Vehicular Ad Hoc Networks and Security related issues

2009 Sendai International Workshop on New Information Technologies and Related Health and Welfare Topics

Background on Safety

- In the US:
  - 6x million traffic accidents per year
  - 90% driver errors
  - 43,000 deaths
  - 3 million injuries.
  - Financial cost: $230 billion
- Overall Goal: Reduce traffic accidents
  - Fewer injuries and fatalities
  - Lower direct and indirect cost
  - Reduced traffic congestion
- In Europe:
  - Specific Goal: to reduce the car accidents of 50% by 2010

VANET characteristics

- Vehicular Ad hoc Networks (VANET) have recently become one of the most attractive areas of research, both in academia and industry.
- High mobility, high speed of vehicles, fast topology changes and predictable vehicle movements are the characteristics that make VANET different from other types of ad hoc networks.
- Vehicles communicate with each other via ad hoc routing protocols, or they can exchange data with road infrastructure units.

Some Applications (1/2)

- Collision Avoidance
  - Warn a driver that is not safe to enter an intersection
  - Prevent many vehicle rear-ending each other after a single accident
    - Early braking, Distance keeping and speed management, Lane changing/merging/crossing
- Cooperative Driving
  - Violation warning,
  - Turn Conflict and Curve warning
  - Lane merging warning

  High speed wireless communication: reliable-fast delivery
=> save many lives and prevent injuries

Connecting VANET to Internet: An efficient routing protocol

Motivations

- Unregulated traffic cost much
- Congestion is a big source of waste
  - 3.6 billion vehicle-hours of delay
  - 5.7 billion gallons of wasted fuel
- Improve traffic flow and reduce congestion
  - Smart traffic signals
  - Variable message signs
  - Enhanced transit system
  - Central traffic management
  - Electronic toll collection

Outline

Motivations
Security issues
Optimized Dissemination of Alarm Messages
Connecting VANET to Internet: An efficient routing protocol
Conclusion
Bibliography

DSRC Network Architectures

- a) Distributed mobile multi-hop network
- b) Centralized one-hop network

Some Applications (2/2)

- Traffic Optimization
  - Traffic delay continues to increase: Waste time, specially when peak time travellers
=> Vehicles can serve as data collectors
  - Transmit the traffic condition information: Number of neighbors and their mean velocities
- Payment Services
  - Toll collection: automatic payment
    - Waste time: decelerate, waiting in line, etc.
- Location-based Services
  - Finding the closest fuel station, restaurant, lodge, etc.
Security Requirements

- Detect the actual and not the virtual
  - Sybil attack: an adversary can transmit safety-related packets
    - i.e., falsely identify a road as congested
- Authenticate Message and Detect replay (Timestamp)
- Assure Driver Privacy and Anonymity
- Verify properties of the sender: vehicle, ambulance, traffic sign
- Verify if the sender is actually at the claimed position

Challenges

- Trade-off between authentication and non-repudiation versus privacy
- Nature of VANET
  - High speed
  - Limited amount of time
- Some protocols cannot be employed: voting, consensus and based-reputation
- Sheer scale
  - not for protocols that require pre-stored information about participants
- Opposing incentives of participants
  - Law enforcement agencies vs Drivers

Attacks

- Rational or Malicious
  - Rational – seeks personal benefit, more predictable attack
  - Malicious – No personal benefit, intends to harm other users
- Industrial Insider is a valid user: very harmful
- Snoops: collect information about everybody
- Activeness or passiveness attacks
  - Active: Generates packets, participates in the network
  - Passive: Eavesdrop, track users

Security Requirements

- Integrity
- Non-repudiation
  - Information sent must reflect the actual state and not virtual state
    - Malicious can send notification of abrupt deceleration
  - High availability and strict message delivery deadline
    - Adversaries will always be able to reduce availability: Denial-of-service attacks
    - Real Time guarantees

Mitigating characteristics

- Mobility of VANET can sometimes be beneficial
- Circulation in two opposite directions
- Well specified limits: road, motorway, determined number of lanes, etc.
- Normally, no need of Confidentiality
- Not limited in power: complex cryptographic operations
- All vehicles are to be registered in a central authority
- Vehicles can leverage their knowledge from the driver’s response

Some Solutions 1/5

- Security Hardware
  - Event Data Recorder (EDR)
    - Record all emergency-related information received: position data, speed data, acceleration data, time, etc.
  - Tamper-Proof device (TPD)
    - Provide the ability of processing
    - Verifying and signing messages
    - Hardware protection: a set of sensors to detect hardware tampering
    - Own battery, own clock,
    - High cost++

Some Solutions 2/5

- Authentication
  - Digital Signature (DS)
    - Symmetric cryptography is not suitable
      - messages are standalone, large scale, non-repudiation requirement
    - So, cryptosystem based on public-private key pairs
    - Issued by a CA, trusted certification authority
    - Each message should be signed with a DS + Timestamp/replay
    - One-way cryptographic function: message space -> hash-codes of specific size
    - Liability-related messages should be stored in the EDR

Some Solutions 3/5

- Non-repudiation
  - Vehicle identification
    - A single unique identity (UI)
      - Manufacture: Electronic License Plate
      - Government: Electronic Chassis Number
      - A CA can store a mapping between the UI of the vehicle and the set of public keys
      - Save anonymity of drivers
Some Solutions 4/5

- Authentication of aggregated data
  - Emergency road condition warning applications: significant overhead
- Message related to the same road condition
  - Fusion, extrapolation, etc.: Some theories
  - Reduce overhead: redundant transmissions

Some Solutions 5/5

- Group formation and Communication
  - Predefined? specific vehicles are part of specific group
    - Rigid and not scalable => not suitable for VANET
  - Dynamic?
    - Vehicles form groups based on “how close they are” or “what their driving pattern”
- Difficult issue:
  - Overhead of group formation must be very small: group of small amount of time

Optimized Dissemination of Alarm Messages

Safety-related application

Defer Time Distance

Connect to Internet: An efficient routing protocol

Connecting VANET to Internet

VANET II (VANET Internet Integration) is a new approach to discover gateways and to create routes to them.

There are three phases that are supported by VANET II:

- Agent (gateway) discovery
- Route selection
- Handing the connection to the new gateway.

The aims:

- Reduce the overhead during the gateway discovery process
- Select the most stable route to gateways
- Perform seamless handovers.
Connecting VANET to Internet
VANET II: Proposed protocol

- VANET II network is composed of two types of nodes:
  - vehicles that are stationary or mobile, and
  - gateways that are considered stationary.
- Each vehicle is equipped with a positioning system, e.g., GPS, allowing it to obtain its location.
- The coordinate of a vehicle \(u\) is denoted as \((x_u, y_u)\). Each vehicle is also able to calculate its speed, \(v_u\), and direction, \(\delta_u\).
- Links between vehicles are established if the distance between them is less than their transmission range \(R\).

Connecting VANET to Internet
VANET II: Proposed protocol

Stability metric

- Link Expiration Time (LET) duration of the time when tow nodes will remain connected.
- Let \((x_i, y_i)\) and \((x_j, y_j)\) be the coordinate of the vehicles \(i\) and \(j\) which are moving in direction \(\theta_i, \theta_j\) \((-\pi < \theta < \pi\) with the speed of \(v_i\) and \(v_j\). We can estimate the amount of time they will stay connected, LET, as follows:

\[
LET_{ij} = \frac{\sqrt{(a^2 + c^2 - b^2)}}{v_i v_j \cos \theta_i \cos \theta_j} \frac{1}{d}
\]

Where:
- \(a = v_i \cos \theta_i - v_j \cos \theta_j \)
- \(b = x_i - x_j \)
- \(c = v_i \sin \theta_i - v_j \sin \theta_j \)
- \(d = y_i - y_j \)

Connecting VANET to Internet
VANET II: Proposed protocol

Stability function:

\[
S = 1 - e^{-\frac{LET}{\alpha}}
\]

Where: \(\alpha\) is a constant that defines the rate at which the function is rising; the lower is \(\alpha\), the faster the function rises as shown in Graph.

Connecting VANET to Internet
VANET II: Proposed protocol

With analytical studies, we compute \(\alpha\), and then the stability function will be:

\[
S = 1 - e^{-\frac{LET}{\alpha}}
\]

Duplications: What happens if two nodes have the same stability function value? We need to introduce a second function to eliminate duplications.

We will take into account the progress that the packet has made in the opposite direction of the movement:

We define the second function as follows:

\[
P = \frac{\cos(\theta - \theta_j) \sin \delta_j}{\sqrt{d}}
\]

Connecting VANET to Internet
VANET II: Proposed protocol

We should combine \(S\) and \(P\) together. However, \(P\) should not be as effective as \(S\) for next hop selection. We take advantage of weighted mean to reduce the effect of \(P\) in the final function:

\[F = \alpha \times S + (1 - \alpha) \times P\]

For the contention in our protocol we select the timer runtime as:

\[t(F) = \tau(1 - F)\]

Where \(T\) is the maximum forwarding delay. We will be sure that the next hop will be the one with the longest lifetime and the largest progress in the opposite direction of the packet.
Connecting VANET to Internet
VANETII: Performance evaluation

With $\alpha = 0.8$, maximum speed 30m/s; effect of changing node densities ...

Conclusion

- We presented Security issues of vehicular networks
- We proposed:
  - ODAM, a protocol for disseminating alarm messages
  - VANETII, a protocol for connecting VANET to Internet
    - predictive gateway selection scheme, which uses vehicles movement parameters to select the path with longest life time by predicting the future location
- Still open field:
  - Group formations and management of public/private key, group signature
  - Preserving privacy: attacks against privacy at different layer

Further readings

- Efficient Secure aggregation in VANETs, M. Raya, A. Aziz and J.P. Hubaux, VANET 06.
- A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks, Computer Communications, 2008.

Thank you ?