Hybrid anonymous message broadcast for VANETs

Andrea Huszti, Szabolcs Kovács, Norbert Oláh

University of Debrecen

October 11, 2021

Content

Motivation

- Rapid increase in the number of cars
- Increasing the level of security
- Apply in the world of IoT

Vehicular Ad-Hoc Networks - VANET

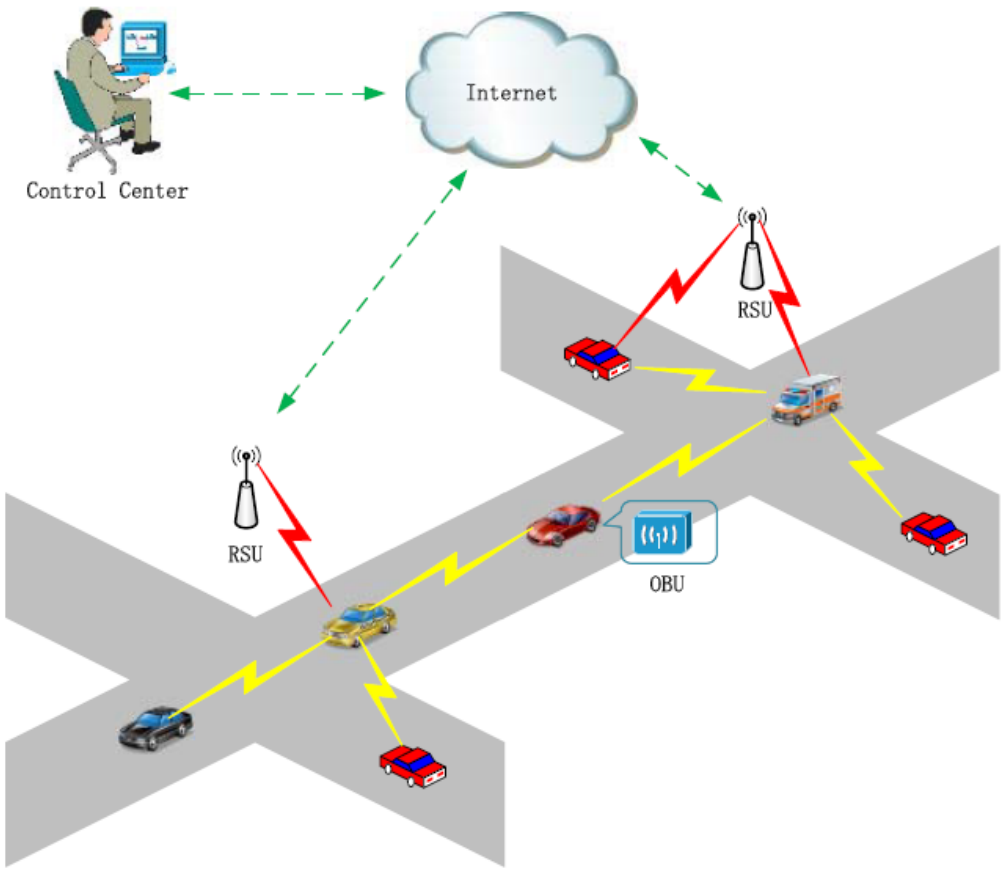


Figure: Vehicular Ad-Hoc network

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.
- Z. Lu–W. Liu–Q. Wang–G. Qu–Z. Liu: A privacy-preserving trust model based on blockchain for vanets. IEEE Access, 6. évf. (2018), 45655–45664. p.

Bilinear pairing

Definition:Let G_1 and G_2 be two groups of order q for some large p. A map $\hat{e} : G_1 x G_1 \rightarrow G2$ is an admissible bilinear map if 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 $P, Q \in G_1$

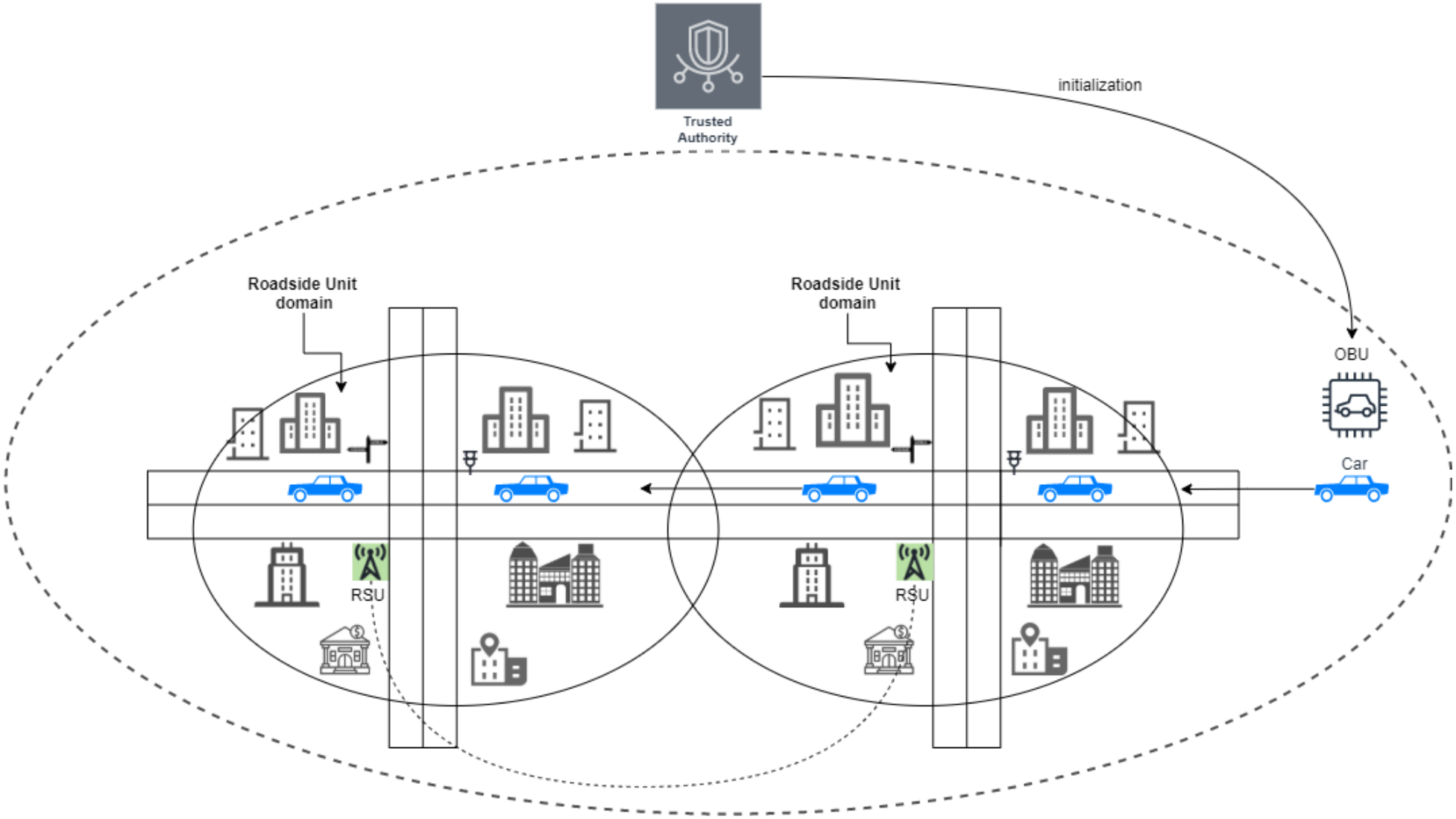
Application of bilinear pairing

- D. He–S. Zeadally–B. Xu–X. Huang: An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Transactions on Information Forensics and Security,10. évf. (2015) 12.sz., 2681–2691.p.
  - 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

Protocol


Trusted Authority
initialization
Roadside Unit domain
Roadside Unit domain
OBU
Car
RSU
RSU

Initialize

Initialization		
OBU (V)	TA:$P, \gamma P$	RSU (R)
$Q_V = H(ID_V \| T)$	$\rightarrow$Long-lived public key	$Q_R = H(ID_R \| T)$
γQ_V	$\rightarrow$Long-lived secret key	γQ_R

Communication setup

Communication Setup

OBU (V)		RSU (R)
		$x_i \rightarrow$local secret key
$t, s \in \mathbb{Z}_q^*$ random		$x_i Q_R \rightarrow$ public key
$A_1 = \hat{e}(\gamma Q_V, Q_R)$		$Sign_{\gamma Q_R}(x_i Q_R)$
$M_1 = Enc_{Q_R}(Q_V, A_1, t, s\gamma Q_V)$		
Check Q_R on Rev. List	$\xrightarrow{M_1}$	
		Decrypt: $Dec_{\gamma Q_R}(M_1)$
		Q_V on the Rev. List?
		$A_1 \stackrel{?}{=} \hat{e}(Q_V, \gamma Q_R)$
		Anonymized User List:
		$\hat{e}(x_i Q_V, Q_V)$
	$\xleftarrow{tx_iQ_V, x_i s\gamma Q_V}$	TA: $\hat{e}(x_i Q_V, Q_V)^\gamma$
$x_i s\gamma Q_V \cdot s^{-1}, tx_i Q_V \cdot t^{-1}$		
$\hat{e}(x_i Q_V, Q_R) \stackrel{?}{=} \hat{e}(Q_V, x_i Q_R)$		
$\hat{e}(x_i \gamma Q_V, Q_R) \stackrel{?}{=} \hat{e}(\gamma Q_V, x_i Q_R)$		
$x_i Q_V, x_i \gamma Q_V$		

Incident report

Incident report

OBU (V)		RSU (R)
$a \in \mathbb{Z}_q^*$ random		
$b \in \mathbb{Z}_q^*$ random		
$A_{ID} = aQ_V$		
$A_1 = ax_i Q_V$		
$A_2 = bH(M\|\|T) + a\gamma Q_V$		
$A_3 = a^{-1} x_i \gamma Q_V$		
	$\xrightarrow{A_{ID}, A_1, A_2, A_3, bP, M, T}$	
		Check: T
		Check: $\hat{e}(A_{ID}, x_i Q_R) \stackrel{?}{=} \hat{e}(A_1, Q_R)$
		Check: $\hat{e}(A_2, P) \stackrel{?}{=} \hat{e}(A_{ID}, \gamma P)\hat{e}(H(M\|\|T), bP)$
		Check: $\hat{e}(A_3, A_{ID})$ on the Anonymized User List?

Malicious user management

Malicious user management

OBU (V)		RSU x_i TA γ
A_{ID}, A_1, A_2, A_3		
	$\xrightarrow{A_{ID}, A_1, A_2, A_3}$	
		$\hat{e}(A_{ID}, A_3)^{x_i^{-1}\gamma^{-1}} = \hat{e}(Q_v, Q_v)$
		Using $\hat{e}(Q_V, Q_V)$, add Q_V to the Revocation List

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

ProVerif events

OBU		RSU
	Setup Communication	
Event OBU_auth_start $(A1)$		
	$\xrightarrow{M_1 = Enc_{Q_R}(Q_V, A_1, t, s\gamma Q_V)}$	
		Event OBU_auth_RSU $(As1)$ Event RSU_auth_start $(txiQv)$
	$\xleftarrow{tx_iQ_V, x_is\gamma Q_V}$	
Event RSU_auth_end Event OBU_auth_end $(xiQv)$		
	Incident Report	
Event OBU_mess_auth_start $(A1, A2_1, bMT)$		
	$\xrightarrow{A_{ID}, A_1, A_2, A_3, bP, M, T}$	
		Event OBU_mess_auth_end $(AC1, AC3, MC2)$

Security analysis I.

- Secrecy of authorized ID and authorized secret key:
  query attacker:xiQv
  query attacker:xiγQV.
- Mutual authentication, Authenticity and data integrity of messages:
  query a1:nonce,a2:E, a3:nonce; inj-event(OBU_auth_end(a1))
  ==>
  (inj-event(OBU_auth_RSU(a2)) ==>
  inj-event(OBU_auth_start(a3))).
  inj-event(RSU_auth_end(a4)) ==>
  inj-event(RSU_auth_start(a5)).
  event(OBU_mess_auth_end(a6)) ==>
  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
  Check: $\hat{e}(A_3, A_{ID})$ *on the Anonymized User List?*
  $\hat{e}(A_{ID}, A_3)^{x_i^{-1}\gamma^{-1}} = \hat{e}(Q_v, Q_v)$
  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

	PC	RasPi 4
Communication setup - Authorized ID request (OBU)	0.0199 s	0.1453 s
Communication setup - User authentication (RSU)	0.0297 s	0.1949 s
Communication setup - Authorized ID confirmation (OBU)	0.0179 s	0.1333 s
Incident report - send	0.0086 s	0.0593 s
Incident report - receive	0.0281 s	0.2076 s

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.
IEEE Transactions on Information Forensics and Security, 10(12):2681–2691, 2015.

Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu.
A privacy-preserving trust model based on blockchain for vanets.
IEEE Access, 6:45655–45664, 2018.

Ádám Vécsi, Attila Bagossy, and Attila Pethő.
Cross-platform identity-based cryptography using webassembly.
Infocommunications (SETIT Project), 2019.

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, financedunder 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