FastTrust: Fast and Anonymous Spatial-Temporal Trust for Connected Cars on Expressways

Chen Lyu[*+], Amit Pande, Yuanyuan Zhang[+], Dawu Gu[+], Prasant Mohapatra

[*]Shanghai University of Finance and Economics, Shanghai, China

[+]Shanghai Jiao Tong University, Shanghai, China

University of California, Davis, CA

Outline

- Introduction
- Our proposed FastTrust Mechanism
- Security Analysis
- Performance Evaluation
- Conclusion

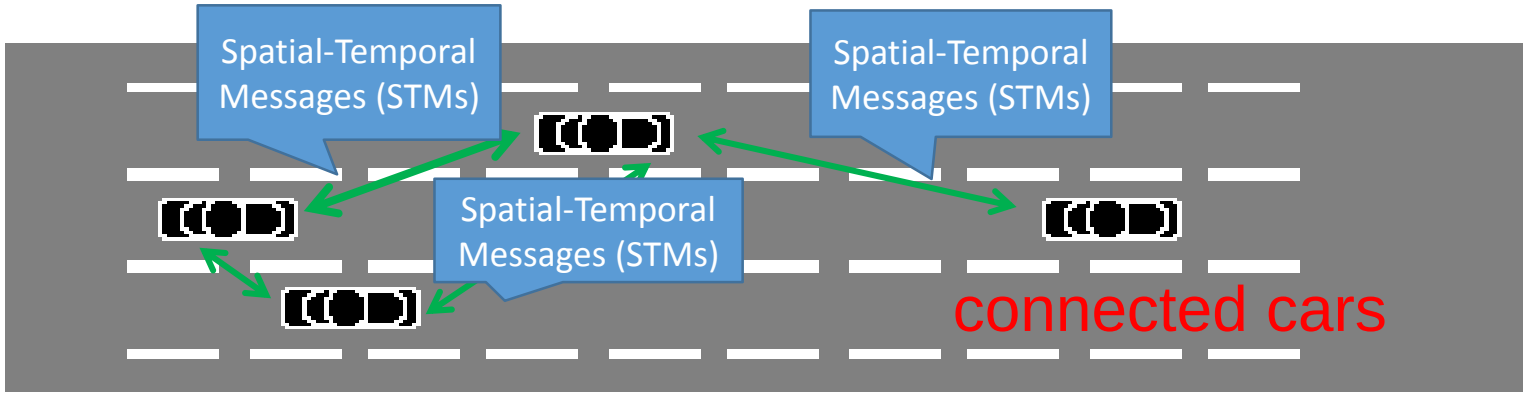
Outline

- Introduction
- Our proposed FastTrust Mechanism
- Security Analysis
- Performance Evaluation
- Conclusion

Motivation

- An increasing trend of connected cars or connected vehicles due to their potential in enhancing users' safety and convenience

- Two applications of connected cars :
  - Forward Collision Warning (FCW)
  - Intersection Collision Warning (ICW)



Motivation

- Security problem of frequent STMs (i.e., 10 Hz):
  - STMs may be broadcast by invalid cars or modified during connections-**broadcast authentication**
  - Frequently exchanging STMs among cars reveal a lot of personal information -**privacy preserving scheme**

- Broadcast authentication : IEEE 1609.2 security standard suggests using ECDSA algorithm
  - **Using ECDSA algorithm is vulnerable to signature flooding attack**
  - **a fast and low-cost broadcast authentication is mandatory for an STM-broadcast system**

- Privacy-preserving scheme:
  - **a solution to preserve cars' location privacy and anonymity**
  - **there is an inherent conflict between fast broadcast authentication and privacy.**

Objective

- In this work, we propose a Fast and Anonymous Spatial-Temporal Trust (FastTrust) mechanism, trying to address the problem of "**fast broadcast authentication with privacy**" for fast-moving cars.

- No additional third parties, i.e, infrastructures or cars, are required to be involved in our system.

- FastTrust provides security and privacy protection of STMs
  - **Fast verification**
  - **Non-repudiation**
  - **Packet loss resilience**
  - **Anonymity**
  - **Unlinkability**

Related Work

- **Efficient broadcast authentication**
  - Car-to-roadside connections (expensive public-key cryptographic ops)
    - Identity-based batch verification (Zhang et al., Huang et al.)
    - Aggregate signature (Jiang et al.)
  - Car-to-car connections (symmetric cryptographic ops)
    - TESLA authentication scheme: TESLA, VAST++ (Perrig et al., Studer et al.)
      - Delayed verification
    - One-time signature (Hsiao et al.)
      - Vulnerable to packet losses
- **Location privacy and anonymity**
  - Silence Periods, Pseudonyms and Group Signature

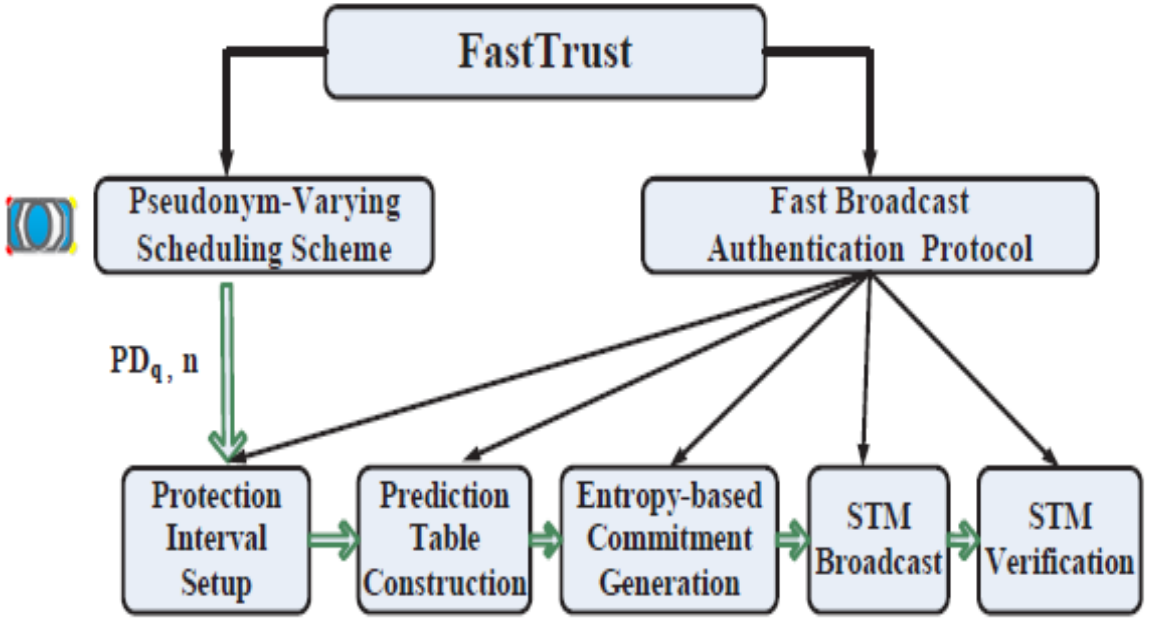
None of these solutions considered to achieve the two requirements during car-to-car connections.

Outline

- Introduction
- Our proposed FastTrust Mechanism
- Security Analysis
- Performance Evaluation
- Conclusion

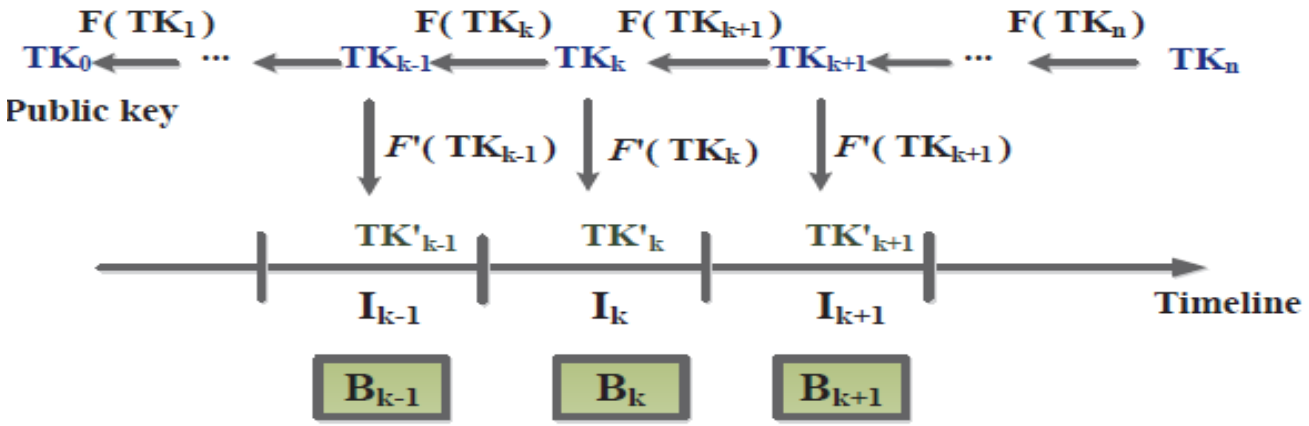
Protocol Overview

- Pseudonym-Varying Scheduling Scheme
- Fast Broadcast Authentication Protocol
  - Sender
    - *1. protection interval setup*
    - *2. prediction table construction*
    - *3. entropy-based commitment generation*
    - *4. STM broadcast*
  - Receiver
    - 5. STM verification



1. Protection Interval Setup

- Sender divides the timeline into a number of protection intervals
  - Each protection interval includes a sequence of STM events B_1, B_2,.., B_n
- Pseudonym (e.g., *PDq*) and the length of protection interval *n* are determined by our privacy-preserving scheme.
- **TESLA framework: generating n chained private keys for signing and a public verification key TK_0**

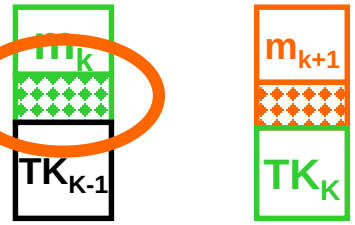


F: a one-way hash function

$TK_{k+1} = F(TK_k)$, k=0,1,…n-1

- **Keys disclosed one time intervals after use**
- **TESLA signature of m_K: MAC(TK_K, m_k)**

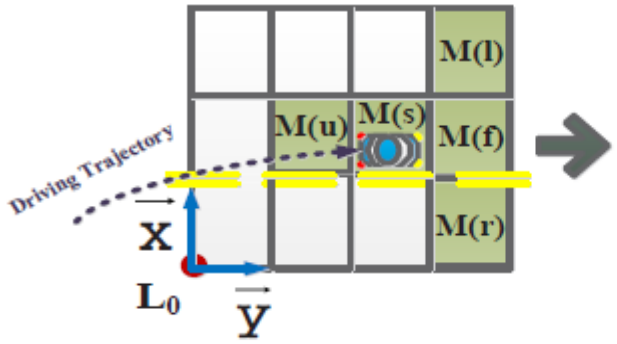
Verify TESLA sig.



Delayed Authentication?

2. Prediction Table Construction

- An STM's information except position is almost deterministic.
- Sender predicts its own movements
- Narrow down possible movements for efficiency
  - sender's speed limits
    - e.g., slower than 180km per hour->can not move >5m per 0.1s
  - sender's mode of movement
    - e.g., mostly go along the road rather than making a U-turn



Prediction Table W_k

Result	*Pr*
$M_k(f) = (1, 0)$	*0.40*
$M_k(l) = (1, 1)$	*0.25*
$M_k(r) = (1,-1)$	*0.20*
$M_k(s) = (0, 0)$	*0.10*
$M_k(u) = (-1,0)$	*0.05*

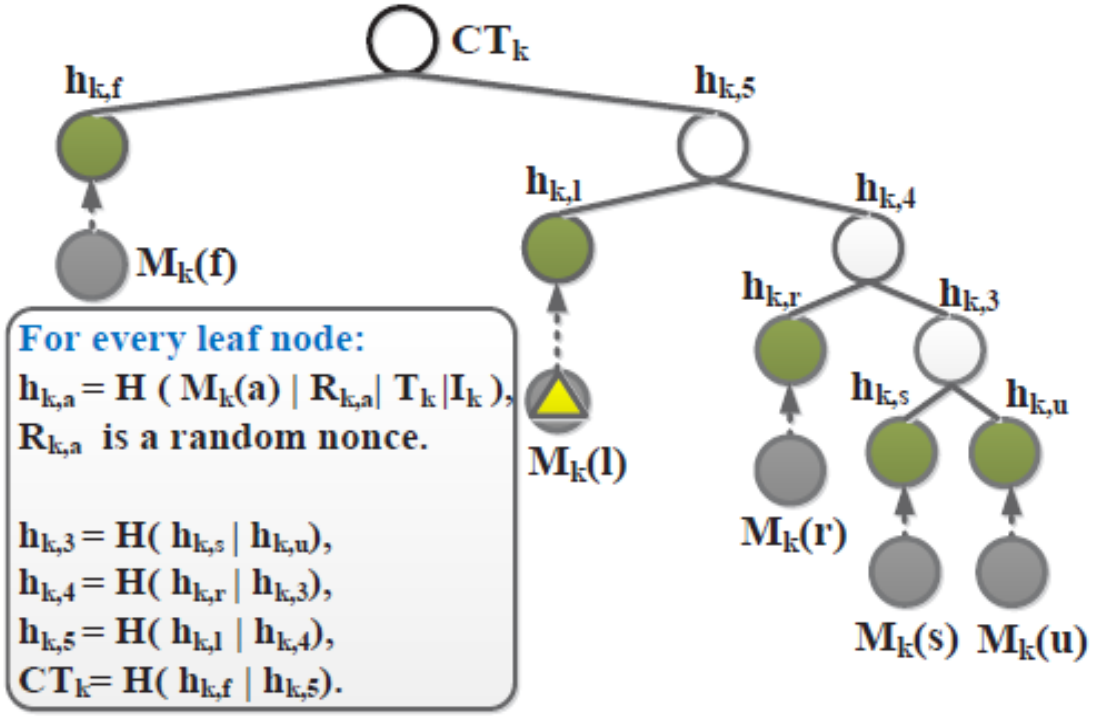
The entropy of two subsequent STMs is relatively low

3. Entropy-based Commitment Generation

CT_k: the commitment for all the possible results in Prediction Table with **Huffman Hash Trees(HHT)**

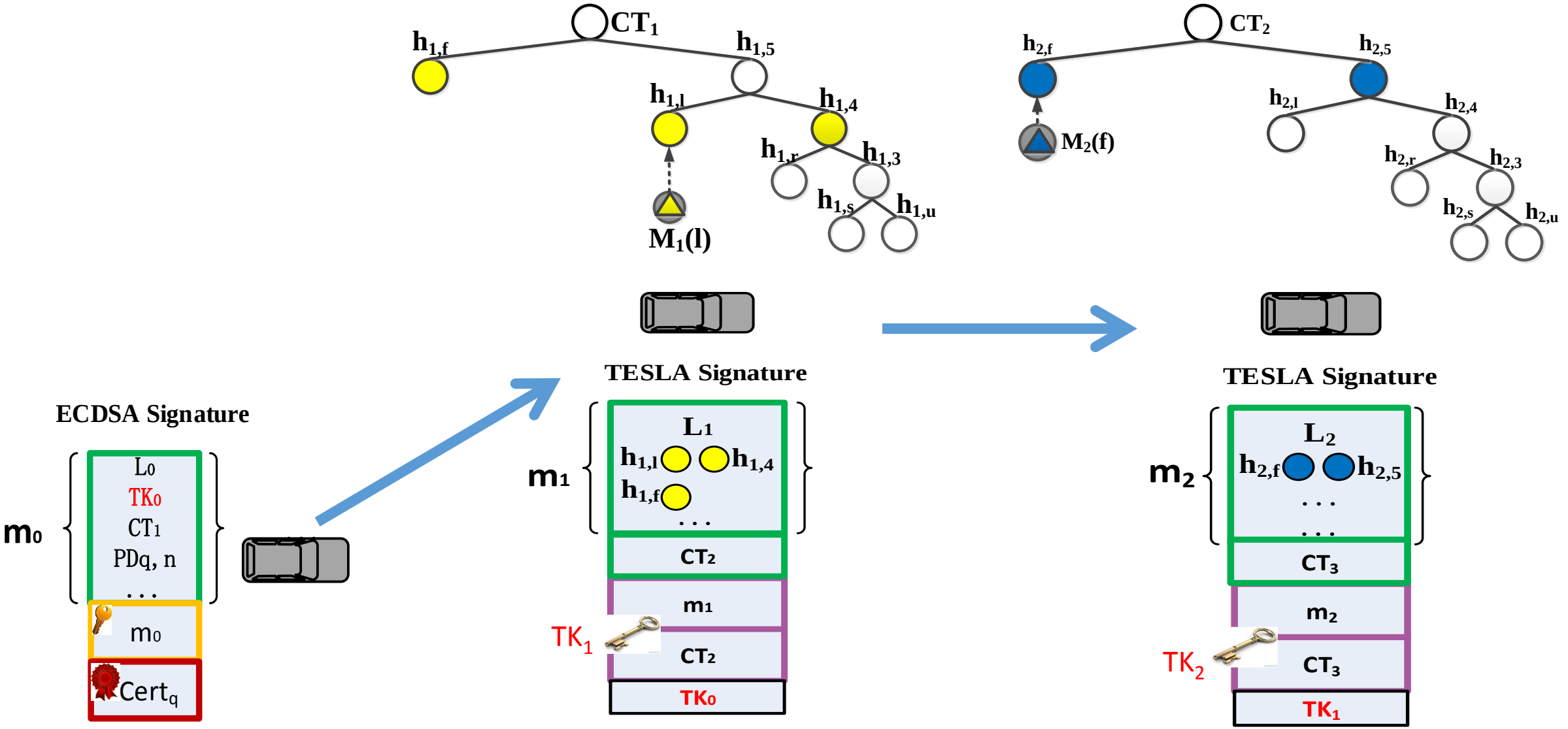
Prediction Table W_k

Result	*Pr*
$M_k(f) = (1, 0)$	*0.40*
$M_k(l) = (1, 1)$	*0.25*
$M_k(r) = (1,-1)$	*0.20*
$M_k(s) = (0, 0)$	*0.10*
$M_k(u) = (-1,0)$	*0.05*



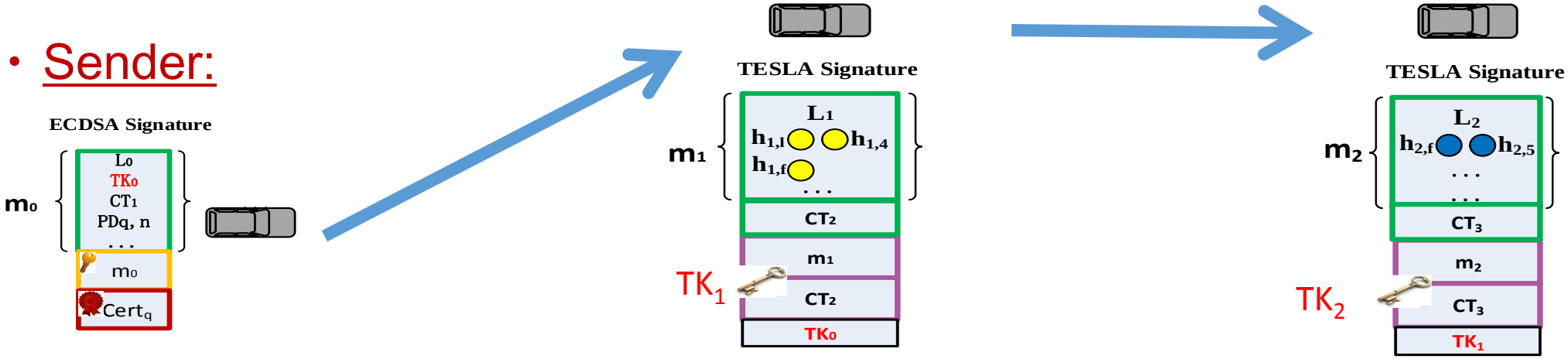
We construct the commitment to achieve instant verification!

4. STM broadcast



5. STM verification

- **Sender:**



- **Receiver:**

Check the Cert.

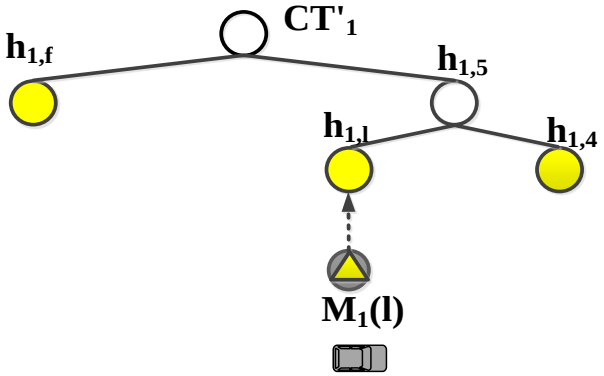
Verify ECDSA Sign.

Non-repudiation

Verify TK_0

Compute CT'_1, and verify if $CT_1 = CT'_1$

$L_1 = L_0 + M_1(l)$

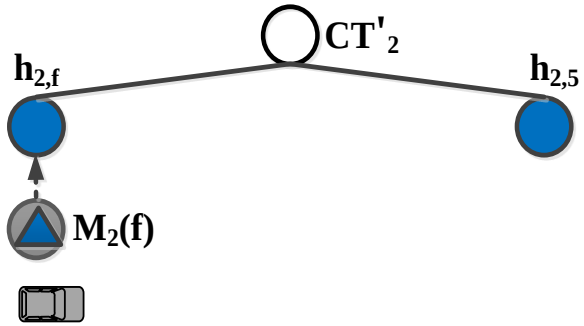


Verify if $TK_1 = F(TK_0)$

Verify TESLA Sign.

Compute CT'_2, and verify if $CT_2 = CT'_2$

$L_2 = L_1 + M_2(f)$



Pseudonym-Varying Scheduling Scheme

- Pseudonym
  - Pseudonyms are varied in the order of $PD_1, PD_2, \ldots, PD_z$ circularly.
  - Generating z distinct parameters for these pseudonyms, such that $\lambda = \sum_{q=0}^{z} \lambda_q$
  - For each pseudonym PD_q, a car determines the length of a protection interval n, which follows the **Poisson distribution** with λ_q
- Silent Period
  - The beginning time of a protection interval is delayed a silent period.

Outline

- Introduction
- Our proposed FastTrust Mechanism
- Security Analysis
- Performance Evaluation
- Conclusion

Security Analysis

- Proposition 1: FastTrust provides a negligible probability that a valid authenticated message could be forged by an attacker
- Proposition 2: A car cannot repudiate his own STM broadcast.
- Proposition 3: A car can verify STMs in presence of packet losses.
- Proposition 4: A car cannot obtain another car's real identity information.
- Proposition 5: A car cannot link multiple pseudonyms of another car used in different protection intervals.

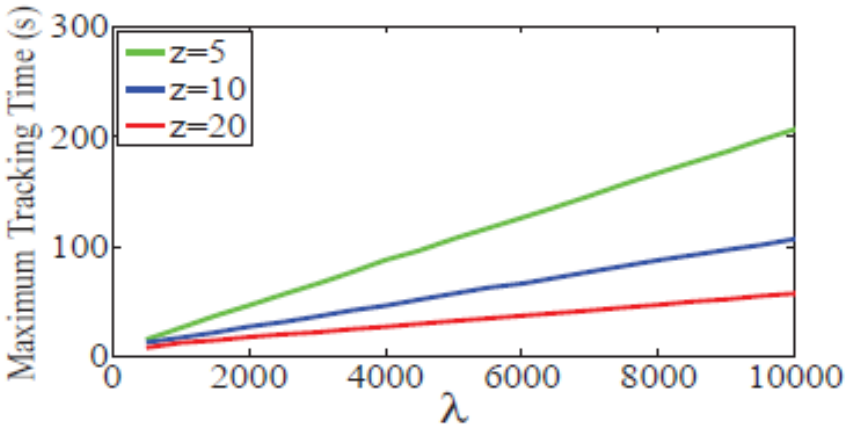
Outline

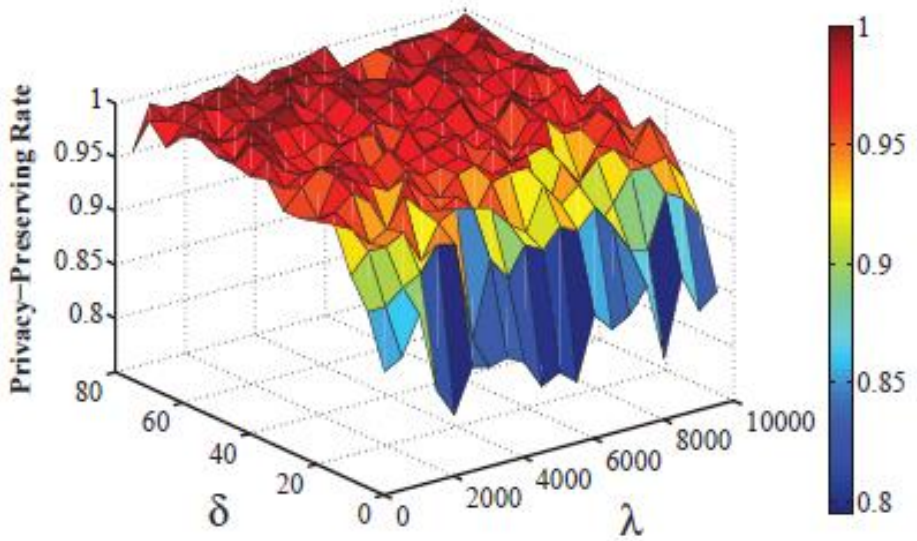
- Introduction
- Our proposed FastTrust Mechanism
- Security Analysis
- Performance Evaluation
- Conclusion

Privacy Evaluation

- Each car is equipped with z pairs of 256-bit public/private keys.
- We use a Poisson distribution with parameter λ to determine when we change these pseudonyms.

Parameter	Value
Poisson parameter λ	1000
Standard deviation δ	30
Number of pseudonyms z	10
Number of STM events	10000
Length of STM interval $\lvert I_B \rvert$	100 ms





Protocol Simulation

- In the simulation, 30 cars broadcast STMs every 100 ms

Parameter	Value	Parameter	Value
Hash, MAC operation	1 μs	Hash, MAC size	20 Bytes
ECDSA generation	7 ms	ECDSA verification	22 ms
ECDSA key size	32 Bytes	STM size	328 Bytes
STM's lifetime	1 s	Number of cars	30
Packet loss rate p	0.3		

- Communication Overhead

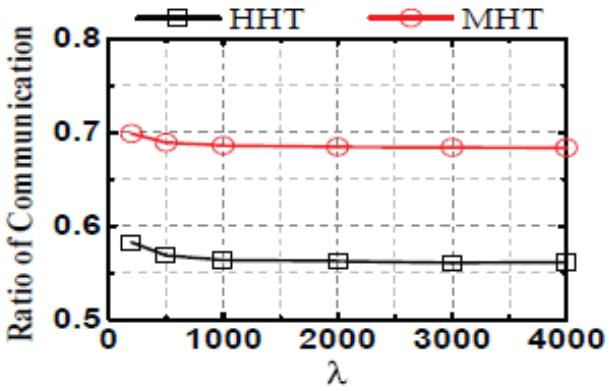


Fig. 10. The communication overhead of HHT and MHT compared to ECDSA.

Protocol Simulation

- Impact of Privacy:

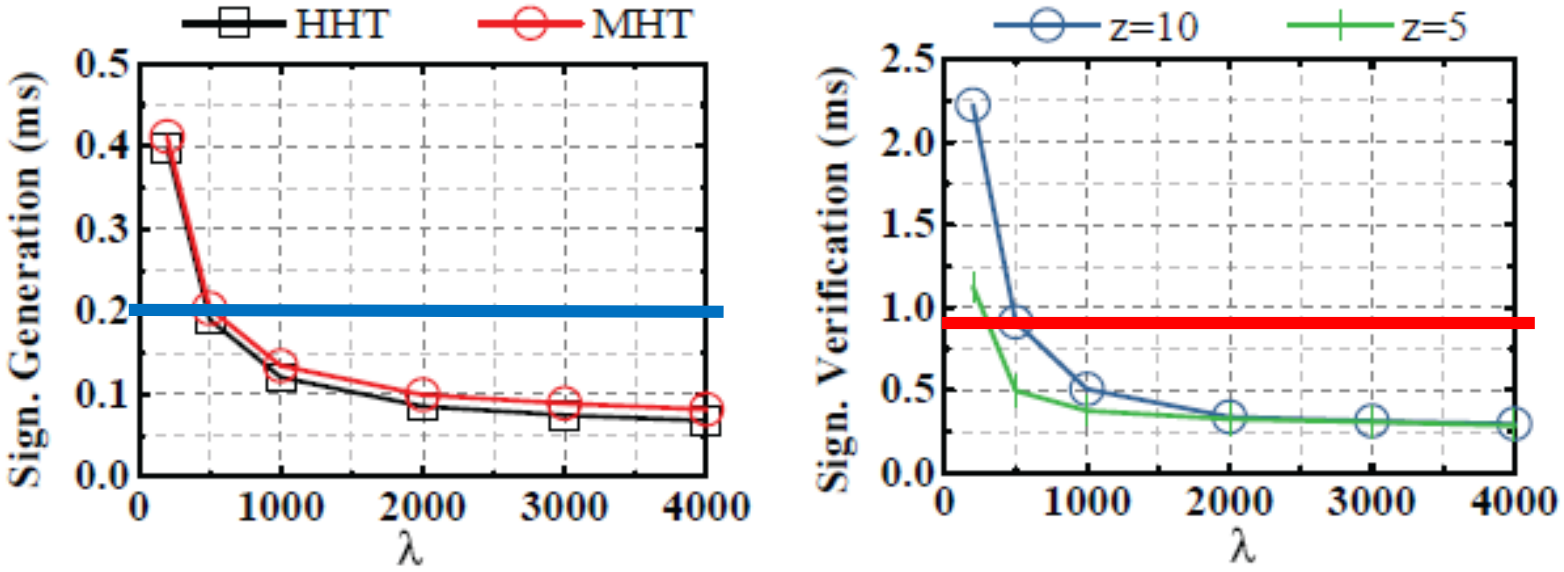


Fig. 11. Signature generation time and signature verification time with different privacy parameters.

Protocol Simulation

- Impact of Packet Loss:

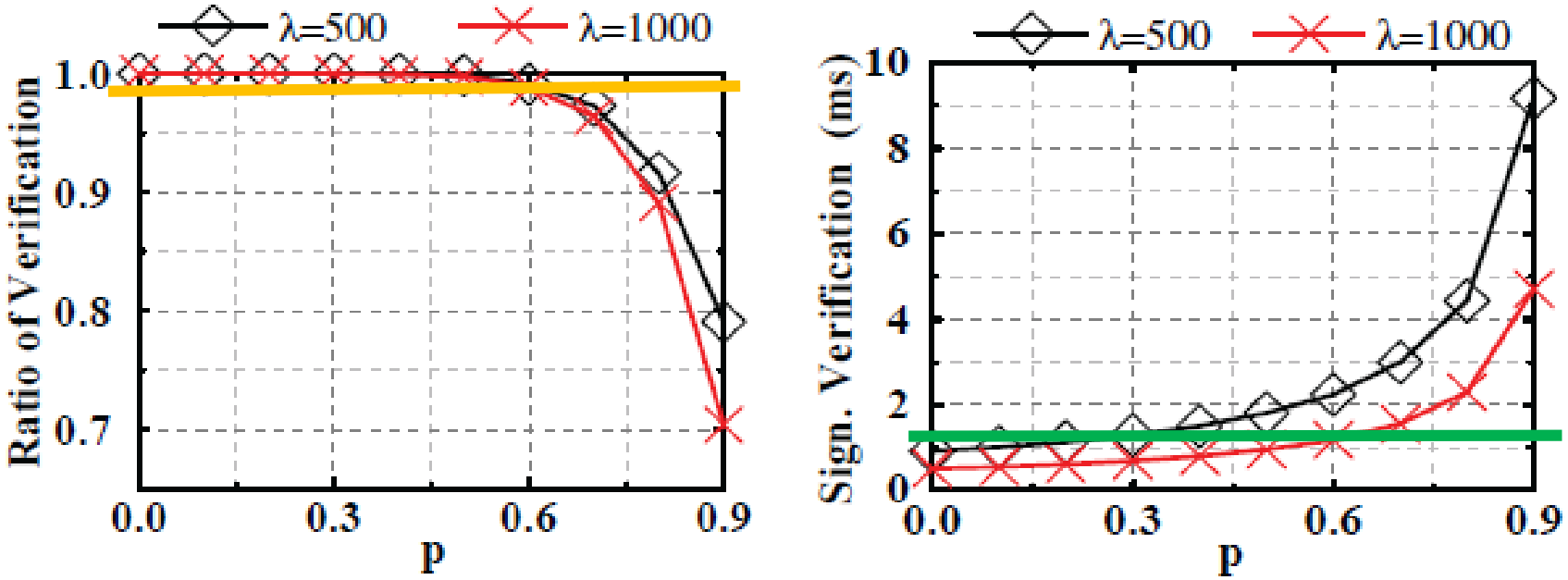
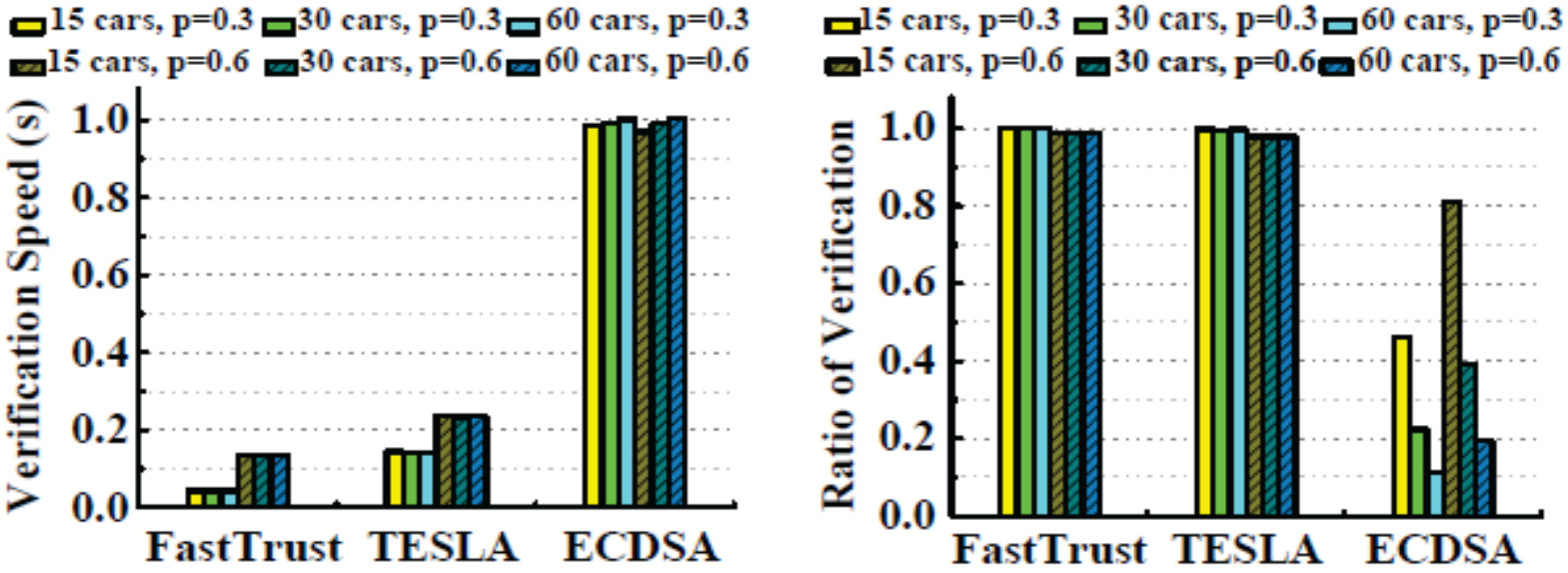


Fig. 12. Impact of packet losses on FastTrust.

Protocol Simulation

- We compare FastTrust with ECDSA and TESLA under different *p* and car density



(a) verification speed

(b) ratio of verification

Fig. 13. Performance comparison.

Outline

- Introduction
- Our proposed FastTrust Mechanism
- Security Analysis
- Performance Evaluation
- Conclusion

Conclusion

- In this work, we propose FastTrust to address the problem of "fast broadcast authentication with privacy".
- First, we design a fast broadcast authentication protocol based on symmetric key cryptography to mitigate signature flooding attack.
- To provide real-time and faster authentication, an entropy-based commitment is constructed with the structure of HHT in our protocol.
- We develop a pseudonym-varying scheduling scheme to protect users' privacy while also supporting fast broadcast authentication.
- Our simulation results indicate that FastTrust could achieve a high privacy preserving rate, and fast authenticate STMs with low computational and communication cost.

Thank you !

Email: lyu.chen@sufe.edu.cn