Hybrid anonymous message broadcast for VANETs

Andrea Huszti, Szabolcs Kovács, Norbert Oláh

University of Debrecen

October 11, 2021
Introduction

1. Introduction
   - Motivation
   - VANET
     - Security requirements of the VANET
   - Bilinear pairing

2. Hybrid anonymous message broadcast
   - Our security goals
   - Protocol
   - Security analysis
   - Implementation and prototype
   - Result
Motivation

- Rapid increase in the number of cars
- Increasing the level of security
- Apply in the world of IoT
Vehicular Ad-Hoc Networks - VANET

Figure: Vehicular Ad-Hoc network
Features of the VANET

- High mobility: In the general case, participants move in different directions and at different speeds.

- Dynamic Topology: The VANET topology is rapidly changing, dynamic and unpredictable.

- Common restrictions
Security requirements

- **Eligibility**: It must be ensured that only authorized participants can send valid messages.

- **Conditional anonymity**: V2V and V2I communications must be anonymous, on the other hand, anonymity must be revocable.

- **Transparency**: The activities of authorities must be transparent to all participants in the network.

- **Efficiency**: A suitable cryptographic protocol must work efficiently for both congestion and low traffic.
Hybrid anonymous message broadcast

- **Locally IBE**: vehicles under the supervision of the same TA are communicating through the identity-based infrastructure.

- **Globally PKI**: vehicles from a different TA’s territory will be authenticated with certificates.
Disadvantages of local certificate-based systems

- Higher resource requirements
  - Requires higher storage capacity
  - The devices check the recipient’s certificate before each message is sent

- Due to the finite validity period of the certificates, they need to be updated from time to time.

**Definition:** Let $G_1$ and $G_2$ be two groups of order $q$ for some large $p$. A map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ is an admissible bilinear map if it satisfies the following properties:

1. **Bilinear:** We say that a map $\hat{e} : G_1 \times G_2 \rightarrow G_2$ is bilinear if $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $P, Q \in G_1$ and all $a, b \in \mathbb{Z}$

2. **Non-degenerate:** The map does not send all pairs in $G_1 \times G_2$ to the identity in $G_2$. Since $G_1$ and $G_2$ are groups of prime order, if $P$ is a generator of $G_1$ then $\hat{e}(P, P)$ is a generator of $G_2$.

3. **Computable:** There is an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in G_1$.
Application of bilinear pairing

  - Each device stores the master secret key.
  - If a device is compromised, so is the whole system.

- It allows easy authentication, but only the TA has the master secret key.
- Public key revocation list without certificate.
Our security goals

- **Sender anonymity** and **unlinkability of messages**
- **Mutual authentication** - Communication phase
- **Secrecy of authorized ID and authorized secret key** - Communication phase
- **Authenticity and data integrity of messages** - Incident report
- **Anonymity revocation, non-repudiation of malicious messages** - Incident report
Hybrid anonymous message broadcast protocol for VANETs

Andrea Huszti, Szabolcs Kovács, Norbert Oláh

DE-IK
Initialize

\[
\begin{align*}
\text{OBU (V)} & : \text{TA: } P, \gamma P \\
Q_V &= H(ID_V || T) \rightarrow \text{Long-lived public key} \\
\gamma Q_V & \rightarrow \text{Long-lived secret key} \\
\text{RSU (R)} & : \text{TA: } P, \gamma P \\
Q_R &= H(ID_R || T) \\
\gamma Q_R &
\end{align*}
\]
Communication setup

OBU (V)

\[ t, s \in \mathbb{Z}_q^* \text{ random} \]
\[ A_1 = \hat{e}(\gamma Q_V, Q_R) \]
\[ M_1 = Enc_{Q_R}(Q_V, A_1, t, s\gamma Q_V) \]
\[ Check \ Q_R \ on \ Rev. \ List \]

RSU (R)

\[ x_i \rightarrow \text{local secret key} \]
\[ x_iQ_R \rightarrow \text{public key} \]
\[ Sign_{\gamma Q_R}(x_iQ_R) \]

Decrypt: \ \text{Dec}_{\gamma Q_R}(M_1)
\[ Q_V \ on \ the \ Rev. \ List? \]
\[ A_1 \overset{?}{=} \hat{e}(Q_V, \gamma Q_R) \]

Anonymized User List:
\[ \hat{e}(x_iQ_V, Q_V) \]
\[ TA: \ \hat{e}(x_iQ_V, Q_V)^\gamma \]

\[ x_i = s^{-1}, tx_iQ_V \cdot t^{-1} \]
\[ \hat{e}(x_iQ_V, Q_R) \overset{?}{=} \hat{e}(Q_V, x_iQ_R) \]
\[ \hat{e}(x_i\gamma Q_V, Q_R) \overset{?}{=} \hat{e}(\gamma Q_V, x_iQ_R) \]
\[ x_iQ_V, x_i\gamma Q_V \]
Incident report

OBU (V)

- $a \in \mathbb{Z}_q^*$ random
- $b \in \mathbb{Z}_q^*$ random

$A_{ID} = aQ_V$

$A_1 = ax_iQ_V$

$A_2 = bH(M||T) + a\gamma Q_V$

$A_3 = a^{-1}x_i\gamma Q_V$

$A_{ID}, A_1, A_2, A_3, bP, M, T$

Check: $T$

Check: $\hat{e}(A_{ID}, x_iQ_R) = \hat{e}(A_1, Q_R)$

Check: $\hat{e}(A_2, P) = \hat{e}(A_{ID}, \gamma P)\hat{e}(H(M||T), bP)$

Check: $\hat{e}(A_3, A_{ID})$ on the Anonymized User List?
Malicious user management

\[
\begin{align*}
\text{OBU (V)} &\quad A_{ID}, A_1, A_2, A_3 \\
\quad &\quad A_{ID}, A_1, A_2, A_3 \\
\quad &\quad A_{ID}, A_1, A_2, A_3 \\
&\quad e(A_{ID}, A_3)^{x_{i}^{-1}\gamma^{-1}} = e(Q_v, Q_v) \\
&\quad \text{Using } e(Q_v, Q_v), \text{ add } Q_v \text{ to the Revocation List}
\end{align*}
\]
Hybrid anonymous message broadcast

Security analysis

ProVerif

- Applied Pi Calculus
- ProVerif 2.02pl1: For automatic evaluation of cryptographic protocols.
- The Pi Calculus is designed for representing concurrent processes that interact using communications channels such as the Internet.
- Any number of protocols executed.

Model:
- Dolev-Yao model: read, modify, delete, and inject messages

Assumptions:
- TA, RSU are trusted and the parties will not release their secret keys

Andrea Huszti, Szabolcs Kovács, Norbert Oláh

Hybrid anonymous message broadcast for VANETs
ProVerif events

---

**Setup Communication**

- **Event OBU_auth_start**
  - $(A1)$
  - $M_1 = \text{Enc}_{Q_v}(Q_v, A_1, t, sy_{Q_v})$

- **Event OBU_auth_RSU**
  - $(As1)$

- **Event RSU_auth_start**
  - $(tx_{iQ_v})$

---

**Incident Report**

- **Event OBU_mess_auth_start**
  - $(A1, A_2, bMT)$
  - $A_{ID}, A_1, A_2, A_3, bP, M, T$

- **Event OBU_mess_auth_end**
  - $(AC1, AC3, MC2)$
Security analysis I.

- Secrecy of authorized ID and authorized secret key:
  \[\text{query attacker:xiQv}\]
  \[\text{query attacker:xi} \gamma QV.\]

- Mutual authentication, Authenticity and data integrity of messages:
  \[\text{query a1:nonce,a2:E, a3:nonce; inj-event(OBU\_auth\_end(a1))} \]
  \[\Rightarrow \]
  \[\text{(inj-event(OBU\_auth\_RSU(a2))} \Rightarrow \]
  \[\text{inj-event(OBU\_auth\_start(a3))).} \]
  \[\text{inj-event(RSU\_auth\_end(a4))} \Rightarrow \]
  \[\text{inj-event(RSU\_auth\_start(a5))).} \]
  \[\text{event(OBU\_mess\_auth\_end(a6))} \Rightarrow \]
  \[\text{event(OBU\_mess\_auth\_start(a7)).} \]
Security analysis II.

- **Sender anonymity and unlinkability of messages**
  Each report message a fresh, secret random value \( a \in \mathbb{Z}_q^* \) is generated, the pseudonyms and authorized pseudonyms are different and not linkable.

- **Anonymity revocation and non-repudiation of malicious messages**
  \[ \hat{e}(A_3, A_{ID}) \text{ on the Anonymized User List?} \]
  \[ \hat{e}(A_{ID}, A_3)^{-1} \gamma^{-1} = \hat{e}(Q_V, Q_V) \]
  *Using* \( \hat{e}(Q_V, Q_V) \), *add* \( Q_V \) *to the Revocation List.*
Implementation

- Selected programming language (Python and MicroPython).
- We used a standard curve for the implementation and implemented all the necessary operations.
- We used projective coordinates to perform operations to improve performance.
Prototype

- To demonstrate the effectiveness of the implementation, we compiled a simple prototype using constrained devices.

- Communication takes place over a local 2.4 GHz Wi-Fi network.


**Result**

- **Areas of application:**
  - Autonomous or connected vehicles
  - Downtown or extra-urban traffic

<table>
<thead>
<tr>
<th>Source/Activity</th>
<th>PC</th>
<th>RasPi 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication setup - Authorized ID request (OBU)</td>
<td>0.0199 s</td>
<td>0.1453 s</td>
</tr>
<tr>
<td>Communication setup - User authentication (RSU)</td>
<td>0.0297 s</td>
<td>0.1949 s</td>
</tr>
<tr>
<td>Communication setup - Authorized ID confirmation (OBU)</td>
<td>0.0179 s</td>
<td>0.1333 s</td>
</tr>
<tr>
<td>Incident report - send</td>
<td>0.0086 s</td>
<td>0.0593 s</td>
</tr>
<tr>
<td>Incident report - receive</td>
<td>0.0281 s</td>
<td>0.2076 s</td>
</tr>
</tbody>
</table>

**Table:** Computational time
References

D. He, S. Zeadally, B. Xu, and X. Huang. 
An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. 

A privacy-preserving trust model based on blockchain for vanets. 

Ádám Vécsi, Attila Bagossy, and Attila Pethő. 
Cross-platform identity-based cryptography using webassembly. 
This work was supported by the SETIT Project (no. 2018-1.2.1-NKP-2018-00004), which has been implemented with support provided by the National Research, Development and Innovation Fund of Hungary, financed under the 2018-1.2.1-NKP funding scheme. Project no. TKP2020-NKA-04 has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the 2020-4.1.1-TKP2020 funding scheme.
Thank you for your attention!
Future plans

- Provable security analysis
- Blockchain
  - Public parameters
  - Revocation List