An ECDSA based Anonymous Authentication Scheme Using WFQ Mechanism for Verification in VANETs

Dr. Ganesh Babu T.V.J.[#1], **Mrs. Anuradha T** [*2]
[#1]Dept. of ECE, St. Martin's Engineering College, Hyderabad,.[*2]Dept. of ECE, MLR Institute of Technology, Hyderabad
[1]drganesh2014@gmail.com, [2]arun_anu04@yahoo.co.in

***Abstract*—**We use an anonymous authentication involving a central authority and a prioritized weighted fair queuing based verification scheme for the IEEE Wireless Access in Vehicular Communications based vehicular ad-hoc networks (VANETs). The proposed approach has reduced computational load for processing periodic road safety messages. Based on vehicle's current GPS position information, a group ID based elliptic curve digital signature algorithm is used. This excludes the necessity of third party public key certificate for message authentication in VANETs. A high-density road traffic condition constitutes a challenge for authentication of vehicular messages, since the required verification time is much longer than the average inter-arrival time. In order to reduce the effects of this issue, messages of each traffic class are verified following the VANET's medium access control (MAC) layer priorities with a Weighted Fair Queuing (WFQ) strategy and the application relevance of individual safety messages. Simulation shows that this approach is secure, privacy preserving, and resource efficient.

***Keywords*—** **Elliptic Curve Digital Signature Algorithm (ECDSA), Authentication, WFQ, Enhanced Distributed Channel Access (EDCA), OBU, RSU, IEEE 802.11p**

I. INTRODUCTION

Vehicular ad hoc network (VANET) uses cars as mobile nodes in a MANET to create a mobile network. A VANET turns every participating car into a wireless node, allowing cars over a distance of 1km or less to communicate with each other and, in turn, create a network. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Network is created. But with Road Side Units (RSUs), the vehicle's On-Board Units (OBUs) can access the infrastructure related services also. A typical VANET structure is shown in Fig. 1.

VANETs have attracted extensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles [1][2]. VANETs consist of entities including On-Board Units (OBUs) and infrastructure Road-Side Units (RSUs). Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are the two basic communication modes, which, respectively, allow OBUs to communicate with each other and with the infrastructure RSUs[11]. Since vehicles communicate through wireless channels, a variety of attacks such as injecting false information, modifying and replaying the disseminated messages can be easily launched.

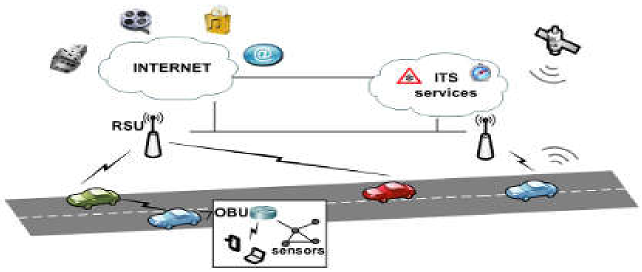


Fig. 1 Vehicular ad hoc networks

A security attack on VANETs can have severe harmful or fatal consequences to legitimate users. Consequently, ensuring secure vehicular communications is a must before any VANET application can be put into practice. A well recognized solution to secure VANETs is to deploy Public Key Infrastructure (PKI), and to use Certificate Revocation Lists (CRLs) for managing the revoked certificates. In PKI, each entity in the network holds an authentic certificate, and every message should be digitally signed before its transmission. A CRL, usually issued by a Trusted Authority (TA), is a list containing all the revoked certificates. In a PKI system, the authentication of any message is performed by first checking if the sender's certificate is included in the current CRL, i.e., checking its revocation status, then, verifying the sender's certificate, and finally verifying the sender's signature on the received message. Vehicular Ad Hoc Networks (VANET)[3][5] have been envisioned to play an important role in the future wireless communication service market for safety communications as well as for information and entertainment applications. Examples of safety oriented applications for VANET are the notifications of emergency situations, such as car accidents or bad weather conditions. A typical secure communication between OBUs is shown in Fig. 2.

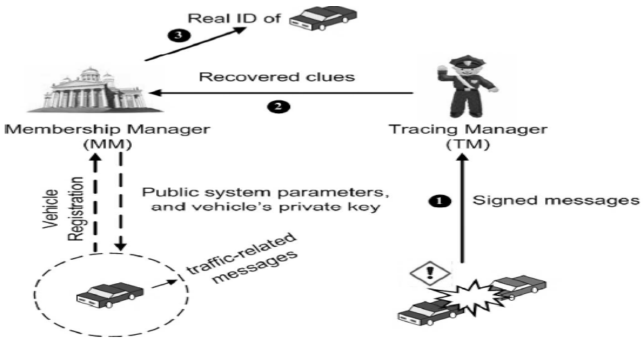


Fig. 2. Secure Communication between OBUs and CA.

A VANET entity is required to transmit periodic safety messages containing its current coordinates, speed, and acceleration to neighbouring devices. The typical interval for safety message broadcasts ranges from 100 to 300 ms. Received messages are verified by the receiving entity to ensure message integrity and authenticity of the sender's identity. Although the verification delay is on the order of milliseconds, under a heavy-traffic scenario, many of the safety messages would be either discarded due to the constrained buffer size of the verification process or accepted without any verification. Therefore, during a busy traffic hour, 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 as soon as its maximum verification capacity is reached.

We consider a WAVE-based WFQ based scheme of conditional privacy-preserving authentication for signing and verifying vehicular safety application messages. We use a variant of ECDSA mechanism incorporating an identity-based (ID-based) authentication scheme [14],[16] 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 on 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 verification mechanism considers medium access control (MAC) layer priorities to derive weights for WFQ mechanism for verification of received messages.

II. SYSTEM DESCRIPTION AND DESIGN

A WAVE standard based VANET using anonymous authentication and verification procedures can be implemented in various ways as discussed in the literature [1]-[11]. Anonymous authentication can be implemented using short-lived anonymous certificates. A certificate is used from the pool every time an OBU signs a message. However, because of the large certificate pool, rigorous effort would be needed to resolve an identity dispute. In addition, revocation of a user's certificate pool becomes harder since the size of the revocation list grows at a severe rate.

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. Verification of a large number of signed messages in a given time has been addressed in two major ways: random verification and aggregated (batch) verification of messages. In a random verification scheme, received messages are randomly selected for verification by a receiving entity. A batch verification technique in a VANET allows verification of all received messages simultaneously. Most batch verification schemes proposed for VANETs use a costly bilinear-pairing-based verification technique. A fast batch verification mechanism has been presented by Cheon *et al.* [15] using the ECDSA authentication scheme. A batch verification mechanism is an efficient way of ensuring the trust of multiple messages received in a unit time. Nevertheless, the implementation of this approach depends on the underlying mechanism of the signature protocol.

The design goal is to overcome the anticipated attack and vulnerabilities on an anonymous authentication scheme for VANET. We suggest a third-party trusted authority called a 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., the police, the courts, and the Department of Transportation). The CA is secured and protected against all sorts of physical attacks and adversarial compromises. To provide anonymous authentication through signed messages in a VANET, each participating OBU in a given area must have a common identifier. Identity information on 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. 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 when resolving a traffic dispute that involves VANET communications. This particular aspect can be implemented by using most significant bits of GPS position information so that all OBUs, will have same value in a region, to derive the anonymous identifier.

Additionally, the design goal also involves prioritized verification of messages especially when the message traffic is high leading to mitigating the effect of vulnerabilities. For example, when performing random verification of messages, the high priority messages will be verified more frequently than the low priority messages thus mitigating the effect of random verification attack of high priority application messages.

III. ECDSA BASED ANONYMOUS AUTHENTICATION

The steps involved in this authentication method are based on the modification of the original ECDSA mechanism as explained below. The first step involves obtaining the group identifier.

I. CA chooses system secret x, where $1 < x < q$, and computes $Q = xG$, where Q is master public key.

II. CA associates random primary secret k_i (where $1 < k_i < q$) with each individual OBU_i of a particular type. The vehicle-type identifier $R_i = k_iG$. Suppose, $i, i + 1, i + 2, \ldots, i + N - 1$ are registered vehicles. CA computes the group identifier $R_i = k_i(mod\ q)G = k_{i+1}(mod\ q)G = k_{i+2}(mod\ q)G = \cdot\cdot\cdot = k_{i+N-1}(mod\ q)G.$

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 master secret x using the corresponding primary secret k_i and h_i values, as succeedingly indicated.

$$s_i = 1 + xh_ik_i^{-1} \ mod\ q. \qquad (1)$$

Derived user secret $s_{ui} = s_i \oplus Password$ is securely copied to the corresponding OBU_i's disk space.

The second step involves pre-processing. In the beginning of OBU activation, a user enters his password, which is then XOR-ed with the saved secret s_{ui} 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 acci-dent 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 follows:
The signing vehicle determines k_p for message m, i.e.,

$$k_p = H_2(loc_p \,||\, t). \qquad (2)$$

where loc_p is the area identifier of a user during session p.

It then computes session parameter x_p as

$$(x_p, y_p) = k_p R_i mod\ q. \qquad (3)$$

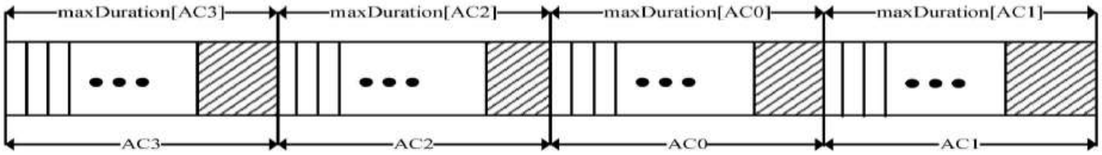
The next step is to generate the signature, which is performed by multiplying by inverse of kp with sum of H1(m) and *si xp* with entire result taken modulo of q. The signature payload and the message are combined as (m||Ri||*sp,i*), to deliver to neighbouring OBUs and RSUs.

The final step of verification is done by a receiving entity which computes kp from its own area information and the current timestamp using the relationship given in Equation 2. And Equation 3 is used to obtain (xp,yp) values by the verifier and hi is computed as H1(Ri).

Finally, if $(x_p, y_p) = (H_1(m)R_i + x_p(R_i + h_iQ))s_{p,i}^{-1}$
$mod\ q$ holds, the signature is verified as valid.

IV. WFQ BASED VERIFICATION

The Fig. 3 shows prioritized scheduling of message verification, where the shaded area represents unused timeslots in a buffer. As shown in Fig. 3, 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
$\gamma = 0, \ldots, 3$). The verification probability ($p_{v\gamma}$) and the time frame $maxDuration[AC_\gamma]$ of a particular access category are proportional to the successful delivery ratio of the corresponding AC_γ messages.



Prioritized scheduling of message verification. Shaded area represents unused timeslots in a buffer.

Fig. 3 WFQ prioritised scheduling of message verification

Verifications of buffered messages are done in a WFQ fashion over the message buffers in order of their priorities. If the total number of received safety messages in a WFQ cycle exceeds the receiver's verification capacity, highest priority messages from across the prioritized buffers would be verified in each cycle. The messages are stored in the order of relevance so that the messages carrying sensitive information will be buffered ahead of less sensitive information carrying messages. The WFQ policy is adaptive in the sense when the required amount of service is to be given to high priority queues during high traffic condition, the available capacity will be shared once again according to the priorities set to the low priority queues, during the times of low traffic.

We select the weights in such a way that during heavy traffic condition, high priority message queues are given more time. The weights are selected as a function of AIFS (Arbitration Inter-frame space) interval, contention window and the transmit opportunity (TXOP) limit.

V. PERFORMANCE EVALUATION

We use network simulator 2, to simulate this WAVE based security system with four MAC priorities. A simple urban vehicular traffic scenario in a 1500 m × 100 m bidirectional road with two lanes in each direction is considered. Vehicle speeds vary following a Gaussian distribution with a mean of 60 km/h and a standard deviation of 5 km/h. An RSU is installed at the roadside, whereas different number of OBUs are mounted with moving vehicles on road. We allow the RSU and OBUs to broadcast a WSMP (WAVE Short Message Protocol) 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, whereas an 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 s following a 10-s warm-up period. Each experiment has been conducted ten times using different seeds, whereas individual results are averaged for the final outcome. Payloads for the ordinary WSM broadcast is set to 254 bytes as indicated in the WAVE Standard[3]. Since our authentication scheme does not require any third-party certificates, the payload size in our scheme is reduced to 128 bytes. We perform simulation with number of OBUs set to 20, 40, 60, 80, 100 and 120. The following Fig. 4 shows the typical initial set up for 20 OBUs.

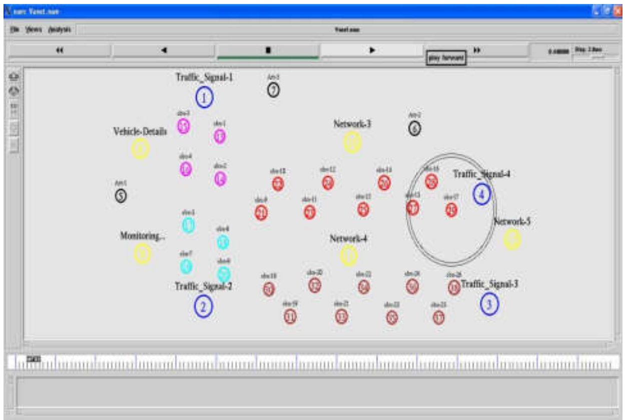


Fig. 4 Vehicle nodes OBUs and RSU Initialisation

The following Fig. 5 shows the scenario of message exchanges between OBUs and RSU during the scenario of an accident.

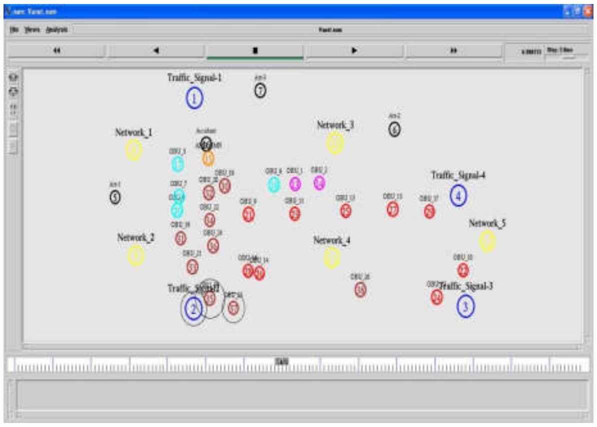


Fig. 5 Information exchange during traffic accident scenario.

Table II shows the results of average packet drop probability and verification probability comparison of access categories with WFQ scheme and with IEEE 1609.2 fixed priority scheme, for 120 OBUs. As can be seen WFQ based scheme achieves better results.

TABLE II

SIMULATION VALUES COMPARISON FOR 120 OBUS

Access Category	WFQ based scheme		IEEE 1609.2	
	Average packet drop probability	Verification Probability	Average packet drop probability	Verification Probability
AC3	0.025	0.31	0.10	0.33
AC2	0.029	0.29	0.12	0.30
AC1	0.031	0.26	0.16	0.24
AC0	0.038	0.15	0.4	0.22

VI. CONCLUSIONS

A group ID-based anonymous user authentication scheme and a WFQ based verification approach to WAVE-enabled VANET's safety messages is analysed. A variation of the conventional ECDSA approach is used with the ID-based signature approach, where the common geographical area information on 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, whereas a user is still identifiable by the trusted third party upon a dispute. A WFQ based message verification scheme verifies the received messages based on their MAC traffic class. This ensures that under rush-hour congestions or after a traffic accident, most important messages will not be missed by the verifier. Security analysis and performance evaluation justify our authentication and verification approach to WAVE-enabled vehicular communications by providing better performance.

ACKNOWLEDGMENT

The first author would like to acknowledge the management of St. Martin's Engineering College, Hyderabad for its continued support.

The second author would like to express the gratitude for the management of MLR Institute of Technology, Hyderabad.

REFERENCES

[1] T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in Proc. CRYPTO, Santa Barbara, CA, USA, Aug. 1985, pp. 10–18.

[2] D. Johnson and A. Menezes, "The elliptic curve digital signature al-gorithm (ECDSA)," Certicom, Mississauga, ON, Canada, Tech. Rep., Aug. 1999.

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

[4] Digital Signature Standard (DSS), Nat. Inst. Stand. Technol., Washington, DC, 2000, Fed. Inf. Process. Std. 1862. [Online]. Available: http://csrc. nist.gov/publications/fips/

[5] C. Cocks, "An identity based encryption scheme based on quadratic residues," in Proc. IMA Int. Conf., Cirencester, U.K., Dec. 2001, pp. 360–363.

[6] F. Hess, "Efficient identity based signature schemes based on pairings," in Proc. Revised Papers 9th Annu. Int. Workshop Sel. Areas Cryptograph., Aug. 2003, vol. 2595, pp. 310–324, Lecture Notes in Computer Science.

[7] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services, IEEE Std. 1609.3, Apr. 2007.

[8] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)—Multi-channel Operation, IEEE Std. 1609.4, Nov. 2006.

[9] Draft Amendment for Wireless Access in Vehicular Environments (WAVE), IEEE Draft 802.11p, Jul. 2007.

[10] IEEE Standard for Wireless Access in Vehicular Environments –Security Services for Applications and Management Messages, IEEE Std. 1609.2, 2016.

[11] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," IEEE Wireless Commun., 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 com-munications," IEEE Trans. Veh. Technol., vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

[13] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: A robust signature scheme for vehicular networks using binary authentication tree," IEEE Trans. Wireless Commun., vol. 8, no. 4, pp. 1974–1983, Apr. 2009.

[14] J. Guo, J. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in Proc. Mobile Netw. Veh. Environ., Anchorage, AK, USA, May 2007, pp. 103–108.

[15] J. H. Cheon and J. H. Yi, "Fast batch verification of multiple signatures," in Proc. 10th Int. Conf. Pract. Theory PKC, Beijing, China, Apr. 2007, pp. 442–457.

[16] Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," IEEE Trans. Veh. Technol., vol. 59, no. 2, pp. 559–573, Feb. 2010.