ADVANCECRT
Centre for Research Training
Science Foundation Ireland For what's next

Security and Privacy in Vehicular Communication

Alia -, Supervisor: Dr. Paolo Palmieri, Co-supervisor: Dr. Aisling O' Driscoll

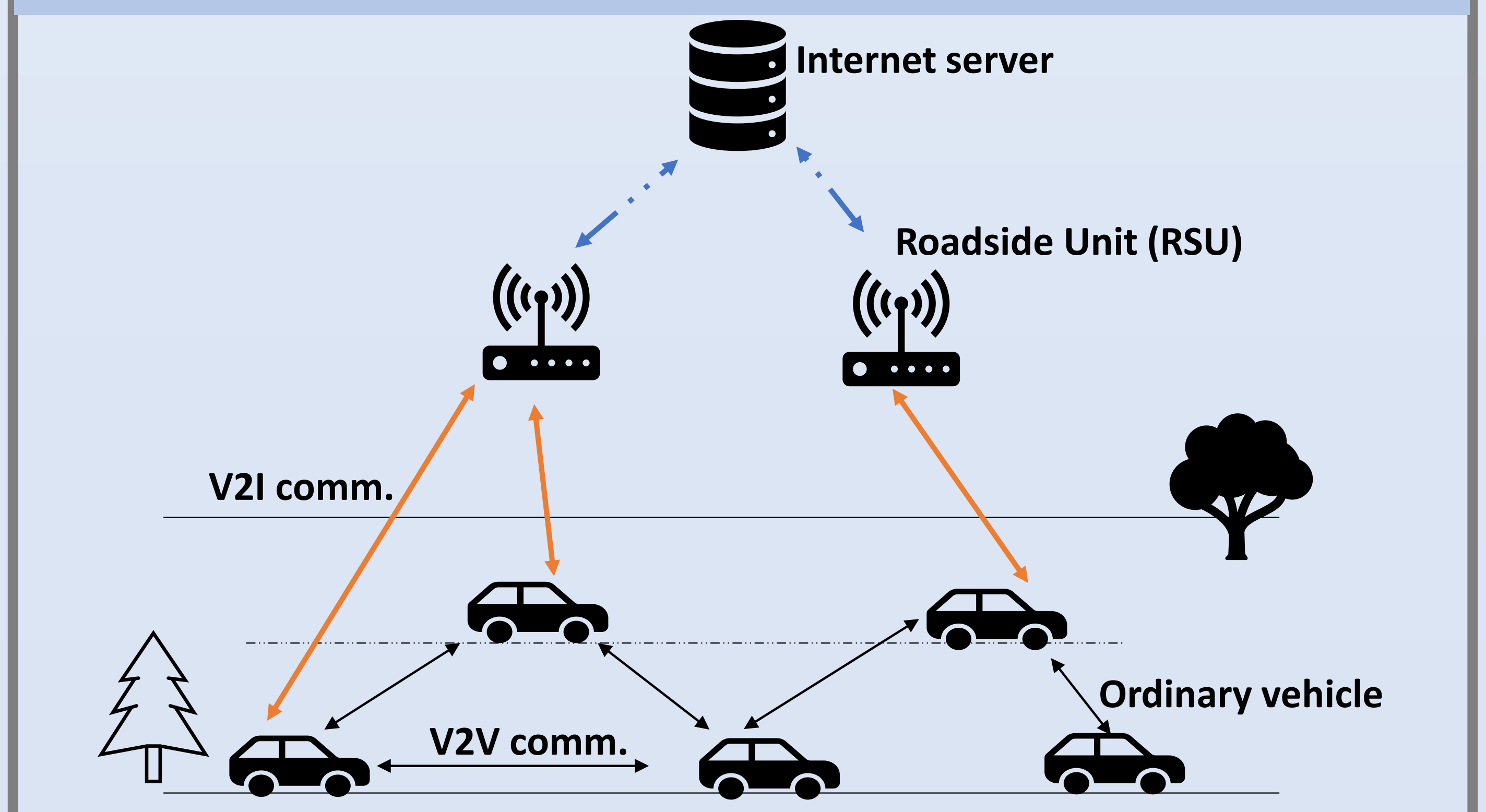
Vehicular Ad hoc Networks (VANETs)

The Vehicular ad hoc network (VANET) is a growing application in Intelligent Transportation Systems (ITS) that allows communication between Vehicle-to-Vehicle and Vehicle–to-Infrastructure.

The objective of VANET is to efficiently manage traffic by communicating with other vehicles in order to avoid

- Road accidents
- Traffic congestions
- Natural disastrous conditions

VANET Architecture



V2V Communication security issues

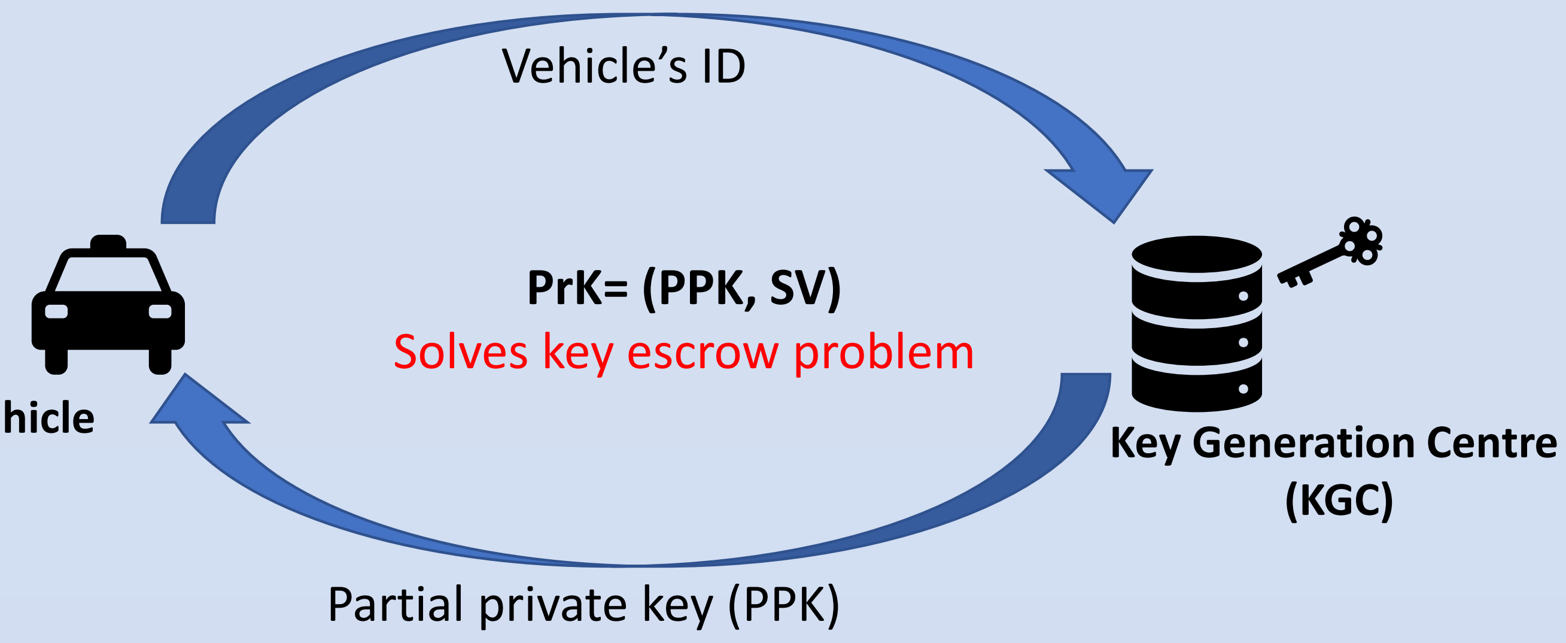
Autonomous vehicles collect data about weather or road conditions, traffic jams, rail crossings, etc., and send this data to other vehicles over an **insecure** wireless channel.

Basic security requirements:

- Authentication of vehicles
- Ensuring confidentiality
- Prevention against replay attacks

Certificateless PKI Signcryption scheme

Signature
Encryption
Signcryption


Vehicle's ID
PrK= (PPK, SV)
Solves key escrow problem
Vehicle
Key Generation Centre (KGC)
Partial private key (PPK)

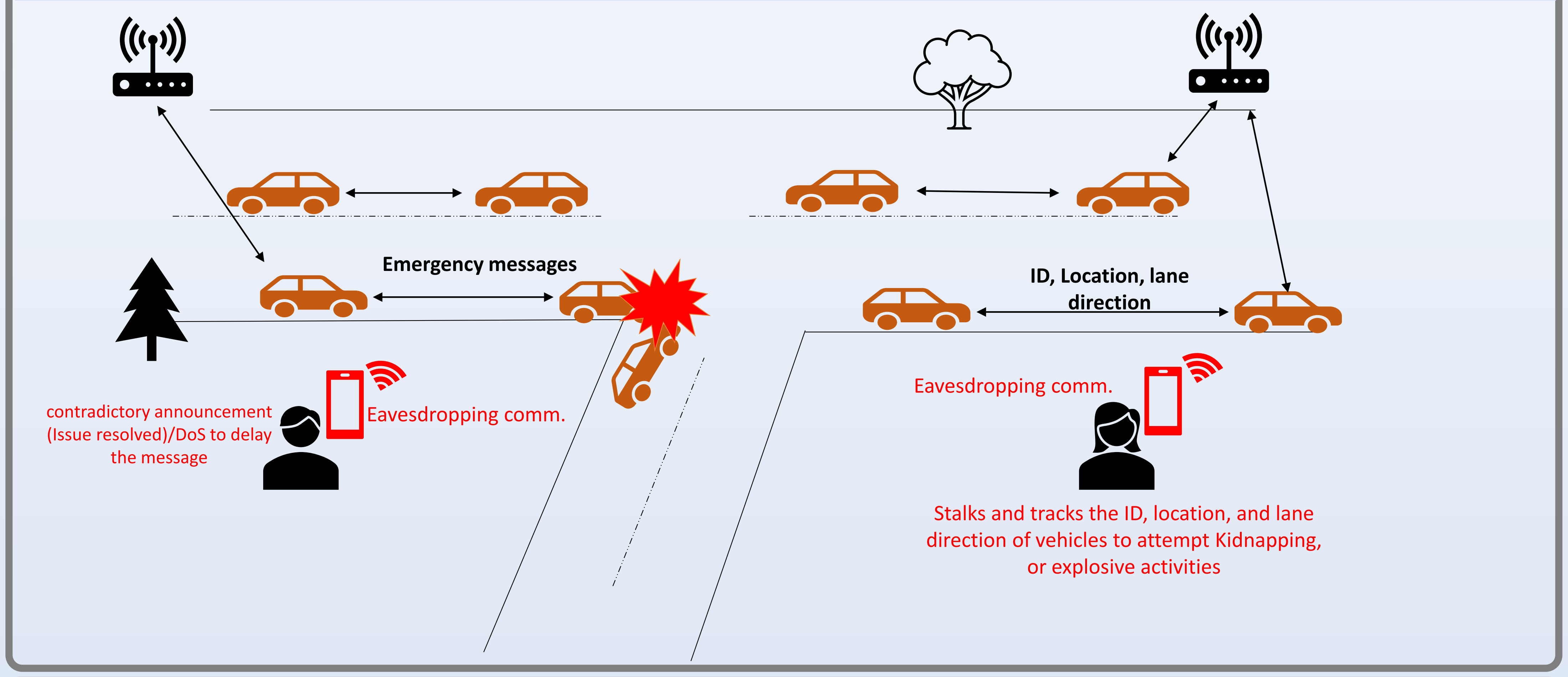
V→KGC: ID

KGC→V: PPK= (s.H(ID))

V: PrK=(PPK, SV)

PPK: partial private key
s: master secret key
SV: secret value
PrK: private key

Security attacks in V2V communication



contradictory announcement (Issue resolved)/DoS to delay the message

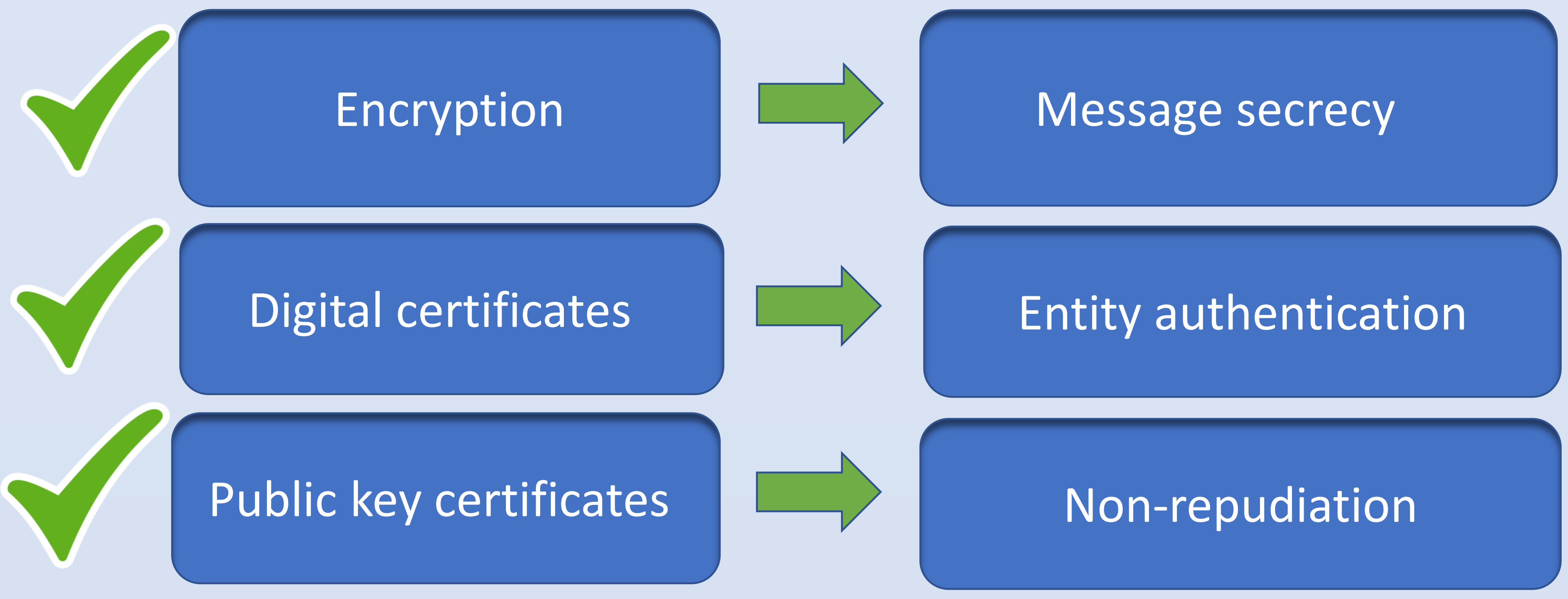
Stalks and tracks the ID, location, and lane direction of vehicles to attempt Kidnapping, or explosive activities

Motivation

- To verify the authenticity of vehicles taking part in the communication
- To secure messages exchanged between vehicles
- To provide vehicle authentication and message confidentiality while reducing communication delay and cost

Vehicle authentication + Message confidentiality

V2V Communication security solutions



Encryption → Message secrecy

Digital certificates → Entity authentication

Public key certificates → Non-repudiation

Conclusion

Certificateless cryptography CLC provides authentication and non-repudiation without the extra burden of certificate management and avoids key escrow problem.

Signcryption primitive performs the both functions of digital signature and encryption in one logical step with more efficiency than signing and encrypting separately.

In the rest of the project:

- we will focus on developing an efficient certificateless signcryption scheme to achieve security goals in vehicular communication such as confidentiality, authentication, and non-repudiation.
- since VANET infrastructure is extremely time constrained, our goal is to meet security requirements with high efficiency in terms of minimum communication delay and computation cost.

Project contribution to the UN SDG challenges

Since the main objective of UN SDG is making transportation infrastructure resilient, affordable and safer using cutting-edge technology. The project contributes to providing:

- secure vehicle communication by utilizing information security technology
- more efficient urban traffic management
- avoiding traffic accidents, and disastrous traffic conditions.

We intend to bridge the gap between industry and academic research by introducing secure traffic environment considering the safety, security, and efficiency as a concern of the industrial transportation.

Host Institution
UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaige