Short-term Linkable Group Signatures with Categorized Batch Verification

Lukas Malina[1], Jordi Castella-Rocà[2], Arnau Vives-Guasch[2], Jan Hajny[1]

[1]Department of Telecommunications
Faculty of Electrical Engineering and Communication
Brno University of Technology
Czech Republic

[2]Department of Computer Engineering and Mathematics
Universitat Rovira i Virgili
Catalonia (Spain)

Outline

Scope

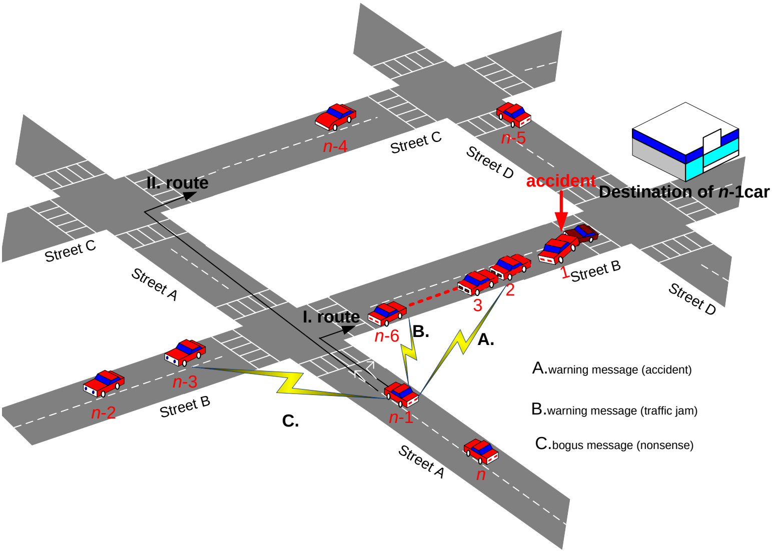
In ad hoc wireless networks like Vehicular ad hoc Network (VANETs) or Wireless Sensor Networks (WSN), data confidentiality is usually a minor requirement contrary to **data authenticity** and **integrity**.

Messages broadcasted from a node to other nodes should be authentic but also keep **user's privacy** in plenty scenarios working with personal data.

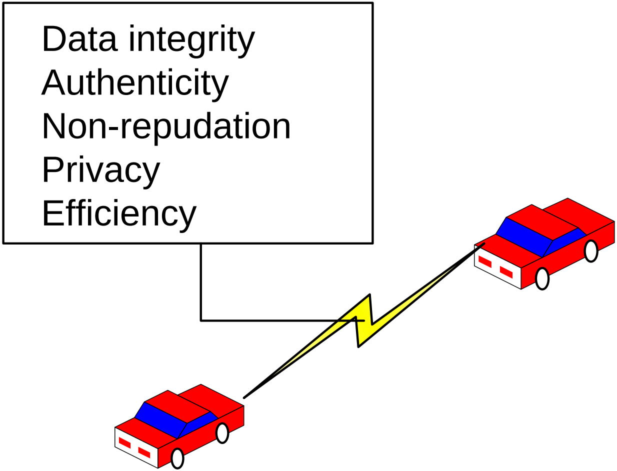
$$\Downarrow$$

Appropriate schemes: **Group Signatures** (GS).

Scenario


II. route
n-4
Street C
n-5
Street D
accident
Destination of n-1car
Street C
Street A
I. route
n-6
B.
3
2
1
Street B
Street D
A.
n-3
n-2
Street B
C.
n-1
Street A
n
A.warning message (accident)
B.warning message (traffic jam)
C.bogus message (nonsense)

Security Requirements in VANETs



The current solutions have practical drawbacks:

- Expensive tamper-proof hardwares.
- Computation bottlenecks of the verification and revocation phases.
- Complicated certificate distribution/revocation.
- Omitting important properties like a short-term linkability demanded in several applications, e.g. change lanes of vehicles in VANET.

Requirements and Cryptographic Background

- Security properties of our solution:
  - Non-repudiation, message integrity and authenticity,
  - user privacy (revocable anonymity),
  - traceability.
- Used cryptography:
  - **ECDSA** signature scheme,
  - probabilistic **ElGamal** encryption,
  - **group signatures** based on q-SDH problem and Decision Linear problem (**BBS04** scheme [1]).

Pairing-based Group Signatures

We employ **Group Signatures** (GS) based on the **BBS04** scheme [1].

General properties:

- Message integrity, authenticity and non-repudiation,
- anonymity,
- unlinkability,
- traceability.

Pros of GS:

- Only 1 public key (suitable for VANETs, WSN, WBSN ...),
- shorter security overhead than solutions using certificates,
- providing user **privacy**.

Cons of GS:

- Expensive due to pairing operations,
- growing a revocation list,
- vulnerability against several attacks, e.g. Denial of Services (DoS).

How to Reduce the Drawbacks of GS?

Expensive due to pairing operations.

- Minimize the number of pairings in verification due to a **batch verification**.
- Reduce pairings in signing.
- Redesign scheme.

Growing a revocation list.

- Use time restrictions of pseudonyms.
- Recompute the secret keys.

Vulnerability against several attacks.

- Check the hashes of signatures.
- Apply the time stamps (against replay attack).
- Sort out the potential honest/bogus messages due to a **short-linkability** and **categorized verification**.

Advanced Properties of Our Solution

Short-linkability:

- more efficient signing (reducing the pairing operations),
- possible sorting of the messages,
- no harming the privacy in long term (long-term unlinkability).

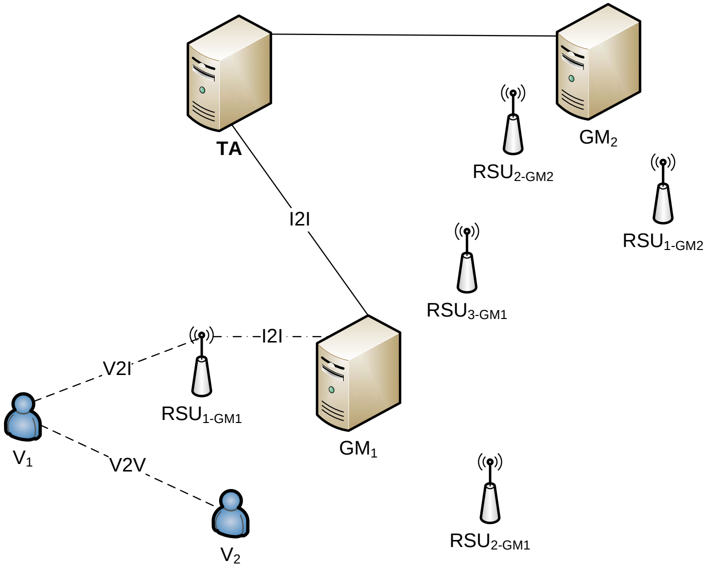
Categorized Batch Verification:

- sorts out potentially honest and bogus messages due to linkability,
- less errors in the 1. batch $\rightarrow$ O(1),
- robust against the Sybil and Denial of Services attacks.

The Parties in Our Model

- Trusted Authority **TA**:
  - Issues certified pseudonyms,
  - generates cryptographic parameters,
  - reveals ID of a user.
- Group Manager **GM**:
  - Generates group member secret keys,
  - traces and opens malicious message.
- User **V**:
  - A driver with the certified pseudonym,
  - uses devices with VANET applications,
  - signs, sends and verifies messages.

Communication Pattern



Our Scheme

- Setup **Set**$(0,1)^l \rightarrow$ *parameters*
  - establishing cryptographic *parameters*,
  - setting keys of TA and GMs.
- Registration **Reg**$(ID_{Vi}) \rightarrow \pi_{Vi}$
  - a driver V_i is authenticated by TA (ECDSA, ElGamal),
  - TA issues pseudonym π_{V_i} to V_i.
- Join **Join**$(\pi_{Vi}) \rightarrow gsk_{Vi}$
  - V_i with π_{V_i} is anonymously authenticated by GM_i (ECDSA, ElGamal),
  - V_i obtains a group member secret key gsk_{V_i} from the GM_i.

Our Scheme

- Signing **Sig**$(M, gsk_{V_i}, gpk) \rightarrow \sigma$
  - using the modified group signature scheme (BBS04 [1]),
  - V_i signs M and outputs a group signature σ.
- Verification **Ver**$(M, gpk, \sigma) \rightarrow$ valid/invalid
  - sorting the signed messages to 3 levels of credibility,
  - batch verification of group signatures.
- Trace **Trace**$(M, \sigma, gmsk) \rightarrow gsk_{V_i}, \pi_{Vi}$
  - bogus signatures can be opened by GM_i,
  - GM_i reveals the part of pseudonym π_{Vi} from database.
- Revocation **Rev**$(\pi_{Vi}) \rightarrow ID_{V_i}$
  - the cooperation of GM_i and TA,
  - TA reveals ID_{V_i} from π_{Vi}.

The Performance Evaluation - Signing

In **Signing**, **pairing operations** are reduced 3 $\Rightarrow$ **0**, exponentiations 10 $\Rightarrow$ 9 and multiplication 14 $\Rightarrow$ 9.

V2V scheme:	Our scheme	WLZ [4]	GSIS [3] & Zhang et al. [5] & Ferrara et al. [2]
Short-term linkability:	**yes**	no	no
The performance of Signing, excluding the first message			
Pairings	**0**	3	3
Exponentiation	**9**	10	12
Multiplication	**9**	14	12

The Performance Evaluation - Verification

In Categorized batch verification, **pairing operations** are reduced $5n \Rightarrow$ **2** (n - number of messages in one batch)

V2V scheme:	Our scheme & WLZ scheme[4]	GSIS [3]	Zhang et al. [5]	Ferrara et al. [2]
Batch:	yes	no	yes	yes
Length of signature:	$5G_1, G_T, 5Z_p$ (2380 bits)	$3G_1, 6Z_p$ (1500 bits)	$7G_1, G_T, 5Z_p$ (2570 bits)	$3G_1, G_T, 6Z_p$ (2032 bits)
Performance of batch verification				
Pairings	**2**	5n	2	2
Exponentiation	**11n**	12n	14n	13n
Multiplication	11n+1	**8n**	17n	10n+1
Performance of individual verification				
Pairings	5	5	5	5
Exponentiation	**10**	12	12	12
Multiplication	9	8	8	8

Experimental Implementation

A proof of concept implementation in JAVA.

Properties:

- the Java Pairing Based Cryptography (jPBC) Library,
- MNT curves type D with the embedding degree $k = 6$, 171 b order curve,
- the implementation of signing, verification and batch verification.

-	Our scheme	BBS schemes
Signing	60 ms	160 ms
Single Verification	207 ms	224 ms
Verification of 10 messages	500 ms (batch)	2240 ms

Tested on machine: Intel(R) Xeon(R) CPU X3440 @ 2.53GHz, 4 GB Ram.

Conclusion

Contribution

- Practical and secure registration, join and revocation of members.
- Secure and anonymous inter-vehicle communication.
- Using short-term linkability $\longrightarrow$ more efficient performance in Signing.
- Categorized batch verification $\longrightarrow$ protection against DoS attacks in Verification.

Future work

- The investigation of categorized batch verification and short-term linkability in dense urban traffic.
- The determination of parameters.

Thank you for your attention.

References

D. Boneh, X. Boyen, and H. Shacham.
Short group signatures.
In *Proc. Adv. Cryptology-Crypto 04, ser. LNCS 3152*, pages 41–55. Springer-Verlag, 2004.

A. L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen.
Practical short signature batch verification.
In *Topics in Cryptology - The Cryptographers' Track at the RSA Conference*, volume 5473, pages 309–324. Springer, April 2009.

X. Lin, X. Sun, P. han Ho, and X. Shen.
Gsis: A secure and privacy preserving protocol for vehicular communications.
In *IEEE Transactions on Vehicular Technology*, volume 56, pages 3442–3456, 2007.

L. Wei, J. Liu, and T. Zhu.
On a group signature scheme supporting batch verification for vehicular networks.
In *International Conference on Multimedia Information Networking and Security*, pages 436–440, Los Alamitos, CA, USA, 2011. IEEE.

L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer.
A scalable robust authentication protocol for secure vehicular communications.
In *IEEE Transactions on Vehicular Technology 59(4)*, pages 1606–1617, 2010.