GRAS: A Group Reliant Authentication Scheme for V2V communication in VANET

Auxeeliya Jesudoss
jauxeeliya@nur.ac.rw
National University of Rwanda
Butare, Rwanda

Sulaiman Ashraph
asulaiman@nur.ac.rw
National University of Rwanda
Butare, Rwanda

and

Ratnakar Kotnana
ratnakar@nur.ac.rw
National University of Rwanda
Butare, Rwanda

ABSTRACT

Unlike fixed or wired networks, mobile ad-hoc networks pose a number of challenges for peer-to-peer communication due to their dynamic nature. This paper presents a novel framework for vehicle-to-vehicle communication controlled and facilitated by a group leader within a group of vehicles. A communication model for a pure ad-hoc network is developed with much concern about the privacy and security of the system, for the ease of effective communication between vehicles with a reduced communication and computational overhead when no fixed infrastructure is present in the roadsides. In the proposed protocol, vehicles within a radio frequency form a group. They elect their leader based on some criteria who is then responsible for generating a group public and private key pair. Each vehicle is equipped with a tamper resistant OBU which is capable of generating public/private keys pairs and also self-certifies the generated keys based on one way hash chaining technique. Any vehicle joins the group communicates the group leader, authenticates itself to obtain the group key. Later, the vehicle uses the group key to send traffic related messages to the group leader who is responsible for batch verifying the authenticity of the message from different sources and one hop broadcast them to reduce the computation overhead on message verification in each vehicle. In addition, our scheme adopts the k-anonymity approach to protect user identity privacy, where an attacker cannot associate a message with the sending vehicle. Extensive analysis and simulations show that the proposed architecture provides an efficient and fully self organized system management for car-to-car communication without the need of any external infrastructure.

Keywords: VANET, V2V, group communication, hash chaining, security, privacy.

1. INTRODUCTION

VANET technology enables the communication between vehicle to vehicle (V2V) and vehicle to roadside infrastructure (V2I) units [5][6]. All vehicles use a communication device called onboard units (OBU) to communicate with the RSUs. In most cases of V2V, the system topology is divided into smaller partitions of disjoint groups of hosts, who can act with independent control [1]. In general, groups can be categorized into predefined groups and dynamic groups. In predefined groups, vehicles that belong to specific category are part of specific groups. This type of approach is not very scalable and too inflexible and thus not suitable for VANETs. In case of dynamic groups, the groups are formed dynamically, presumably based on how close they are or what their driving pattern is [2].

In this paper we propose a group based authentication scheme in which vehicles use self generated anonymous public keys and certificates to authenticate themselves to a group leader when they want to join in a group or to any vehicle in normal situation. The group leader verifying the trustworthiness of a vehicle, issues a group key to the joining vehicle, which will be used later for sending safety messages within the group. At the time of sending messages, every vehicle sends its message to the group leader who will aggregately verify all the signatures of all the messages and broadcast a single aggregated message to all its members at a particular time interval. Here the OBUs (On Board Units) of each vehicle generates the anonymous keys and they themselves certify those keys with the help of a check value computed by the TA (Trusted authority) based on the one-way hash chaining mechanism. The same check values are issued to multiple vehicles by the TA in order to avoid the vehicle being tracked by any adversary during the time of message sending in a network. But at the same time, each OBU automatically attaches a tracking hint to all the traffic related messages it generates in VANET. This tracking hint is again computed by the TA using its master secret key and therefore useful for later tracking in case of any dispute.

2.OUR APPROACH

2.1 Network Model

For the proposed scheme, we address only vehicle-to-vehicle communication (V2V) for safety related applications. In this, vehicles are arranged into non-overlapping groups which are dynamic in nature. More precisely, vehicles form groups with their closest neighbors in their mobility. In addition to that, each vehicle is equipped with a GPS and tamper proof hardware devices such as OBUs which are capable of generating short lived anonymous public/private key pairs for message authentication. Moreover, our scheme does not depend on any fixed infrastructures such as RSU for key establishment or certification services, as the OBUs themselves are able certify their anonymous public keys which can be authenticated by the receiver (*in this case group leader is the receiver*) and could be revoked by the trusted authority as well based on the check values issued during system initialization.

2.2 Notations

In this paper, we use the notations that are described in Table 1 and also adopt the system parameters that are used by [20]:

G= (G, $*$). Finite cyclic group of order q (for some large q), $g \in G$ is a generator of G, and we assume that computing discrete logarithms in G with respect to g is computationally infeasible. For example, G might be a large multiplicative subgroup of Z_p^* for some large prime p, where q is a large prime dividing $p-$ 1; alternatively, G could be the group of points on an elliptic curve (usually written additively).

h Cryptographic (one way) hash function mapping arbitrary length binary strings to strings of a fixed length l (where a typical value for l might be 224).

f Cryptographic (one way) hash function mapping the set {0, 1,... ,$q-1$} onto itself; in practice, f might, forexample, be derived from h.

$m \geq 1$, Positive integer that determines the maximum number of key pairs that can be generated by a vehicle.

Notation	Description
sk_{TA}	TA's master secret key
PK_{TA}	TA's public keys
V	the vehicle
OBU$_v$	the OBU equipped by the vehicle V
$Cert_{TA}$	TA's certificate
Ћ	Tracking hint
cv	Check value
PK$_x$	Public key x at time T_x
sk$_x$	Corresponding private key x at time T_x
H$_x$	Helper value for the public key PK$_x$
$jreq$	Group joining request
Pu	Short lived public key of vehicle V
Pr	Corresponding private key
$Cert_{OBU}$	OBU certificate on Pu and the signed check value cv
$Encr_x$	Encryption on key x
Dcr_x	Decryption on key x

Table 1: Notations

2.3 Assumptions

Our proposal is based on some assumptions:

- Each vehicle contains a tamper proof hardware also known as on-board units (OBU) and a global positioning system (GPS).
- The OBU equipped in each vehicle is able to generate anonymous public and private keys and self certifies the generated public keys.
- We also assume that, the OBUs are configured in such a way that they automatically attach a tracking hint provided by the TA with every message it sends in the network.
- The revocation is controlled by the TA using RTC protocol by mapping the tracking hint to the vehicle ID issued during the registration phase.
- We also assume a straight road scenario for representing a highway. Vehicles in their mobility, forms dynamic groups and elect their leaders who can later batch verify and aggregate the messages sent by different vehicles.

2.4 Role of OBUs

In this paper, we espouse the one way hash chaining scheme proposed by [20]. During the vehicle registration TA generates a check value for each OBU and certifies them. This is done through the following steps.

1) TA randomly chooses $sk_{TA} \in Z_p^*$ as its master secret key and computes its public key $PK_{TA} = g^{sk_{TA}}$

2) During registration, Vehicle V equipped with OBU$_V$ submits its unique vehicle-id V$_{ID}$ to the TA. The TA chooses a secret key s for the OBU$_V$. and generates a positive integer P such that

$$P = f^m(s) \leftarrow f^{m-1}(s) \ldots\ldots f^{m-i}(\mathrm{s}) \leftarrow f^{m-i-1}(s) \ldots\ldots f^2(s) \leftarrow f(s) \leftarrow s$$
$$= \prod {}_{j=0}^{m} f^j(s)$$

3) TA also chooses two positive integers a, b and computes a large positive integer Q such that Q=(P *a)+ b and stores Q as secret. TA then calculates the check value cv and a unique tracking hint Ћ for OBU$_V$ as follows:

$cv = h(g^{R*Q})$, where R is a large positive integer.

$$Ћ = Encr_{PK_{TA}}(V_{ID} * g^{sk_{TA}})$$

4) Then the following parameters are transferred from TA to OBU$_V$

$Cert_{TA}\{cv\}$, Ћ, P, R, a, g^b, s, TS

where $Cert_{TA}\{cv\}$ is the CA's certificate for the check value cv and TS is the validity time of each public key that are going to be generated by the OBU.

5) In each time interval T_x ,OBU$_V$ chooses a random integer r_x in such a way that, $r_x \neq r_{x+n}$ for $x \in$ {0 ... m-1} and $n \in$ {1 ... m-x-1}, and ($R * r_x * b$) mod $P = 0$ and generates a private/public key pair sk_x, PK_x, and a helper value H_x for the generated public key as follows.

$$sk_x = R * r_x * a * \prod {}_{(j=0)}^{(m-x-1)} f^j(s) and$$

$$PK_x = g^{(R*r_x*a*\prod {}_{(j=0)}^{(m-x-1)} f^j(s))}$$

$$H_x = \prod {}_{(j=0)}^{(m-x-1)} * r_x^{(-1)}$$

6) When Vehicle V wants to join in a nearby group, OBU$_V$ generates a public/private key pair Pu/Pr and the

corresponding certificate $Cert_{OBU}$ that contains the signed check value *cv*, where sk_x is used by the OBU to sign the certificate $Cert_{OBU}$ it issues for the generated public key *Pu.*

7) The vehicle V then sends the following parameters together with the group joining request *jreq* to the leader of the group to which it wants to join, intending to authenticate itself to the leader in order to obtain the group key.

   jreq, Pu,$Cert_{OBU}$, PK_x, H_x and g^y,

   where $y = R * (\frac{r_x * b_i}{P_i}) * \Pi_{(j=0)}^{(m-i-1)} f^j(s)$

2.4 Overview of GRAS

Using PKI for vehicle-to-vehicle communication is costly and inefficient. Whereas, using symmetric keys between vehicles is an efficient procedure bur rather, establishing them is more complicated [22]. Hence, for our protocol we choose vehicle groups such that, vehicles that are moving in close proximity of each other forms a group. Soon after group formation, the members of the group elect a leader for the group who is then responsible for generating a group key and shares it with the other group members.

a. Group construction and Leader selection

We restrict the group formation in such a way that, vehicles can form a group if every member in a group hears the broadcasts of all other members in that group. Based on the assumptions made in 4.1, the vehicles in a group will have almost the same velocity on average and will move relative to each other in the same direction. Such a type of group can then be represented by a head called group leader. As we mainly focus on the message authentication and aggregation, any existing optimal algorithms can be adopted by the proposed GRAS scheme for group construction and leader election.

b. Member join and authentication

In general, every vehicle V broadcasts periodic safety messages once they join in the network. At the same time, V looks for any nearby group and attempts to join if it exists. If V hears any hello message from a group leader GL, it will immediately communicate the GL with a joining request *jreq* along with its self generated public key *Pu,* its OBU certificate $Cert_{OBU}$ signed with the private key sk_x, the corresponding public key PK_x and helper value H_x permitting the verification of $Cert_{OBU}$, in order to obtain a membership in the group. The group leader then verifies the credentials submitted by the requesting vehicle for its authenticity and discloses the group public key of its group. The algorithm works as follows:

Algorithm: Member join and authentication

```
if (V hears "hello" message from a group leader GL)
{
        1.  V_i computes
                $sk_x = R * r_x * a_i * \Pi_{(j=0)}^{(m-i-1)} f^j(s)$
                $PK_x = g^{(R*r_x*a_i*\Pi_{(j=0)}^{(m-i-1)} f^j(s))}$
                $H_x = \Pi_{(j=0)}^{(m-i-1)} * r_x^{(-1)}$
        2.  $V_i \rightarrow GL : Encr_{PK_{gl}}$ (jreq, Pu,Cert_OBU, PK_x, H_x, g^y)
        3.  GL computes
                $cv' = (PK_x * g^y)^{H_x}$
        4.  GL checks
          if ( $cv = h(cv')$ )
            {
                GL stores Pu,cv
                $GL \rightarrow V_i : Encr_{PK_x}\left(PK_{gp} \| \{PK_{gp}\}_{sk_{gp}}\right)$
            }
            else
            {
                GL : no reply
            }
}
```

c. Batch verification

In GRAS, the safety message *Msg* will hold the following format:

$$Msg = Pu \| M \| \text{Ћ} \| TS \| \{Pu \| M \| TS \| \text{Ћ}\}_{\sigma_{pr}}$$

A vehicle V with the group public key *Pu* can generate a valid signature σ_{pr} which is composed of (μ, γ) for a given message *M* as follows.

1) OBU selects a random number $x \in Z_p^*$
2) It then computes α, λ and γ such that
   $\alpha = g^x, \lambda = f(M \| PK_x \| \alpha \| TS) \in Z_p^*, \gamma = Pr + x\lambda$
   (α, γ) is a valid signature on message *M*

Any verifier (group leader in this case) can verify the above signature and accept the message if the following equation holds:

$$\hat{e}(g,\alpha)^{\gamma} = \hat{e}(g,\alpha)^{(Pr+x\lambda)}$$
$$= \hat{e}(g,\alpha)^{Pr}.\hat{e}(g,\alpha)^{x\lambda}$$
$$= \hat{e}(g^{Pr},\alpha).\hat{e}(g^x,\alpha^{\lambda})$$
$$= \hat{e}(g^{(R*r_x*x_i*\Pi_{(j=0)}^{(m-i-1)} f^j(s))},\alpha).\hat{e}(\alpha,\alpha^{\lambda})$$
$$= \hat{e}(Pu,\alpha).\hat{e}(\alpha,\alpha^{\lambda})$$
$$= \hat{e}(,Pu.\alpha^{\lambda})$$

Consider the group leader receives $(\alpha_1,\gamma_1)\ (\alpha_2,\gamma_2) \ldots\ldots (\alpha_n,\gamma_n)$ which are the signatures on the messages M_1, M_2,.. M_n, respectively. Then, those signatures can be aggregately verified as follows.

1) GL calculates $\lambda_1, \lambda_2 \ldots\ldots \lambda_n$ and α', γ' such that

$$\alpha' = \prod_{i=1}^{n} \lambda_n \alpha_n, \gamma' = \sum_{i=1}^{n} \gamma_n$$

2) GL accepts the message if the following equation holds:

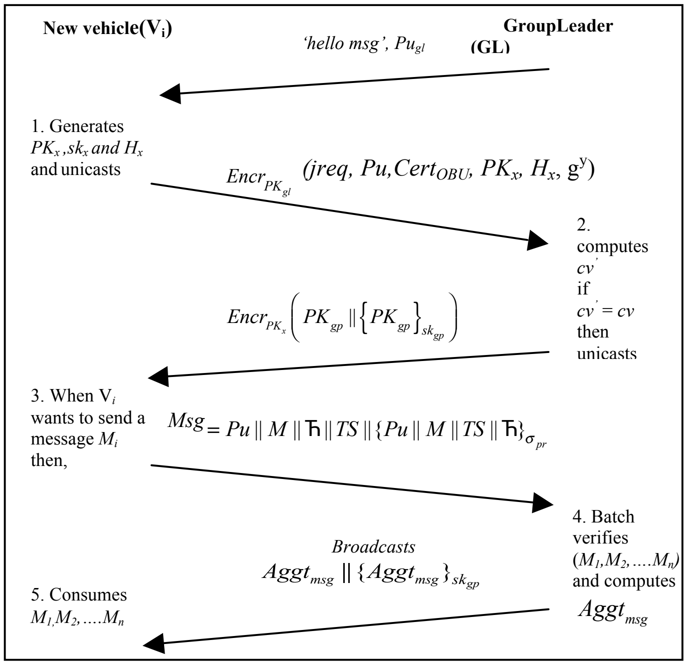
$$\hat{\mathrm{e}}(g,\alpha')^{\gamma'} = \hat{e}(\alpha', \prod_{i=1}^{n} Pu_i \alpha_i^{\lambda_i})$$

d. Message Aggregation

Once the group leader GL batch verifies all the message sources that sent messages to it at time *t*, it aggregates all the messages as follows:

$$Aggr_{msg} = (Pu_1 \| M_1 \| \hbar) \| (Pu_2 \| M_2 \| \hbar) \| \ldots \| (Pu_n \| M_n \| \hbar)$$

Then it signs the above with the group private key sk_{gp} and one hop broadcasts $Aggt_{msg} \| \{Aggt_{msg}\}_{sk_{gp}}$ to vehicles in its group who are within its communication range.



New vehicle(V_i)
GroupLeader (GL)
'hello msg', Pu_{gl}
1. Generates PK_x, sk_x and H_x and unicasts
$Encr_{PK_{gl}}$ (jreq, Pu, $Cert_{OBU}$, PK_x, H_x, g^y)
2. computes cv' if $cv' = cv$ then unicasts
$Encr_{PK_x}\left(PK_{gp} \| \left\{PK_{gp}\right\}_{sk_{gp}}\right)$
3. When V_i wants to send a message M_i then,
$Msg = Pu \| M \| \hbar \| TS \| \{Pu \| M \| TS \| \hbar\}_{\sigma_{pr}}$
4. Batch verifies ($M_1, M_2, \ldots. M_n$) and computes $Aggt_{msg}$
Broadcasts $Aggt_{msg} \| \{Aggt_{msg}\}_{sk_{gp}}$
5. Consumes $M_1, M_2, \ldots. M_n$

Figure 1: Protocol: GRAS

2.5 *k*-anonymity property

For identity preservation, we employ the concept of k-anonymity [24] in the proposed GRAS scheme to mix *k* vehicles. With GRAS, the TA assigns a common check value *cv* to *k* vehicles, where the *k* number of vehicles will take the same check value during their registration. When an adversary (including the group leader) intends to trace a specific vehicle through its check value, it cannot succeed as more than one vehicle may have the same check value in a group. The highest value of *k* can be determined by the TA which could be less than or equal to the total number of vehicles registered to the TA.

2.6 Member joining and leaving

When a vehicle V leaves a group, the GL simply removes V's information from its member list but rather do not make any changes in the group key. While at the same time, when a GL wants to leave the group, it sends a *leave* message to other members of the group before leaving, which will allow the group members to elect the node with next highest weight as the new GL.

However, if there are very few vehicles in an area, a group may not form, due to the lack of the leader [21]. But these shortcomings do not affect the functionality of the VANET, since a vehicle falls back automatically into the digital signature mode when it cannot join a group. In such case, any vehicle can send its messages directly to the network using traditional PKI model by attaching the corresponding helper value, check value and its certificate together with the self generated public key and it's tracking hint.

3. RELATED WORK

3.1 RSU based authentication

As the message authentication with digital signature put forth a big question on privacy, some solutions were proposed by researchers relying on an infrastructure to provide a certification service for vehicles. Authors in [15] proposed a conditional privacy preservation scheme, which talks about three layers of privacy. First, an RSU is responsible for issuing temporarily anonymous certificate to vehicles, and thus, it can map the vehicle with the issued anonymous certificate. Second, however, for an IVC, a vehicle's identity is absolutely anonymous to other vehicles. Third, the trust authority (TA) can track the vehicle's real identity. Furthermore, this scheme addresses certificate revocation issues, since the expiration date in the certificate indicates the validity period of the certificate. However, it does not take scalability issues into consideration. RAISE [17] explores an important feature of VANETs by employing RSUs to assist vehicles in authenticating messages. In this protocol, the messages sent by neighboring vehicles are stored in a temporary buffer of the receiving vehicles. When the RSU broadcasts the aggregated hashes of all received messages, the receiving vehicles compare them with the stored messages and consume them if they find a match. Though this significantly reduces the verification overhead, this approach still leaves a lot of room for improvement.

3.2 Pseudonym based authentication

Message authentication and anonymity are the two major security challenges identified in [9]-[13]. To achieve message authentication and anonymity, [14] proposed that each vehicle should be preloaded with a large number of anonymous public and private key pairs together with the corresponding public key certificates. Traffic messages are signed with a public-key-based scheme. To achieve privacy, each public and private key pair has a short lifetime, and a pseudo ID is used in each public key certificate. However, this scheme requires a large storage capacity to store this security information. The pseudonym based approach that has been proposed by [14, 19] is an idea to help the vehicles exchange their communications without revealing their real identity.

3.3 Group based authentication

Group based protocols have been proposed as a complementary approach to privacy preservation. The key idea is to hide in a group a vehicle's explicit identity and location. This is a tradeoff between privacy preservation and information accuracy. The protocol proposed by the authors of [23] elects a group leader who then communicates with the RSU on behalf of the group. This protocol also suffers the disadvantage of the overhead associated with the RL (Revocation List) management required to authenticate group membership. Group signature (GSB) which was first introduced in [18] which allows a group member to sign messages anonymously on behalf of the group. The identity of a signer can still be revealed by the group manager in case of a dispute. Lin *et al.* [3] proposed a group signature- based scheme to sign each message. In this protocol, the recipients can verify a message's signature with the group's public key. If the signature is authentic, the recipient can confirm that the sender is a group member but cannot identify a specific person. Since there is no identity information included in messages, this approach can also achieve identity privacy preservation, reduced storage cost and low bandwidth consumption. They considered the short group signature scheme that was introduced by Boneh et al. [4], which is secure and considered to be best suited to the V2V application. Authors in [3] propose a geographic based group formation that is a hybrid approach of both predefined and dynamic group formation. In this approach, the map is divided into overlapping cells using GPS. So every vehicle is aware of its current group at any moment by knowing its current location. Also the vehicle which is closest to the cell center is will be assigned as the group leader. A symmetric cryptographic key is shared between group members for mutual communication. However, this approach meets a serious communication overhead as the members have to communicate each other to agree upon the symmetric key.

To reduce the overhead of the group signature-based scheme, a similar scheme [16] was developed in which a vehicle can generate public and private key pairs by itself by using a group key. This scheme can achieve a tradeoff between the group-signature-based scheme and the traditional PKI-based scheme. The scheme proposed in [8] proposes the privacy preserving group communication scheme for VANETs to satisfy forward and backward secrecy, authentication, protection against collusion, and privacy under symmetric-key cryptography. Additionally, a node can calculate the new group key as well as update its compromised key list (i.e., keys which are utilized by misbehaving nodes) even if the node misses the group rekeying process. This assumes that every node has knowledge of the revoked node's key set in advance and retains the information. This increases the storage requirement of each node as well as the bandwidth consumed by communications between each node and the key server. Though, group signature is a stronger property than pseudonymous authentication, as any two group signatures generated by a node cannot be linked [7], group formation in VANET is yet not clear as it has not been clearly discussed in many papers.

4. PERFORMANCE EVALUATION

A. Communication Overhead

In this section, we calculate the communication overheads of the proposed GRAS protocol. We consider the Tate pairing implementation on an MNT curve with embedding degree 6. Accordingly, each point on this MNT curve is represented by 21 bytes. With GRAS, the communication overhead of GRAS is 21+98+21+21+21+77 bytes, where public keys *Pu*, PK_x, helper value H_x and the parameter g^y takes 21 bytes each, along with the 98 bytes OBU certificate and TA's certificate on the check value as 77 bytes are shared for *n* message generated by one public key *Pu*, because vehicles submit those information to the GL once per the self generated public key.

Also it is indicated in section VI that, an OBU_i with $Cert_{OBU}$ can generate a valid signature (α,γ) while sending an arbitrary message *M* to the GL. Since α and γ are points on the elliptic curve, the size of a signature in GRAS takes 42 bytes. Consequently, the communication overhead incurred in a signed message transmitted by an OBU is 62 bytes, which is the signature size plus the size of the tracking hint encrypted using SHA-1 algorithm which is also shared by *n* vehicles as the GL verifies every message on behalf of all the other members in the group. Note that the other group members need to verify only the group signature generated by the GL for *n* aggregated messages where *n* is determined by the number of vehicles with the packet release interval of 300 ms to the GL to broadcast a batched packet. This shows that the GRAS scheme is more feasible with respect to the incurred communication overhead.

B. Verification Delay

We compare the verification delay of the GRAS batch signature verification with the signature verification of ECDSA and CAS. CAS is a certificateless aggregate signature scheme [26]. The time needed to verify one ECDSA signature is $2T_{mul}$, and that for CAS is $3T_{pair}+2T_{mtp}$, where T_{pair} represents the time required to perform a pairing operation, T_{mtp} denote the time required for a hash function to perform one map to point operation, and T_{mul} corresponds the time required to perform one point multiplication. In [25], T_{pair}, T_{mtp}, and T_{mul} are found for a super singular curve with embedding degree $k = 6$ to be equal to 4.5 *msec*, 3.9 *msec*, and 0.6 *msec*, respectively. For CAS, there is no certificate; however CAS takes $2T_{pair}$ to perform check process in order to verify the sender. For the GRAS scheme, the verification delay of a message signature requires $(3T_{pair} + T_{mul})/n$ which include an additional $2T_{pair}$ to verify the sender once per public key and *n* is the number of vehicles in the group (every message is verified by the GL alone on behalf of the group with *n* members).

Scheme	One signature verification	*K* signature verification
ECDSA	$2T_{mul}$	$2KT_{mul}$
CAS	$5T_{pair}+2T_{mtp}$	$(4K+1)T_{pair}+2KT_{mtp}$
GRAS	$(3T_{pair} + T_{mul})/n$	$(3T_{pair} + KT_{mul})/n$

Table 2: Signature verification delay

Table 2 shows a summary of the signature verification delays for ECDSA, CAS and the GARS schemes.

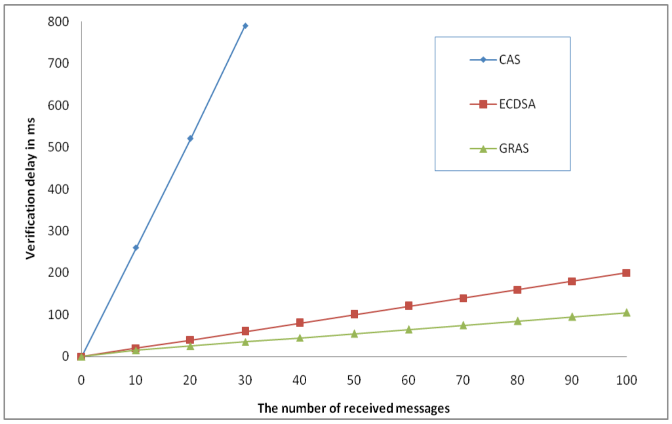


Figure 2: Verification delay for CAS, ECDSA and GRAS schemes

Figure 2 shows the verification delay for ECDSA, CAS and the GRAS schemes. It can be seen that the GRAS scheme has the lowest verification delay. In GRAS, the number of the pairing operations required for signatures verification is independent on the number of the signatures to be verified.

5. CONCLUSION

In this paper, we proposed a group based pseudonymous authentication scheme GRAS which can work effectively during the absence of any fixed infrastructure in the road sides. The proposed protocol vehicles with relative velocity and direction form groups and shares traffic related messages in the network. For that, they rely on the support of a group leader who can verify the messages collectively and broadcasts them by aggregating all the messages after performing enough authentication of the message sender. While preserving both privacy and authenticity of the message originator, GRAS drastically reduces the signature verification cost by freeing the other group members to do so. Simulations have been conducted to demonstrate the effective performance of the proposed protocol.

6. REFERENCES

[1] Chunhung Richard Lin and Mario Gerla, Adaptive Clustering for Mobile Wireless Networks, *IEEE Journal on Selected Areas in Communications,* 15(7): 1265-1275

[2] A. Stampoulis and Z. Chai. Survey of Security in Vehicular Networks. Technical report, 2007. Project CPSC 534

[3] X. Lin, X. Sun, P.-H. Ho, and X. Shen, GSIS: A secure and privacy preserving protocol for vehicular communications, *IEEE Transaction on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[4] Dan Boneh and Hovav Shacham. Group Signatures with Verifier-Local Revocation. *In Proceedings of CCS 2004,* pages 168–177. ACM Press, 2004.

[5] Routing in Vehicular Ad hoc Networks: *A survey Vehicular Technology Magazine, IEEE Issue Date: June 2007,* Vol. 2 Issue 2, pp. 12-22.

[6] Sardari, M.Hendessi F. Fekri F, A New Paradigm for Collaborative Content Distribution from Roadside Units to Vehicular Networks, *IEEE conference on Senor, Mesh and Ad hoc communication and Networks 2009,* pp. 1-9

[7] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy. Efficient and Robust Pseudonymous Authentication in VANET. *In Proceedings of the ACM International Workshop on Vehicular Ad hoc Networks (VANET)*, pages 19–28, September 2007.

[8] A. Wasef and X. Shen, PPGCV: Privacy Preserving Group Communications Protocol for Vehicular Ad Hoc Networks, *in Communications, 2008. ICC'08. IEEE International Conference* on, pp. 1458{1463, May 2008.

[9] M. E. Zarki, S. Mehrotra, G.Tsudik and N. Venkatasubramanian, Security issues in a future vehicular network, *in Proc. Euro Wireless Conference,* 2002, pp. 270-274

[10] B. Parno, A. Perrig, Challenges in securing vehicular networks, *in Proc. 4th Workshop HotNets,* 2005.

[11] P. Papadimitratos, V. Gligor and J-P. Hubaux, Securing vehicular communications- Assumptions, requirements and principles, *in Proc. Workshop ESCAR,* 2006, pp. 5-14.

[12] A. Aijaz, B. Bochow, F. Dotzer A. Festag, M. Gerlach, R.Kroh and T. Leinmuller, Attacks on inter vehicle communication systems-An analysis, *in Proc. 3rd Int. Workshop Intell. Transp.,* 2006, pp.189-194.

[13] P. Papadimitratos, L.Buttan, J-P. Hubaux, F. Kargl, A. Kung and M.Raya, Architecture for secure and private vehicular communications, *in Proc. 7th Int. Conf. ITS Telecommunication,* 2007, pp.1-6.

[14] M. Raya and J.-P. Hubaux, Securing vehicular ad hoc networks, *Journal on Computer Security, vol. 15, no. 1,* Jan. 2007, pp. 39–68.

[15] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications, in *Proc. IEEE INFOCOM*, Phoenix, AZ, 2008, pp. 1229–1237.

[16] G. Calandriello, P. Papadimitratos, A. Lioy, and J.-P. Hubaux, Efficient and robust pseudonymous authentication in VANET, in Proc. Int. Workshop VANET, 2007, pp. 19–28.

[17] Chenxi Zhang, Xiagong Lin, RongXing Lu, Pin-Han Ho, Xuemin Shen, An efficient message authentication scheme for vehicular communications, *in IEEE Transaction on Vehicular Technology,* vol, 57, No. 6, Nov 2008.

[18] D. Chaum and E. Ven Heyst, Group Signatures, *In Advances in Cryptology – EUROCRYPT 1991*, LNCS 547, pp. 257-265, Springer-Verlag, 1991.

[19] X. Lin, X. Sun, X.Wang, C. Zhang, P.–H. Ho and X. Shen, TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving, *IEEE Transactions on Wireless Communications*, vol. 7, no, 12, pp. 4987-4998, December 2008.

[20] G. Kounga, T. Walter, and S. Lachmund, Proving reliability of anonymous information in VANETs, *IEEE Trans. Veh. Technol.*, vol. 58, no. 6, pp. 2977–2989, Jul. 2009.

[21] M. Raya and J,P, Hubaux, Securing Vehicular Ad Hoc Networks, *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks,* Vol. 15, pp. 36-68 , January 2007.

[22] Mayank Verma, Dijiang Huang, SeGCom : Secure Group Communication in VANETs,

[23] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, AMOEBA: robust location privacy scheme for VANET, *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1569–1589, 2007.

[24] M.Raya, P. Papadimitratos, I. Aad, D. Jungels and J-P. Hubaux, Eviction of misbehaving and faulty nodes in vehicular networks, *IEEE journal on selected areas of communication,* Vol 25, No. 8, Oct 2007.

[25] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, An efficient identity based batch verification scheme for vehicular sensor networks, *Proc. IEEE INFOCOM 2008*, pp. 6–250, 2008.

[26] Z. Gong, Y. Long, X. Hong, and K. Chen, Two certificateless aggregate signatures from bilinear maps, *Proc. 8th ACIS Inter. Conf. on SNPD 2007*, vol. 3, pp. 188–193, 2007.