



Is it that easy to detect sybil attacks in C-ITS: a position paper

Badis HAMMI

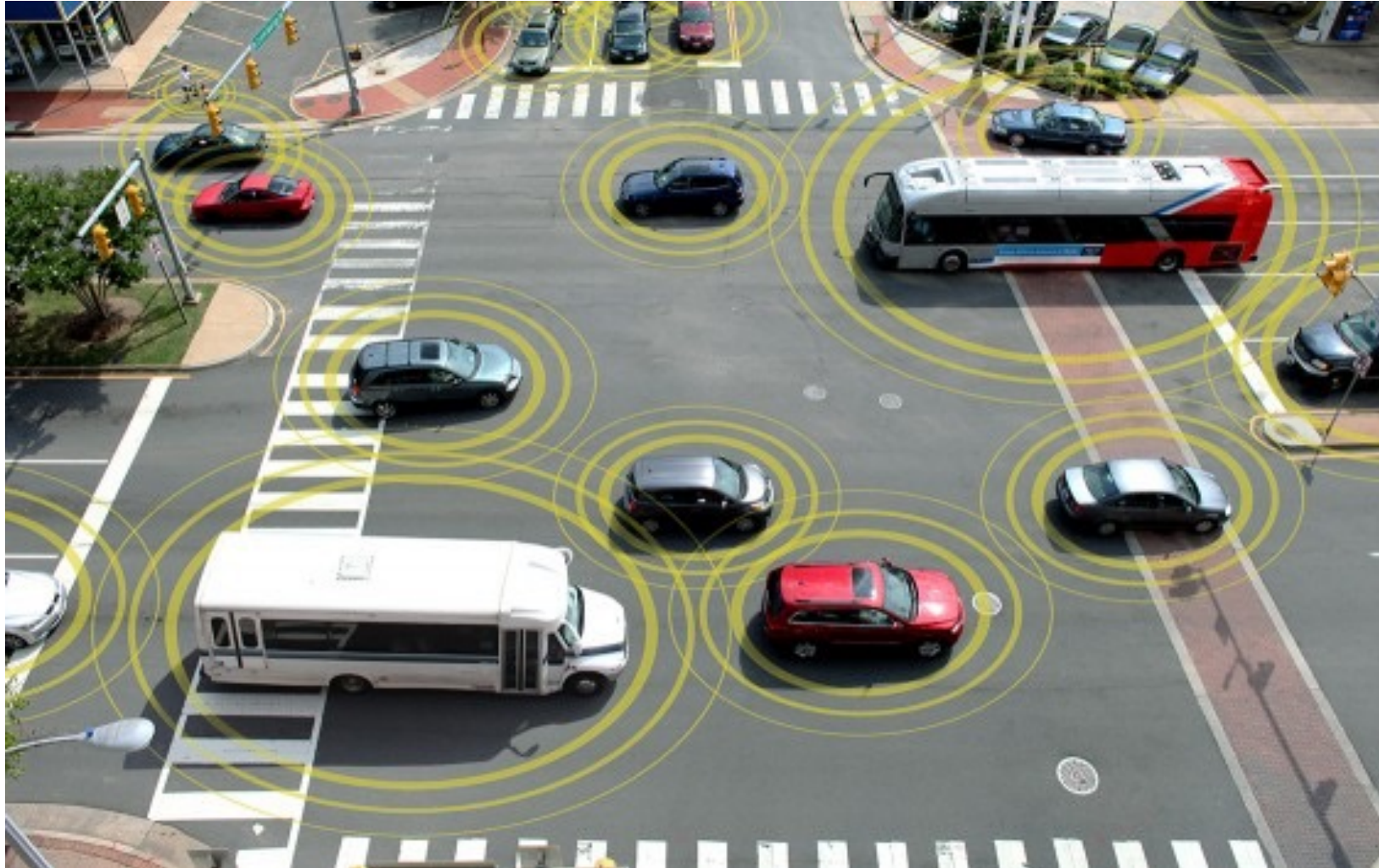


Smart cities

- Smart cities rise
- Automobile manufacturers gave more interest into Cooperative Intelligent Transportation Systems (C-ITS)
- Numerous deployment projects : SEVECOM, EVITA, PRESERVE, CORRIDOR, CVPS, California PATH, ISE, ECO-AT, SCMS, MIT PORTUGAL, ITS Japan and ITS India



Cooperative Intelligent Transportation Systems





Cooperative Intelligent Transportation Systems

- **ITS applications**

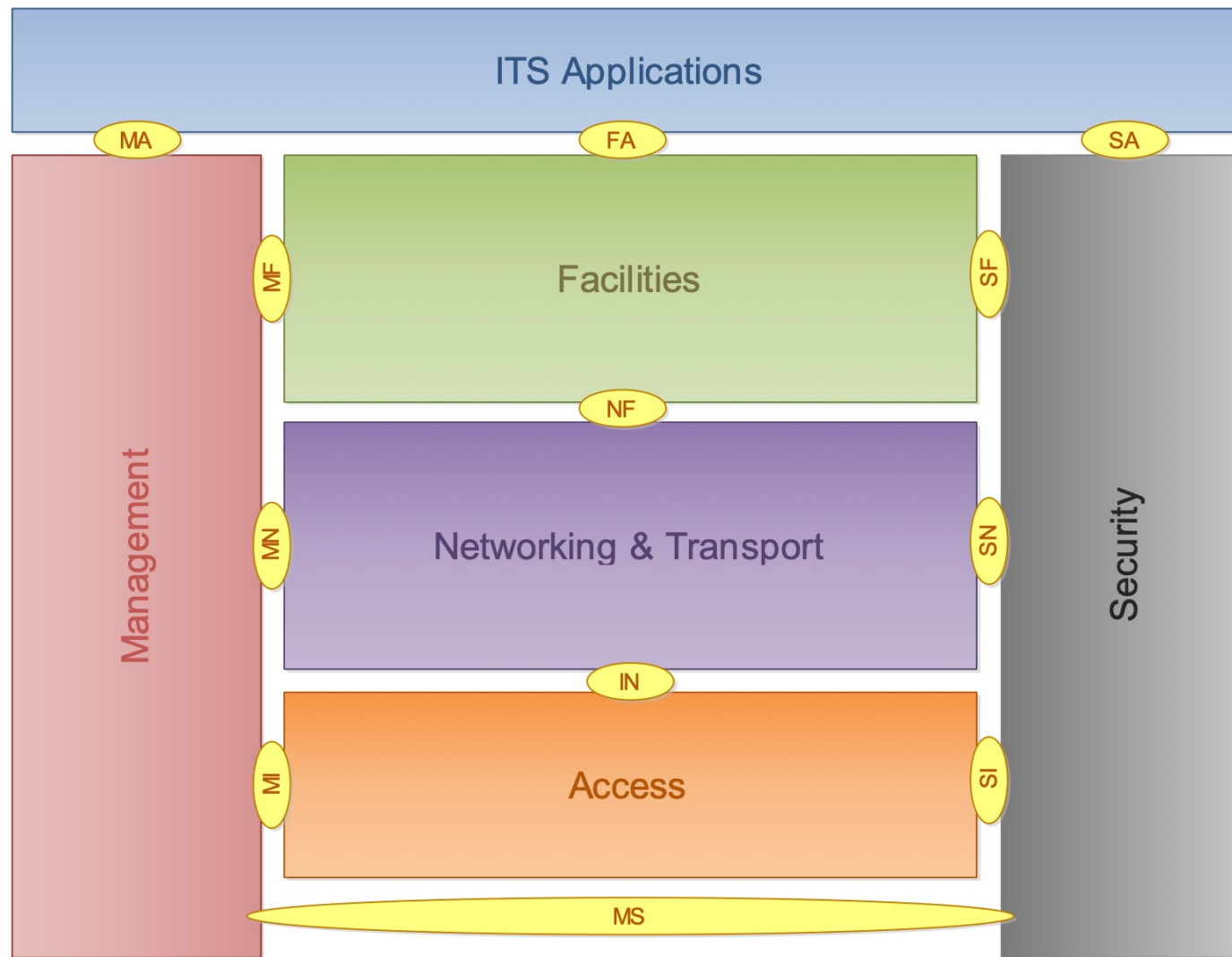
- Safety and security applications
 - BSM has the potential to prevent up to 75% of all roadway crashes [U.S. Department of Transportation, W. Whyte 2013]
- Efficiency applications
- Interactive entertainment applications

Cooperative Intelligent Transportation Systems

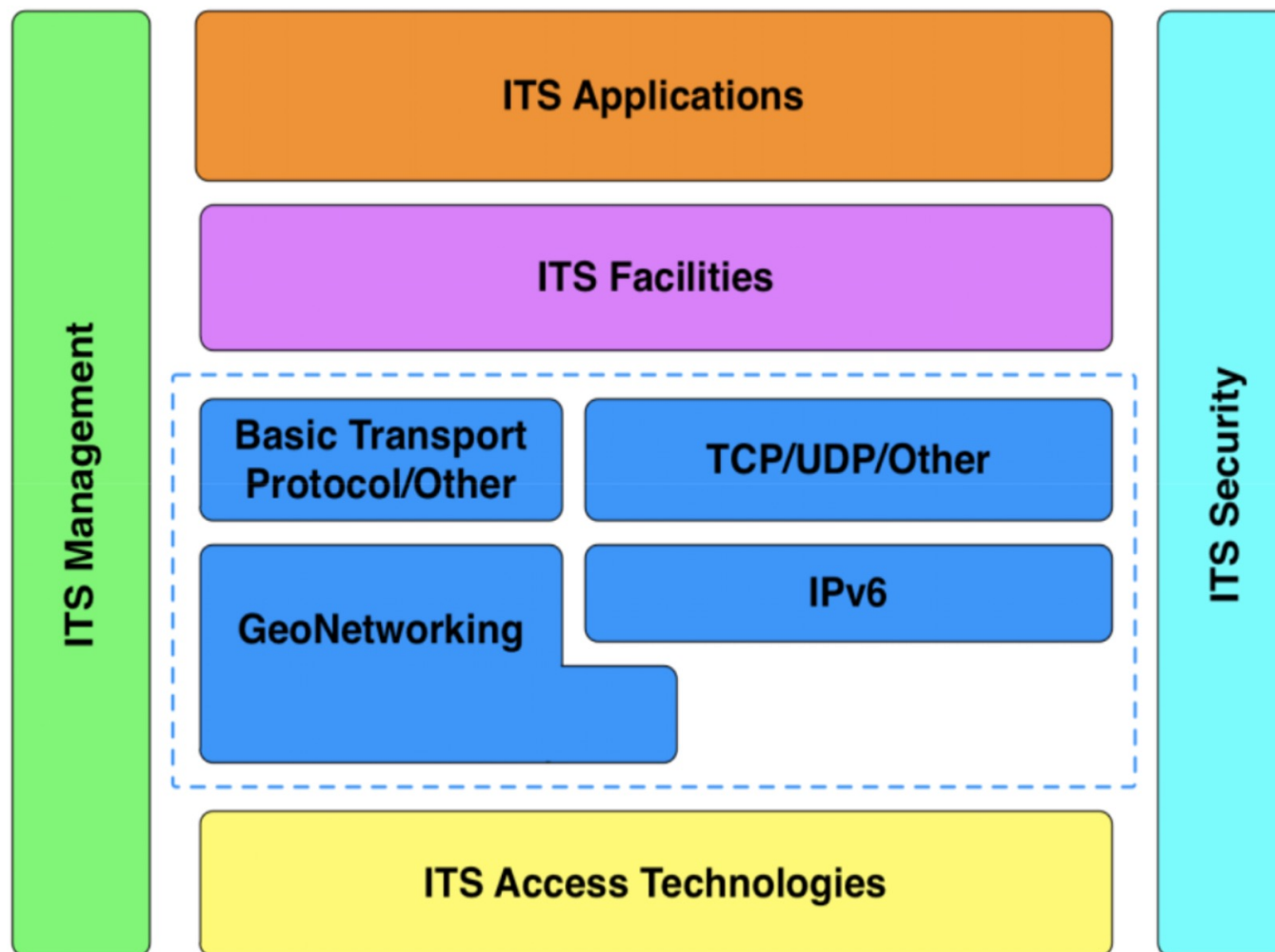
- **A network needs security !!!**



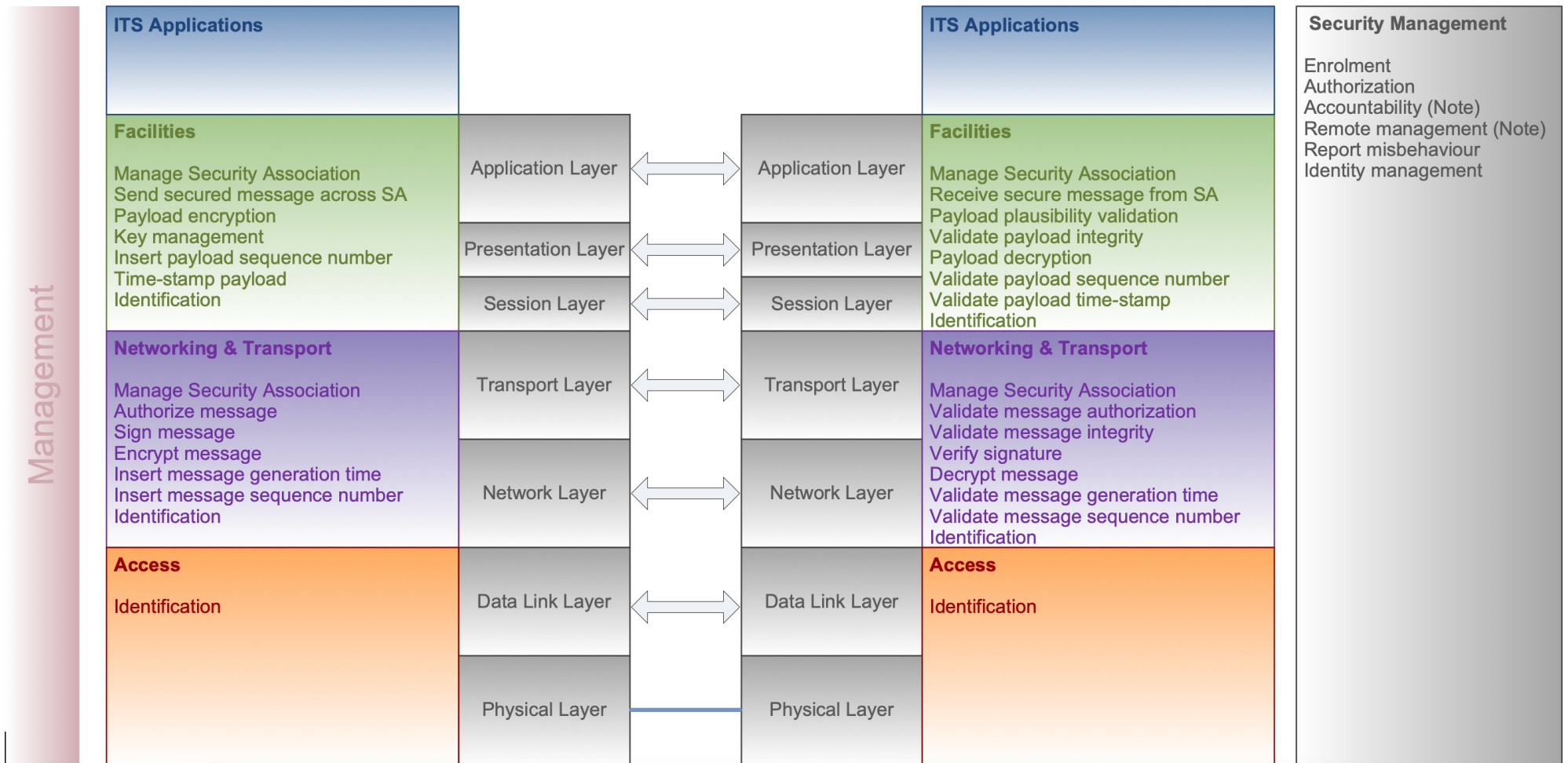
C-ITS networking architecture



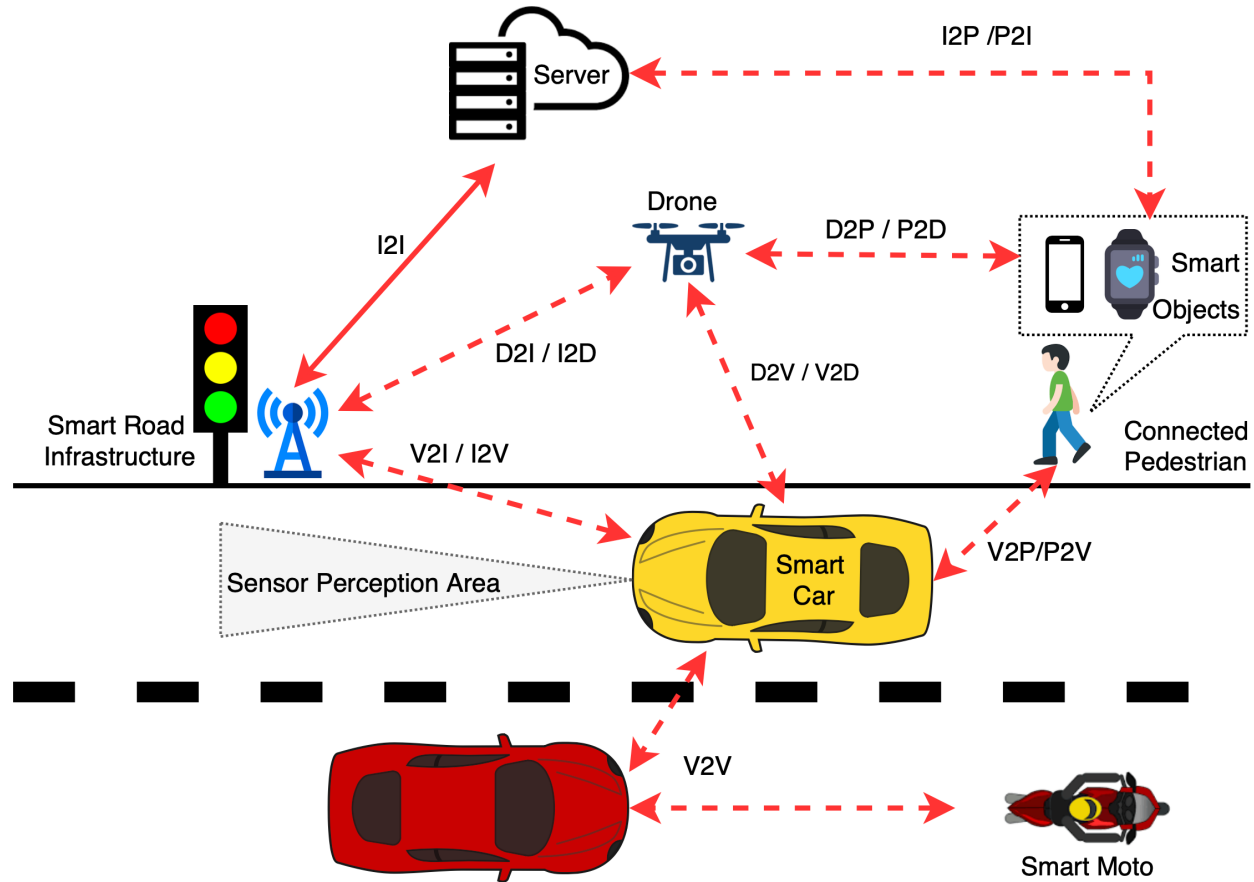
C-ITS networking architecture



C-ITS networking architecture

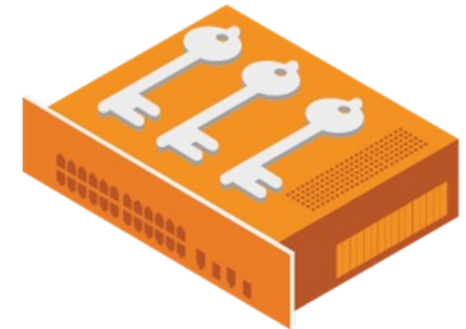


C-ITS Environment



Cooperative Awareness Message (**CAM**), Decentralized Environmental Notification Message (**DENM**), Basic Safety Messages (**BSM**), Signal Phase and Timing (**SPAT**), MapData Messages (**MAP**), In Vehicle Information (**IVI**), Traffic Light Control (**TLC**)

ITSS-R ITSS-V



C-ITS Messages

antenne_arrière_test_1.pcapng

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	CohdaWir_00:00:01	Broadcast	DENM	416	[Secured]
2	0.039607	Routerbo_14:d2:d8	Broadcast	GeoNet...	294	Beacon[Secured]
3	0.100147	ce:db:fc:bd:e3:03	Broadcast	GeoNet...	365	Secured[Malformed Packet]
4	0.138266	AtgUvTec_12:63	Broadcast	CAM	370	[Secured]
5	0.275587	CohdaWir_00:00:01	Broadcast	GeoNet...	503	Secured[Secured]
6	0.421594	66:1a:13:b5:0d:ed	Broadcast	GeoNet...	400	Secured[Malformed Packet]
7	0.507752	Azureway_cd:37:b1	Broadcast	CAM	333	[Secured]

► GeoNetworking: Secured (GeoBroadcast Circle)
► Basic Transport Protocol (Type B)
▼ DENM
 ▼ DENM
 ► header
 ▼ denm
 ► management
 ► situation
 ► location
 ▼ alacarte
 ► roadWorks

```
0000  ff ff ff ff ff ff 04 e5 48 00 00 01 89 47 02 00 ..... H....G..
0010  f1 01 02 80 a9 80 02 02 01 4c 37 b1 cf 94 c9 15 ..... .L7....
0020  4d 01 00 36 00 00 02 2d 64 70 aa 20 ef 5a 60 8c M..6...- dp. .Z`.
0030  c3 15 23 8a 24 66 64 7a 50 5d e1 66 82 a8 ea d0 ...#.$fdz P].f....
0040  7f ab d2 62 6e 64 1c 02 00 21 0f 24 03 01 ff fc ...bnd... !.$.
0050  25 04 01 ff ff ff 80 8d 01 00 0b 01 1a a5 d9 c0 %.....
0060  1b 1f 23 c0 03 00 00 00 69 04 2d 42 42 42 e2 77 ..#..... i.-BBB.w
0070  e2 c0 73 2f 1c bf f0 8e 03 7b 1b c2 4f f9 e3 87 ..s/.... .{..0...
0080  6d d4 ee 21 5c 0c 85 16 3c 34 3c dc a3 75 03 6d m.!\... <4<..u.m
0090  f8 0e 01 e0 ec 4b 50 4a ca 36 e1 ba 5c 56 8a 6e ....KPJ .6..\V.n
00a0  4e 55 79 e7 b7 41 65 2e 00 00 01 9a b3 df 98 62 NUy..Ae. ....b
00b0  94 03 1d 59 df 42 02 6b ce 12 00 00 05 25 01 80 ...Y.B.k .....%..
00c0  9b 20 40 01 80 00 67 01 00 27 1f 00 00 bc 00 04 . @...g. .'.
00d0  e5 48 00 00 01 23 ce bc 0f 1d 59 df 42 02 6b ce .H...#... .Y.B.k.
00e0  12 80 04 0b f6 1d 59 de dc 02 6b cd fe 03 e8 00 .....Y. ..k....
```

Frame (416 bytes) Bitstring tvb (6 bytes) Bitstring tvb (6 bytes)

Frame (frame), 416 bytes

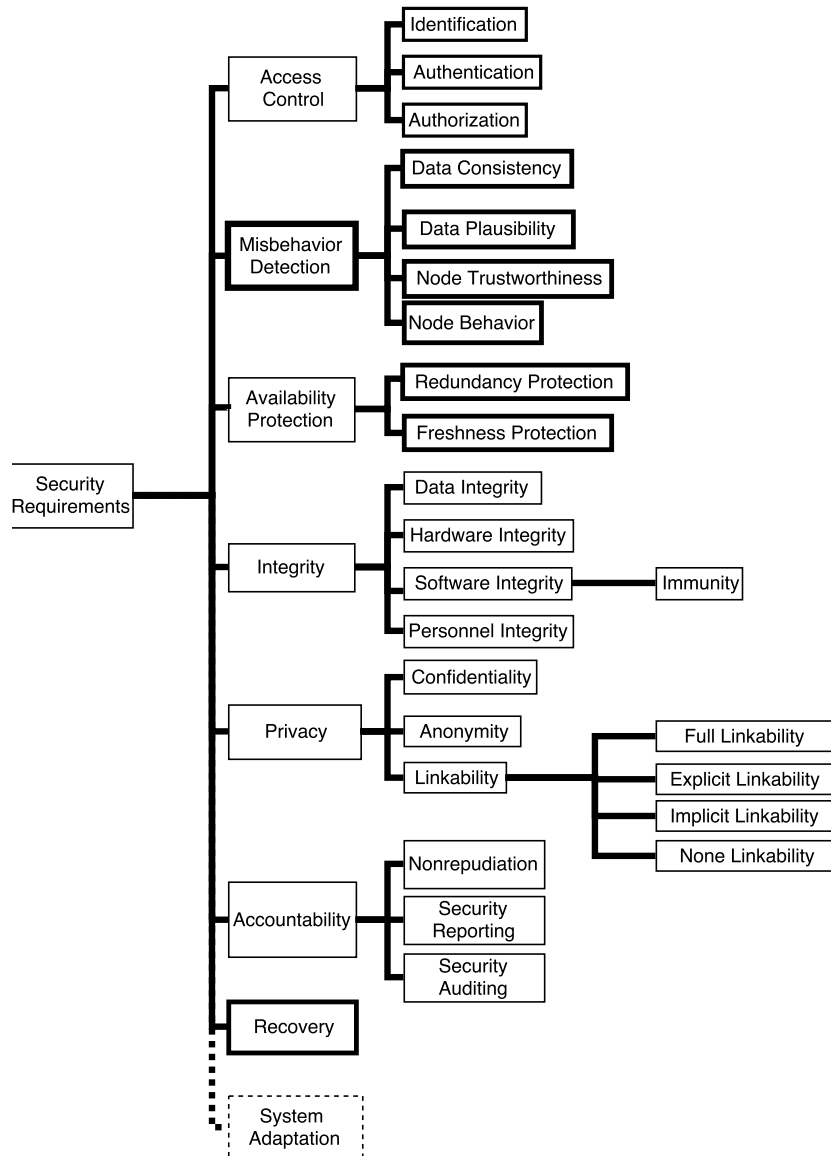
Packets: 46367 - Displayed: 46367 (100.0%) - Load time: 0:0.88 - Profile: Default



Evolution

- C-ITS applications have evolved and become very greedy in terms of transmitted traffic and used bandwidth
- Huge amounts of data and messages are exchanged continuously, e.g., CAM, DENM and BSM
- Most of the exchanged messages contain critical data that should be confidential
- Numerous requested services require authentication to be accessed

Security and privacy requirements



- Integrity
- Authentication
- Non repudiation
- Privacy (no tracking)
- Authorization
- Confidentiality (some use cases)



Public Key Infrastructure

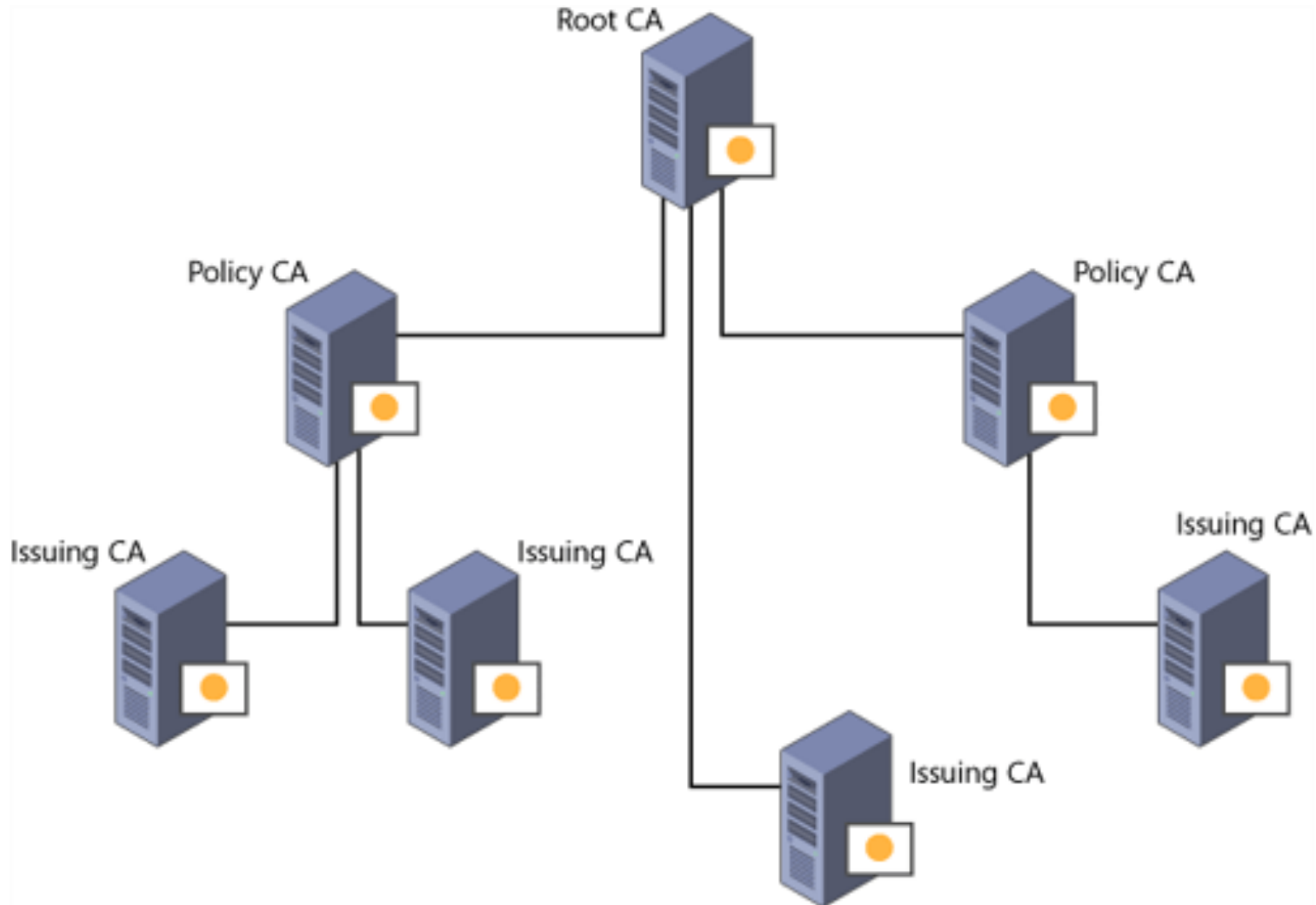
▪ Public Key Infrastructure

- Set of authorities, policies and procedures
- Manages public-key mechanisms
- Binds public keys with respective identities of entities
- Binding is established through a process of registration and issuance of certificates
- Creates, manages, distributes, uses, stores, and revokes certificates

Security requirements

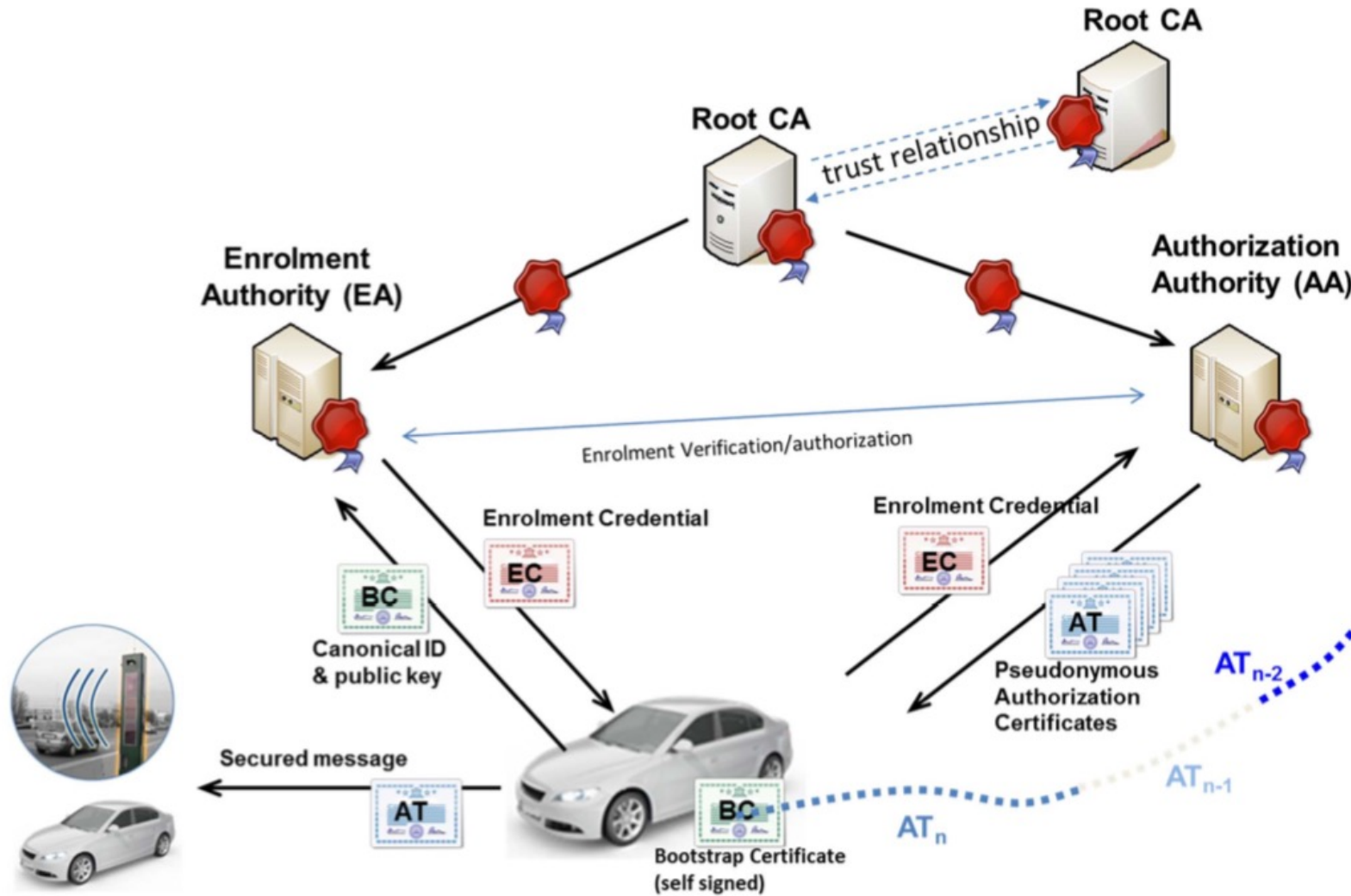
Requirement	Mechanism/Algorithm
Confidentiality	Encryption (ECIES)
Authentication	Certification (PKI), Signature (ECDSA)
Integrity	Signature (ECDSA)
Non repudiation	Signature (ECDSA)
Privacy	Certificate change
Authorization	SSP

C-ITS PKI



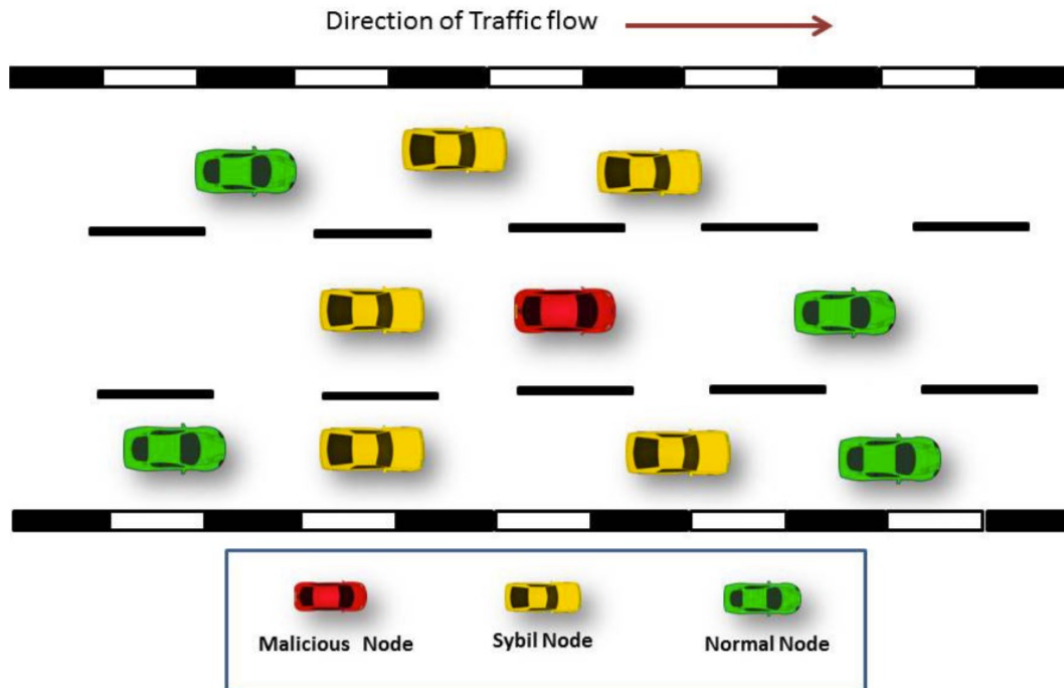
Design of a traditional PKI

C-ITS PKI



Design of a C-ITS PKI

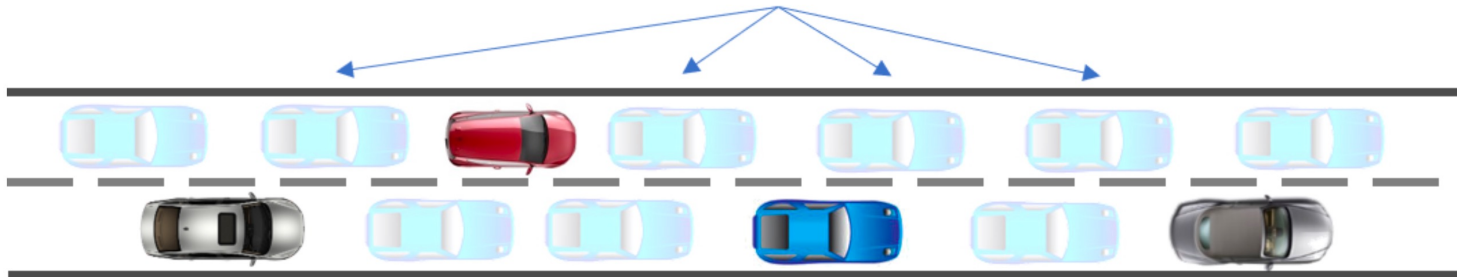
Sybil attack



- The attacker node creates different virtual nodes (also called sybil ghosts) in order to have a certain influence on the network's decisions especially in voting based protocols and applications
- The creation of the sybil ghosts is performed by creating different messages using different fake identities and different fake locations

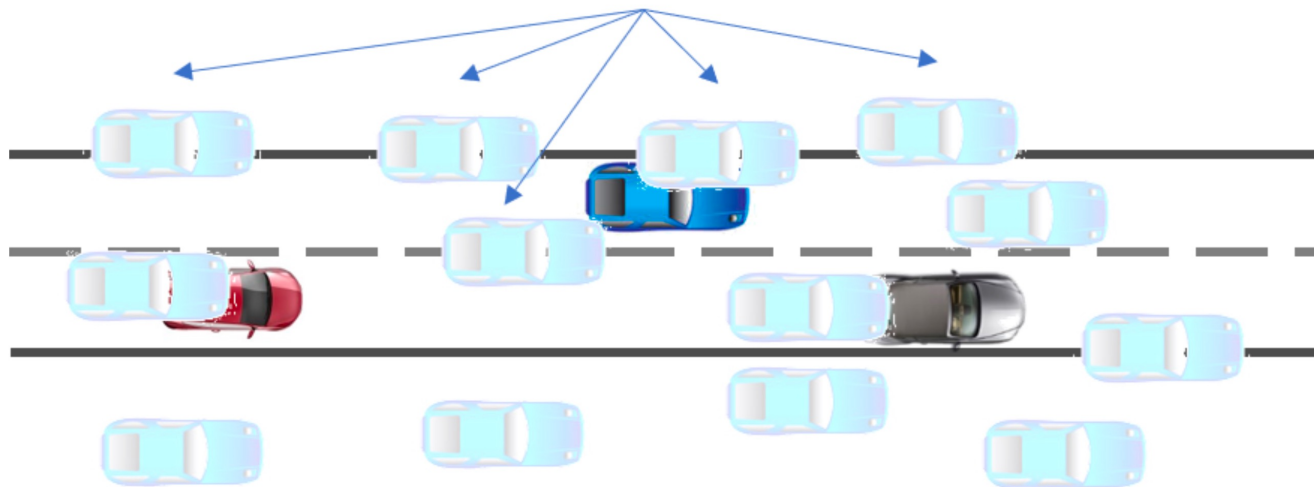
Sybil attack

Ghost vehicles creation



Sybil goals : (a) Traffic congestion

Ghost vehicles creation



Sybil goals : (b) Denial of Service



Contribution

- Research requirements
- State of the art review regarding the requirements defined
- Recommendations for a research methodology that can be considered in future works
 - Provision of one dataset for an urban scenario and another dataset for a highway scenario
 - Provision of network model
 - Provision of attack models (three realistic attack scenarios)



Contribution: Research requirements

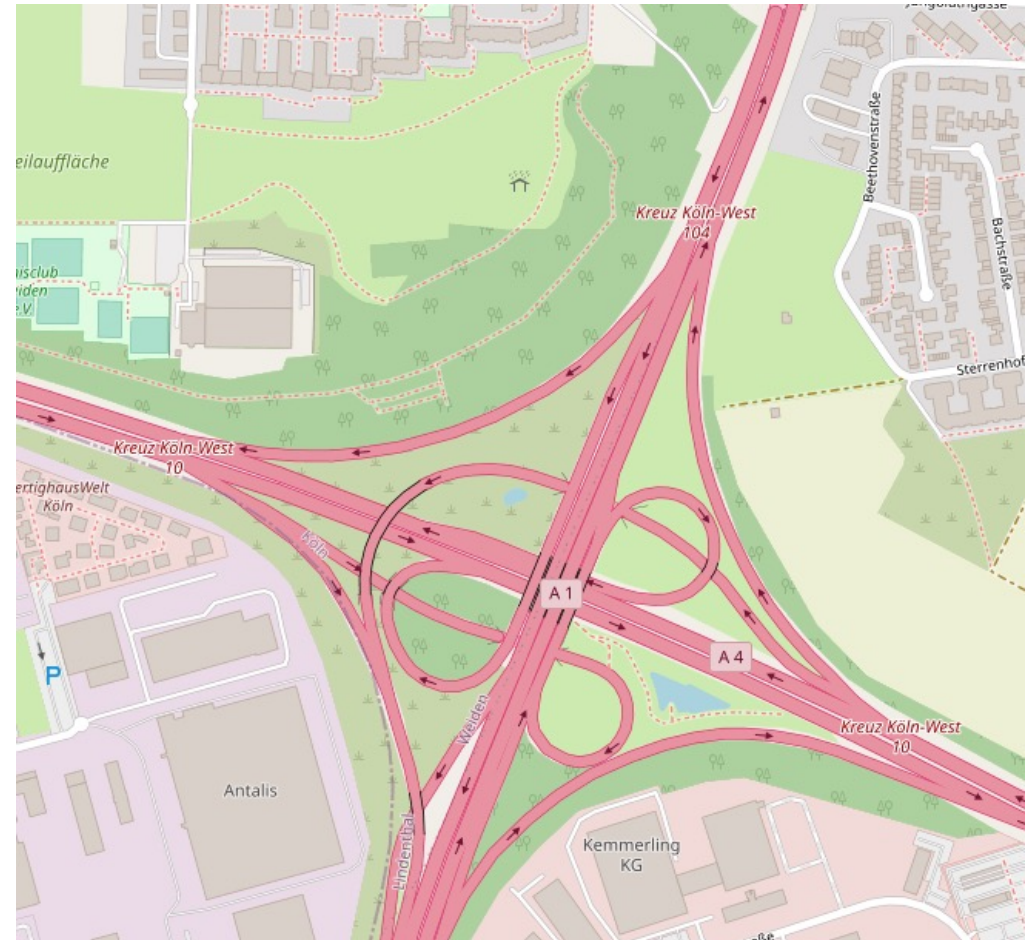
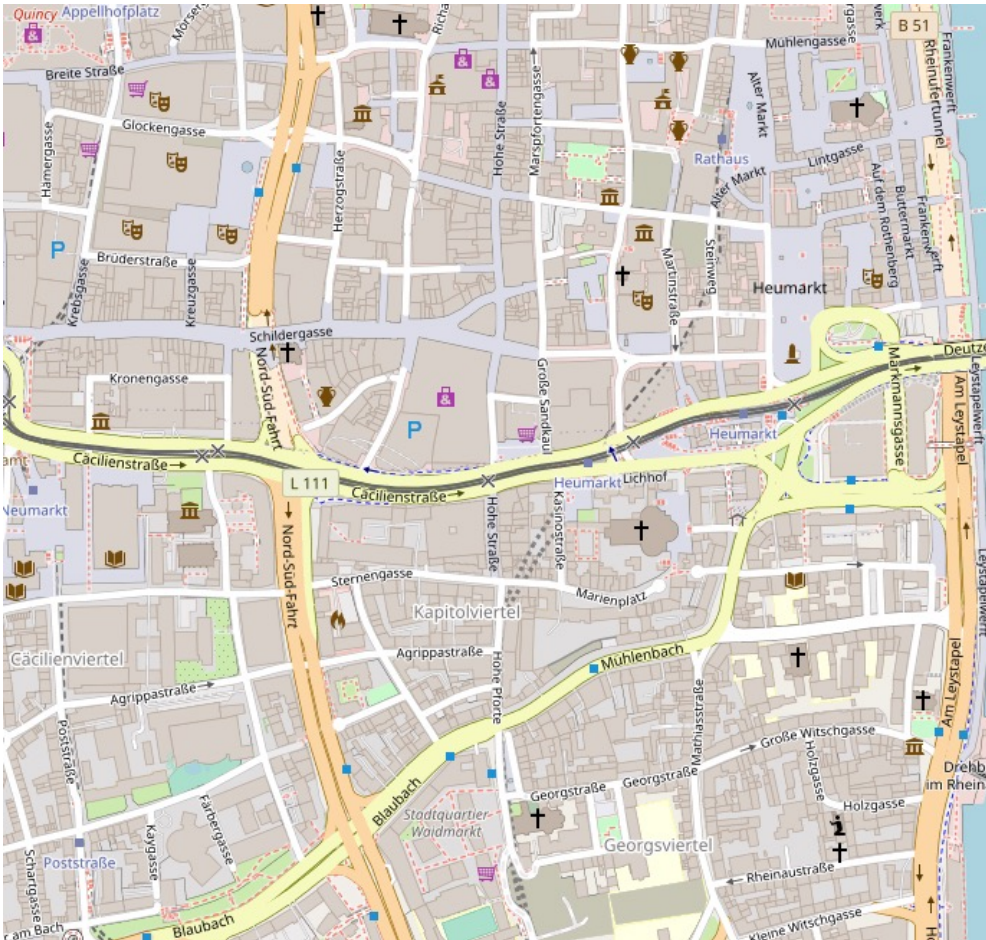
- The proposal of a sybil detection solution that requires the complete modification of the messages structures or their replacement by other structures cannot be considered
- The proposal of a solution that requires a new security architecture or security mechanisms different from the standards cannot be considered
- An approach that relies on a station's history or assumes that a station does not change its identity multiple times during a journey, cannot be considered
- If the history of the vehicle must be considered in the detection process, the linkage of the different PCs must be provided by the Linkage authority while adhering to the PKI disclosure policies



Contribution: State of the art analysis

- Scalability issues
- Do not meet privacy and non-tracking requirements
- Do not satisfy the requirements of current standards (formats of messages, security, and PKI architecture)
- Limited evaluations where only few use case scenarios (such as single lane) were tested

Contribution: recommendations: Network model

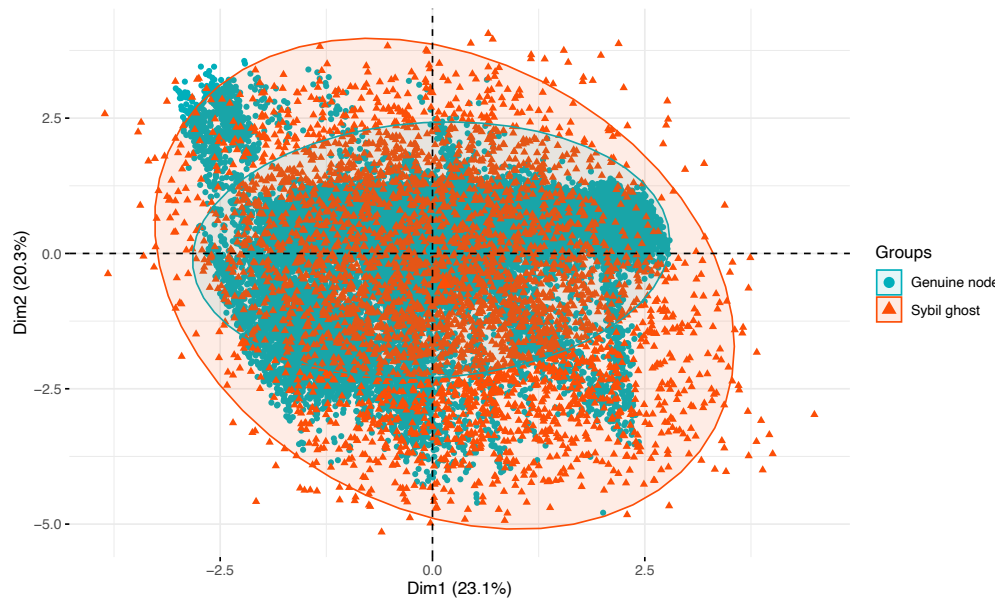




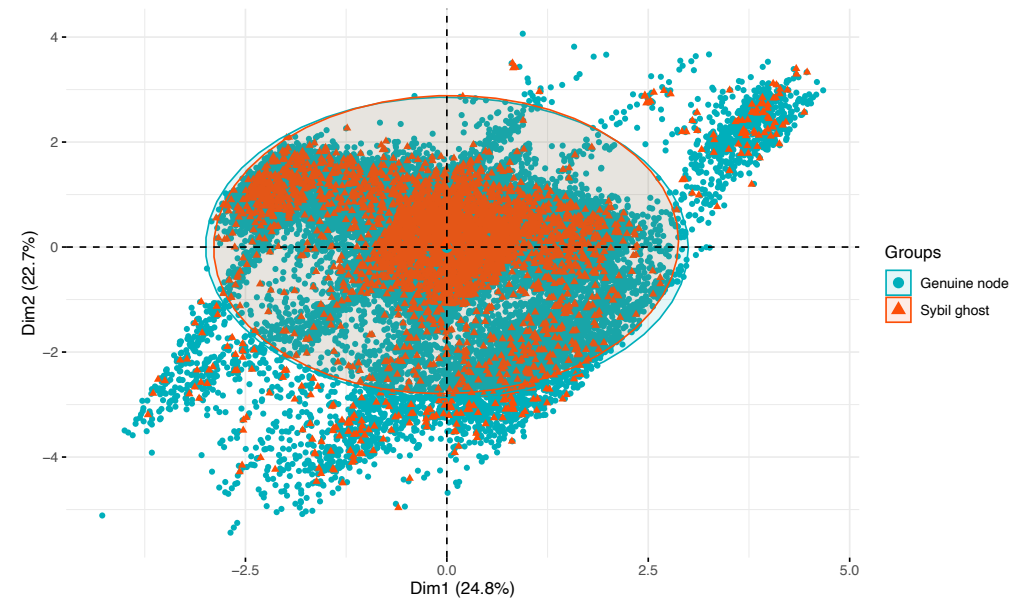
Contribution: recommendations: Attack scenarios

- Sybil scenario with random values
 - Chosen locations from other messages
- Sybil scenario with static values
- Sybil scenario with replayed values

Attack scenarios: statistical characterization



Random scenario



Replayed scenario



Conclusion

- A **position paper** is an essay that presents an arguable opinion about an issue – typically that of the author or some specified entity. Commonly, such a paper will substantiate the opinions or positions put forward with evidences from an extensive objective discussion of the topic.



Future works

- The proposal of a sybil detection approach that cope with different needs and requirements
- The proposal of a fully distributed sybil detection approach that can address scalability issues