Securing Vehicular Ad Hoc Networks: A Research Survey

Chin-I Lee
Ling Tung University

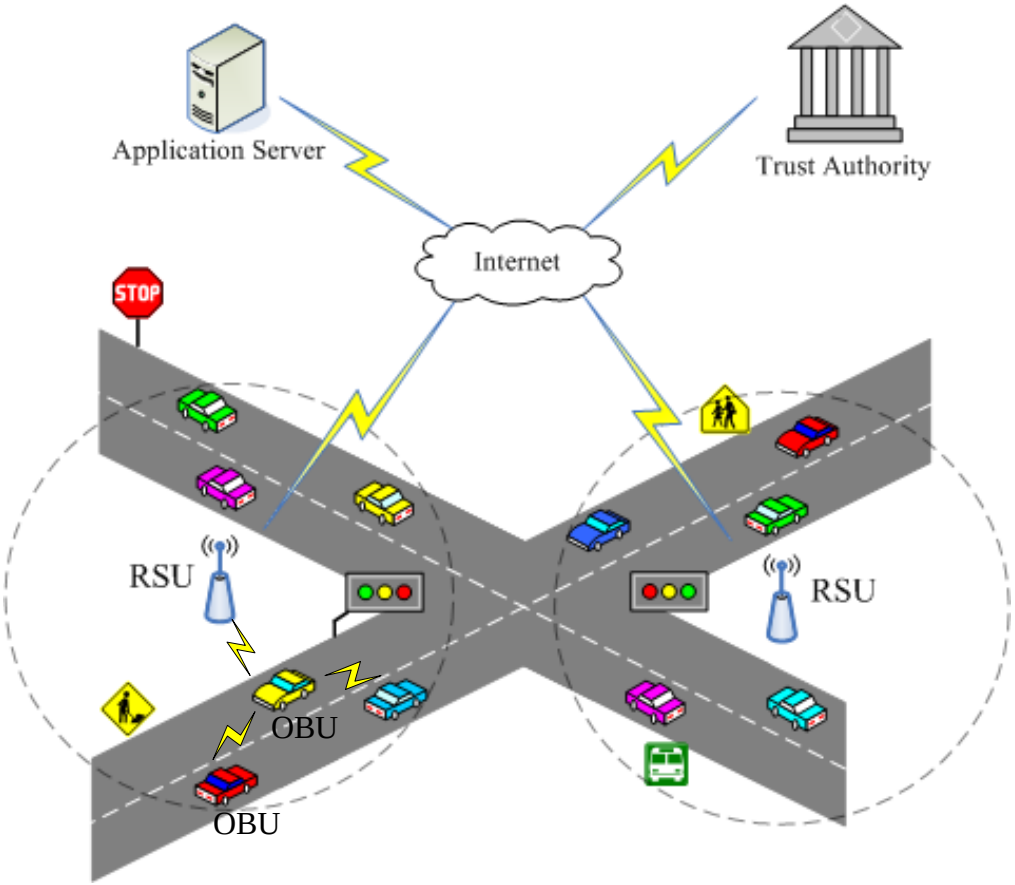
2011/05/27

Outline

- What is a Vehicular Ad Hoc Network(VANET)?
- Problems and Security requirements
- Related work
- Discussions and Conclusions

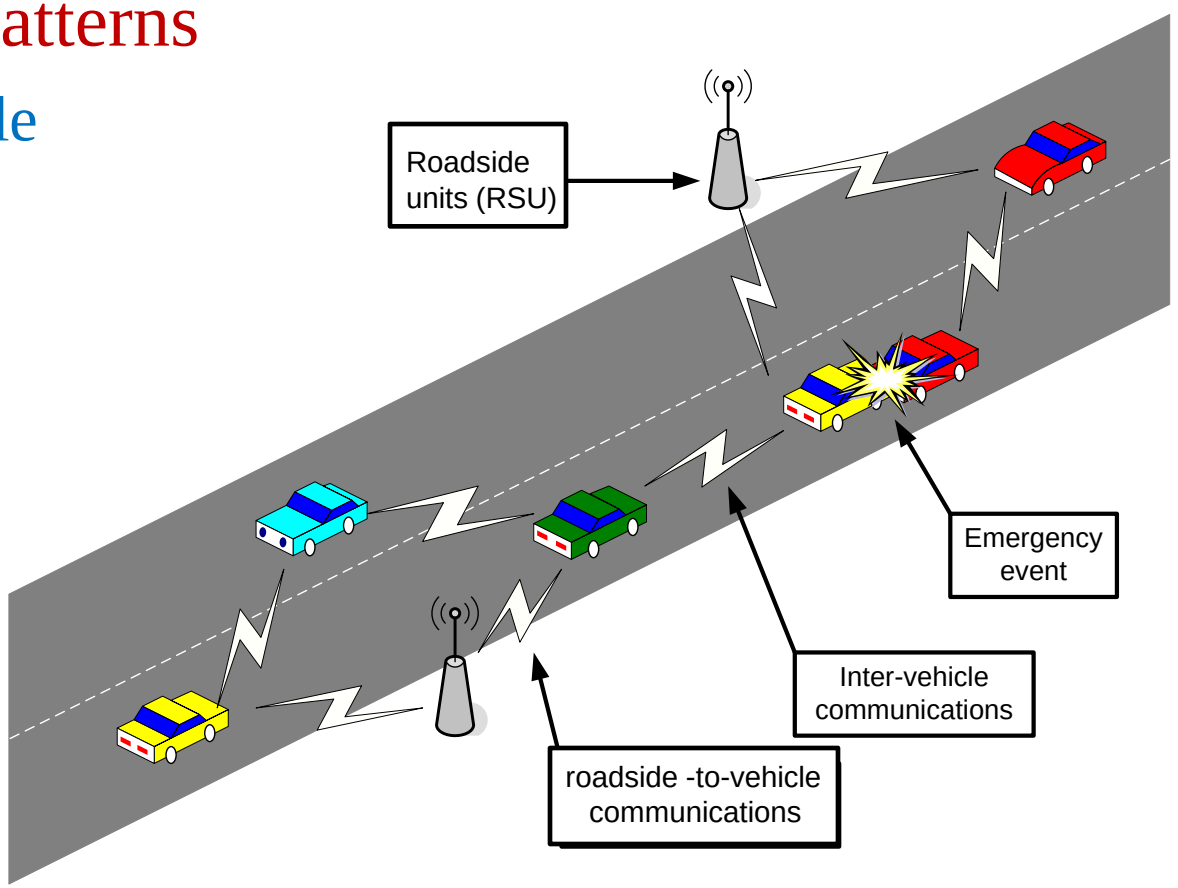
What is a Vehicular Ad Hoc Network (VANET)?

- VANET
  - OBU (On-Board Units)
    - communication devices mounted on vehicles
  - RSU (RoadSide Units)
    - communication units located aside the roads
  - OBU used to communicate with other vehicles or RSUs
  - RSUs connect with application servers and trust authorities



What is a VANET? – Cont.

- Communication patterns
  - Roadside-to-Vehicle Communications (RVC or V2I)
  - Inter-Vehicle Communications (IVC or V2V)



Why do we need VANETs?

- Safety is the primary incentive
  - 1960s - safety goal led to the seatbelt
    - Survive the crash
  - 1980s - safety goal led to the airbag
    - Survive a worse crash
  - 2000s - safety goal enabled by new technology
    - Eliminate the crash
- Infotainment applications
  - Traffic information, location of gas stations, Internet access

DSRC (Dedicated Short Range Communications) is the heart of the technology advance

Introduction – DSRC

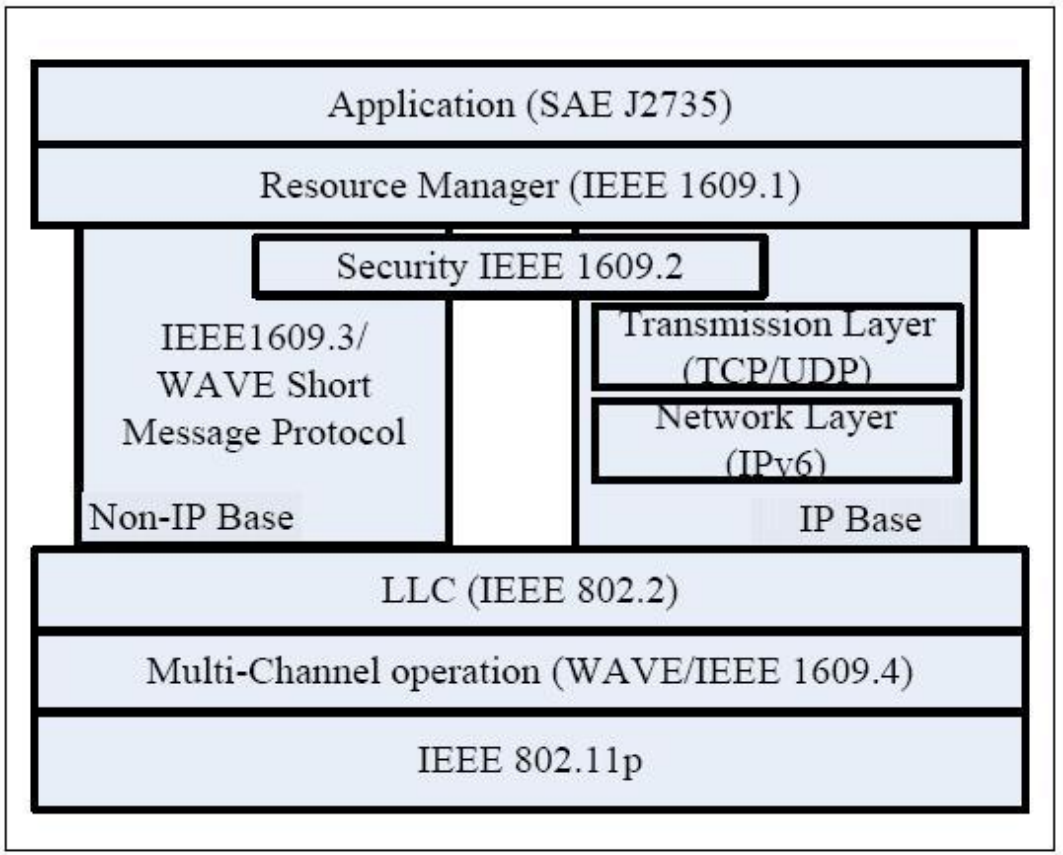
- A short range communication system for safety and infotainment applications in both roadside-to-vehicle and vehicle-to-vehicle environment

- Designed to provide the high data transfer rates and minimum latency in the communication link

- Federal Communication Commission allocated 5.9 GHz band (5.850-5.925 GHz) for DSRC to be used by Intelligent Transportation Systems

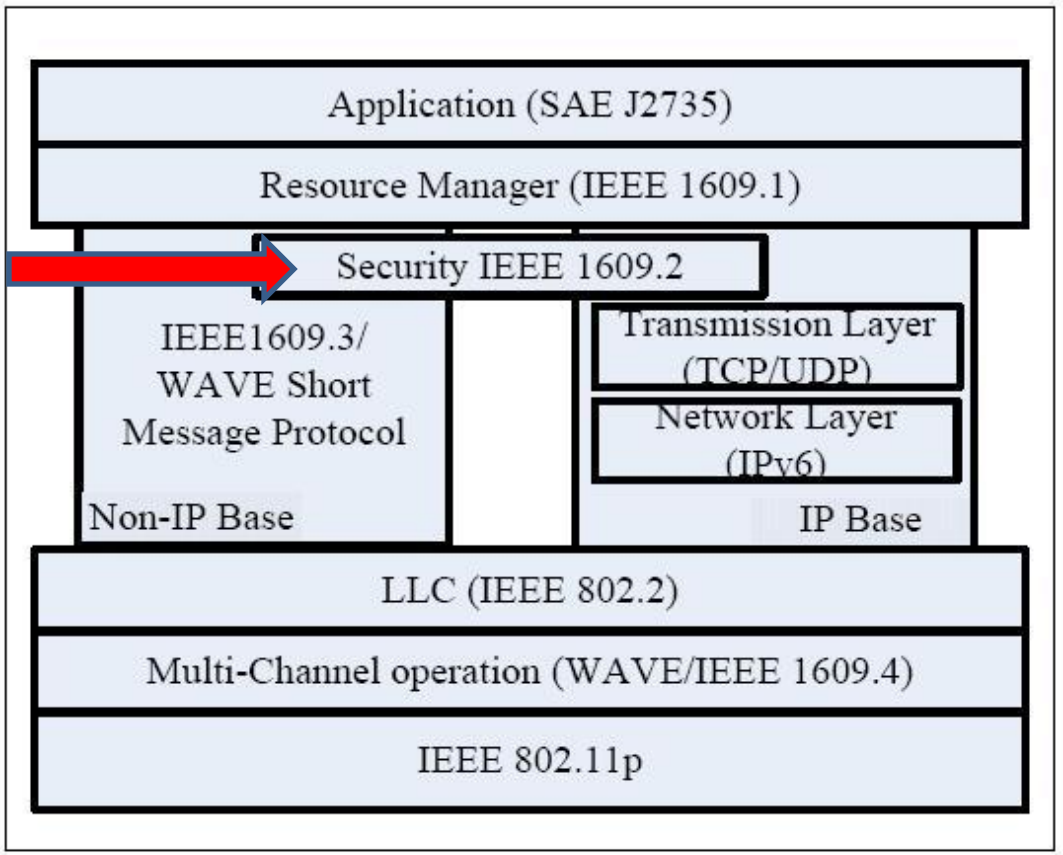
Introduction – 5.9 GHz DSRC

- IEEE 802.11p
  - an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE)
- IEEE 1609
  - a higher layer standard on IEEE 802.11p



Introduction – 5.9 GHz DSRC

- IEEE 1609.1
  - WAVE-Resource Manager
- IEEE **1609.2**
  - WAVE-**Security** Services for Applications and Management Messages
- IEEE 1609.3
  - WAVE-Networking Services
- IEEE 1609.4
  - WAVE-Multi-channel Operations

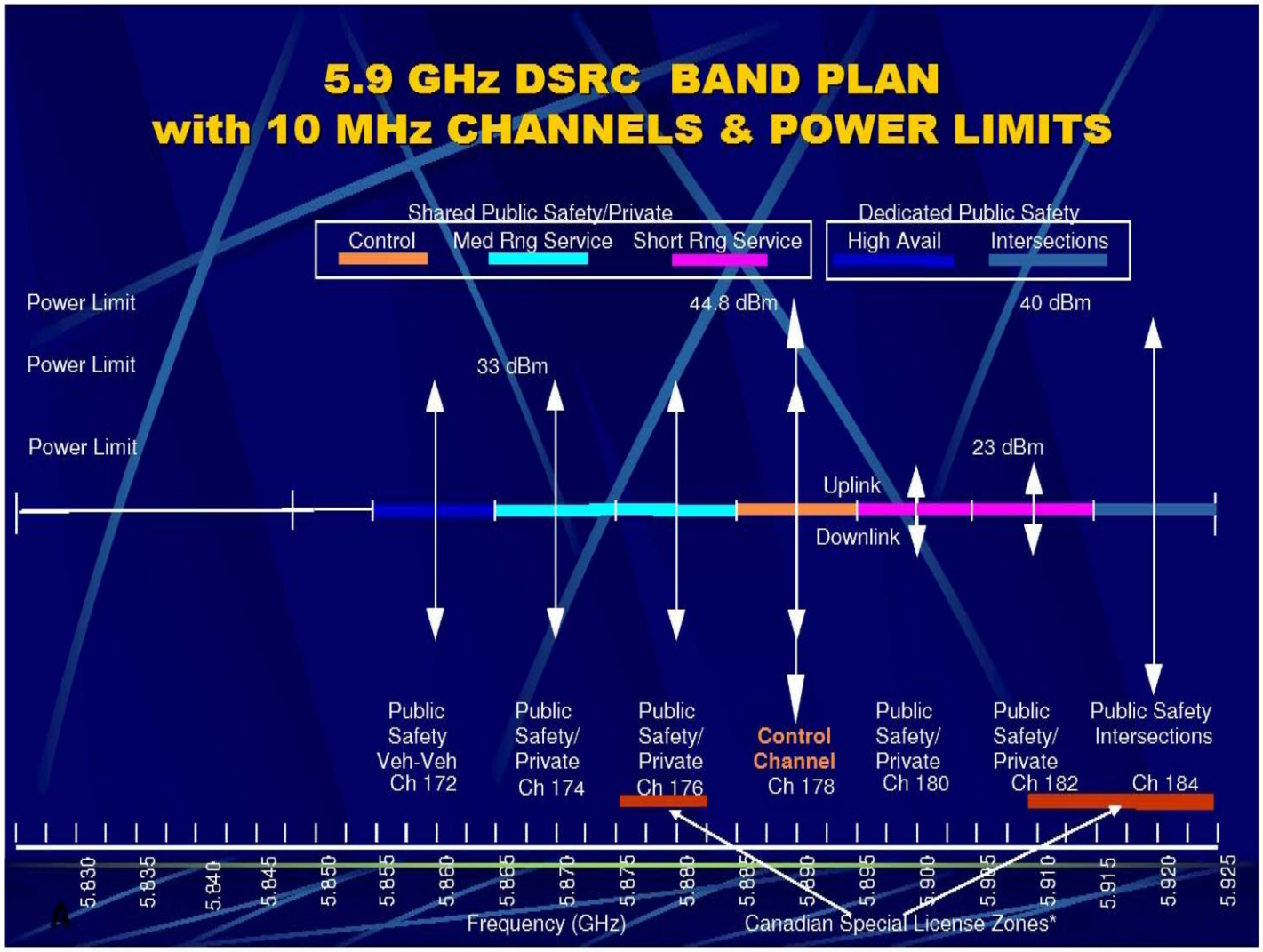


Introduction – IEEE 1609.2

- ***Public key algorithm***
  - All implementations of this standard shall support the signing algorithm ECDSA over the two NIST curves p224 and p256
  - All implementations of this standard shall support the encryption algorithm ECIES over the NIST curve p256

- ***Symmetric algorithm***
  - The only symmetric algorithm currently supported is AES-128 in CCM mode

Introduction – 5.9 GHz DSRC



5.9 GHz DSRC implementation

- Spectrum 75MHZ (5.850-5.925 GHz)
- Channels 7 channels
  (1 control channel, 6 service channels)

- ***Implementation***

Communication range	Data rate	Broadcast period
300 meters	**6 Mbps**	**300 ms**

VANET Characteristics

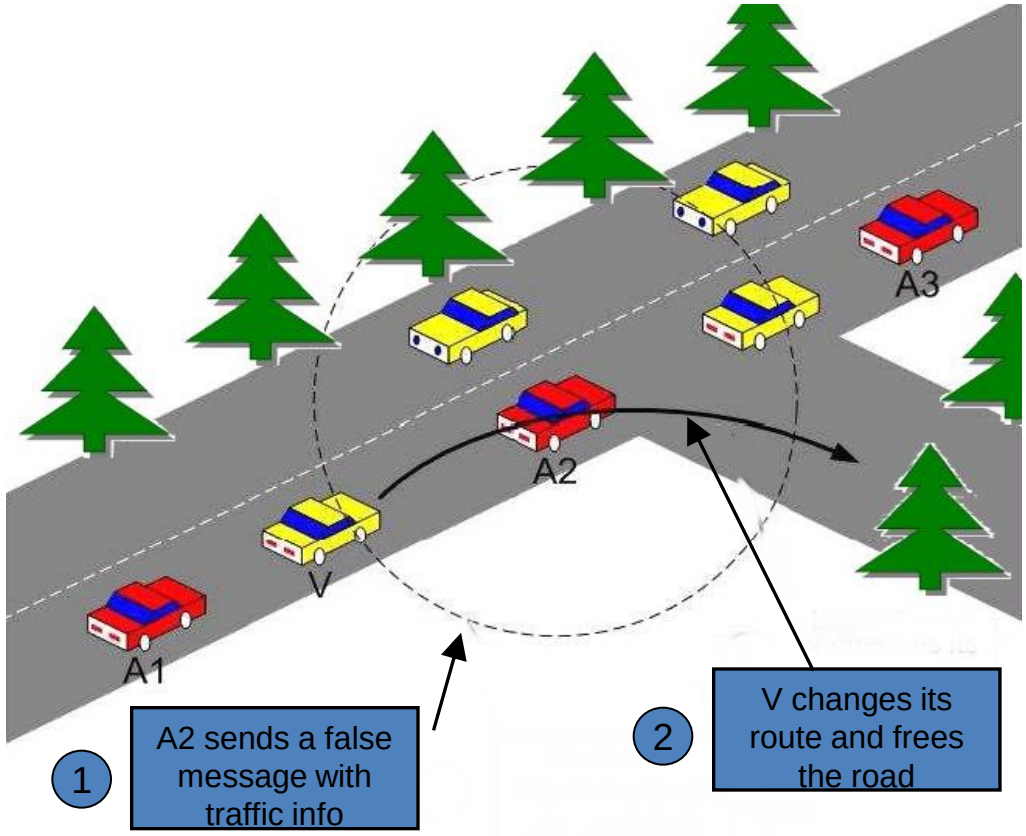
- High mobility nodes
- Critical latency requirements
- No problem with power
- Fast verification of high data amount

Outline

- What is a Vehicular Ad Hoc Network(VANET)?
- Problems and Security requirements
- Related work
- Discussions and Conclusions

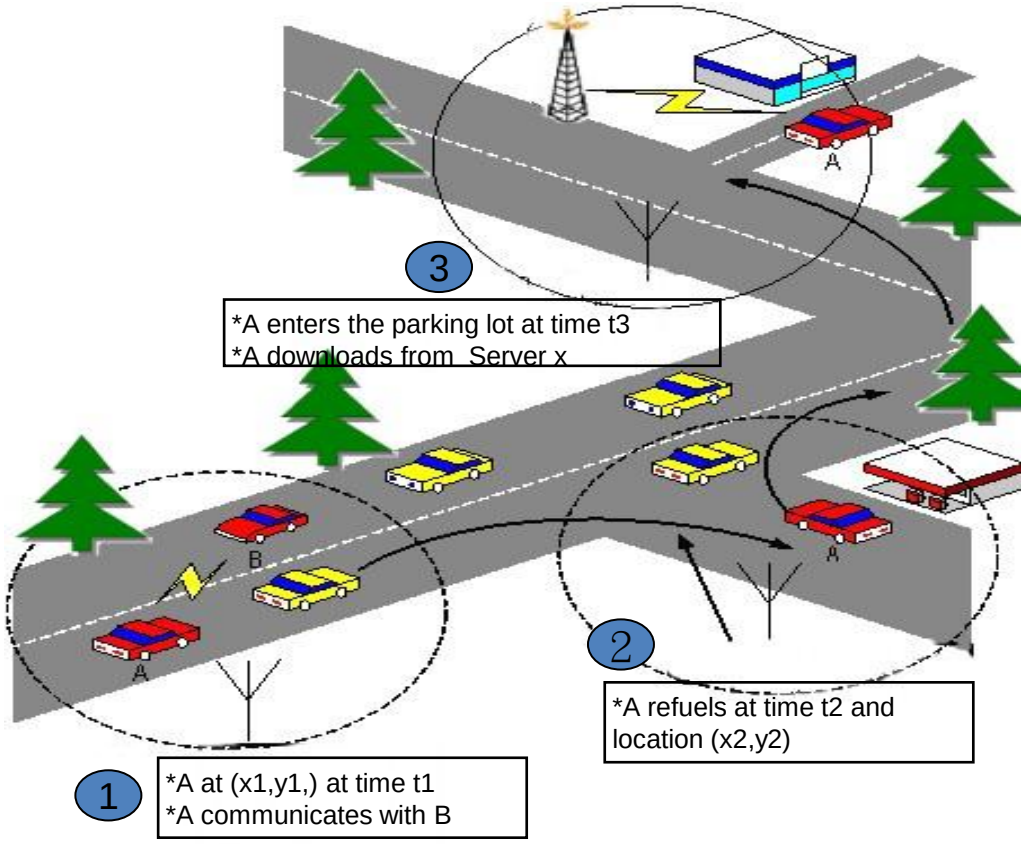
Problems in VANET

- Bogus information
  - Attackers diffuse false information to affect the behavior of other drivers



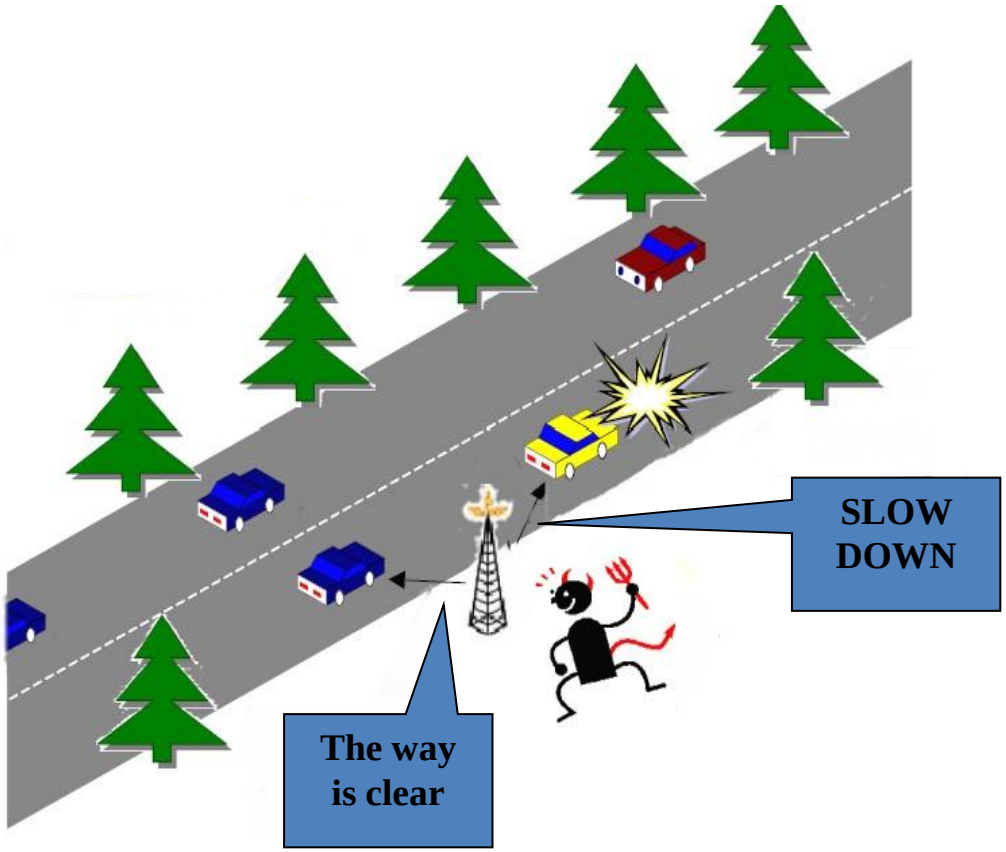
Problems in VANET

- ID disclosure
  - Attackers tracks vehicles to obtain those drivers' private information



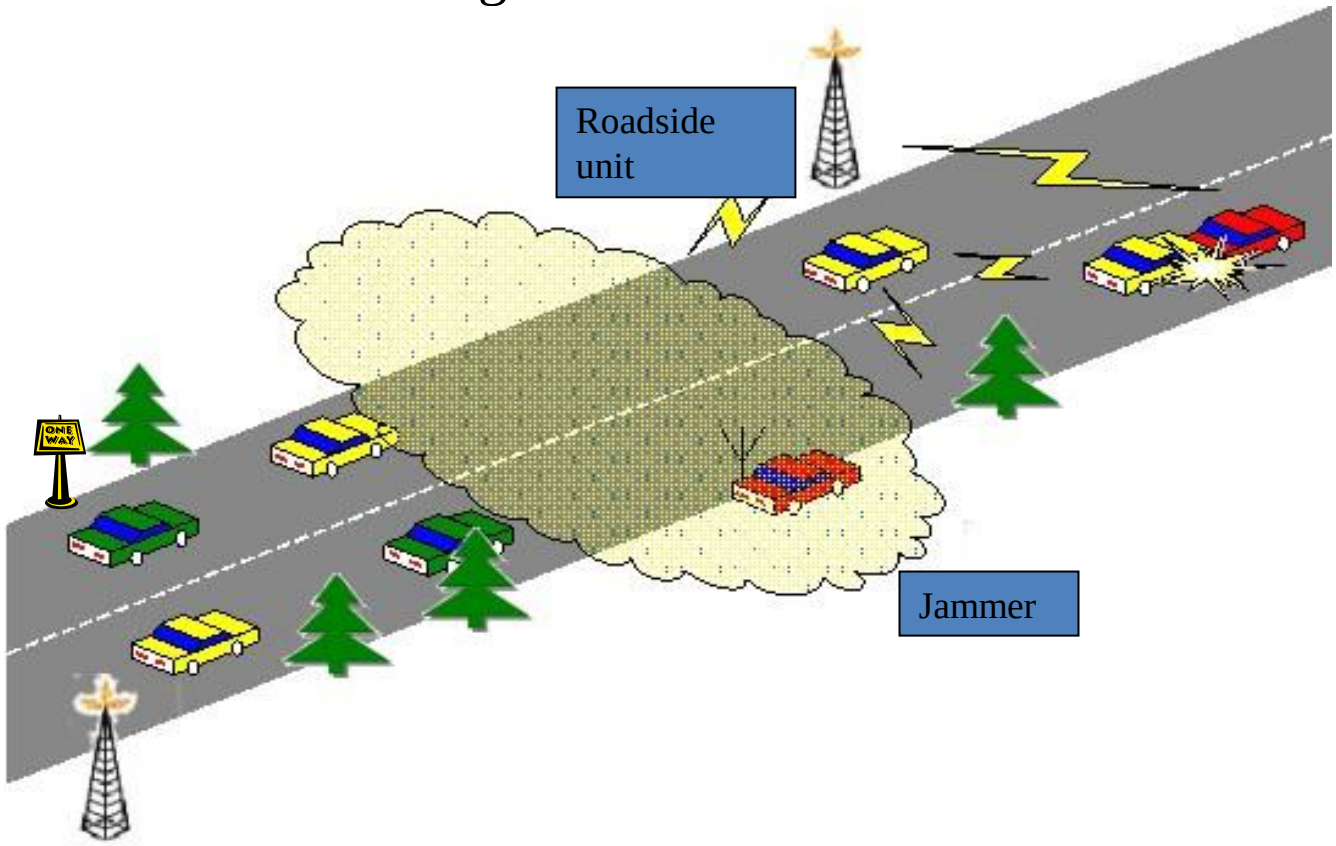
Problems in VANET

- Masquerade
  - Attackers use false identities to pretend another vehicles



Problems in VANET

- Denial of Service
  - Attackers want to bring down the VANET



Security Requirements

- Authentication
  - Authenticate legitimate OBUs and senders of messages
- Message Integrity
  - Ensure data integrity
- Privacy
  - Provide message unlinkability and prevent driver's tracking
- Traceability and revocation
  - Trace and disable abusing OBUs by the authority
- Availability
  - Provide network availability under jamming attacks
- Efficiency
  - Impose low computation and communication overheads due to constraints on time

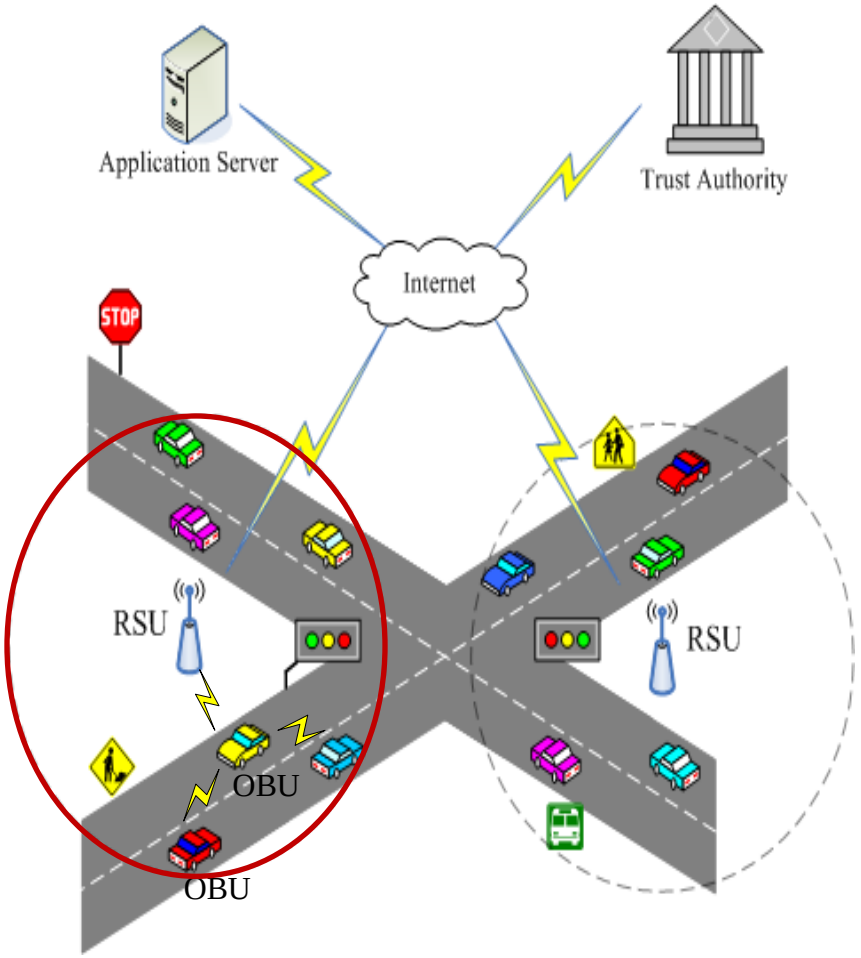
Outline

- What is a Vehicular Ad Hoc Network(VANET)?
- Problems and Security requirements
- Related work
- Discussions and Conclusions

Assumptions

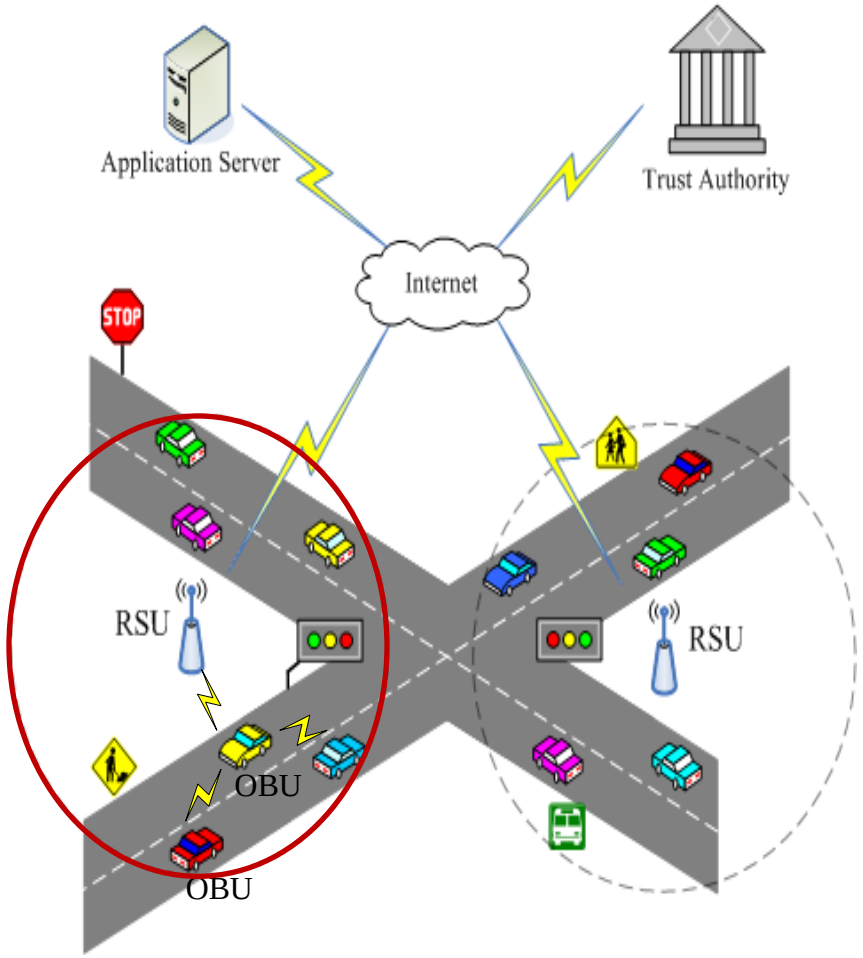
- Roadways are divided into geographic regions

- Trusted authorities
  - Define regions to identify the positions of the RSUs
  - Issue certificates to RSUs and OBUs



Assumptions

- RSUs
  - Act as the regional authorities for their regions
  - Are the tamper-proof devices
  - Get a copy of the authority's public key
- OBUs
  - Know their ***current location***
    - GPS provides enough accuracy
  - Know how to ***contact a RSU***
  - Get a copy of the authority's public key



Related Work – 1

- Public Key Infrastructure (Blum & Eskandarian, 2004…)
  - They use PKI and virtual infrastructure to resist the collisions intentionally caused by malicious vehicles
  - PKI using certificates and fixed public key can authenticate message, identify valid vehicles and remove malicious vehicles
  - OBU signs a safety message using its private key, and then sends the message, signature and its certificate

$$OBU \rightarrow OBU : M, Sig(prk\_OBU, M), cert\_OBU$$

Fixed public keys allow an eavesdropper to associate a key with a vehicle so as to violate driver's privacy

Related Work – 2

- Multiple Certificates Per OBU (Raya & Hubaux, 2007…)
  - Each OBU owns a set of certified public/private key pairs
  - A large set of keys needs to periodically renewed (during regular vehicle maintenance visits)
  - OBUs contact trust authorities through RSUs and send the created pseudonym and public key. Authorities send the built certificates back
  - Each key is used for a short period of time

Suffering from a Sybil attack

- A malicious OBU can pose as multiple vehicles

Large overhead to revoke a OBU

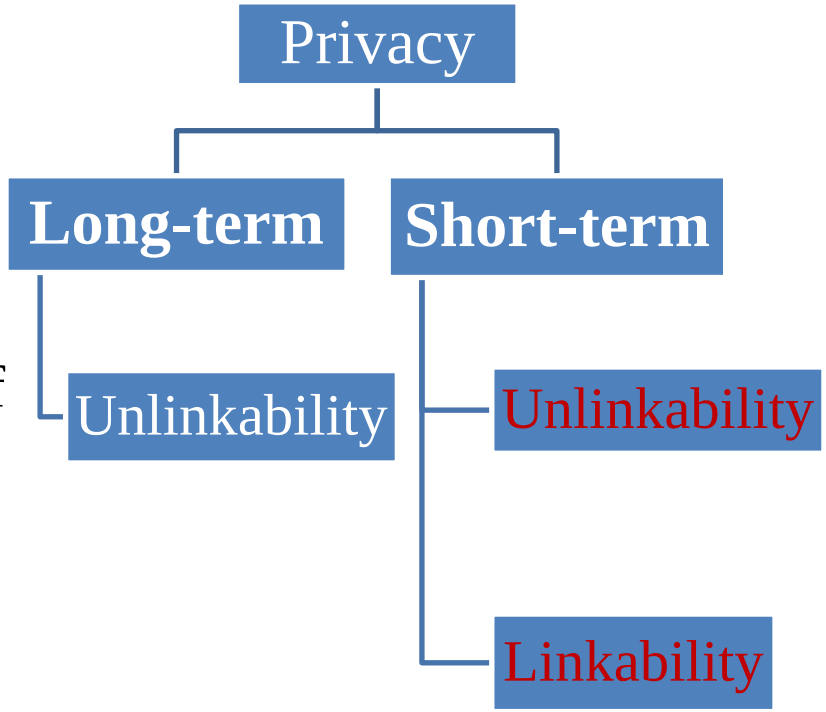
Related Work – 3

- Group Signatures (Lin et al., 2007…)
  - Group signature guarantees the unlinkability of the messages since group member can anonymously sign on behalf of the group
  - OBU uses a group signature to sign a message to prove that the signer is ***a valid OBU*** (***not which OBU***)
  - ***Group manager*** can trace the identity of a signer from the group signature and revoke the group member

Reduce the storage cost of multiple public/ private key pairs and the bandwidth consumption used to transmit the certificate revocation list
Computationally expensive

Security Requirements – Privacy

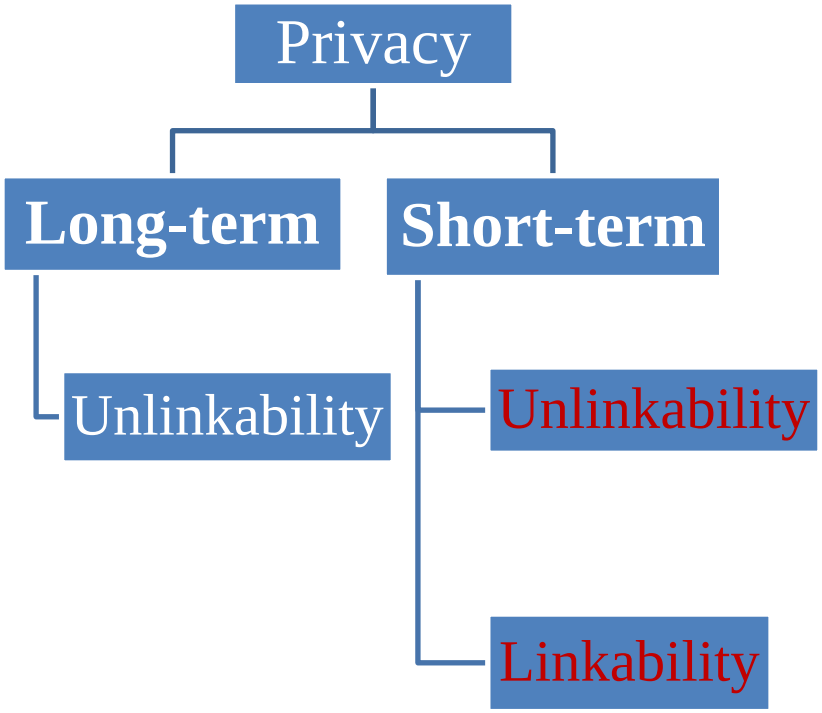
- RSUs act as the regional authorities for their regions
- Long-term unlinkability
  - An attacker cannot identify messages from the same OBU in the communication range of the different RSUs (inter-domain)
- Short-term linkability
  - A OBU can identify messages sent by the same sender in the communication range of the same RSU (intra-domain)



Security Requirements – Privacy

- Short-term unlinkability
  - RVC ➔ Signcryption
  - V2V ➔ Group signature (batch verification)

- Short-term linkability
  - inter-domain ➔ Group signature
  - intra-domain ➔ ECDSA , TELSA



Outline

- What is a Vehicular Ad Hoc Network(VANET)?
- Problems and Security requirements
- Related work
- Discussions and Conclusions

Discussions and Conclusions

- VANET security is an emerging area
- As different VANET protocols and applications are based on different assumptions, a common evaluation framework is needed to compare different security research contributions
- Detection of malicious vehicles is still a challenge
- Multicast source authentication which essentially guarantees that the received data is sent from the claimed source

References

- J. Blum and A. Eskandarian, "The threat of intelligent collisions," IT Professional, vol. 6, no. 1, pp. 24–29, 2004
- R. Chen, D. Ma, and A. Regan, "TARI: Meeting delay requirements in VANETs with efficient authentication and revocation," In Proceedings of WAVE, 2009
- X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442–3456, 2007
- A. Perrig, R. Canetti, D. Tygar, D. Song, "The TESLA broadcast authentication protocol," CryptoBytes, vol. 5,2002
- M. Raya and J. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Secur., vol. 15, no. 1, pp. 39–68, 2007

References

- A. Studer, E. Shi, F. Bai, and A. Perrig, “TACKing Together efficient authentication revocation, and privacy in VANETs,” In Proceedings of SECON, pp. 22–26, 2009
- C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, “ An efficient message authentication scheme for vehicular communications,” IEEE Trans. Veh. Technol., vol. 57, no. 6, pp. 3357–3368, 2008
- C. Zhang, R. Lu, X. Lin, P.-H. Ho and X. Shen, “An efficient identity-based batch verification scheme for vehicular sensor networks,” In Proceedings of INFOCOM, 2008
- L. Zhang, Q. Wu, A. Solanas, D.-F. Josep, “A scalable robust authentication protocol for secure vehicular communications,” IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606–1617, 2010

Thanks for your patience