A Message Authentication Protocol using Proxy Blind Signatures in Vehicular Ad Hoc Networks

S. Prabhadevi
Nandha Engineering College

Dr. A. M. Natarajan
Bannari Amman Institute of Technology

***Abstract*- Nowadays, transportation systems play an important part in our daily activities. One transportation system that has recently attracted a lot of attention from both academia and industry is vehicular ad hoc networks (VANET). However, because of the ad hoc nature and high mobility of nodes, it is unfeasible to authenticate VANET components in advance while operating on road. VANET entities must be able to authenticate the message sender and retain integrity of the message sent through a suitable signature scheme. We propose VANET message delivery protocol has two separate components for RSU and OBU messages in a vehicular network environment. The proposed protocol uses a modified proxy blind signature mechanism to comply with VANET's message integrity and privacy requirements.**

1. INTRODUCTION

A Vehicular Ad Hoc Network (VANET) is subgroup of the Mobile Ad Hoc Networks (MANET) in which the operating nodes are the vehicles on the road. The elemental parts that constitute a VANET are Road Side Unit (RSU), On Board Unit (OBU), and convenient framework that support the whole system in addition to the connectivity to the Internet. The complete VANET structure is depicted in Figure 1. VANET communications are facilitated by Dedicated Short Range Communication (DSRC). The three groups of message transmission are: RSU-to-OBU/ Infrastructure-to-Vehicle (I2V), OBU-to-RSU/ Vehicle-to-Infrastructure (V2I), and OBU-to-OBU/ Vehicle-to-Vehicle (V2V) communications. Although a great many of the messages deal with road security and safety information, an increasing number of other commercial and infotainment messages aid amenities for drivers as well as passengers.

Nevertheless, these communications can be catastrophic if an adversary exploits the system for personal benefits. Hence vehicular communication should have the potential to verify the identity of the message sender and to maintain the integrity of the delivered message. This can be accomplished by employing convenient signature scheme Because of the inherent vehicle characteristics: highly variable speed of vehicles, varying concentration in a particular area/time, uneven road characteristics and weather conditions pose threat in developing such a protocol. Too many messages from vehicles and RSUs on a particular road may increase the message transmission rate and thus impair the performance of the network. Hence, our scheme should have low computational complexity, reliable and provide fast authentication mechanisms.

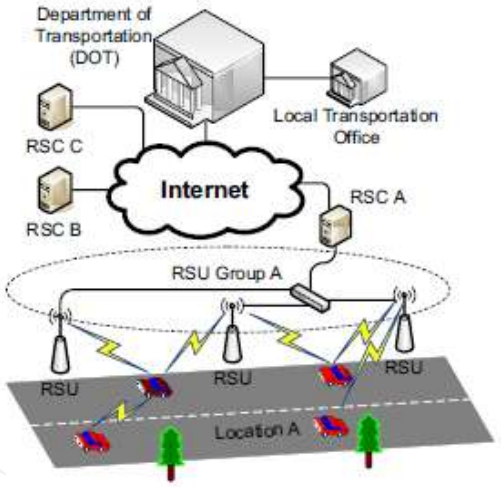

Figure 1. VANET architecture for authentication of messages.

The participating nodes in the network are the individually owned network vehicles, so the prime responsibility of the underlying communicating protocol is to preserve the privacy and anonymity of the user (vehicle). While the system should also ensure sure that no OBUs take privilege of the anonymity by instilling false messages i.e. VANET has to be culpable when a conflict arises, given that the appropriate legislative measures would be taken beforehand.

We organize the paper in the following manner. Section 2 discusses the evolution of proxy signature and proxy blind signature scheme stogether with alternative technologies for signatures in VANET. A brief account of the network assumptions is given in section 3. Section 4 delineates the proposed protocol for RSU and OBU message signing and verification. The section also deals with revocation phase and system accuracy. The signature overhead calculation is carried out in Section 6. The security analysis is provided in Section 5 and followed by Section 7 which concludes the paper.

2. RELATED WORK

The original proxy signature scheme, proposed by Mambo et al. [1], was further extended by Kim et al. [4] 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 [5], [6], [7] by which a proxy

signer is made unable to manipulate the message contents (and, replay the expired messages).

Number of papers has addressed the problem of anonymity in VANET [8]. Raya et al. in [9] suggested the use of a large number of short lived anonymous keys that would expire immediately after being used. This scheme requires a rigorous effort to find the original identity of a vehicle, while resolving a dispute.

In a group signature based approach (e.g. [10], [11], [12]), a member of a group can sign a message on behalf of a group and the identity of the signing member remains hidden within the group so that no one knows the actual identity of the sender. A group manager in each group can open any signature signed by a member of that particular group using its group manager secret key. However, each group member has to maintain a large node revocation list to prevent from potential attacks. When required by the authority to disclose the actual identity of a vehicle, group based schemes in VANET possesses the peer discovery phase which might involve significant communication overhead.

Another similar approach [13] uses the combination of group signature and ID-based signature scheme for secure and privacy preserving protocol for vehicular communication.

Lin and Jan [19] first introduced a proxy blind signature scheme based on Discrete Logarithm Problem (DLP) and Elliptic Curve Discrete Logarithm Problem (ECDLP) to take the advantage of security properties of both the blind and proxy signature mechanisms. It is derived from the Schnorr blind signature scheme. Later, Tan et al. [21] introduced a new a proxy blind signature mechanism but it was susceptible to a kind of forgery attack. This was proved by Lal and Awasthi [18] who also introduced a new proxy blind mechanism based on Mambo's scheme and was found to be a more efficient and secure one.

In 2005, Wang and Wang [22] introduced a proxy blind signature scheme by using ECDLP. However, Yang and Yu [23] in 2008 proved that the above scheme did not meet the security properties, and therefore, introduced an improved scheme. Nevertheless, this scheme did not satisfy the unforgeabilty property. Later, in 2009, Qi and Wang [24] introduced a proxy blind signature mechanism that implemented factoring and ECDLP but again this scheme did not fulfill the unlinkability and unforgeability properties. Later, Alghazzawi et al [17], and Pradhan and Mohapatra [20] in 2011 introduced a new proxy blind signature mechanism that implemented ECDLP, which was asserted to be secure and efficient.

A proxy blind signature refers to a digital signature mechanism that fulfills the security properties of proxy as well as blind signatures. In such a scheme, the original signer assigns his signing right to the proxy signer due to special reasons. This means that the proxy signer produces a blind signature on behalf of the actual signer. Therefore, a proxy blind signature scheme is a special kind of signature that enables a designated user termed as a proxy signer to sign on behalf of multiple actual signers without viewing the message content. The delegation relationship is, thus, created between the original and proxy signers. The blindness property here signifies that the proxy signer is unaware of the content of the message that he or she signs. The scheme blends the advantages of blind, proxy and multi-signature schemes. A majority of proxy blind signature schemes were established on the basis of the hard problems such as Integer Factorization (IFP) and DLP that feature sub-exponential time.

The proxy blind signature mechanism is useful in ensuring the security of e-commerce transactions. Because it focuses on both authentication and privacy, the scheme should fulfill the following security properties [20]:

- Verifiability: Any arbitrary verifier or the signature's receiver can accurately validate the proxy blind signature.
- Distinguishability: The normal signature made by the actual signer should be different and distinguishable from the proxy blind signature made by the proxy signer.
- Unforgeability: Only the proxy signer has the right to produce a legitimate proxy blind signature.
- Unlinkability: Once the requester exposes the unblinded form of the signature for verification, the proxy or the actual signer cannot link the relation between the blinded message she or he signed and the exposed signature.
- Non-repudiation: The actual signer as well as the proxy signer cannot later deny that they were not involved in the signing procedure.
- Identifiability: Anyone can verify the identity of the original as well as of the proxy signer from the corresponding signature.
- Prevention of Misuse: The proxy key pair is available only for producing proxy signature.

Our protocol is an alternative to the group signature based approach. In addition to the group signature features, our approach provides signatures that contain higher degree of anonymity, are easily identifiable, non-repudiable, and less demanding on communication bandwidth.

3. NETWORK ASSUMPTIONS

The RSUs in a particular area (streets, highways) are connected to the designated Road Side Controllers (RSCs) as shown in Fig. 1. Thus a number of RSCs are set up throughout the VANET, which are in turn connected to the Internet. The principal authority in VANET system is the Department of Transportation (DOT) works as the Certificate Authority (CA) that protects an exhaustive dataset containing all necessary information of each RSU under an RSC. For instance, the RSU's location data, stationing history of RSUs along with the public key of the RSC are stored. DOT's public key is openly available to all the members including the vehicles in the VANET. The DOT may in turn be assisted by the local transportation authorities with information necessary to negotiate any dispute, including issuing licensing materials for a vehicle and/or commercial aspects of VANET.

Initially, an RSU announces the certificate containing ID_{RSC}, ID_{RSU}, $ADDR_{\mathrm{RSU}}$ (MAC address of the RSU), and the LOC_{RSU} (location information of RSU). An OBU obtains the public key of the RSC, the original MAC

addresses of the RSU, and the designated RSU location. The initial (beacon) message has the following certificate:

$$((ID_{RSC}, ID_{RSU}, LOC_{RSU}),$$
$$H(ID_{RSC}, ID_{RSU}, LOC_{RSU})Sign_{CA})$$

where $H(.)$ is a one-way hash function and $(.), H(.)Sign_{CA}$ indicates a signature using CA's secret key. The CA's signature endorses the message integrity and that the RSU is a valid member of the affiliating RSU group governed by the particular RSC.

By accepting the beacon frame [14], [15], the OBU checks the received MAC address with the MAC address of the transmitting RSU. The OBU joins the RSU group after the RSU's MAC address is validated. The position and time of the OBU are synchronized with the position and time information from the RSU.

4. PROXY BLIND SIGNATURE BASED MESSAGE DELIVERY SCHEME

To handle the above requirements stated in the introduction, we derive two schemes:

- RSU Message Delivery which consists of 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 Road Side Controller (RSC).
- OBU Message Delivery which consists of anonymous authentication of the OBU to the RSU and other OBUs as a valid delegate of the Department of Transportation (DOT), and delivering the signed messages to the RSU and to other vehicles.

A malicious RSU may attempt to misguide the on road vehicles by retransmitting an expired safety message. Therefore, RSUs are not always trustworthy and all the messages delivered through the RSU should be authenticated by the RSC. In our approach, RSUs in a given geographical area are grouped together to work under an RSC, where RSUs are connected to the RSC by high bandwidth secure links.

In order to accomplish the message integrity and trust requirements of RSU-to-OBU communications, we deploy proxy signature that would authorize an RSU to sign a message on behalf of the message originator while in the process, the RSU cannot alter the message or replay the expired messages.

We exploit the features of delegation with warrant proxy signature for the RSU message delivery. The term proxy signature refers to a variation of digital signature that designates an entity (called a proxy signer) to sign a message on behalf of the original signer. We considered a number of signature schemes and found Schnorr's scheme [2], [3] most suitable for fast and efficient signing of messages over the VANET. RSUs in a VANET would be the proxy blind signers, signing non-safety application messages to the OBU recipients on behalf of CA, the original creator of the messages. Therefore, the control of the message delivery is kept with the message originator (CA). A recipient OBU can verify the identity of the original signer, and it can also verify the integrity of the contents of the received message.

Furthermore, we deploy delegation with warrant proxy signature for the message integrity and privacy of OBU message delivery that covers OBU-to-RSU, and OBU-to-OBU message delivery.

Two large prime numbers, p and q (q is a prime factor of $p-1$), are conglomerated with VANET inception. Both p, q are attached to a large geographic region such as p to a country, and q to a state or province in that country.

Then a generator g for Z_p^* , is picked to be associated with a comparatively small area (for example a city, or a town).

Table 1. List of parameters and their extensiveness for message delivery in VANET

Parameter	Vastness in the Network					
	Original Signer		Proxy Signer		Receiver	
	Public	Private	Public	Private	Public	Private
p, q, g, r, T	✓					
s, v, r_s		✓				
y_{pr}, t, s'			✓			
s_{pr}, k				✓		
e^*, s^*					✓	
a, b, r', e						✓

4.1 System parameters

The parameters used in the proposed scheme are:

A: Original Signer - RSC
B: Proxy Signer
RSU (when OBU message delivery) / OBU (when RSU message delivery)
R: Signature Requester
RSU (when OBU message delivery) / OBU (when RSU message delivery)
CA: Central Authority or DOT
p, q: Two large prime numbers such that, $q|p-1$
g: An element of order q in Z_p^*
$x_A; x_B; x_R \in Z_q^*$: Secret key of *A*, *B*, *R* respectively.
$y_A = g^{x_A}(mod\ p)$: RSC's public key
$y_B = g^{x_B}(mod\ p)$: Proxy signer's public key
$y_R = g^{x_R}(mod\ p)$: Receiver R's public key
t_s: Message timestamp
H (.): Cryptographically secure one way hash function
$||$: Concatenation of two strings
m_w: Message warrant
m: Message

4.2 Proxy delegation

The RSC randomly picks out $v \in Z_q^*$ and computes,

$$r = g^v(mod\ p) \quad (1)$$
$$s = x_A + v.H(m_w||r)\ (mod\ q) \quad (2)$$

RSC sends (r, s) along with the message warrant m_w to the proxy signer *B* and *CA*, via a secure channel.

Now the proxy signer calculates,

$$s_{pr} = s + x_B y_A \quad (3)$$

The value of s_{pr} obtained is the secret identity of an individual proxy signer; hence it is usually kept within its RAM and is obscured from other parties.

4.3 Blind signing

Proxy signer, *B* randomly selects an integer $k \in Z_q^*$, and computes

$$t = g^{k+x_B} (mod\ p) \quad (4)$$

The tuple (r, t, m_w) is sent to the receiving OBU/RSU *R*.

R checks A's (i.e. RSC's) and B's identities and the delegation lifetime of the warrant m_w. This checking helps to prevent the attacks such as message forgery, impersonation if somehow the proxy signer is compromised.

If the above checking is successful,

R selects two random numbers $a, b \in Z_q^*$ and computes

$$r' = t.g^{a+x_R}.y_{pr}^b \ (mod\ p) \quad (5)$$

where $y_{pr} = g_{pr}^s \ (mod\ p)$ is the public key for the proxy blind signature.

$$e = H(r'||m)\ (mod\ q) \quad (6)$$

$$e^* = b - e\ (mod\ q) \quad (7)$$

If $r' = 0$, then *R* needs to select a new tuple (a, b) otherwise, *R* sends e^* to proxy signer and *CA*.

For signing blinded message, *B* must request a time stamp for the message.

When there is a message to be transported 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 supplement the message content m with a message expiry time t_s. It is crucial for the VANET system to thwart the RSU from abusing the proxy blind signature by posting invalid messages, or replaying the old messages. The message m is thus jointly signed by the RSC and the subsequent RSUs before it is delivered to the vehicles on road.

RSC chooses a random number $k_s \in Z_q^*$ and computes

$$r_s = g^{k_s} (mod\ p) \quad (8)$$

$$T = H(r_s \,||\, t_s \,||\, e^*)\ (mod\ p) \quad (9)$$

RSC sends *T* to the proxy signer *B* and receiver *R*.

The proxy signer applies the gained e^* and T values to estimate the final signed message as

$$s' = k + e^* s_{pr} + T \quad (10)$$

The proxy blind signature (m, s') can now be delivered to the receiver.

4.4 Verification

Upon acquiring s' from *B*, the receiving node computes,

$$s^* = g^{a+s'-T} (mod\ p) \quad (11)$$

Thus, the proxy blind signature on message m is the tuple (m, m_w, s^*, e). Verifier can now verify the proxy blind signature by checking whether

$$e = H(s^* y_B y_R y_{pr}^e || m)\ (mod\ q) \quad (12)$$

where $y_{pr} = g^{s_{pr}} \ (mod\ p)$ is the public key for the proxy blind signature.

4.5 Revocation phase

Under any circumstances if the RSC wants to revoke the delegation before the specified delegation period, then that particular RSC looks up in its revocation list. The CA/DOT maintains the entire list of the revoked nodes (RSU/ OBU). On demand from the RSC, CA provides the revocation list from its repository. During the computation of T, the RSC checks the validity of delegation period specified in the proxy warrant m_w and the revocation list. If it is within the valid delegation period and the proxy signer is not found in the revocation list, RSC computes T, sends it to proxy signer *B* and receiver *R* for the message. If *B* is in the revocation list then RSC does not compute T. Hence, the proxy signer cannot sign the message. Also, suspicious node will be communicated to the CA. Soon after, the CA will update its revocation database which may be passed down to subsequent RSCs.

4.6 System accuracy

Consider the verification equation given in (12). The main component of the equation is $(s^* y_B y_R y_{pr}^e || m)$

Now, $s^* y_B y_R y_{pr}^e || m$

$= s^* g^{x_B} g^{x_R} y_{pr}^e || m$

$= g^{u+s'-T+x_B+x_R} y_{pr}^e || m$

$= g^{k+u+e^* s_{pr}+x_B+x_R} y_{pr}^e || m$

$= g^{k+u+(b-e)s_{pr}+x_B+x_R} y_{pr}^e || m$

$= g^{k+u+bs_{pr}-es_{pr}+x_B+x_R} y_{pr}^e || m$

$= g^{k+u+bs_{pr}+x_B+x_R} y_{pr}^{-e} y_{pr}^e || m$

$= g^{k+u+bs_{pr}+x_B+x_R} || m$

$= g^{k+u+x_B+x_R} y_{pr}^b || m$

$= t g^{u+x_R} y_{pr}^b || m$

$= r' || m$

$$H(s^* y_B y_R y_{pr}^e || m)\ (mod\ q) = H(r' || m)\ (mod\ q) = e$$

5. OVERHEAD CALCULATION

Consider the proxy blind signature on the message m, (m, m_w, s^*, e). To calculate the signature payload on the message we only deal with the quantities m_w, s^*, e. The prime numbers p and q are of 512 and 140 bits respectively, the total size of the signature payload in the authentication of the proxy blind signature would amount to 102 bytes with the standard SHA-1 hash operation.

Table 2. Signature payload

Parameter	Size (in Bytes)
m_w	20
s^*	64
e	18
Total	102

6. INVESTIGATION OF THE SCHEME

The security of the proposed scheme relies mainly on the inherent difficulty of solving discrete logarithm problem of proxy signature scheme. For the message signature, the proxy signer uses a new secret which is derived from the actual secret key of the original signer. The intractability of the discrete logarithm problem from proxy signature scheme assumes that an adversary can't reverse the process to generate the actual secret from the knowledge of a proxy key.

In the first part of our security analysis, we focus on the secure RSU-to-OBU message delivery approach of the VANET, while in the next part; we analyze the anonymous OBU message delivery.

6.1 RSU message delivery

False Message Injection: The original signer (i.e. RSC) produces a message to be delivered to the OBUs while it allows its corresponding subordinate RSUs to sign on behalf of it. In proxy blind signature scheme over VANET, a new proxy tuple has to be generated and delivered to the proxy signer for every single new message. The RSU cannot voluntarily input malevolent messages into the network. Since the key x_A of the original signer (RSC) is attached to the secret key of the proxy blind signature s_{pr}, only the RSC can produce a valid proxy key pair for which the message will be accepted by an OBU.

There is a possibility that an adversary can successfully get a false message verified by an OBU. The probability for a false or modified message to be verified by an OBU is $1/(q-1)$. The probability that an OBU will be deceived by a false message is $1/(p-1)$. Hence, the overall chance that an OBU would be misled by an adversary is $(1/(p-1)+1/(q-1))$. Therefore, the values for both p and q should be large enough in order to avoid such scenarios.

Unforgeability: Only a valid proxy-signer RSU can create a given signature on behalf of the RSC. The receiver OBU cannot forge the signature after receiving (m, m_w, s^*, e) on message m. When an adversary with the new modified message m' tries to forge a signature (m', s^*, e') on message m', it must verify that the equation given below is correct.

$$s^* y_B y_R y_{pr}^{e} \pmod p = t g^{a+x_R} y_{pr}^{b} \pmod p \quad (13)$$

By using the equations(4) to (8)

$$s^* y_B y_R y_{pr}^{e} \pmod p$$

$$= g^{a+s'-T} g^{x_B} g^{x_R} y_{pr}^{e'} \pmod p \quad (14)$$

$$= g^{a+s'-T+x_B+x_R} g^{e' s_{pr}} \pmod p \quad (15)$$

$$= t g^{a+(v-e)s_{pr}+x_R} g^{e' s_{pr}} \pmod p \quad (16)$$

$$= t g^{a} + x_R y_{pr}^{b} \quad (17)$$

From the above,

$$g^{(b-e)s_{pr}} g^{s_{pr} e'} \pmod p = g^{b s_{pr}} \pmod p \quad (18)$$

This cannot hold true, as $e \neq e'$. Therefore the OBU fails to forge a valid proxy blind signature on message m'.

Non-repudiation and Impersonation: As an RSU is strictly assigned to only one proxy, it cannot generate any valid proxy signature which would not be identified as a signature of only that particular RSU. The s_{pr} value of a valid signature for a given session is unique and can only be generated by a particular RSU. An adversary cannot generate a valid proxy signature from the public parameters, since s_{pr} the derived secret key of the proxy blind signature is dependent on the RSC's private key.

Even if an adversary succeeds in generating a new proxy key pair (s_{pr}, y_{pr}) launching an impersonation attack is not possible, since a malicious RSU cannot provide its exact identity to the receiver with a considerable probability for computing a valid e using (6) in the stipulated time t_x for the message m.

Due to the inclusion of the original signer and proxy signer identities information, message type to be signed by the proxy signer, delegation period, etc. in the warrant itself the proposed scheme is capable of preventing proxy key pair misuse.

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 when it informs the CA about the corrupt node in the network.

Although, the compromised proxy is still a valid one and can be used by the adversary, it cannot harm the system by signing an illegitimate or expired message. This is due to the fact that e requiring the original message m itself, the expiry information t_x and the primary secret x_A generated only by the RSC. Nevertheless, the misbehaving RSUs must be replaced once identified, after conducting an investigation by the VANET administrator.

6.2 OBU message delivery

We discuss below some of the security issues concerning our proposed scheme for OBU message broadcasts in VANET.

Anonymity: At the time of registration/license renewal an OBU is preloaded with *n* different delegations. The size of *n* is important for the vehicle's anonymity and may vary according to the owner's preference of privacy. The OBU uses one of them while sending a new message in VANET. This proxy is chosen randomly from the preloaded set of proxies. Thus, the original identity of the vehicle is not exposed to other parties during the message communication. Generally, the proxy blind signature is un-linkable at the receiving end which provides an adaptive anonymity and privacy to a VANET user while the original MAC address of the sender is also undisclosed as indicated by the standards [15]. Thus, the original identity of the vehicle is not exposed to other entities during an OBU message transmission.

Accountability: Under a critical situation when it is necessary and permitted by the appropriate law enforcement authorities, a vehicle's identity can be traced by investigating a sent message. From the warrant m_w, anyone

can mark original signer and proxy signer. On the other hand, as the verification equation contains the public key of the proxy signer and original signer, one can determine them. The message is reconstructed at the DOT using the identity assigned to that particular vehicle, the parameters, m_w, t_x from the signed message, and s^* from the reporting RSU. While the reconstructed message matches, the complete identity of the vehicle is retrieved by the DOT.

False Message Injection*:* A malicious OBU may try to transmit a false or modified message m' in the VANET. The only necessity for an adversary is to compute a valid public key y_{pr} for the message m'. As y_{pr} is modulo p operation, the probability that the false (or, modified) message would get through is $1/(p-1)$, meaning that a large (usually, at least 512 bit for a proxy signature) p would be required.

Replay Attacks: A malicious party may attempt to replay a valid message at the same location where the signed message was originally delivered. However, the expiry information of the message is associated with the main message content which would make the signed message invalid once the validity expires. As proxy blind signature requires a new proxy tuple to be generated securely delivered to the proxy signer for every single new message, replay attacks are impractical in this system.

Node Compromise and Sybil Attacks: An adversary may launch several useless and misguiding messages to distract a VANET upon an OBU compromise. The malicious behavior of a vehicle must be reported to the DOT as soon as identified. The DOT would release a revocation order for the tainted vehicle over the VANET if it is confirmed about the malicious act. It would then incorporate that vehicle in the revocation list which should be published to all the RSCs. Later the RSU generates an alert, so that the other vehicles can ignore the vehicle. This process would continue till the issue is resolved and the DOT further notifies the VANET about it.

A malicious vehicle may want to launch a Sybil attack where a vehicle sends out several identities usually to misdirect a VANET. To thwart such an attack, an entity would not be allowed to create or store pseudonymous identities.

7. CONCLUSION AND FUTURE WORK

In this paper, we presented VANET message delivery protocol that has two separate components for RSU and OBU messages in a vehicular network environment. The proposed protocol uses a modified proxy blind signature mechanism to comply with VANET's message integrity and privacy requirements. Security analysis shows that our approach has strong resistance against potential forgery and attacks launched by adversaries. Our protocol has low communication overhead, and is applicable to IEEE 802.11p WAVE standards for vehicular communication. In future, we will be working on extending our protocol with low power cryptographic primitives with experimental evaluation of the schemes, and deploying it in an IEEE 1609.2 [16] framework.

REFERENCES

1. 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.
2. 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.
3. C. P. Schnorr, "Efficient Signature Generation by Smart Cards," Journal of Cryptology, vol. 4, no. 3, pp. 161–174, 1991.
4. 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.
5. 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.
6. 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.
7. 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.
8. [8] S. Biswas, M. M. Haque, and J. Mi˘si´c, "Privacy and Anonymity in VANETs: A Contemporary Study," Ad Hoc & Sensor Wireless Networks, 2010.
9. [9] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing Vehicular Communications," Wireless Communications, IEEE, vol. 13, no. 5, pp. 8–15, October 2006.
10. [10] D. Chaum and E. van Heyst, "Group Signatures," in EUROCRYPT, 1991, pp. 257–265.
11. [11] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," Advances in Cryptology CRYPTO 2004, Lecture Notes in Computer Science, Springer Berlin / Heidelberg, vol. 3152/2004, pp. 41–55, Dec.2004.
12. [12] J. Guo, J. Baugh, and S. Wang, "A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework," May 2007, pp. 103–108.
13. [13] 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.
14. [14] "Draft Amendment for Wireless Access In Vehicular Environments (WAVE)," IEEE, New York, NY, IEEE Draft 802.11p, Jul. 2007.
15. [15] "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)- Networking Services," IEEE, New York, NY, IEEE Std 1609.3, Apr. 2007.
16. [16] "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)- Security Services for Applications and Management Messages," IEEE, New York, NY, IEEE Standardd 1609.2, Jul. 2006.
17. [17] Alghazzawi, D. M., Salim, T. M. and Hasan, S. H. "A New Proxy Blind Signature Scheme Based on ECDLP," IJCSI International Journal of Computer Science Issues, vol. 8, No. 3, May 2011.

18. [18] Lal, S. and Awasthi, A. K. “Proxy Blind Signature Scheme”, Journal of Information Science and Engineering, Cryptology e-Print Archive, Report 2003/072, 2003.
19. [19] Lin, W. D. and Jan, J. K. “A Security Personal Learning Tools using a Proxy Blind Signature Scheme”, Proc. of Intl Conference on Chinese Language Computing, pp. 273-277, 2000.
20. [20] Pradhan, S. And Mohapatra, R. K. “Proxy Blind Signature Based on ECDLP”, International Journal of Engineering Science and Technology, Vol. 3, No. 3, March 2011.
21. [21] Tan, Z. “Efficient Pairing-Free Provably Secure Identity-Based Proxy Blind Signature Scheme”, Security and Communication Networks, Vol. 6, No. 5, pp. 593-601, 2013.
22. [22] Wang, H. Y. and Wang, R. C. “A Proxy Blind Signature Scheme Based on ECDLP”, Chinese Journal of Electronics, vol. 14, no. 2, pp. 281-284, 2005.
23. [23] Yang, X. and Yu, Z. “Security Analysis of a Proxy Blind Signature Scheme Based on ECDLP”, Proc. 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM'08), pp. 1-4, Oct. 2008.
24. [24] Qi, C. and Wang, Y. “An Improved Proxy Blind Signature Scheme Based on Factoring and ECDLP”, Proc. International Conference on Computational Intelligence and Software Engineering, pp. 1-4, 2009.