

A Robust Conditional Privacy-Preserving Authentication Protocol in VANET

Chae Duk Jung

Pukyong National University, Korea

CONTENTS

- I Vehicular Ad-hoc Network
- II ECPP & Universal Re-Enc.
- III System Model
- IV Proposed Protocol
- V Discussion
- VI Conclusion

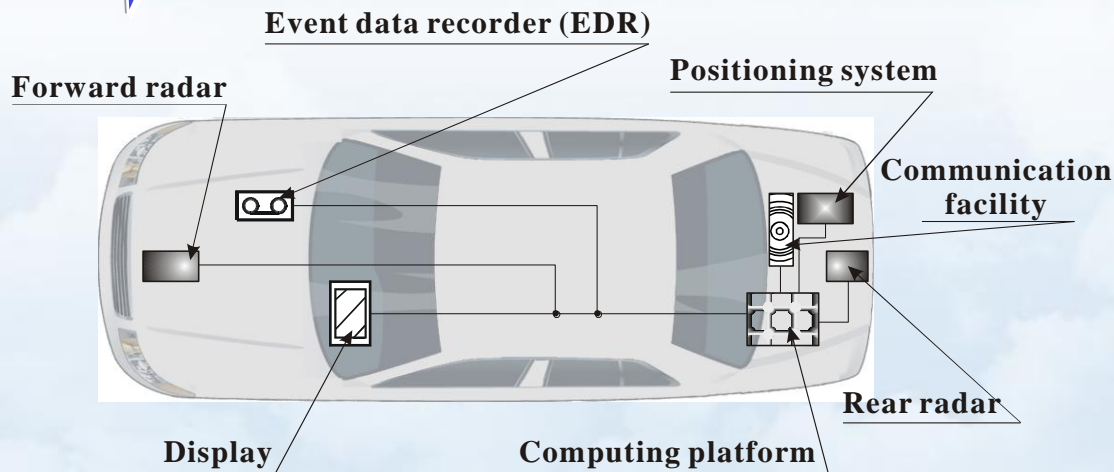
Vehicular Ad-hoc Network

Change of road vehicles

- ❑ Plummeting costs of electronic components
- ❑ Increase of users requiring road safety



Vehicle has become computer networks form



Vehicular Networks are likely to become the most relevant form of mobile ad hoc networks.

Vehicular Ad-hoc Network

Necessity of VANET



Most of these problems can be solved by providing appropriate *information* to the driver or to the vehicle

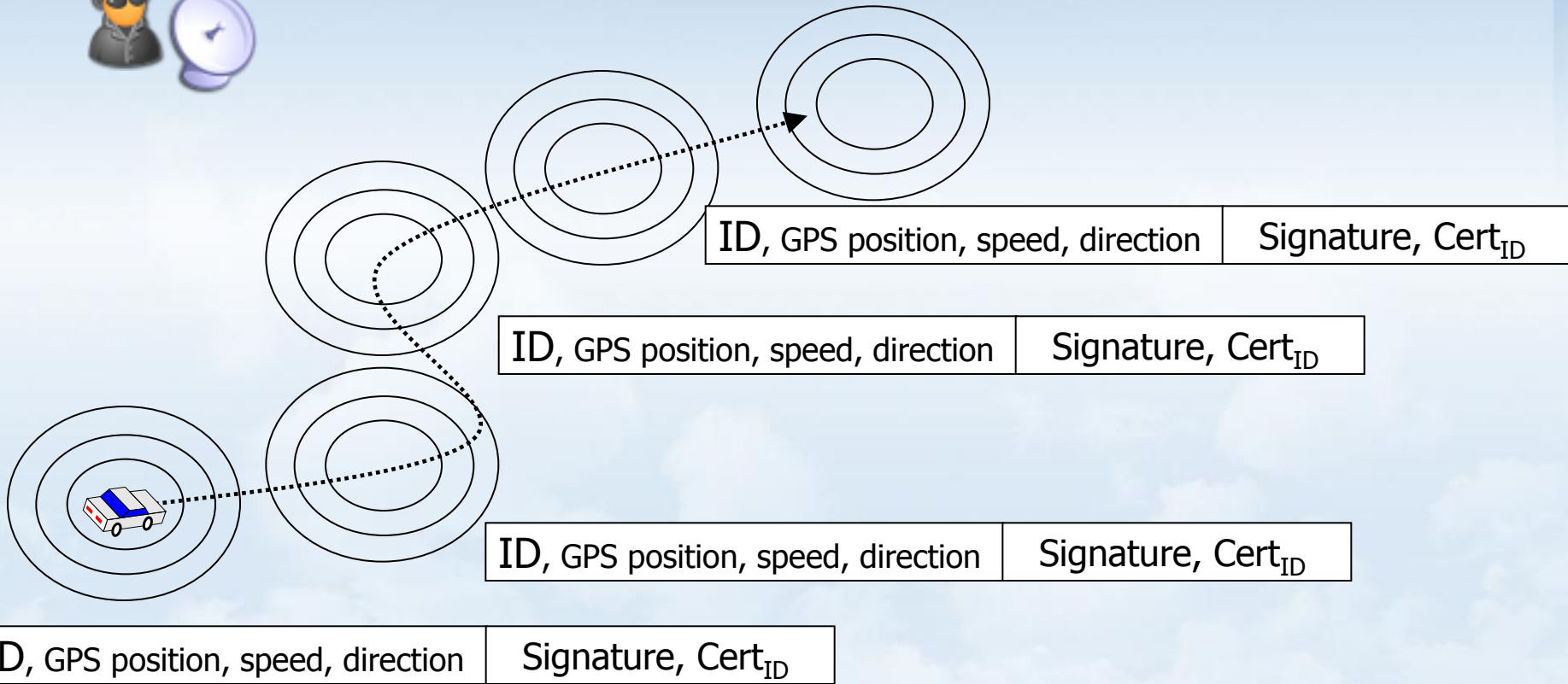
Security Requirement

Conditional Privacy-Preserving Authentication



Vehicular Ad-hoc Network

Movement tracking

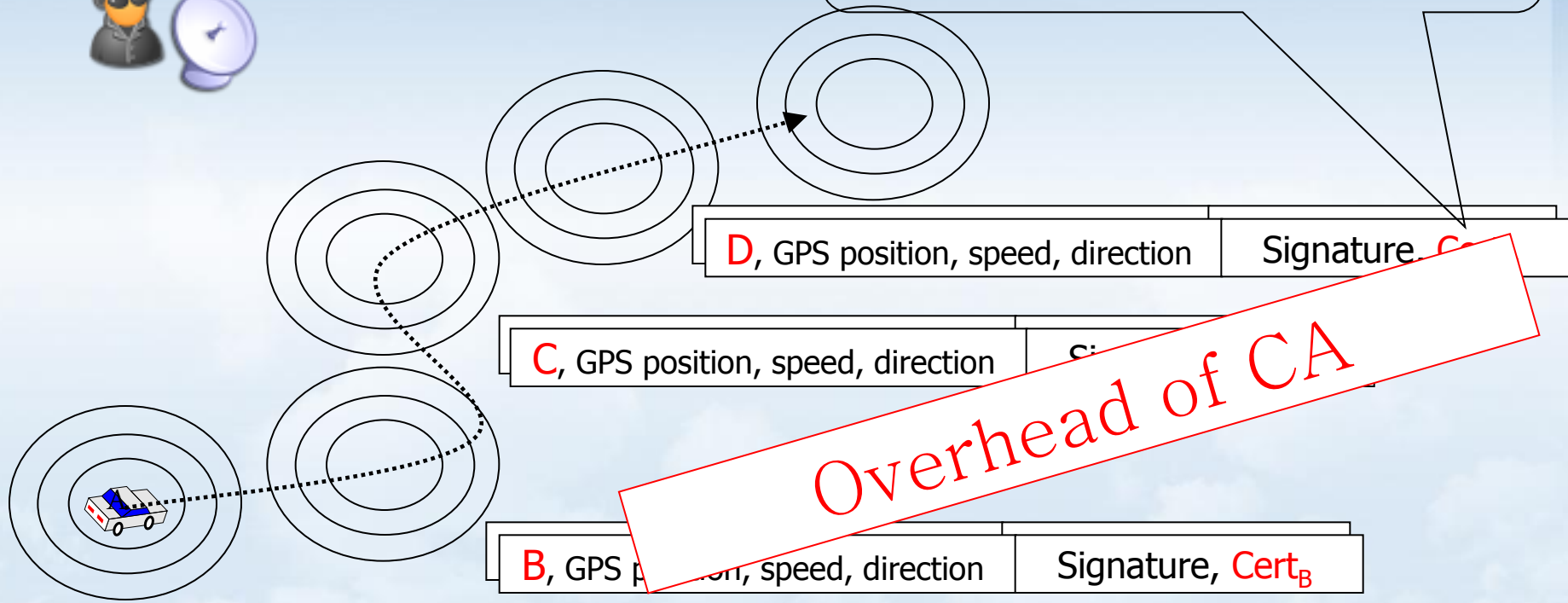


Vehicular Ad-hoc Network

Countermeasure



1 certificate/min * 2 hours * 365 days
= 43,800 certificate/year



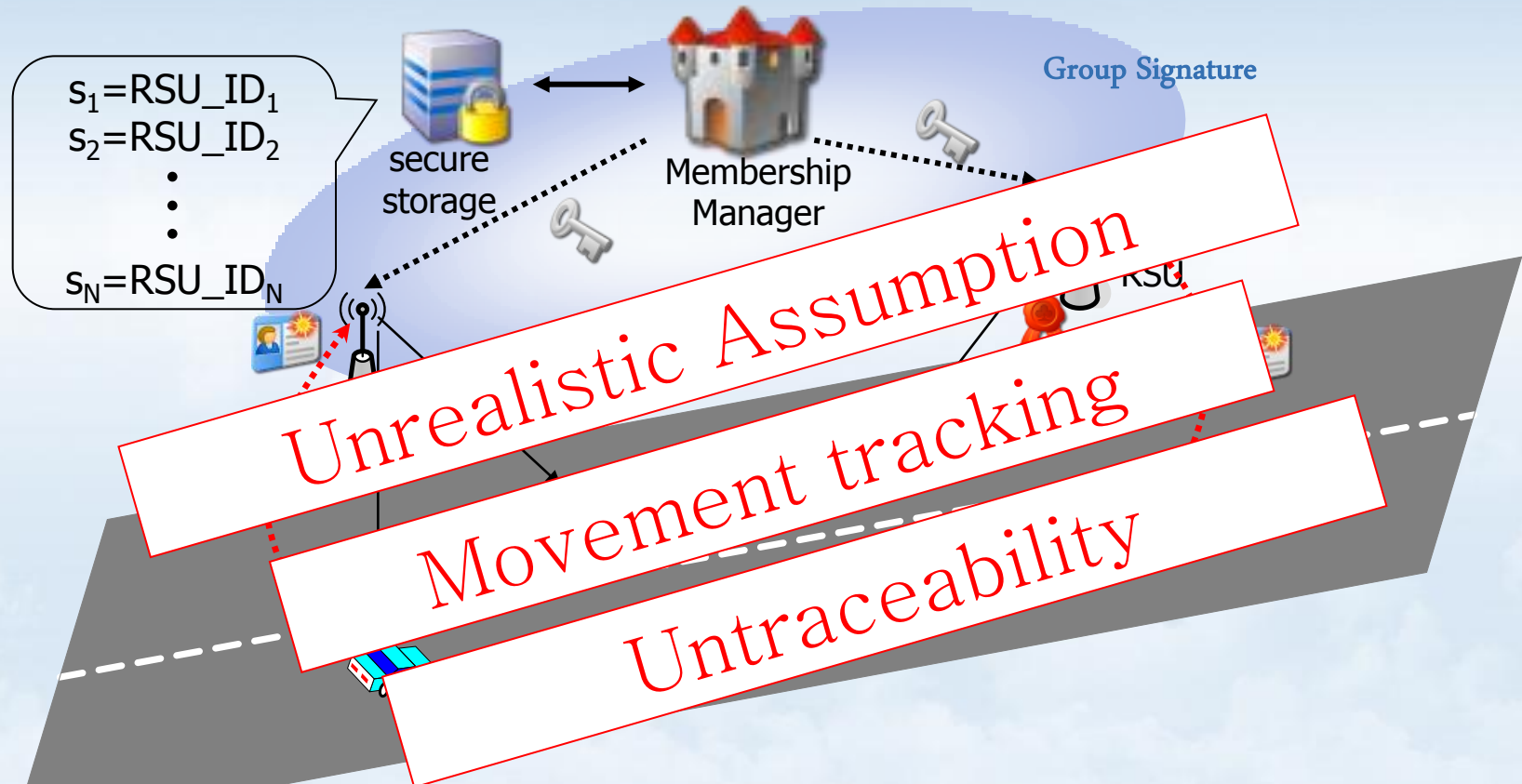
A, GPS position, speed, direction | Signature, Cert_A

Pseudonym

Pseudonym Certificate

ECPP

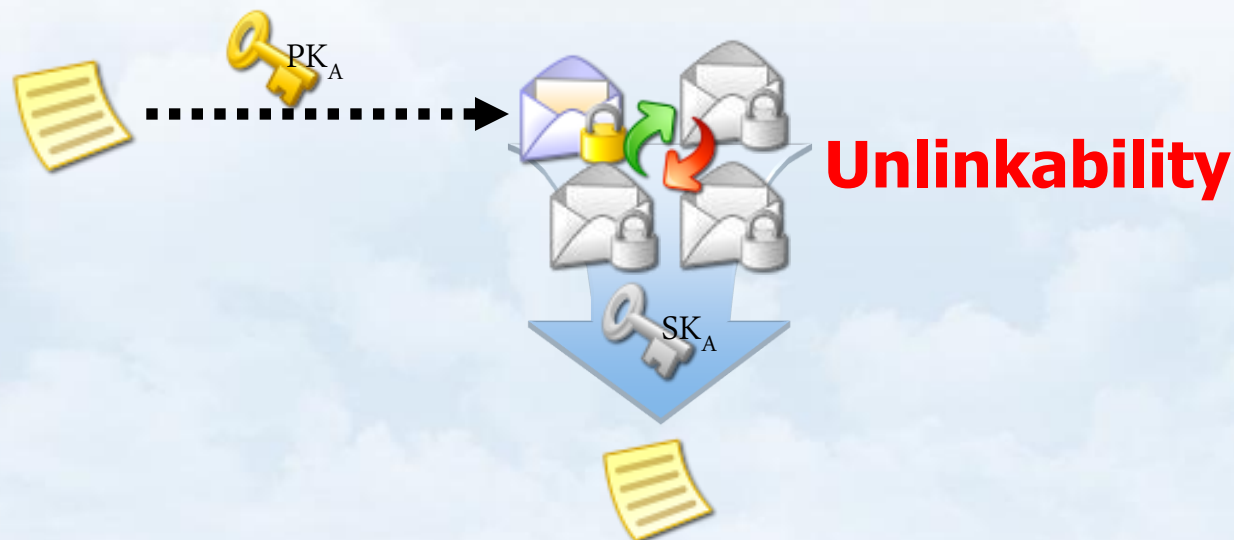
- Lu. *et al.*, IEEE INFOCOM 2008
 - Efficient Conditional Privacy Preservation Protocol



Universal Re-encryption

Universal Re-encryption

- Golle *et al.*, CT-RSA 2004
 - based on ElGamal encryption scheme
- lead to new types of functionality in mixnet architectures
 - hide information permitting traffic-analysis



System Model

Design Principles

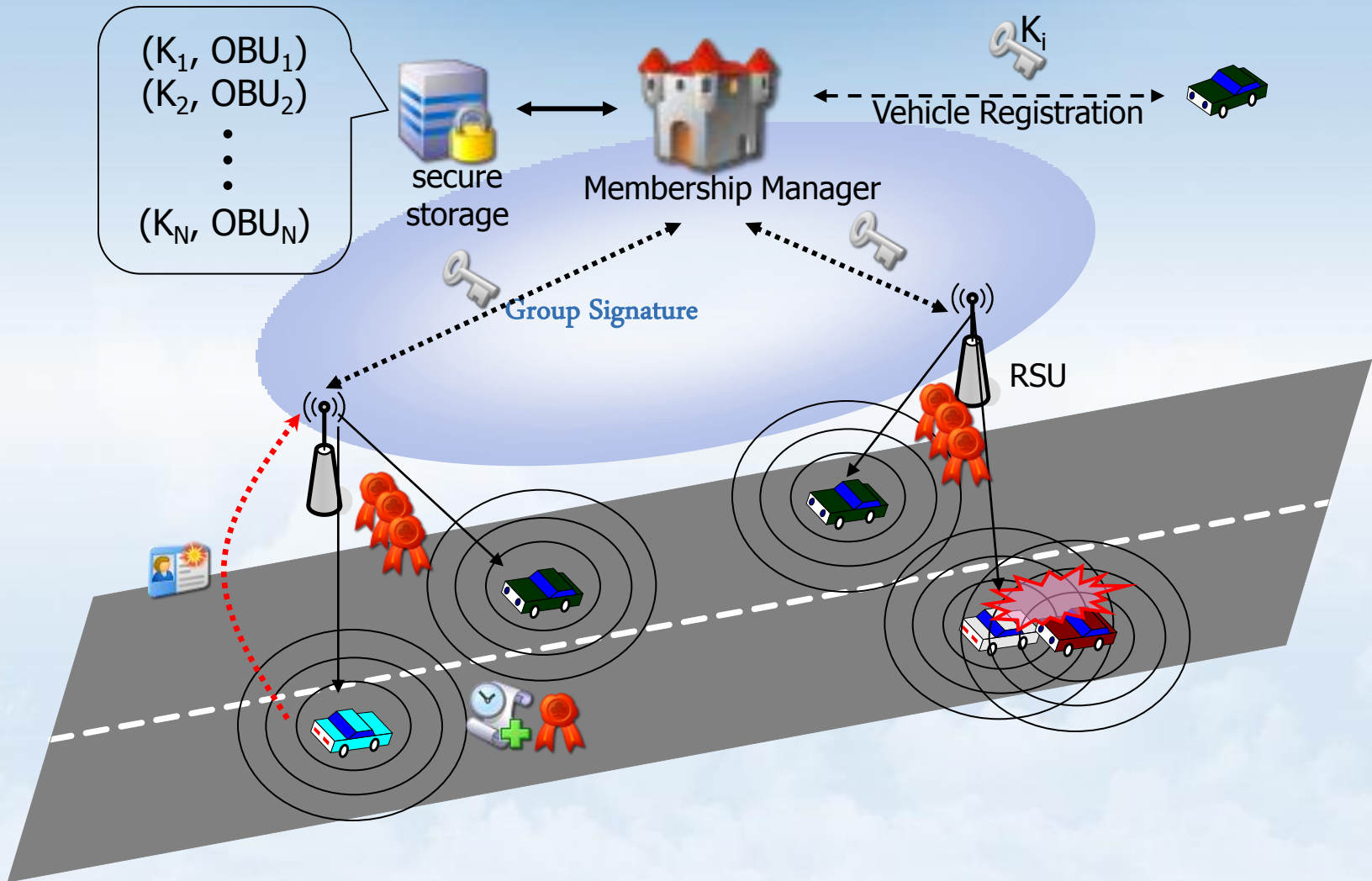
- Prevent **movement tracking**
 - Even though some RSUs are compromised
- Reduce **system overhead**
 - one-authentication \Rightarrow **multiple**-certificates issue
- Provide **simple traceability**
 - without cooperation with RSUs

System Model

Assumptions

- Each OBU has a unique electronic identity.
- Each OBU periodically sends traffic information message including its digital signature every 0.3 seconds.
- Safety messages are transmitted over a single-hop with a sufficient power to warn OBUs.
- Membership manager can inspect all the RSUs at high level and detect

System Model

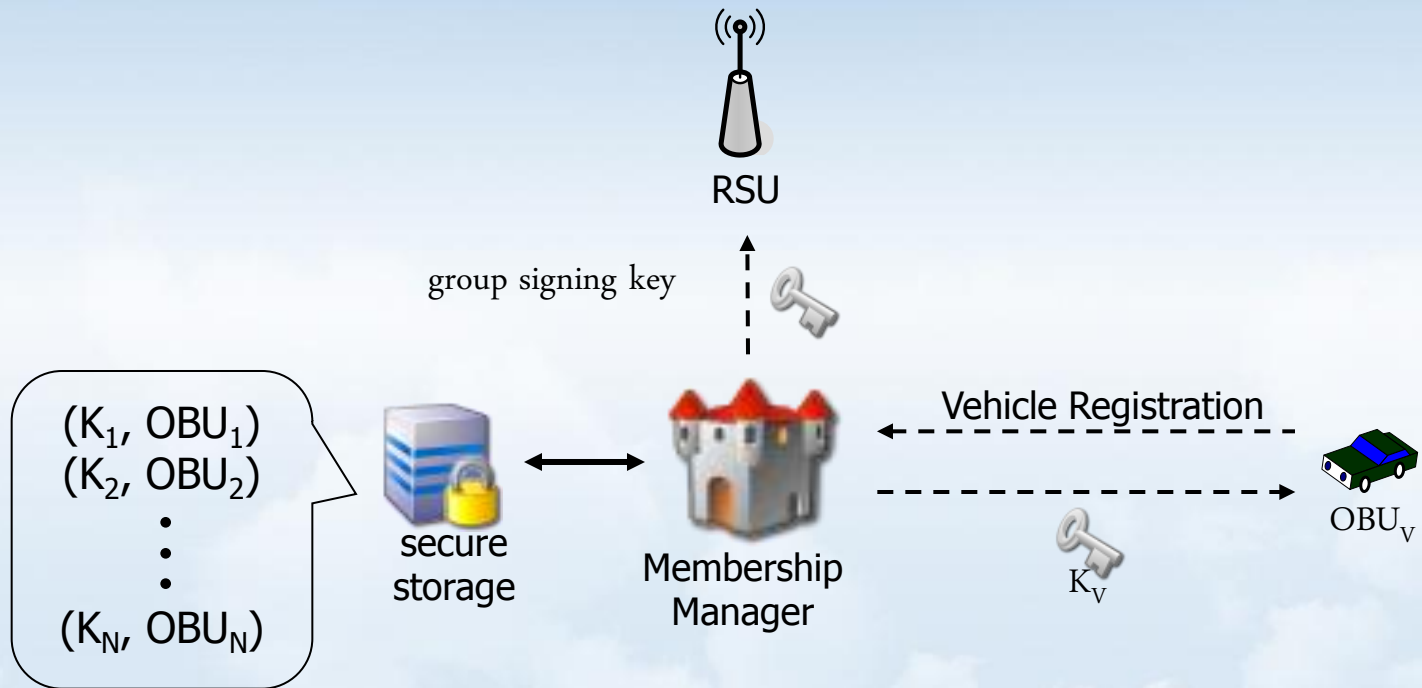


Proposed protocol

- Registration
- Multiple-Certificates Generation
- Safety Message Authentication
- Vehicle ID Trace

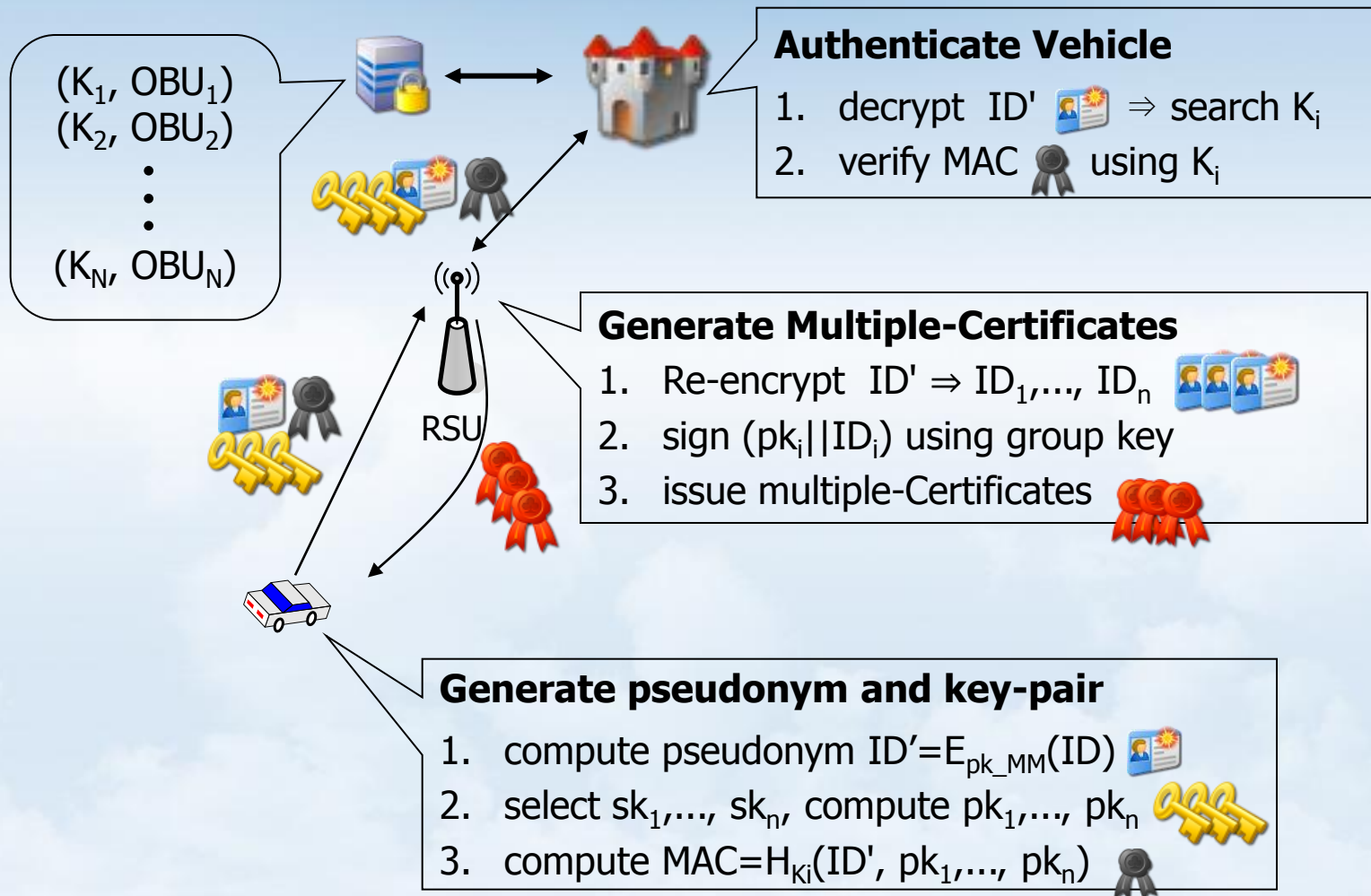
Proposed protocol

Registration



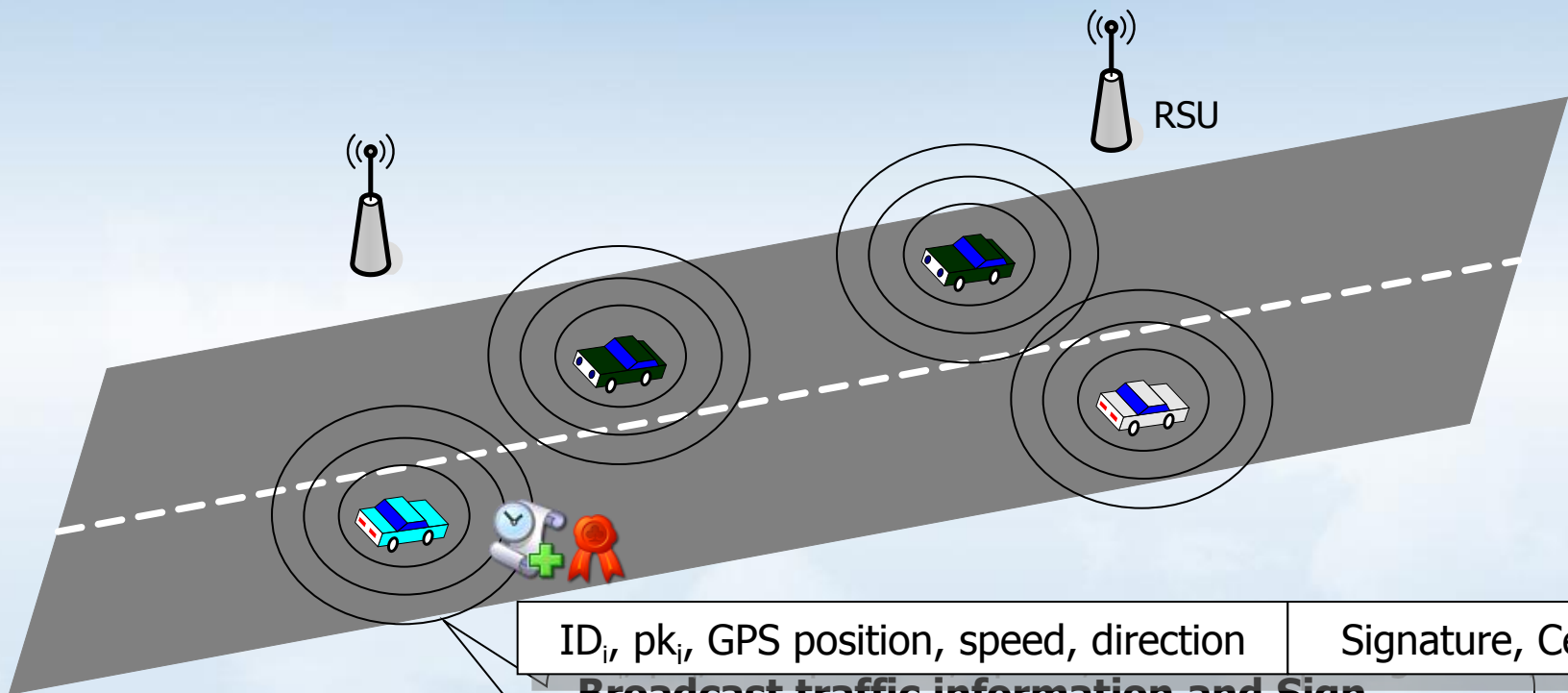
Proposed protocol

Multiple-Certificates Generation



Proposed protocol


Safety Message Authentication



$ID_i, pk_i, \text{GPS position, speed, direction}$

Signature, Cert

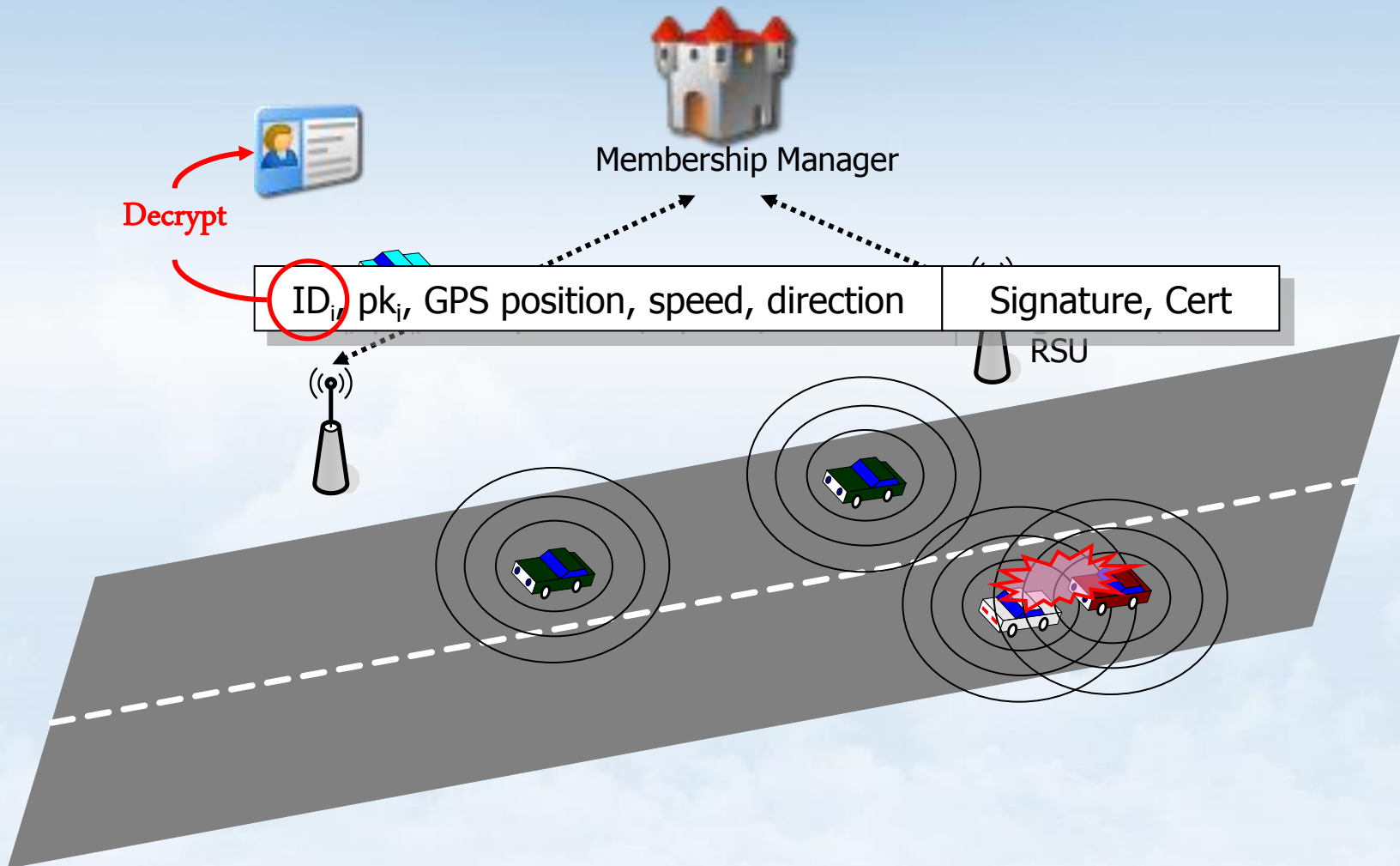
Broadcast traffic information and Sign.

1. add time-information to the traffic info. 

2. sign traffic info. with anonymous signing key

Proposed protocol

Vehicle ID Trace



Discussion

Robustness

- Against compromised RSUs
 - provide **unlinkability**
 - Change pseudonym in mutual authentication phase
 - Provide **Vehicle ID Traceability**
 - eliminate the cooperation with RSUs

Discussion

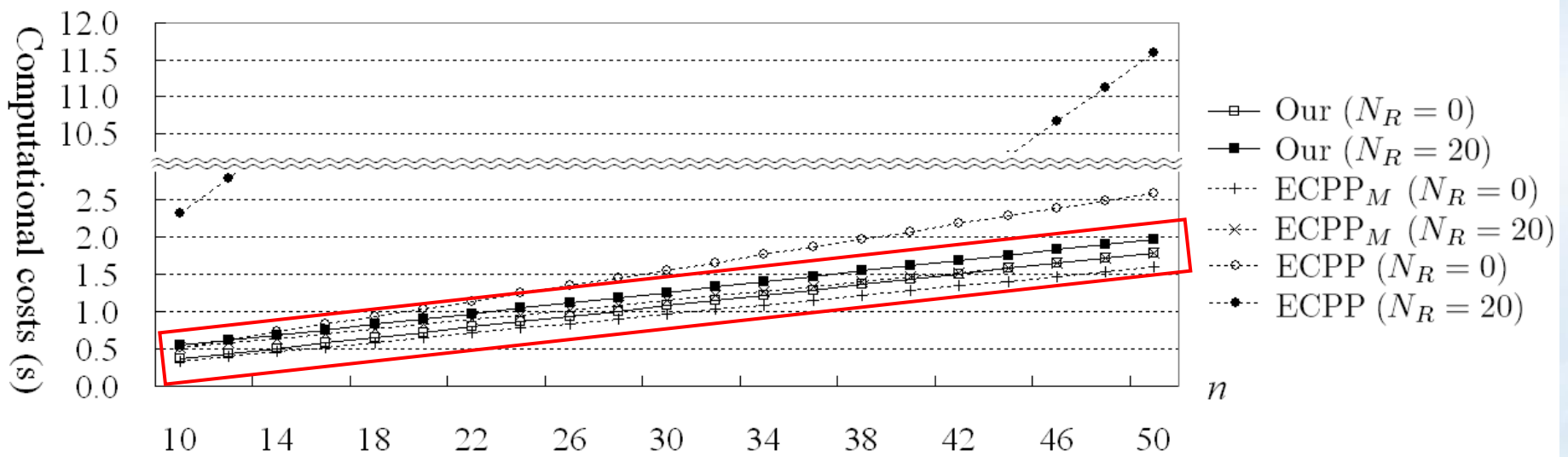
Efficiency

Cryptographic operation time	Time(ms, millisecond)	
\hat{e} bilinear pairing operation	4.5	
point multiplication on \mathbb{G}_1	0.6	
exponentiation on Z_p	2.1	
Protocol execution time	ECPP _M (ms)	Our Protocol(ms)
time for n certificates issue	$20.4+14.4n$	$6.3+18.6n$
time for n certificates verification	$17.1n$	$17.1n$
time for validity check of RSU	$9N_R$	$9N_R$
total time for n certificates generation	$20.4+31.5n + 9N_R$	$6.3+35.7n+9N_R$

- n : the number of Requesting certificates
- N_R : the number of Revoked RSUs

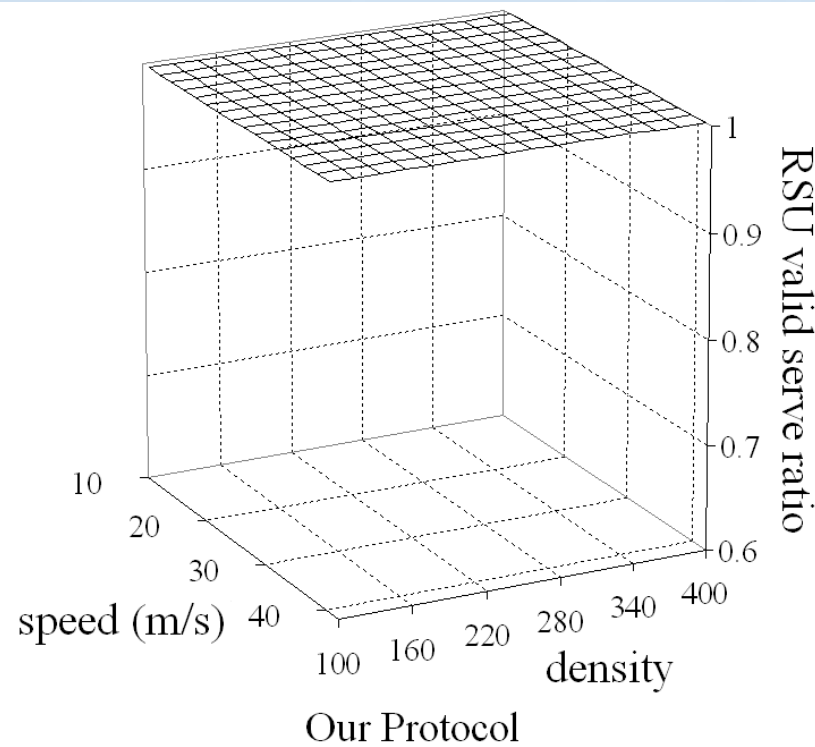
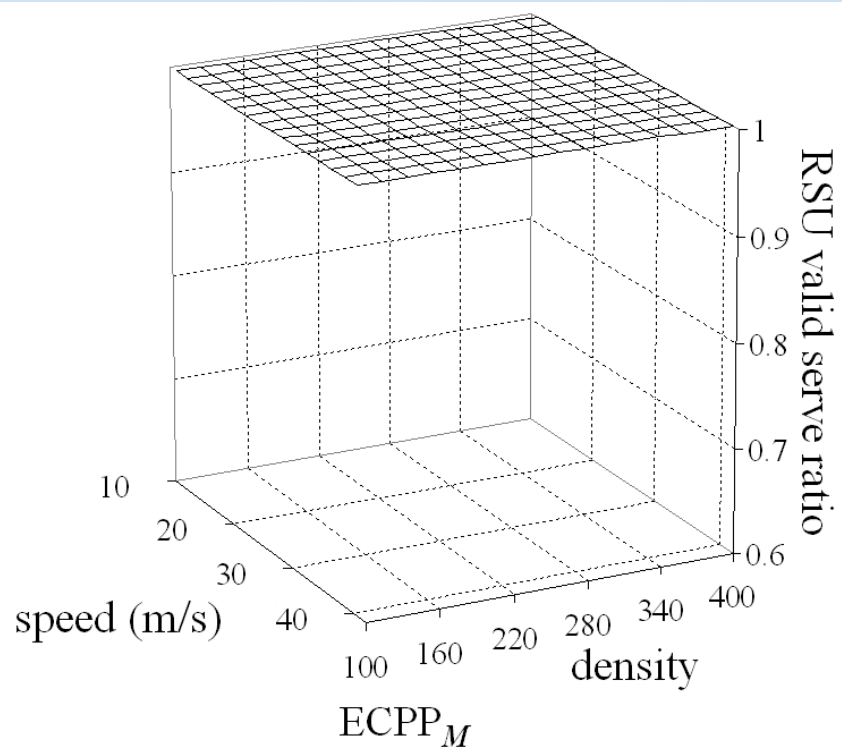
Efficiency

Computational cost of OBU



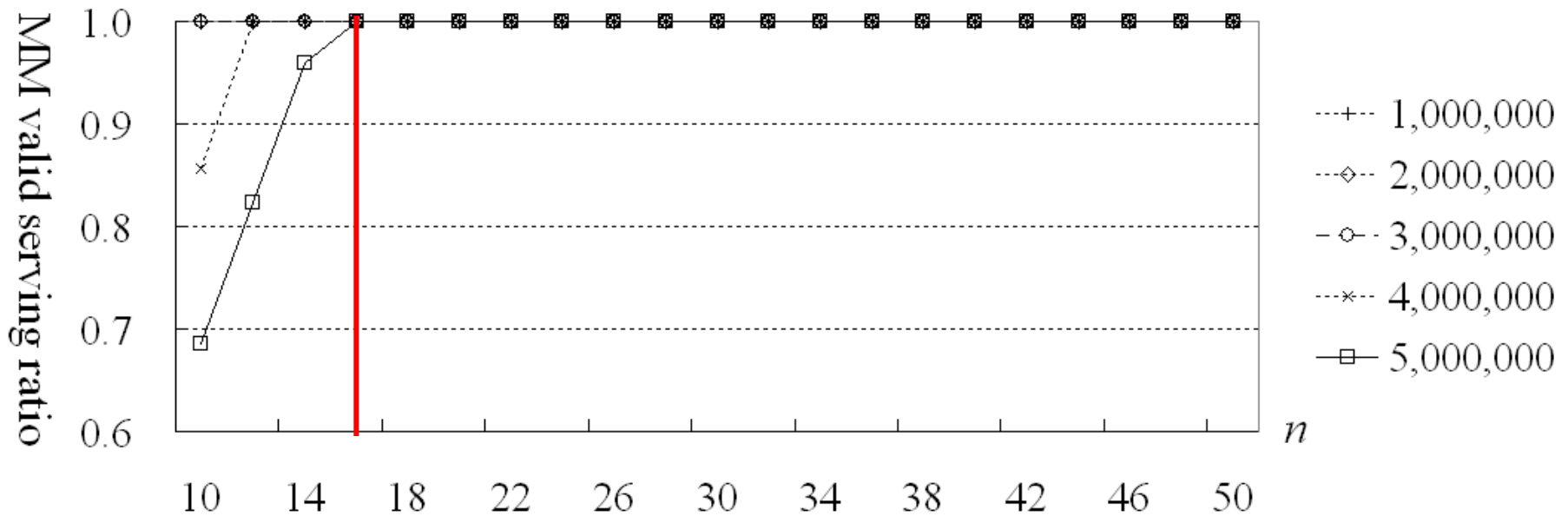
Efficiency

RSU valid serving ratio



Efficiency

Membership Manager valid serving ratio



Conclusion

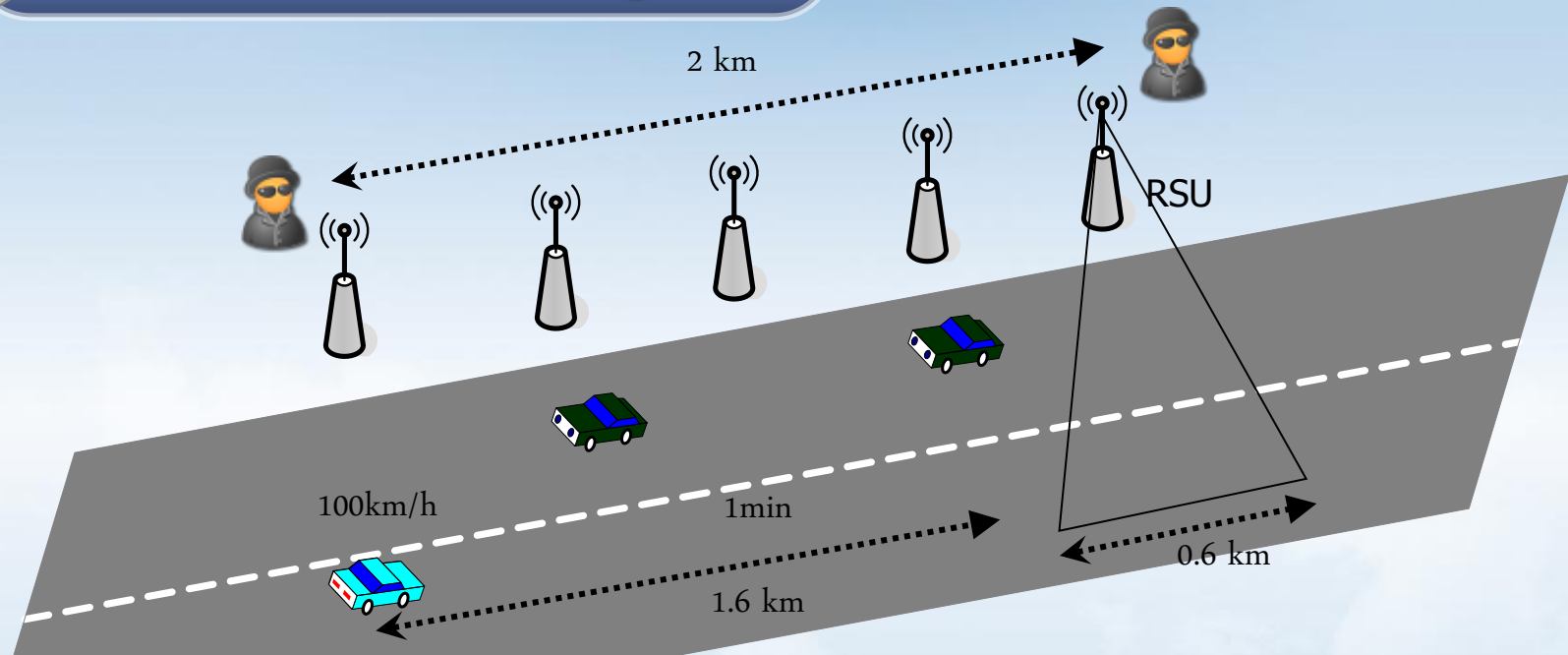
- Proposed an Efficient and Robust Conditional Privacy Preserving Authentication Protocol
 - Prevent **movement tracking** against compromised RSUs
 - Provide **traceability** without cooperation with RSUs
 - issue **multiple**-certificates by one-authentication of OBU



Thank you

Vehicular Ad-hoc Network

Movement tracking



Typical tracking scenario

- attacker controls stationary RSUs separated by 2km
- captures all the safety messages to illegally track vehicles

Result (to provide Anonymity and Unlinkability)

- upper (lower) bound on the key changing interval : 72s (50s)