Proxy Signature-based RSU Message Broadcasting in VANETs

Subir Biswas
Dept. of Computer Science
University of Manitoba
Winnipeg MB, Canada R3T 2N2
Email: bigstan@cs.umanitoba.ca

Jelena Mišić
Dept. of Computer Science
Ryerson University
Toronto ON, Canada M5B 2K3
Email: jmisic@scs.ryerson.ca

***Abstract*—We propose a framework for a secure RSU-to-OBU message broadcasting in VANETs using proxy signatures. We consider a VANET infrastructure for which the network assumptions are similar to the current standards of VANET communications. The main purpose of our scheme is to provide message integrity, authenticate the broadcast messages, and authenticate the RSU to the OBUs. We set the appropriate liabilities to the network components enabling the OBU to verify the received message for its validity and integrity. Our contribution includes modification of the proxy signature scheme in order to fulfill the security requirements of a VANET's message broadcast. The security analysis of our scheme strongly supports the applicability of our proposed framework.**

***Keywords*-proxy signature; legacy warrant; discrete logarithm; Schnorr signature;**

I. Introduction

The RSU-to-OBU communication must have the capability of verifying the identity of the message sender as well as the integrity of the delivered message, both of which can be accomplished through a suitable signature protocol. However, high and variable node velocity, varying node density, and the need to operate on roads with varying characteristics pose significant challenges to VANET architecture and, by extension, to the chosen protocol. Thus, the issue of scalability is of prime importance as, under heavy traffic, a single controller might need to attend to hundreds, perhaps even thousands of vehicles in a given segment of the transportation network. The presence of many messages from vehicles and RSUs on a particular road may increase the message collision rate and thus impair the performance of on-road vehicular communication. Eichler et al. [1] have shown that the WAVE standard can't deal with many high priority messages in a dense network scenario. Therefore, our scheme should have low computational complexity, high scalability, as well as a reliable and quick verification mechanism.

To cope with these requirements, we propose to exploit the features of proxy signature [2] for the RSU-to-OBU message broadcast. The term proxy signature refers to a variation of digital signature that designates a person (called a proxy signer) to sign a message on behalf of the original signer. We considered a number of signature schemes and found that Schnorr's scheme [3], [4] is most suitable as the main signature protocol for fast and efficient signing of messages over the VANET. RSUs will be proxy signers signing safety and other application messages to the OBU recipients on behalf of the original creator of the messages. A recipient of the messages can verify the identity of the original signer, but it can also verify the integrity of the contents of the received message.

As mentioned before, RSUs may broadcast several messages including routine messages on road-safety issues, accident notifications, traffic congestions alert, and commercial messages etc. An RSU is supposed to keep broadcasting each message repeatedly for a particular period of time. However, a message validity information is type-specific and normally decided by the applications at the RSU-controller. An occurrence of re-broadcasting an old message by the RSU may cause a significant damage to users. For instance, a corrupt RSU may attempt to misguide the vehicles on road by re-broadcasting an old accident notification. Therefore, all these broadcasts through RSUs should be restrained by an appropriate body.

In order to accomplish that capability in our framework, we deploy a proxy signature that would authorize an RSU to sign a message on behalf of the message originator while in the process, the RSU can not alter the message or replay the expired messages.

The original proxy signature scheme, proposed by Mambo et al. [2], was further extended by Kim et al. [5] who proposed two additional features – proxy signature by partial delegation with warrant and the threshold delegation based proxy signature. Further enhancements include blind proxy signature schemes [6], [7], [8] by which a proxy signer is made unable to manipulate the message contents (and, replay the expired messages). However, blind proxy signatures are not practical for VANET applications, since they require a new proxy tuple to be generated and delivered to the proxy signer every time there is a new message to broadcast.

Our proposed scheme also includes a modification of the original proxy signature protocol [2], in which we introduce a mechanism called *legacy warrant* which is a signed tuple of the message expiry information along with a proxy-signature component. Because of this warrant, the corresponding RSU can neither replay the expired message, nor alter the original message. Therefore, the control of the message broadcast is kept with the message originator.

We organize the paper in the following manner. A brief account of the network assumptions is given in section II. Section III delineates the proposed scheme for secure message broadcasting. The security analysis is in Section IV while Section V concludes the paper.

II. Network Architecture and Assumptions

In our network model, RSUs in a given geographic area are grouped together to work under a road side controller (RSC). RSUs are connected to the RSC using high bandwidth secure links. We consider the communication between an RSU and the RSC to be secured by means of a suitable network layer security protocol. A number of RSCs, apparently independent of each other, are deployed over the VANET but connected to the Internet as shown in Fig. 1. A Certificate Authority (CA) maintains all necessary information of each RSU under an RSC. For instance the CA essentially stores the location information, deployment history of individual RSUs along with the public key of the RSC. CA issues the certificate for each of the RSUs in the VANET.

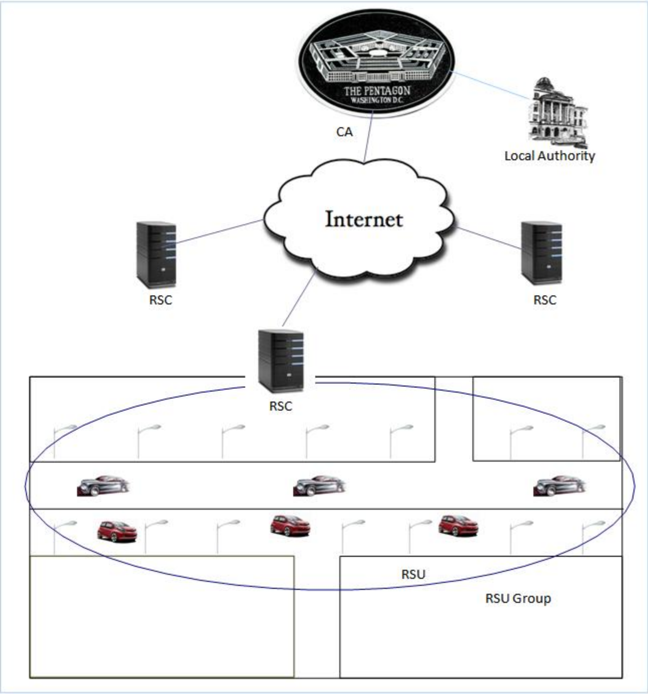

Figure 1. The proposed network architecture for secure VANETs

We assume that the public key of CA is known to all the members including the vehicles in a VANET. Local authorities may communicate with the CA through off- or online transmission to negotiate any dispute, including issuing licensing materials for a vehicle and commercial aspects of VANETs.

RSU-to-OBU communication has two major aspects:

- Authentication of the RSU as a valid member of the corresponding RSU group to the on road OBUs, and
- Delivering the messages to the OBU signed by the RSU on behalf of the RSC.

In our approach, an RSU advertises the certificate containing ID$_{RSC}$, the public key (later denoted as v) of the RSC, ID$_{RSU}$, the MAC address of the RSU, and the RSU's location information, Loc$_{RSU}$. The initial (beacon) advertisement message has the following certificate: (ID$_{RSC}$, ID$_{RSU}$, Loc$_{RSU}$), H(ID$_{RSC}$, ID$_{RSU}$, Loc$_{RSU}$)$_{S_{CA}}$; where, H(.) is a hash function, and (.), H(.)$_{S_{CA}}$ indicates a signature using CA's secret key.

An OBU finds the public key of the RSC, the original MAC addresses of the RSU, and the designated RSU location. The certificate authority's signature confirms the integrity of the message and proves the fact that the RSU belongs to the corresponding RSU group administrated by the particular RSC. Upon receiving the beacon frame [9], [10], [11], the OBU matches the received MAC address with the transmitting RSU's MAC address. Once the RSU's MAC address is verified, the OBU decides to join the RSU group; otherwise, it waits for another beacon. The OBU also compares the location information of the RSU with its GPS information to verify that the RSU is at its designated location.

III. Proposed Proxy-Scheme for Message Broadcast

In the beginning, two prime numbers, p and q are generated, where q is a prime factor of $p-1$. The values for p, q are assigned to an administrative area, for instance, p is assigned to a country, and q is for a given large geographical area (a state, or province) in that country. Then, a generator g for Z_p^* is dedicated to a comparatively small area (for example a city or a town). Here, Z_p^* refers to a *multiplicative group modulo* p.

A. Proxy Initialization Phase

RSC generates a random number $s < q$ which is considered to be the private key of the original proxy signer (RSC) for secure message broadcasting in VANET. The public key is calculated as $v = g^s mod\, p$. This private key/public key pair is pre-calculated at the RSC prior to the actual operation. Parameters p, q, g, and v are made public for the subordinate RSUs and vehicles. The list of parameters used along with their scopes in this scheme is given in Table I.

In addition, RSC generates another random number, $k \in_R Z_{p-1} \backslash \{0\}$; where, $Z_{p-1} \backslash \{0\}$ denotes a *non-zero finite field of modulo* p. We refer to k as the *revocation parameter* of our scheme; the details of the revocation process are given in Section IV-C.

Table I
LIST OF PARAMETERS AND THEIR SCOPES

Parameters	Generated by	Scope in the network
p, q, g, v, K, h_s	RSC	Public
k, s, x, h	RSC	Private to RSC
σ, r	RSC	Private to RSC, RSU
y	RSU	Private to RSU, OBU
x', h'	OBU	Private to OBU

During the initialization phase, the RSC computes

$$K = g^k mod\, p \tag{1}$$

This K value is used for calculating a proxy secret key, σ, as

$$\sigma = s + kKmod\,(p-1) \tag{2}$$

The value of σ will be used as the secret identity of an individual RSU; hence it is usually kept within the RSU's volatile memory and is normally unexposed to other parties. On the other hand, K is defined as the verification parameter, since it is used by an RSU and an OBU for the verification of a proxy pair (σ, K) and the delivered message respectively.

The proxy pair (σ, K) is then delivered to the RSU over a secure IPSec tunnel. The RSU will now be working as a proxy signer for an RSC. Henceforth, we refer to the pair (σ, K) as just a *proxy*.

The RSU, upon receiving the proxy (σ, K), verifies it by checking if the following congruence holds:

$$g^{\sigma} \equiv vK^K mod\, p \tag{3}$$

If the last equation is not satisfied, the produced proxy is discarded and a fresh proxy is requested by the RSU. Values of σ and K are different for individual RSUs, and normally they are valid for a long time unless a proxy is detected to be used by some unauthorized third party.

Should there be a message to be broadcast over the VANET, either for some road-safety application, or, for some other need (e.g. a commercial advertisement, weather update etc.), the RSC must associate the message content m with a message expiry time t_x. It is very important to restrain the RSU from abusing the proxy signature by conducting invalid message broadcast, or replaying the old messages. The broadcast message m is thus jointly signed by the RSC and the subsequent RSUs before it is broadcast to the vehicles on road.

The RSU uses the value of σ instead of s, as the secret key of the basic signature scheme. We propose to apply Schnorr's scheme due to its fast signature and low transmission bandwidth requirements [2], [5]. The signature and the verification procedure, modified from the original proxy signature scheme, is given below.

B. Proxy Signature and Verification

The RSC picks a random *session parameter* $r < q$ to compute,

$$x = g^r mod\, p \tag{4}$$

This session parameter is generated as soon as there is an event for which a broadcast message has to be delivered. RSC subsequently calculates the hash value h of (m, x), and also computes a legacy warrant h_s which contains the signature of hash value h along with the expiry time of the message (t_x):

$$\begin{aligned} h = &\quad H(m, x) \\ h_s = &\quad (h, t_x), H(h, t_x)_s \end{aligned} \tag{5}$$

The message m, legacy warrant h_s, and the session parameter r are delivered to the RSU through IPSec tunneling. This is done every time when there is a message to be broadcast through RSUs. The hash value h and the expiry information t_x are taken and verified from h_s using the proxy public key v. Next, the RSU utilizes the received r and h values to calculate y:

$$y = (r + \sigma h) mod\, q \tag{6}$$

The proxy signature (h_s, y) is concatenated with the (safety application or other) message, which eventually results in a tuple (m, h_s, y, K) broadcast by the RSU. The receiving vehicle (OBU) uses the signature components for verification of proxy signature on the message m:

$$v' = vK^K mod\, p \tag{7}$$

This value is used in the following calculation:

$$x' = g^y v'^h mod\, p \tag{8}$$

Given that the h and t_x are verified from h_s using the public value v, t_x is immediately matched with the current system time of the OBU. Upon detecting an expired message from an RSU, it may release a replay alert to notify the concerning authority after discarding the message. If not, the message is verified through

$$h = H(m, x') \tag{9}$$

If (9) holds, the message is accepted; otherwise, an OBU may generate a false message alarm, or it can simply ignore the message, depending upon the system configuration and application requirements. Note that the RSC must store a copy of each delivered message in its database, along with the corresponding proof h_s, and the generation time of the message. This is done for resolving a potential dispute in future, regarding the liabilities of any RSU or OBU.

IV. Security Analysis

The security of the proposed scheme relies mainly on the inherent difficulty of solving discrete logarithm problem of proxy signature scheme. The proxy signer uses σ as a secret key for the main signature scheme instead of the RSC's actual private key s which is kept secret within the RSC itself and is associated with its public key v. The value of σ is calculated from the private key s using (2). From security point of view, it would be infeasible to compute s from σ values. We use a proxy signature with $legacy - warrant$ approach in which the original signer (RSC) has the complete control over the proxy signature generation, validity of the message, and the revocation of a proxy.

A. Legacy Warrant on Proxy Signature

A warrant is a proof that the original signer designates the proxy signer to sign the particular message. In our scheme, the original signer (i.e., an RSC) generates the message to broadcast and allows the subordinate RSUs to sign on behalf of it. The warrant h_s is a public key cryptography-based signature over the hash value h and the message expiry information t_x. Unlike the conventional warrants in proxy signatures, our approach doesn't need to contain the message itself, and the proxy's public key v with the warrant every time there is a message to be delivered. This mechanism would help the receiving OBUs understand that the message is not reproduced by the RSU (or by some other adversary); also, h would be used for assuring the integrity as well as the verification of the proxy signature.

B. Proxy Signature Security Features

1) Unforgeability: Only a valid proxy-signer RSU can create a given signature on behalf of the RSC. An RSU uses the session parameter r and the newly derived secret σ from its proxy set (σ, K) to sign a message. Each σ value is distinct and is explicitly assigned to only a single RSU. For launching an attack by signing and broadcasting invalid messages, an adversary may try to derive a valid combination of proxy (say, (σ', K')) that satisfies (2) and (3). Since signing also requires a valid h, as per (6), which is solely generated and signed by the RSC, an adversary can never create a valid proxy signature. Again, σ is derived from a randomly generated secret s which is never disclosed by the RSC. Computing a new σ or the secret s from a given σ of a proxy is very hard due to the complexity of solving discrete logarithm.

2) Non-repudiation and Impersonation: As an RSU is strictly assigned to only one proxy, it can not generate any valid proxy signature which would not be identified as a signature of only that particular RSU. The y value of a valid signature for a given session is unique and can only be generated by a particular RSU using (6). An adversary cannot generate a valid proxy signature from publicly available parameters, since s and k values are kept secret in the RSC. Even if an adversary succeeds in generating a new proxy (σ', K') which satisfies (2) and (3), an impersonation attack is not yet possible, since a malicious RSU cannot provide an appropriate session parameter r with a reasonable probability for computing a valid y using (6).

3) Identification Hide: An RSU is always identifiable from its proxy signature for a given message, as no one except the RSC can generate a proxy combination of (σ, K) with a high probability. The last two components of a proxy signature, y and K, represent the identity information of an RSU. Thus, one has to come up with a valid and new combination of (y, K) in order to hide identity information of the RSU. But, the changed values of y and/or K would produce different results in (7) and (8), which would lead to unsuccessful verification in the process. Again, since h value is not changeable for a given message, changing of y using (6) requires simultaneous (and compatible) change of σ and/or r. Note that the r value should always remain smaller than q, and finding a valid combination of (σ, K) with a given public key v, requires extreme efforts as s and k values are kept within the RSC only.

C. Revocation

An adversary may successfully compromise an RSU to get the possession of its designated proxy. Upon detection of the compromise, the RSC must revoke the proxy as the adversary may attempt to use the proxy to sign a malicious message. The revocation process starts at the RSC with regenerating the revocation parameter k to compute the verification parameter K using (1), followed by a set of calculation for all other relevant parameters. Although the compromised proxy is still a valid one and can be used by the adversary, it can't directly harm the system by signing an illegitimate or expired message. Because, the legacy warrant is only generated by the RSC which includes the expiry information of each message. In most cases, the misbehaving RSUs must be replaced after conducting an investigation by the administrator.

V. Conclusion

In this paper, we presented a proxy signature based scheme for secure message broadcasting in a vehicular network environment. The proposed scheme uses the modification of the proxy signature approach to comply with VANET security requirements. Security analysis shows that our scheme has strong resilience against the potential forgery and attacks launched by adversaries. Our scheme is applicable to IEEE 802.11p WAVE standards for vehicular communications. In future work, we will extend our scheme with low power cryptographic primitives and deploy it in a IEEE 1609.2 [12] framework. We also plan to extend the scheme for vehicle-to-infrastructure communication.

Acknowledgment

This work has been partially funded by APMA AUTO21 Project from the Govt. of Canada.

References

[1] S. Eichler, "Performance evaluation of the ieee 802.11p wave communication standard," in *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, 30 2007-Oct. 3 2007, pp. 2199–2203.

[2] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," in *CCS '96: Proceedings of the 3rd ACM conference on Computer and communications security*. New York, NY, USA: ACM, 1996, pp. 48–57.

[3] C.-P. Schnorr, "Efficient identification and signatures for smart cards," in *CRYPTO '89: Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology*. London, UK: Springer-Verlag, 1990, pp. 239–252.

[4] C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, 1991.

[5] S. Kim, S. Park, and D. Won, "Proxy signatures, revisited," in *ICICS '97: Proceedings of the First International Conference on Information and Communication Security*. London, UK: Springer-Verlag, 1997, pp. 223–232.

[6] J.-H. Park, Y.-S. Kim, and J. H. Chang, "A proxy blind signature scheme with proxy revocation," *Computational Intelligence and Security Workshops, International Conference on*, vol. 0, pp. 761–764, 2007.

[7] L. Wei-min, Y. Zong-kai, and C. Wen-qing, "A new id-based proxy blind signature scheme," *Wuhan University Journal of Natural Sciences*, vol. 10, no. 3, pp. 555–558, 2005-05-01.

[8] M. Cai, L. Kang, and J. Jia, "A multiple grade blind proxy signature scheme," *Intelligent Information Hiding and Multimedia Signal Processing, International Conference on*, vol. 2, pp. 130–133, 2007.

[9] "Draft amendment for wireless access in vehicular environments (WAVE)," IEEE, New York, NY, IEEE Draft 802.11p, Jul. 2007.

[10] "IEEE trial-use standard for wireless access in vehicular environments (wave)- networking services," IEEE, New York, NY, IEEE Std 1609.3, Apr. 2007.

[11] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," in *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, May 2008, pp. 2036–2040.

[12] "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.