Deploying Proxy Signature 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 introduce a verifiable, self authenticating, and anonymous message delivery protocol for VANET communications using different implementations of proxy signature scheme, where RSU-to-OBU, OBU-to-RSU, and OBU-to-OBU message delivery issues have been addressed. An RSU-to-OBU message delivery scheme is developed, in which a message is protected against potential forgery launched by a malicious RSU. Also, a new proxy signature based approach is provided for message integrity and anonymity for the OBU message delivery. The total process is accountable. The security analysis confirms the validity of the proposed protocol.

I. INTRODUCTION

A vehicular ad hoc network (VANET) consists of three fundamental components namely road side unit (RSU), on board unit (OBU), and an appropriate infrastructure to coordinate with the whole system as well as the connectivity to the Internet. We can divide the total communications into three major categories: RSU-to-OBU, OBU-to-RSU, and OBU-to-OBU communications. Most of the messages deal with road security and safety information which have important implications for driver behavior; if a malicious entity deliberately transmits false messages, it may mislead the traffic or even impair the transportation safety.

To prevent this risk, vehicular communication must have the capability of verifying the identity of the message sender as well as maintaining the integrity of the delivered message, both of which can be accomplished through a suitable signature protocol. However, identity verification is not a simple task due to high and variable velocity of nodes, varying node density, and the need to operate on roads with nonuniform characteristics. Thus, the issue of scalability is of prime importance as, under heavy traffic, a single controller might need to handle a large number of vehicles. 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. Hence, our scheme should have low computational/communication complexity, high scalability, as well as a reliable and verification mechanism.

Another prime concern in vehicular communication is the privacy and anonymity of a vehicle, while the system has to make sure that no OBUs take advantage of the anonymity by sending false messages. In other words, VANET has to be accountable in case of a dispute, given that the appropriate legislative measures would be taken beforehand. To cope with the above requirements, we develop 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. Fig. 1 depicts the VANET architecture.

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 can not alter the message or replay the expired messages.

We exploit the features of partial delegation proxy signature [1] 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. A partial delegation mechanism of a proxy signature produces a new secret key from the original signer’s secret, and the new secret is used as the key for proxy signing. 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 signers, signing safety and other application messages to the OBU recipients on behalf of RSC-the original creator of the messages. Therefore, the control of the message delivery is kept with the message originator (RSC). 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 partial delegation proxy signature for the message integrity and privacy of OBU message delivery that covers OBU-to-RSU, and OBU-to-OBU message delivery.

We organize the paper in the following manner. Section II discusses the evolution of proxy signature scheme together with alternative technologies for signatures in VANET. A brief account of the network assumptions is given in section III. Section IV and Section V delineate the proposed protocol for RSU and OBU message delivery. The security analysis is provided in Section VI as Section VII concludes the paper.

II. 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). 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 be posted.

Number of papers have addressed the problem of anonymity in VANETs [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 possess 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.

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.

III. NETWORK ASSUMPTIONS

A number of RSCs are deployed over the VANET, which are connected to the Internet as shown in Fig. 1. The Department of Transportation (DOT) works as the Certificate Authority (CA) which maintains all necessary information of each RSC under an RSC. For instance, DOT stores the location information, deployment history of individual RSUs along with the public key of the RSC. DOT issues the certificate for each of the RSUs in the VANET.

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

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 RSC’s location information, Loc\(_{RSC}\). 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 \(H(\cdot)\) is a one-way hash function and \(\cdot\)\(_{S_{CA}}\) 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 [14], [15], 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. The time synchronization among vehicles and RSUs are done using the timing information field of WAVE Service Advertisement (WSA) frame [16].

IV. RSU MESSAGE DELIVERY SCHEME

In the beginning, a VANET is equipped with two large prime numbers, \(p\) and \(q\), where \(q\) is a prime factor of \(p - 1\). These \(p, q\) 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 picked to be associated with a comparatively small area (for example a city, or a town).

A. Proxy Pre-processing

For each RSU, RSC generates a random number \( s < q \) which is considered to be the private key of the original proxy signer (RSC) for reliable message delivery 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, \( k \in R \ Z_{p-1}\setminus\{0\} \); where, \( Z_{p-1}\setminus\{0\} \) 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 VI-A5.

During the initialization phase, the RSC computes

\[ K = g^k \mod p \] (1)

This \( K \) value is dependent on the revocation parameter \( k \) as indicated in Equation 1, and is used for calculating a proxy secret key, \( \sigma \).

\[ \sigma = s + kK \mod (p - 1) \] (2)

The value of \( \sigma \) 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 \((\sigma, K)\) and the delivered message respectively.

The proxy pair \((\sigma, K)\) 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 \((\sigma, K)\) as just a proxy.

Values of \( \sigma \) 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 delivered 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 prevent the RSU from abusing the proxy 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.

The RSU uses the value of \( \sigma \) 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 [1], [4].

The signature and the verification procedure, modified from the original proxy signature scheme, is given below.

B. RSU Proxy Signature

The RSC picks a session parameter \( r = H(s, m, t_x) \mod q \), and computes

\[ x = g^r \mod p \] (3)

This session parameter is generated as soon as there is an event for which a message has to be delivered. RSC subsequently calculates the hash value \( h \) of the message \( m \) concatenated with \( x \),

\[ h = H(m, x, t_x) \] (4)

The message \( m \), expiry information \( t_x, h \), 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 transmitted through RSUs. Next, the RSU utilizes the received \( r \) and \( h \) values to calculate \( y \):

\[ y = (r + \sigma h) \mod q \] (5)

The proxy signature \((h_s, y)\) is concatenated with the (safety application or other) message, which eventually results in a tuple \((m, t_x, h, y, K)\) to be delivered by the RSU.

C. Verification

The receiving vehicle (OBU) uses the signature components for verification of proxy signature on the message \( m \):

\[ v' = vK^\sigma \mod p \] (6)

This value is used in the following calculation of (7):

\[ x' = g^y v^h \mod p \] (7)

The expiry information \( t_x \) is immediately matched with the current system time of the OBU. Upon detecting an expired message from an RSU, it may release a relay alert to notify the concerning authority after discarding the message. If not, the message is verified as below:

\[ h = H(m, x', t_x) \] (8)

If (8) holds then 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 session parameter \( r \), 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.

---

**TABLE I**

**List of parameters and their scopes for RSU-to-OBU message delivery in VANETS**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Generated by</th>
<th>Scope in the network</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p, q, g, v, K, h_s )</td>
<td>RSC</td>
<td>Public</td>
</tr>
<tr>
<td>( k, s, x, h )</td>
<td>RSC</td>
<td>Private (RSC)</td>
</tr>
<tr>
<td>( \sigma, r )</td>
<td>RSC</td>
<td>Private (RSC, RSU)</td>
</tr>
<tr>
<td>( y )</td>
<td>RSU</td>
<td>Private (RSU, OBU)</td>
</tr>
<tr>
<td>( x' )</td>
<td>OBU</td>
<td>Private (OBU)</td>
</tr>
</tbody>
</table>

---

978-1-4244-5637-6/10/$26.00 ©2010 IEEE
V. OBU Message Delivery Scheme

Public parameters $p$, $q$, and $g$ for the OBU-to-OBU and OBU-to-RSU communications are chosen in the same manner as of the public values for RSU-to-OBU communication. We use the partial delegation based signature scheme [1] for OBU message signing. The Department of Transportation (DOT) plays the administrative role as the original signer for the broadcast message, while OBUSs will be the partial delegation based signers for signing messages. This is done so that the sender OBUSs (and the signed messages) are unforgeable, verifiable, identifiable, and non-repudiable to the DOT.

The DOT is connected to the local transportation office which is responsible for the delivery of delegation materials to the vehicles at the time of registration/renewal of the vehicle’s license.

A. Pre-processing

During the pre-processing phase, the DOT generates its private key/public key pair $(s_D, v_D)$ following the same routine as IV-A. The necessary parameters are chosen so that the system can accommodate enough delegation proxies for a large number of vehicles operating in a given geographical area. At the time of registration/license renewal, a car is pre-loaded with $n$ different delegations $(\sigma_i, K_{c,i})$ where, $i = 1, 2, \ldots, n$. The size of $n$ is important for the vehicle’s anonymity and may vary according to the owner’s preference of privacy. A vehicle is pre-loaded with proxies $(\sigma_i, K_{c,i})$ such that for a given one way keyed-hash function $H_{\alpha}()$ where $\alpha$ is a secret key, $H_{\alpha}(K_{c,1}) = H_{\alpha}(K_{c,2}) = \ldots = H_{\alpha}(K_{c,n})$. This is possible by taking advantage of the hash function’s message collisions [18]. Note that the key $\alpha$ is different for each vehicle and kept within the DOT. Table II categorizes the used parameters according to their scopes.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Generated by</th>
<th>Scope in the network</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p, q, g, v_D, K_{c,i}$</td>
<td>DOT</td>
<td>Public</td>
</tr>
<tr>
<td>$\kappa, s_D, \sigma_i$</td>
<td>DOT</td>
<td>Private (DOT)</td>
</tr>
<tr>
<td>$r_c$</td>
<td>sender OBU, RSU</td>
<td>private (sender OBU, DOT)</td>
</tr>
<tr>
<td>$x_c$</td>
<td>sender OBU</td>
<td>private (sender OBU, RSU)</td>
</tr>
<tr>
<td>$x'<em>c, v</em>{new}$</td>
<td>receiver OBU, RSU</td>
<td>private (receiver OBU, RSU)</td>
</tr>
<tr>
<td>$y_c, h_c$</td>
<td>sender OBU</td>
<td>private (receiver OBU, RSU)</td>
</tr>
</tbody>
</table>

B. Signature Generation

We assume that every vehicle using the VANET is equipped with a GPS system that determines its current location. The location information of the vehicle is taken from the GPS data to generate a session value $r_c < q$. The GPS data is passed to a one-way hash function which generates a same rounded output, $r_c$ for all devices in the communication range of the OBU. This is done by taking only the most significant bits of the hashed data so that in the maximum communication range of an OBU (approximately 300 meters), $r_c$ values come same. To prevent potential replay attack, a message $m_c$ is associated with its expiry time $t_{cx}$. The following equations are used for signing a message $m_c$ by an OBU.

$$x_c = g^{r_c} \mod p$$
$$h_c = H(m_c, x_c, t_{cx})$$
$$y_c = (r_c + \sigma_i h_c \mod p)$$

The set $(m_c, t_{cx}, h_c, y_c, K_{c,i})$ is delivered by the OBU to RSUs and/or to other OBUSs in the communication range.

As mentioned before, an OBU is pre-loaded with multiple delegations. To maintain the anonymity on road while communicating, it uses different delegation every time for signing and transmitting a message.

C. Signature Verification

The receiving RSU/OBUSs compute a new proxy public key $v_{new} = v_D K_{c,i}^{-1} \mod p$. The location information, either collected from the local GPS (in case of an OBU), or the pre-determined one (for an RSU), is used for determining $r_c$ value. The following relationship is checked:

$$x'_c = g^{r_c} v_{new} x'_c \mod p = g^{r_c} \mod p$$

If (10) holds, the receiving node verifies the expiry information with the message in the following manner.

$$h_c = H(m_c, x'_c, t_{cx})$$

If the last equation does not hold, the receiving node either ignores the message or an alert to the corresponding RSC, depending on the system configuration.

Assuming that the primes $p$ and $q$ are of 512 bits, and we choose MD5 hashing, the total size of the overhead added by our approach in both the schemes comes to 152 bytes. Replacing the MD5 hashing with SHA-1 would make the signature overhead 156 bytes.

VI. Security Analysis

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.

A. RSU Message Delivery

1) False Message Injection: The original signer (i.e. RSC) produces a message to be delivered to the OBUSs while it allows its corresponding subordinate RSUs to sign on behalf of it. Unlike the conventional warrant based proxy signature approaches where the original signer designates a proxy signature either by signing a declaration or where the original signer signs the message along with a newly derived public
key, our approach determines a session parameter $r$ from the message $m$ and the expiry info $t_x$ using the secret key of the original signer. Since the key $s$ is secret, only the original signer (RSC) can produce a valid session parameter for which the message will be accepted by an OBU.

However, as the $r$ value is computed through a modulo $q$ operation, 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. Choosing $p$ and $q$ of length 512 bits, gives the probability of a false/modified message to be verified by the OBU $< 2/(2^{511} - 1) \approx 1/2^{510}$.

2) 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 $\sigma$ from its proxy set $(\sigma, K)$ to sign a message. Each $\sigma$ 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, $(\sigma', K')$) that satisfies eqn. (2). Since, signing also requires a valid $h$ (refer to (5)) which is solely generated by the RSC, an adversary can never create a valid proxy signature.

Since $\sigma$ is derived from a randomly generated secret $s$, computing a new $\sigma$, or determining the secret $s$ from a given $\sigma$ of a proxy is very hard due to the complexity of solving discrete logarithm problem.

3) 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 equation 5. An adversary cannot generate a valid proxy signature from the public parameters, since $s$ and $k$ values are kept secret in the RSC. Even if an adversary succeeds in generating a new proxy $(\sigma', K')$ which satisfies (2), launching an impersonation attack is not possible, since a malicious RSU cannot provide an appropriate session parameter $r$ with a considerable probability for computing a valid $y$ using (5).

4) Exculpability: The term exculpability refers to the property of a signature scheme, for which a signing entity may not be able to forge a signature so that the signature would appear to come from a different source [12]. 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 $(\sigma, K)$ 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 (6) and (7), which would lead to an unsuccessful verification in the process. Again, since $h$ value is not changeable for a given message, changing of $y$ using (5) requires change of $\sigma$ and/or $r$. Note that the $r$ value should always remain smaller than $q$, and finding a valid combination of $(\sigma, K)$ with a given public key $v$, requires extreme efforts as $s$ and $k$ values are only known by the RSC.

5) 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 $k$ followed by computing a verification parameter $K$ using (1) and so on.

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 the session parameter $r$ can only be generated by the RSC, requiring the original message $m$ itself, the expiry information $t_x$, and the primary secret $s$. Nevertheless, the misbehaving RSUs must be replaced once identified, after conducting an investigation by the VANET administrator.

B. OBU Message Delivery

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

1) Anonymity: An OBU is preloaded with $n$ proxies, and it uses one of them while sending a new message in VANETs. 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. The $K_{c,i}$ values are normally unlinkable 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.

2) Accountability: Under a critical situation when it is necessary and permitted by the appropriate law enforcement authorities, a vehicles identity can be traced by investigating a sent message. A signed message $(m_c, t_{cx}, h_c, y_c, K_{c,i})$ is taken into consideration. Assuming that the message is a valid one (it could be an expired one though), the value $K_{c,i}$ is checked against the database maintained at the DOT. There is a possibility that multiple vehicle entries may come up for a given $K_{c,i}$. The corresponding $\sigma_{c,i}$ values are then taken and the message is reconstructed at the DOT using all the proxies assigned to that particular vehicle, parameters $m_c, t_{cx}$ from the signed message, and $r_c$ from the reporting RSU. The proxy for which the reconstructed message matches with the considered one is the proxy used by the critical vehicle. The complete identity of the vehicle is retrieved by the DOT.

3) False Message Injection: A malicious OBU may try to transmit a false or modified message $m_f$ in the VANET. Since, $r_c$ is available from the location data, and $h_c$ can be determined accordingly using (9), the only odd for an adversary is to
compute a valid \( y_c \) for \( m_f \). As the \( y_c \) is a 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.

4) **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. Given that the validity period is long enough, the adversary may try to replay the same message in a different location (e.g. in a different street with different sets of vehicles on road). Since the receiving node uses its own location information during the message verification phase (refer to (10)), the adversary would not be able to get a false message successfully verified.

5) **Node Compromise and Sybil Attacks:** An adversary may launch several useless and misleading 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 publish the revocation secret \( \alpha \), as well as the value \( H_\alpha(K_{c,i}) \) for that particular vehicle. After that, each RSU in the VANET would compute \( H_\alpha(K_{c,i}) \) upon receiving message from an on-road vehicle. If the computed value matches with the \( H_\alpha(K_{c,i}) \) released from DOT, 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.

Since an OBU is preloaded with multiple proxies, a malicious vehicle may launch a sybil attack where a vehicle sends out several identities usually to misdirect a VANET. To thwart such an attack, an entity would store the \( K_{c,i} \) fields for all the messages received in a short time frame (30 sec). On an average, a vehicle goes out of the communication range of an RSU within this time period. If the stored messages are same or if they trigger the similar course of action, the receiving device can report the incident to the RSC. As the actual identity of a vehicle is traceable based on the contents of its signed messages in VANET, the adversary would not be able to deny the responsibility of the attack.

However, adaptation of these policies is subjected to a country or territory’s law enforcement and legislation system.

**VII. 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 signature mechanism to comply with VANETS’ 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 a IEEE 1609.2 [19] framework.

**ACKNOWLEDGMENT**

This work has been partially supported by the APMA Auto21 project from the Govt. of Canada.

**REFERENCES**


