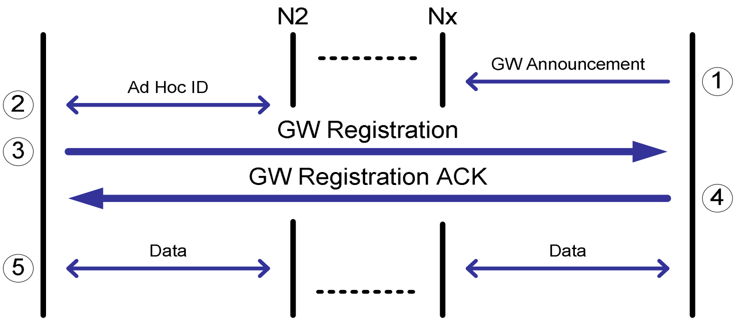
# Secure Multi-hop Ad Hoc Connectivity to Fixed Networks

## Technical Solution

1. Gateway Announcement
   - Periodically
   - Gateway ID cryptographically verifiable
   - Propagated through multiple nodes
2. Ad Hoc ID exchange
   - Between adjacent ad hoc nodes
   - Exchange of temporary identifiers
3. Gateway Registration
   - Encrypted registration message to gateway
4. Gateway Registration Acknowledgment
   - Certificate bound to the temporary node ID
   - Limited lifetime
   - Verifiable by intermediate nodes
5. Data Communication
   - Encrypted traffic signed with certificate
   - Only legitimate traffic is forwarded



N2

Nx

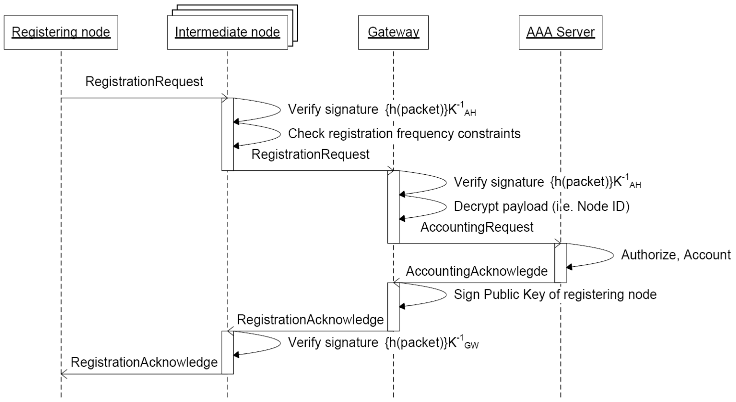
1 GW Announcement

2 Ad Hoc ID

3 GW Registration

4 GW Registration ACK

5 Data --------- Data



Registering node | Intermediate node | Gateway | AAA Server

RegistrationRequest

Verify signature $\{h(packet)\}K^{-1}_{AH}$

Check registration frequency constraints

RegistrationRequest

Verify signature $\{h(packet)\}K^{-1}_{AH}$

Decrypt payload (i.e. Node ID)

AccountingRequest

Authorize, Account

AccountingAcknowlegde

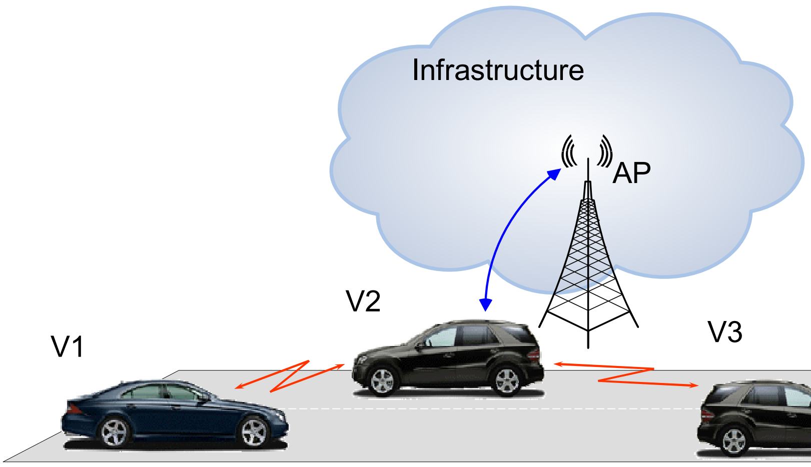
Sign Public Key of registering node

RegistrationAcknowledge

Verify signature $\{h(packet)\}K^{-1}_{GW}$

RegistrationAcknowledge

## Scenario



- Wireless ad hoc communication
- High velocity, high rate of topology changes
- Wireless connectivity between vehicles is used to access roadside Internet gateways
- Position dependent routing and addressing
- Privacy requirements

## Outlook

- Improve security of the underlying position dependent routing
- Develop mechanisms to encourage node co-operation
- Develop mechanisms for handover of established security associations
- Adapt proposed solution to support security of multi-hop unicast communication in the ad-hoc network

## Contact Information

- Frank Egle, Tim Leinmüller, Michael Schäfer
  Frank.Egle@DaimlerChrysler.com
  Tim.Leinmueller@DaimlerChrysler.com
  Michael.f.Schaefer@DaimlerChrysler.com
- Elmar Schoch
  Elmar.Schoch@uni-ulm.de

DAIMLERCHRYSLER