Trusted Routing for VANET

Terence Chen, Olivier Mehani and Roksana Boreli
National ICT Australia Ltd
University of New South Wales, Australia

Presentation Overview

- Introduction:
  - Trust in VANET
  - Challenge
  - Our approach
- Assumptions
- Proposed framework
- Applying the framework to OLSR
- Evaluation of the framework
  - Resilience to attacks
  - Computational and bandwidth overhead
- Conclusion and further work

Introduction

- Trust in VANET
  - Cooperative nature: Vulnerable
  - Lack of trust standard in VANET routing protocol
- Challenges of trust establishment for VANET
  - Highly dynamic
  - Distributed
  - Resource constraints
- Trusted routing framework
  - Authentication of messages, nodes and routes
  - Limited assistance with off-line Certificate Authority (CA)

Proposed Framework

NICTA

- Three-module framework:
  - Message authentication
  - Node-to-node authentication
  - Cumulative routability verification

- Prerequisites:
  - All nodes are loosely synchronized (NTP/GPS)
  - Each node has generated a key pair, K_i^+ / K_i^-
  - Off-line CA distributes following components to each node
    - Public key of CA, K_{ca}^+
    - Certificate that binds its network ID (e.g. IP address) and its public key: $Cert_i = [ID_i, K_i^+, T_v, T_e]_{K_{ca}^-}$

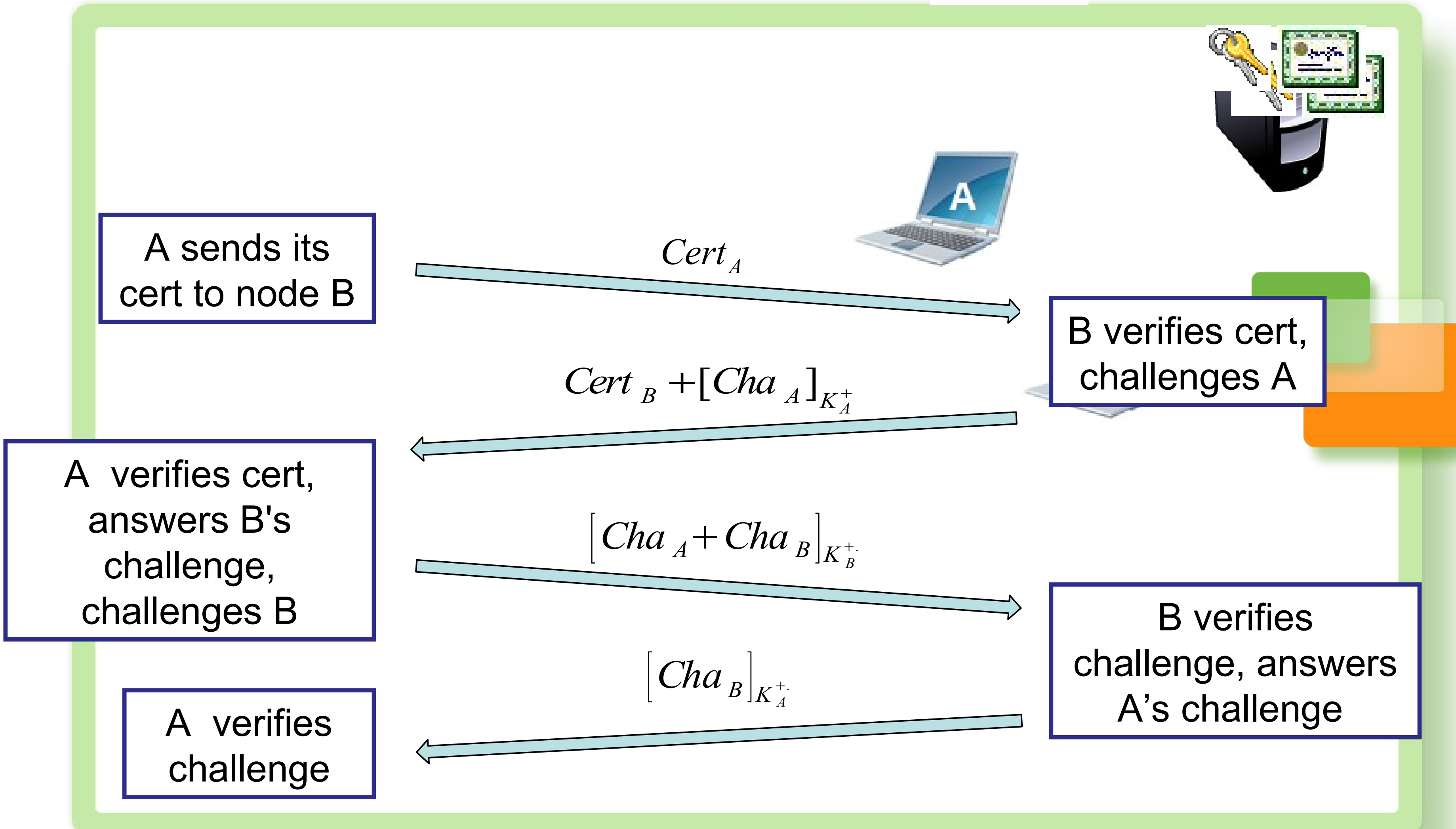
Message authentication

- Purpose:
  - To protect routing control messages
- Originator digitally signs every message
  - Message integrity
  - Message authentication
  - Non-repudiation
- Do not include variable fields
  - Hop-count
  - Time-to-live

Node-to-node Authentication

- Purpose:
  - Defines a way to verify nodes in minimum iterations
- Authentication between two nodes
- Exchange certificate & public keys
- Challenge peer to confirm identity
  - i.e. possession of corresponding private key
- Exchange secrete keys for quick re-authentication

Node-to-node authentication (cont.)



Cumulative Routability Verification

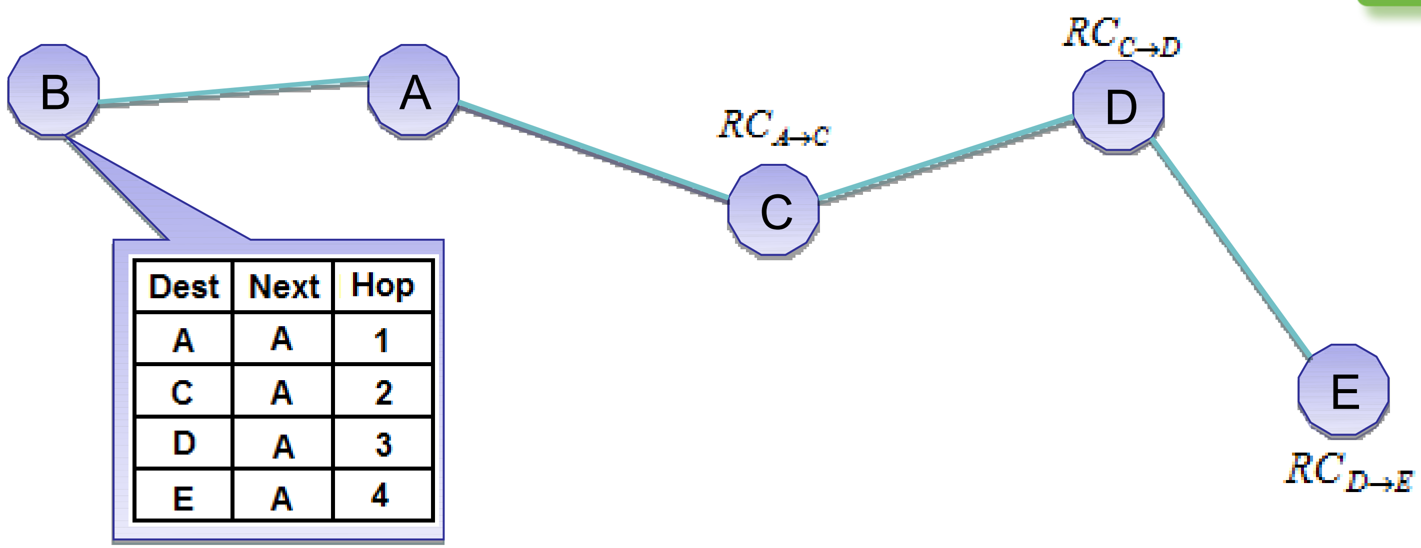
- Purpose:
  - Verify hop-by-hop connectivity along path
- A node must provide a piece of evidence to prove the connectivity
- Evidence: Routability Certificate (RC)
  - Signature from neighboring node regarding to the link
  - Exchange RCs after node-to-node authentication
  - Originator uses RCs to prove connectivity
  - Verify a route cumulatively

Cumulative Routability Verification (cont.)

$$RC = [ID_A, ID_B, T_v, T_e, Sign_B]$$

Where:

$$Sign_B = H([ID_A, T_v, T_e])_{K_B^-}$$



Dest	Next	Hop
A	A	1
C	A	2
D	A	3
E	A	4

Trusted Extension for OLSR

- Optimised Link State Routing (OLSR) protocol
  - Table driven, proactive
  - Use Multipoint Relays (MPR) to reduce control messages
  - Link status is disseminated to the entire network
  - HELLO message
    - Local control message
    - Link sensing
    - Neighbor discovery
    - MPR selector set discovery
  - Topology Control (TC) message
    - Global control mssage
    - Link state announcement

Trusted Extension for OLSR (cont.)

- HELLO message extension
  - Message signature
  - Authentication info is embedded in standard HELLO messages
  - Concurrent handshakes among multiple neighbors

- Operations:
  - Distribute certificates
  - Node-to-node authentication handshake
  - Exchange RCs

Trusted Extension for OLSR (cont.)

- Trusted HELLO message format

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Trusted HELLO Message Extension Format           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       0       |       1       |       2       | 3  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|1|2|3|4|5|6|7|0|1|2|3|4|5|6|7|0|1|2|3|4|5|6|7|0|1|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Message Header                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Originator's Certificate                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Message Signature                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Neighbour 1 Interface Address                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| stat  |  opt  |  len  |
+-+-+-+-+-+-+-+-+-+-+-+-+
|     Neighbour 1 authentication handshake info        |
:        or routability certificate                    :
|                                                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Neighbour 2 Interface Address                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| stat  |  opt  |  len  |
+-+-+-+-+-+-+-+-+-+-+-+-+
|     Neighbour 2 authentication handshake info        |
:        or routability certificate                    :
|                                                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                      |
:                        ...                           :
|                                                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Certificates
- Message Signature
- Handshake info
- RCs

Trusted Extension for OLSR (cont.)

- TC message extensions
  - Message signature
  - Carry RC and certificate after each neighbor address
  - Similar format to trusted HELLO message
- Operation:
  - Verify RC before add links to routing table
  - Confirm connection to each node hop-by-hop

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Trusted TC Message Extension Format              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       0       |       1       |       2       | 3 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|1|2|3|4|5|6|7|0|1|2|3|4|5|6|7|0|1|2|3|4|5|6|7|0|1|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Message Header                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Originator's Certificate                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Message Signature                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Neighbour 1 Interface Address              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  opt  |  len  |
+-+-+-+-+-+-+-+-+
|              Neighbour 1 certificate or
:              routability certificate
|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Neighbour 2 Interface Address              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  opt  |  len  |
+-+-+-+-+-+-+-+-+
|              Neighbour 2 certificate or
:              routability certificate
|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                      |
:                        ...                           :
|                                                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Resilience to Attacks

Attack/ misbehavior	Description	Countermeasure
Illegal Access	Device without permission/certificate	Message signature Node-to-node authentication
Impersonation	Identity spoofing: MAC or IP	Node-to-node authentication
Message modification	Rushing ANSN attack	Message signature
Link spoofing	Spoofing destination that couldn't reach	Routability verification
MPR selector isolation	A node isolate its MPR selector by not include it in the message	Routability certificate sign by all neighbors

Bandwidth and Computational Overhead

- Public key scheme dependent

- Bandwidth overhead

  Size of RC:

$$L_{rc} = 2 \times L_{ip} + L_{time} + L_{sig}$$

  Size of Certificate:

$$L_{cert} = L_{ip} + L_{pub} + L_{time} + L_{sig}$$

Bandwidth and Computational Overhead (cont.

- Benchmark for some cryptographic algorithm

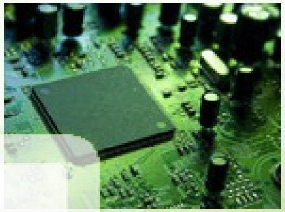
Operation	Milliseconds/Operation
RSA 1024 Encryption / Decryption	0.08 / 1.46
DSA 1024 Signature /Verification	0.45 / 0.52
RSA 2048 Encryption / Decryption	0.16 / 6.08
RSA 2048 Signature / Verificatio	6.05 / 0.16
ECIES 233 Encryption / Decryption	21.17 / 12.15
ECDSA 233 Signature / Verification	10.62 / 12.80
MD5	0.0045 (per 1KB data)
SHA-1	0.0065 (per 1KB data)

Crypto++ 5.6.0, Intel Core2 Duo 1.83 GHz

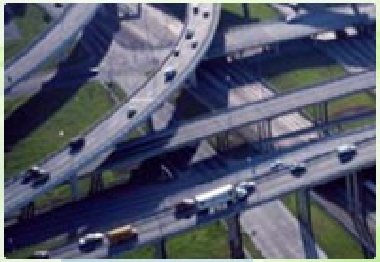
Conclusion and Future Work

- Proposed trust establishment framework
  - Message authentication
  - Node-to-node authentication
  - Routability Verification

- Future work
  - Find a signature scheme to reduce overhead
  - Apply framework to other protocol, e.g. AODV



NICTA



From **imagination** to **impact**