Security of Vehicle to Vehicle Communication Networks

By-
Krishna Nikhila Kalinga and Daniel May

INTRODUCTION

- Vehicle-to-Vehicle (V2V) communication systems (VANETs) lets automobiles communicate to each other, roadside infrastructures and other road users, over a wireless network.
- Uses technologies such as Wi-Fi, 4G cellular and 5.9GHz Dedicated Short Range Communication (DSRC).
- Provides: Collision avoidance, Post - Crash assistance, better driving experience etc.

Fig. 1. B. Howard, "V2V: What are Vehicle-to-Vehicle Communications and How do They Work?", *ExtremeTech*, 2015. [Online]. Available: http://www.extremetech.com/

OUTLINE

- What is a V2V Network
- V2V Security System
- Security Attacks
- Encryption Algorithms
- Potential Methods for Message Authentication and Location Privacy
- Conclusion

What is a V2V Network

- A network consisting of nodes made of CANs and roadside infrastructure
- V2V uses an ad-hoc mesh network structure(VANET) where each node (car, roadside infrastructure) can transmit and receive signals.
- Applications of V2V technology are Electric Brake Lights, Platooning, Traffic Information Systems.

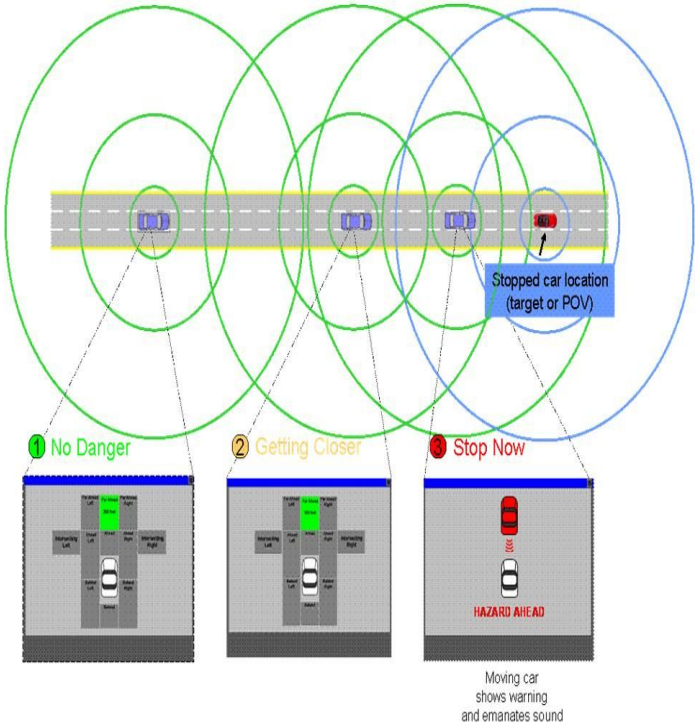


Fig. 2. DENSO Dynamics, "All About V2X: Talking Car Technology", 2015. [Online]. Available: http://www.densodynamics.com/

V2V SECURITY SYSTEM

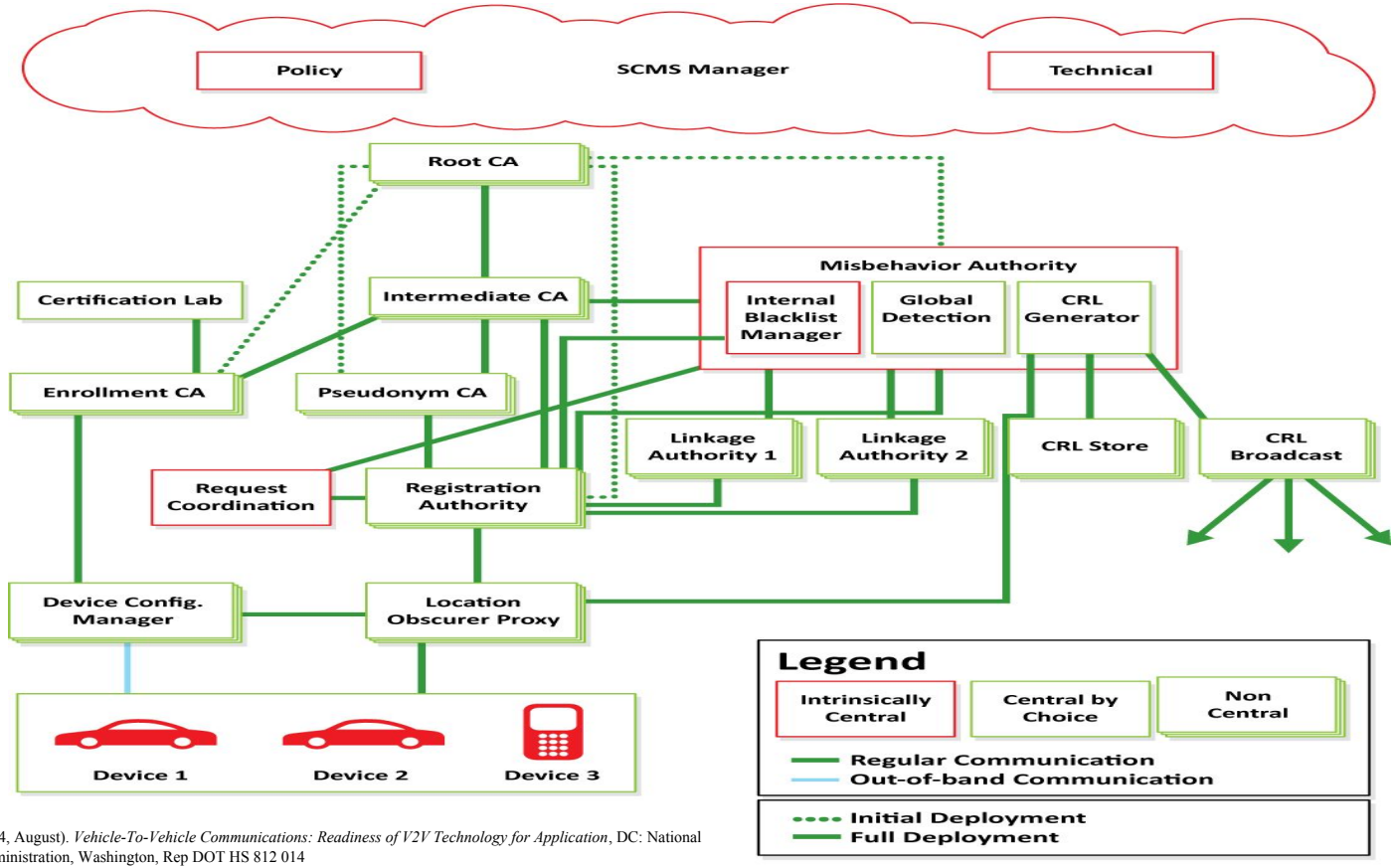
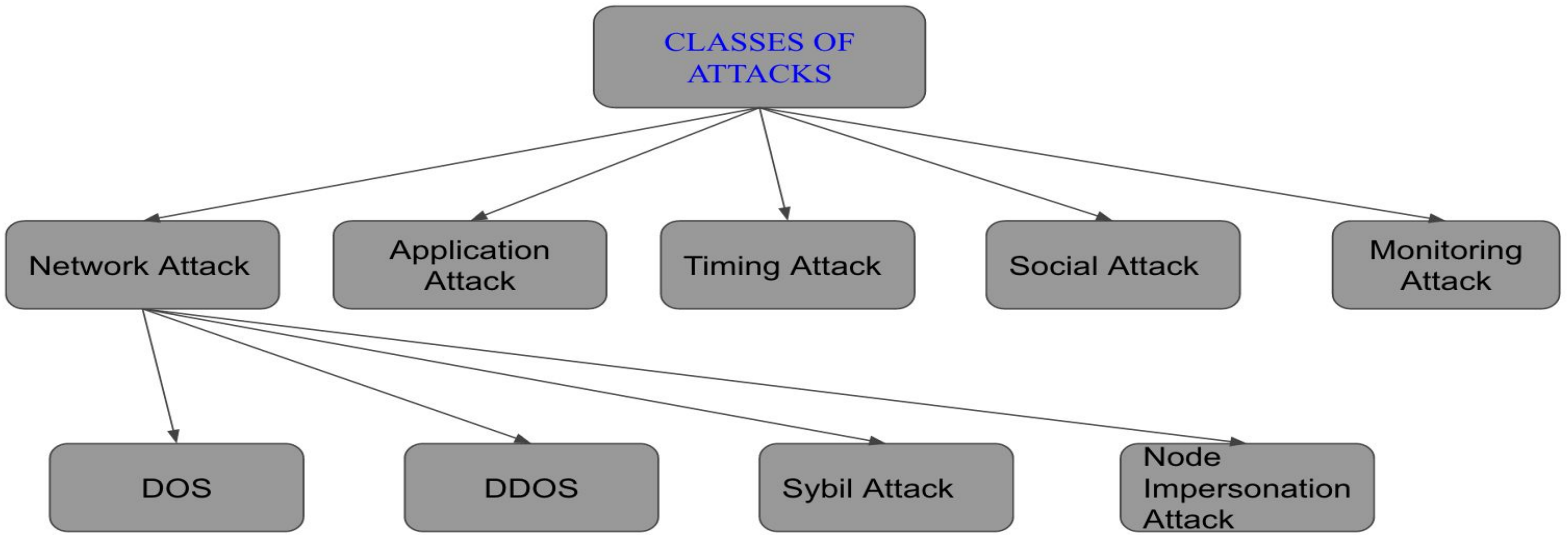


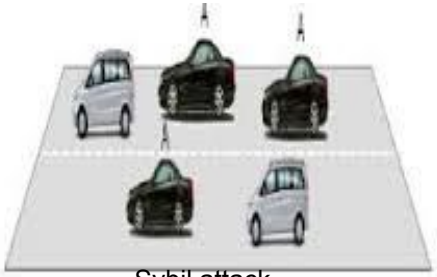
Fig. 3. J. Harding et al. (2014, August). *Vehicle-To-Vehicle Communications: Readiness of V2V Technology for Application*, DC: National Highway Traffic Safety Administration, Washington, Rep DOT HS 812 014

SECURITY ATTACKS

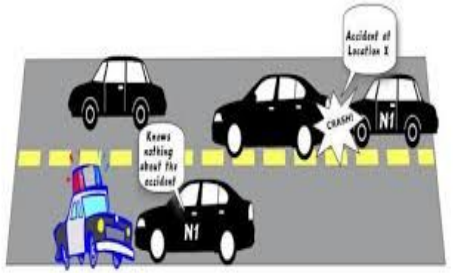


DOS-Denial of Service
DDOS- Distributed Denial of Service

SECURITY ATTACKS (ctd.)



Sybil attack

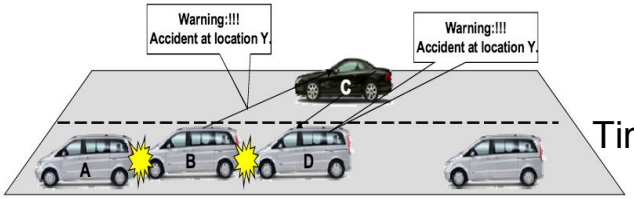


Node Impersonation Attack

Fig. 5. Fig. 6. I. Sumra, I. Ahmad, H. Hasbullah and J. bin Ab Manan, 'Classes of attacks in VANET', in *Electronics, Communications and Photonics Conference (SIECPC)*, Saudi International, 2011.

- NETWORK ATTACK
  - Directly affects vehicle and infrastructure.
    - Denial of service
      - Main goal is to prevent authentic users from accessing the network services
    - Distributed Denial of service
      - Main goal is to bring down the network
    - Sybil attack
      - Attacker creates multiple vehicles on the road with same identity.
    - Node impersonation Attack
      - Attacker changes identity
- APPLICATION ATTACK/FORGED MESSAGE ATTACK
  - Send wrong messages to affect the user's behavior and can cause accidents. For example can change "Work Zone Warning" to "Road is clear"

SECURITY ATTACKS (ctd.)



Timing Attack

Fig. 7. I. Sumra, I. Ahmad, H. Hasbullah and J. bin Ab Manan, 'Classes of attacks in VANET', in *Electronics, Communications and Photonics Conference (SIECPC)*, Saudi International, 2011.

- TIMING ATTACK
  - Objective is to delay the original message such as warnings.eg: delaying a warning for accident, which causes the victim to become part of the accident
- SOCIAL ATTACK
  - Indirectly create problems in the network.
- MONITORING ATTACK
  - Monitoring and listening to V2V and V2I communication
  - Tracking vehicles based on unique identities
- REPLAY ATTACK
  - A message is replayed at a later time.

SECURITY REQUIREMENTS

- Every message must be protected against forgery
- Every message must include an authenticated time-stamp (accurate to at least a millisecond) and an authenticated geographic location of the sender's origin.
- A vehicle must be able to change (or randomize) any identifiable property simultaneously (pseudonym, MAC address, as well as network and security protocol related states).
- DSRC messages must not include publicly known identifiers of vehicles.

ENCRYPTION ALGORITHMS

SYMMETRIC KEY ENCRYPTION:

- SEED
- Camellia
  - Applied in IPSec and OpenPGP
- CAST-128
  - Default ciphers in some versions of GPG and PGP, immunity against differential and linear cryptanalysis attacks
- Blowfish
  - Unpatented and license free, fastest, compact and simple.
  - Key dependent S-boxes are generated using cipher.
- AES
- DES

ASYMMETRIC KEY ENCRYPTION:

- RSA
- Elliptic Curve Cryptography
  - Similar functionality to RSA
  - Requires less computing power and memory, uses smaller keys

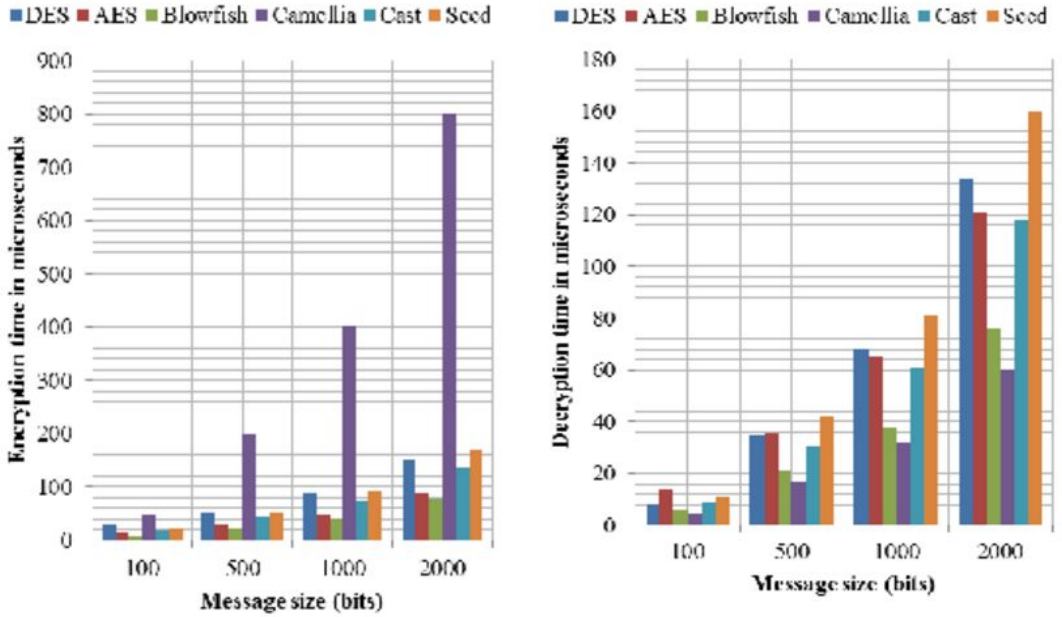


Fig. 8. M. Alimohammadi and A. Pouyan, 'Performance Analysis of Cryptography Methods for Secure Message Exchanging in VANET', *International Journal of Scientific & Engineering Research*, vol. 5, no. 2, 2014.

Potential Methods for Message Authentication

CERTIFICATE EXCHANGE BETWEEN VEHICLES		
Certificate with each message	Periodic broadcast of certificates	Certificate exchange on demand
1) Receiver has a list of trustworthy certificates 2) Receiver verify sender's certificate before verifying message. 3) Presence of OTA overhead causes congestion	1) To reduce Over The Air (OTA) overhead 2) Certificate may not be available before message 3) Not used in emergency warnings	1) A sends its certificate along with identification, B sends its certificate after receiving A's certificate. 2) A and B can request other party certificates

Potential Methods for Message Authentication (ctd.)

Verification on Demand:

1) The criteria when to perform a signature verification does not need to be globally defined, but it can be individually fixed per implementation.
2) Relieves the security module from its heavy load of verification,
3) Allows flexible balancing of verification load.
4) Stays easily compatible with future generation implementations and allows quick deployment

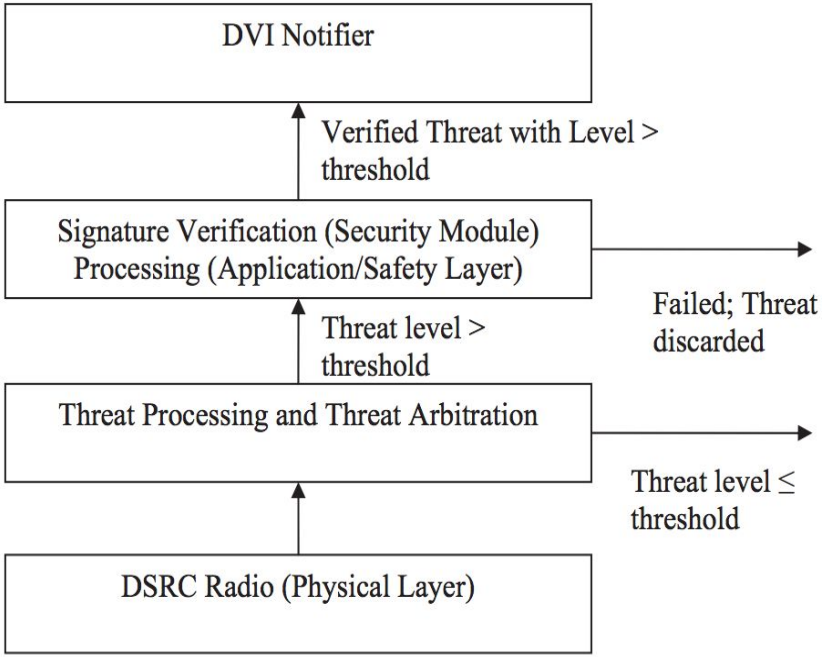


Fig. 10. National Highway Traffic Safety Administration, "Vehicle Safety Communications – Applications (VSC-A)", Department of Transportation, Washington, 2011.

Potential Methods to Provide Privacy

- Change of Identifiable Properties
  - based on DSRC properties such as transmission range, messages per second, speed of the vehicle
  - change pseudonym when there are many cars where it is hard for DSRC radio observer to distinguish the different vehicles
  - Implement multiple certificates
- Use random identifiers to implement pseudonyms via random number generator
- Provide vehicles with ability to change pseudonyms/certificates

Conclusion

- Complex network due to mobile nodes
- Privacy is a major concern
- Increase in security threats as vehicles can talk to Road Side Units
- Blind spot detection, automatic braking system, platooning, autonomy would make driving safer
- V2V can save money and lives