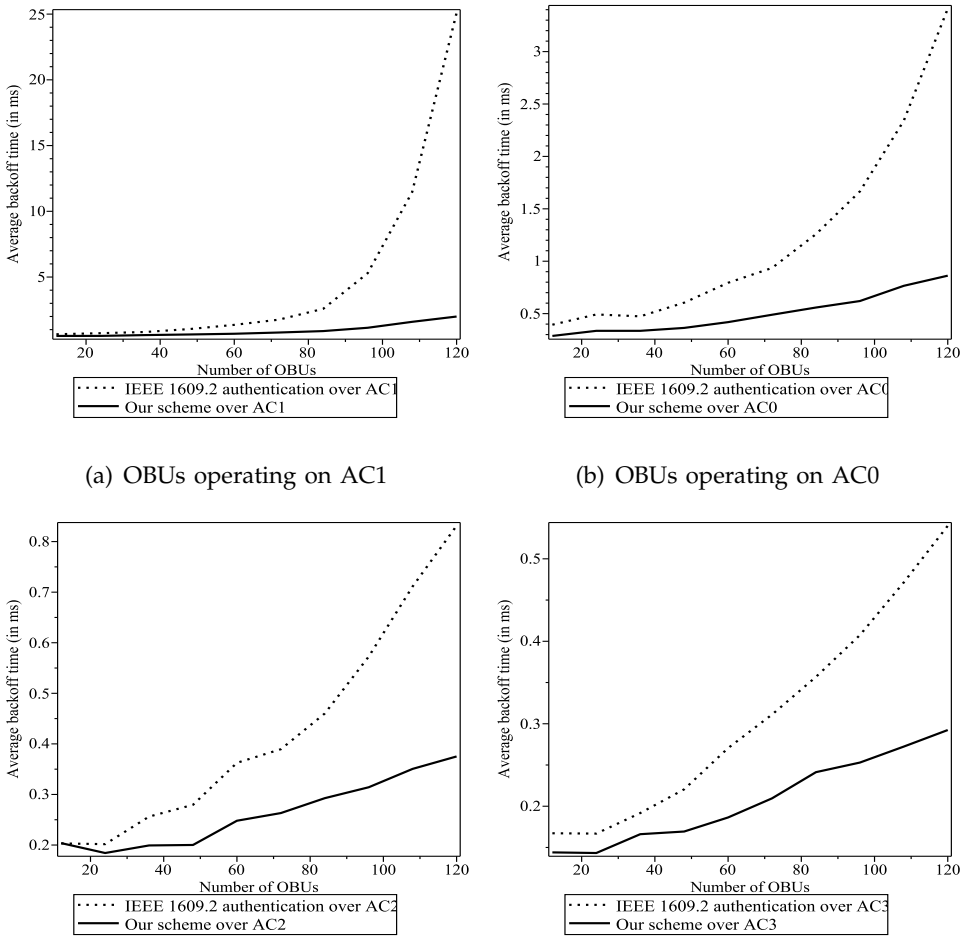
TABLE V

Correlation between drop probability of OBU messages and the average backoff period for different access categories.

	Access Categories			
Approaches	AC1	AC0	AC2	AC3
IEEE 1609.2	0.9998	0.9918	0.9908	0.9835
Our scheme	0.9961	0.9501	0.9659	0.9767

according to the Equation (11). For any number of OBUs in a VANET with different access classes, cumulative message verification probability is always 1.

When traffic load is increasing, verification probabilities for lower priority traffic classes (AC1 and AC0) diverge significantly due to their larger contention windows and AIFSN values compared to the higher priority access classes (AC3 and AC2). This is because back-off times for all access classes are increasing at different rates. For instance, traffic classes with lower priorities have higher increase of back-off time which leads to decrease of their message verification probability as shown in the Equation (11). Therefore, under high traffic-load message verification



(a) OBUs operating on AC1

(b) OBUs operating on AC0

(c) OBUs operating on AC2

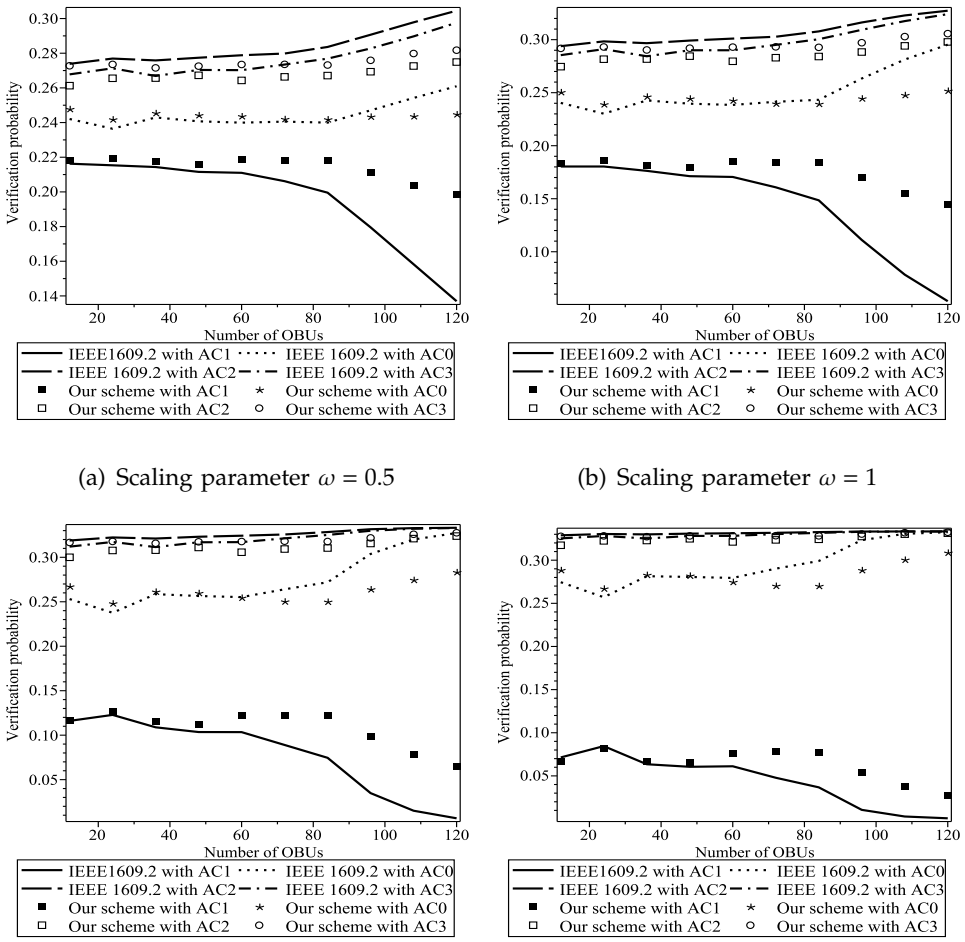
(d) OBUs operating on AC3

Fig. 8. Average backoff delay in periodic transmissions for different access categories.

probability of access classes AC3 and AC2 will increase on behalf of access classes AC0 and AC1. Since high offered load takes place in a VANET due to the rush hour traffic or a consequence of an accident, this scheme allows verification of the most important messages in such critical condition.

Our signature scheme allows a user to have shorter traffic-safety messages compared to the conventional IEEE Std 1609.2-based authentication. Shorter messages allow smaller back-off pause times during the transmission and therefore verification probabilities of different access categories are less diverging for our scheme than that of the standard approach.

A larger ω value emphasizes more on high priority ACs while a smaller value of ω reduces the differences among verification probabilities of the access classes.



(a) Scaling parameter $\omega = 0.5$

(b) Scaling parameter $\omega = 1$

(c) Scaling parameter $\omega = 2$

(d) Scaling parameter $\omega = 3$

Fig. 9. Verification probability of individual access category messages with different values of scaling parameter.

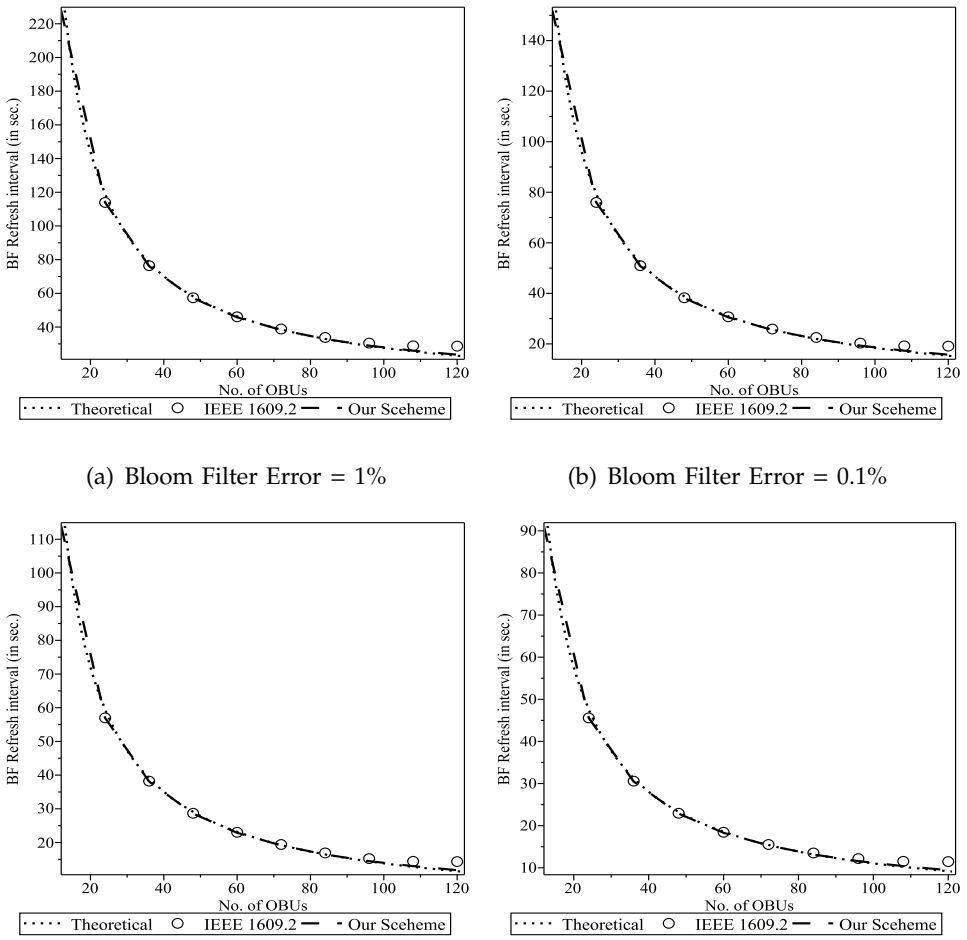
D. Refresh Interval

The refresh interval of a Bloom Filter depends on the number of input data elements (received messages in our case), the size of the filter M, and the error probability P_{error} as given in Equation (12). We choose $M = 32KB$ for our Bloom Filters with P_{error} = 1%, 0.1%, 0.01% and 0.001% for each experiment.

Utilizing the total number of successfully transmitted messages from simulations, we determine the refresh interval of the Bloom Filter for OBUs. Figure 10 presents the Bloom Filter's refresh interval for different error probabilities. Since a Bloom Filter does not store any message payload, the interval values do not depend on the underlying authentication scheme, but on the chosen error probability of the Bloom Filter.

Since a user can not precisely determine the number of neighboring OBUs during an intense traffic condition (due to potential packet loss in broadcast communications), a Bloom Filter should be pre-configured with a fixed value of its refresh interval. The interval must be less

than or equal to the minimum refresh interval for the highest number of neighboring OBUs the Bloom Filter is designed for.



(a) Bloom Filter Error = 1%

(b) Bloom Filter Error = 0.1%

(c) Bloom Filter Error = 0.01%

(d) Bloom Filter Error = 0.001%

Fig. 10. Refresh interval of a Bloom Filter for different combination of RSU and OBU access categories.

IX. Conclusion

We designed an identity-based anonymous user-authentication scheme and a cross-layer verification approach for WAVE-enabled VANET's safety messages. A variation of the conventional ECDSA approach is used with the identity-based signature approach where the common geographical area information of signing vehicles is taken as the signer's identity. This exempts a vehicle from the mandatory inclusion of a trusted third-party certificate with each broadcast message in a VANET while a user is still identifiable by the trusted third-party up on a dispute. A cross-layer message verification scheme verifies the received messages based on their MAC traffic class and traffic intensity. This ensures that under the rush hour congestion or traffic accident most important messages will not be missed by the verifier. Security analysis and

performance evaluation justify our authentication and verification approach for WAVE-enabled vehicular communications.

References

[1] T. El Gamal, "A Public Key Cryptosystem and A Signature Scheme Based On Discrete Logarithms," in *Proceedings of CRYPTO 84 on Advances in cryptology*. New York, NY, USA: Springer-Verlag New York, Inc., 1985, pp. 10–18.

[2] D. Johnson and A. Menezes, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," Certicom Research, Canada; and Dept. of Combinatorics and Optimization, University of Waterloo, Canada, Tech. Rep., 1999.

[3] "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)- Security Services for Applications and Management Messages," IEEE, New York, NY, IEEE Std 1609.2, Jul. 2006.

[4] *Digital Signature Standard (DSS)*. Washington: National Institute of Standards and Technology, 2000, uRL: http://csrc.nist.gov/publications/fips/. Note: Federal Information Processing Standard 1862.

[5] NIST, "NIST: National Institute of Standards and Technology," http://www.nist.gov/index.html, 2011.

[6] C. Cocks, "An Identity Based Encryption Scheme Based on Quadratic Residues," in *Proceedings of IMA International Conference*. Cirencester, UK: Springer-Verlag, Dec. 2001, pp. 360–363.

[7] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," in *Selected Areas in Cryptography*, ser. Lecture Notes in Computer Science, K. Nyberg and H. Heys, Eds. Springer Berlin / Heidelberg, vol. 2595, pp. 310–324.

[8] "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)- Networking Services," IEEE, New York, NY, IEEE Std 1609.3, Apr. 2007.

[9] "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)- Multi-channel Operation," IEEE, New York, NY, IEEE Std 1609.4, Nov. 2006.

[10] "Draft Amendment for Wireless Access in Vehicular Environments (WAVE)," IEEE, New York, NY, IEEE Draft 802.11p, Jul. 2007.

[11] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing Vehicular Communications," *IEEE Wireless Communications Magazine*, vol. 13, no. 5, pp. 8–15, Oct. 2006.

[12] Y. Sun, R. Lu, X. Lin, X. S. Shen, and J. Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3589 –3603, 2010.

[13] F. Zhang, R. Safavi-naini, and W. Susilo, "An Efficient Signature Scheme From Bilinear Pairings and Its Applications," in *PKC 2004, LNCS 2947*. Springer-Verlag, 2004, pp. 277–290.

[14] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," in *Proceedings of he 27th Conference on Computer Communications (INFOCOM)*, Phoenix, AZ, USA, Apr. 2008, pp. 1229–1237.

[15] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[16] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA Broadcast Authentication Protocol," *RSA CryptoBytes*, vol. 5, no. Summer, pp. 2–13, 2002.

[17] S. Biswas and J. V. Misic, "Deploying Proxy Signature in VANETs," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM 2010)*. Miami, Florida, USA: IEEE, 2010, pp. 1–6.

[18] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *SIAM Journal of Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[19] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," in *Proceedings of The 24rd Annual International Cryptology Conference (CRYPTO 04), LNCS series*. Santa Barbara, CA, USA: Springer-Verlag, 2004, pp. 41–55.

[20] Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, "Balanced Trustworthiness, Safety, and Privacy in Vehicle-to-Vehicle Communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 559 –573, 2010.

[21] Massachusetts Institute of Technology, "CIS: The Threshold Cryptography," http://groups.csail.mit.edu/cis/cis-threshold.html, 2009.

[22] G. Calandriello, P. Papadimitratos, J. P. Hubaux, and A. Lioy, "Efficient And Robust Pseudonymous Authentication in VANET," in *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks (VANET '07)*. ACM, 2007, pp. 19–28.

[23] J. Guo, J. Baugh, and S. Wang, "A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework," in *Proceedings of Mobile Networking for Vehicular Environments 2007*, Anchorage, Alaska, USA, May 2007, pp. 103–108.

[24] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "An Efficient Message Authentication Scheme for Vehicular Communications," *IEEE Transactions on Vehicular Technology*, vol. 57, pp. 3357–3368, 2008.

[25] S. Biswas and J. Misic, "Location-based Anonymous Authentication for Vehicular Communications," in *PIMRC 2011: Proceedings of the 22nd IEEE Symposium on Personal, Indoor, Mobile and Radio Communications*. Toronto, ON, Canada: IEEE Communication Society, 2011, pp. 1–5.

[26] Z. Li and C. Chigan, "On Resource-Aware Message Verification in VANETs," in *Proceedings of IEEE International Conference on Communications*. Cape Town, South Africa: IEEE, May 2010, pp. 1–6.

[27] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: A Robust Signature Scheme For Vehicular Networks Using Binary Authentication Tree," *Wireless Communications, IEEE Transactions on*, vol. 8, no. 4, pp. 1974–1983, April 2009.

[28] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," in *Proceedings of The 27th Conference on Computer Communications. IEEE INFOCOM 2008.*, Phoenix, AZ, USA, April 2008, pp. 246–250.

[29] J. H. Cheon and J. H. Yi, "Fast Batch Verification of Multiple Signatures," in *Proceedings of the 10th International Conference on Practice and Theory in Public-Key Cryptography - PKC 2007*, Beijing, China, April 2007, pp. 442–457.

[30] S. D. Galbraith, K. G. Paterson, and N. P. Smart, "Pairings for cryptographers," *Discrete Appl. Math.*, vol. 156, pp. 3113–3121, Sep. 2008.

[31] S. Biswas, J. V. Misic, and V. Misic, "DDoS Attack on WAVE-enabled VANET Through Synchronization," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM 2012)*. Anaheim, CA, USA: IEEE, 2012, pp. 1–6.

[32] S. Biswas and J. Misic, "Relevance-based Verification of VANET Safety Messages," in *Proceedings of IEEE International Conference on Communications, ICC 2012*. Ottawa, ON, Canada: IEEE, June 2012, pp. 1–5.

[33] NIST, "NIST: National Institute of Standards and Technology," http://xlinux.nist.gov/dads/HTML/perfectBinaryTree.html, 2011.

[34] S. Biswas, J. Misic, and V. Misic, "ID-based Safety Message Authentication for Security and Trust in Vehicular Networks," in *Distributed Computing Systems Workshops (ICDCSW), 2011 31st International Conference on*, Minneapolis, MN, USA, June 2011, pp. 323–331.

[35] P. S. Almeida, C. Baquero, N. Preguiça, and D. Hutchison, "Scalable Bloom Filters," *Information Processing Letters*, vol. 101, pp. 255–261, March 2007.

[36] F. Deng and D. Rafiei, "Approximately Detecting Duplicates For Streaming Data Using Stable Bloom Filters," in *Proceedings of the 2006 ACM SIGMOD international conference on Management of data*, ser. SIGMOD '06. Chicago, IL, USA: ACM, 2006, pp. 25–36.

[37] Q. Chen, F. Schmidt-Eisenlohr, D. Jiang, M. Torrent-Moreno, L. Delgrossi, and H. Hartenstein, "Overhaul of IEEE 802.11 Modeling and Simulation in ns-2," in *Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems*, ser. MSWiM '07. New York, NY, USA: ACM, 2007, pp. 159–168.