Scalable Secret Key and Certificate Revocation List Distribution for Hierarchical Vehicular Ad-hoc Networks

Kastuv M. Tuladhar

Department of Computer Science
University of South Dakota

kastuv.tuladhar@coyotes.usd.edu

November 20, 2018

UNIVERSITY OF
SOUTH DAKOTA

Overview

VANETs

Vehicular Ad-hoc Networks (VANETs)

VANETs and its Components

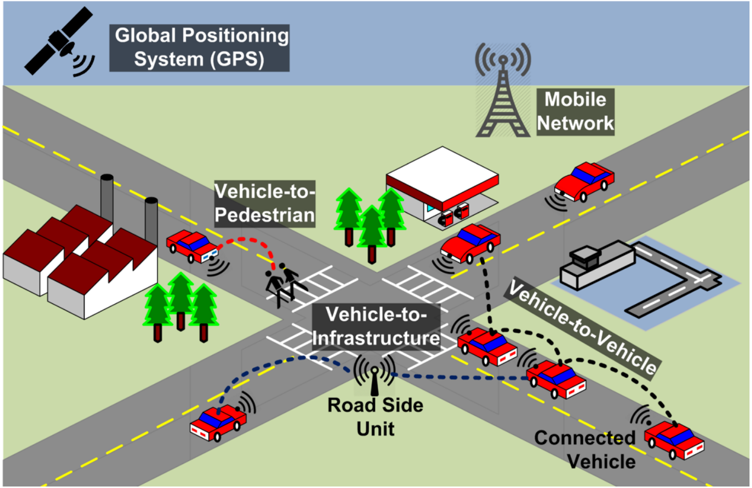
- Vehicular Ad hoc Networks (VANET) are a special type of Mobile Ad hoc Networks (MANETs) is a wireless network formed between vehicles and the infrastructures where vehicles are fast moving and the topology is dynamically changing.
- It consists of the Road-side unit called RSU that manages and controls the vehicles. Vehicle has a on-board unit called OBU that has a computation and communication device.

Vehicular Ad-hoc Networks (VANETs)

Applications of VANETs

- A Vehicular Ad-hoc Network (VANET) is a wireless network formed between vehicles and the infrastructures.
- Applications of VANETs
  1. Share safety informations like broadcasting emergency condition
  2. Weather information
  3. Provide traffic information
  4. Provide navigational support
  5. Vehicle collision avoidance
  6. Value-added services (Vehicle diagnostics, co-operated driving, entertainments etc.)

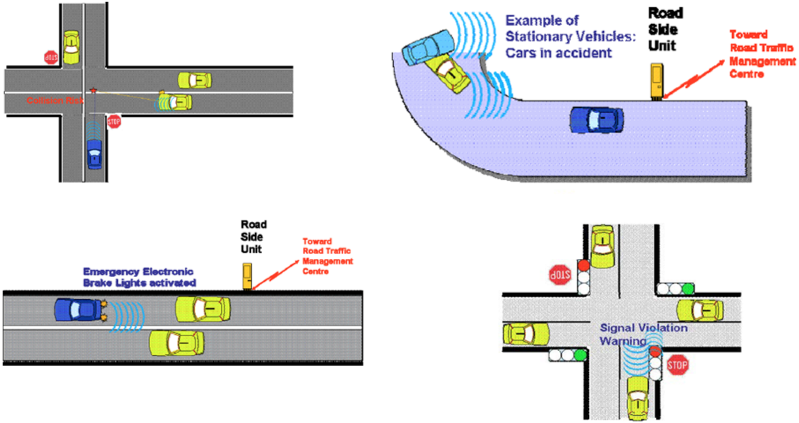
Vehicular Ad-hoc Networks (VANETs)



[1]

[1] Security of Cooperative ITS, Elyes Ben Hamida*, 2015

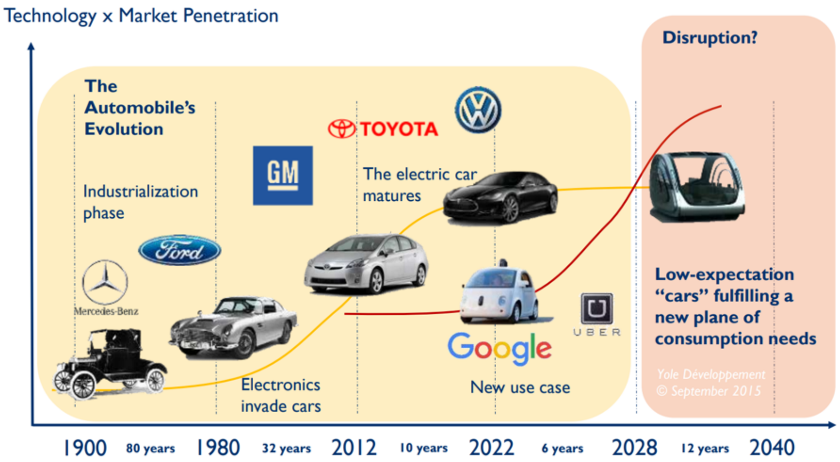
Cooperative Safety Systems – Some Examples



[2]

[2]Security of Cooperative ITS, Elyes Ben Hamida*, 2015

Evolution towards autonomous vehicles



3

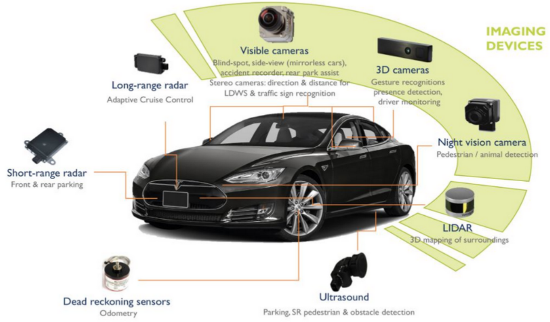
3 MEMS & Sensors for automotive, 2017

Advanced driver assistance systems (ADAS) Sensors

⋆ **Autonomous vehicles heavily relies on sensors ⋆ connected vehicles shares sensor information through V2V communications**

ADAS Applications

- Adaptive Cruise Control
- Blind Spot, Side-view
- Object/Obstacle Detection
- Situational Awareness
- Animal/Pedestrian Detection
- Traffic Sign Detection
- Parking Assistance
- Lane Departure Alert
- Cross Traffic Alert



Yole Développement "https://m.eet.com/media/1301743/sensorsaroundAV.png"

Security in Vehicular Networking

Why VANETs Security is important ?

⋆ Vehicles have to share its information to infrastructure or other vehicles (V2X) in an open wireless medium.
⋆ VANET applications contains the exchange of messages such as emergency, traffic conditions, road accidents that requires the data communication between the nodes.
⋆ The message content can have impact on the drivers' actions to the vehicle.

Presence of Malicious Node

⋆ Malicious node can spread fake information (position/speed/accident) to take advantage of short routes or may have bad intention.

Real World VANET attacks

VolksWagon RKE Hack

⋆ In USENIX Security 2016, Garcia et al. present that only 4 encryption keys are universally used over 100M vehicles produced by VW group over the 20 years.

Fiat Chrysler Automobiles(FCA) hacked

⋆ FCA Jeep Cherokee "remotely" controlled by Charlie Miller and Chris Valasek. ⋆ On 7/24/2015, FCA issued a recall to 1.4M vehicles.

Tesla hacked

⋆ On 2016, team of hackers take remotely controlled Tesla Model car for 12 miles.

Real World VANET attacks

"Cars are already insecure, and you're adding a bunch of sensors and computers that are controlling them...If a bad guy gets control of that, it's going to be even worse." -Miller (Security Specialist)

ANDY GREENBERG SECURITY 04.12.17 07:00 AM

SECURING DRIVERLESS CARS FROM HACKERS IS HARD. ASK THE EX-UBER GUY WHO PROTECTS THEM

Real World VANET attacks

ANDY GREENBERG SECURITY 04.24.17 01:34 PM

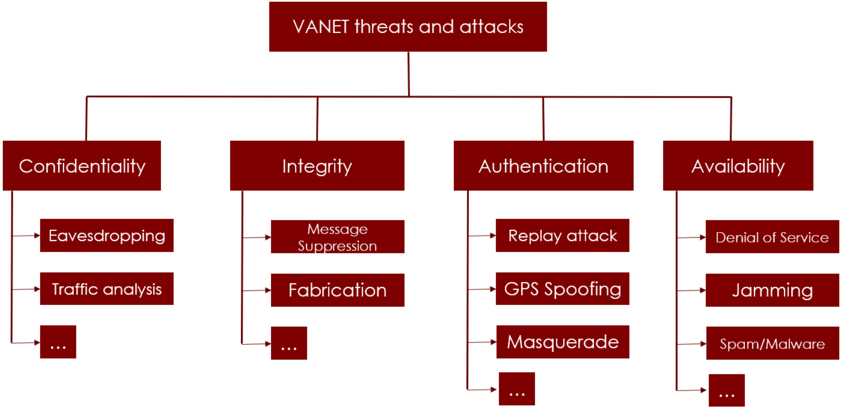
JUST A PAIR OF THESE $11 RADIO GADGETS CAN STEAL A CAR

Example of Replay Attack

The attack essentially tricks both the car and real key into thinking they're in close proximity. One hacker holds a device a few feet from the victim's key, while a thief holds the other near the target car. The device near the car spoofs a signal from the key. That elicits a radio signal from the car's keyless entry system, which seeks a certain signal back from the key before it will open. Rather than try to crack that radio code, the hacker's devices instead copy it, then transmit it via radio from one of the hackers' devices to the other, and then to the key. Then they immediately transmit the key's response back along the chain, effectively telling the car that the key is in the driver's hand.

Classification of VANETs attacks

Propagation of falsified warning messages can mislead towards an accident and damage the life/property.



4

[4] Washington University in St. Louis Computer Science Prof. Raj Jain

Public Key Infrastructure (PKI) Certificate

How to secure VANETs ?

- Private keys are used to cryptographically sign messages that can be authenticated using the matching public key.
- Public key certificates are used for authentication to prevent attackers from causing harm.
- Cryptographically signed messages also provide message integrity; any changes to the message will cause signature verification to fail.
- Certificates have a validity time period.

Elliptic Curve Digital Signature Algorithm (ECDSA)

- The encryption algorithm specified for use in VANETs by IEEE Standard 1609.2 is elliptic curve encryption ECDSA.
- Both 224-bit and 256-bit key sizes are allowed in the standard.

Certificate Revocation List

Certificate Revocation List

IEEE 1609.2- standard for VANETs Security

⋆ IEEE1609.2 standard states to use PKI based certificates for authentication of vehicular nodes and defined Certification Revocation List (CRL).

Certificate Revocation List

⋆ In VANETs, the malicious nodes may exist and such nodes must be prohibited from network access.
⋆ Malicious node can spread fake information (position/speed/accident) to take advantage of short routes or may have bad intention.
⋆ CRL contains the identification of certificates of the malicious nodes that are to be revoked.
⋆ CRL are distributed in the entire VANETs to prevent from the malicious attacks by malicious nodes.

Certificate Revocation List

- CRL is a list of the revoked certificates that are updated timely and disseminated in the Vehicular Network.

Other approaches of Certificate Revocation

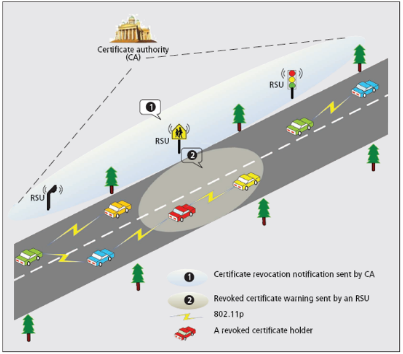
OCSP(Online Certificate Status Protocols)

- Contains real time interactive certificate status server.
- Nodes send query about certificate status prior to any communication.
- Not useful in VANETs ? $\rightarrow$ Latency, infrastructure, scalability.

Typical CRL work flow

CRL work flow

- Certificate Authority (CA) sends the revoked notification to all RSUs.
- RSU notifies CRL to all vehicular nodes.
- Vehicles checks the CRL before communication.
- Revoked certificate holder prevented from communicating with legitimate certificate holder.



Security and Privacy of Intelligent VANETs: Mahmoud et al.

Motivation

CRL and Challenges

- Certificate Revocation Lists (CRLs) contains the identification of the certificates to be revoked.
- The CRL has to be **distributed widely and quickly** as much as possible.
- A compression mechanism is needed to store CRL. A bloom filter does the job but it has **false positive issues**.
- However, preloading the vehicles with a **large number of certificates make it a difficult for distribution & management** due to CRL size.
- **Scalability of the CRL is another issue**.

Motivation

CRL Size

- If one certificate is used for **10 mins.** (Privacy preservation). Average time of a vehicle operation is considered **15 hours/week** in U.S.
- Vehicle will need approximately **5000 certificates** per year.
- If the certificate is valid for five years, **25000 certificates** is required per vehicles.
- If **size of each certificate** is approximately **100 Bytes**.
- The storage size of the **total certificates will be 2.5 MBytes**.

Motivation

CRL Size

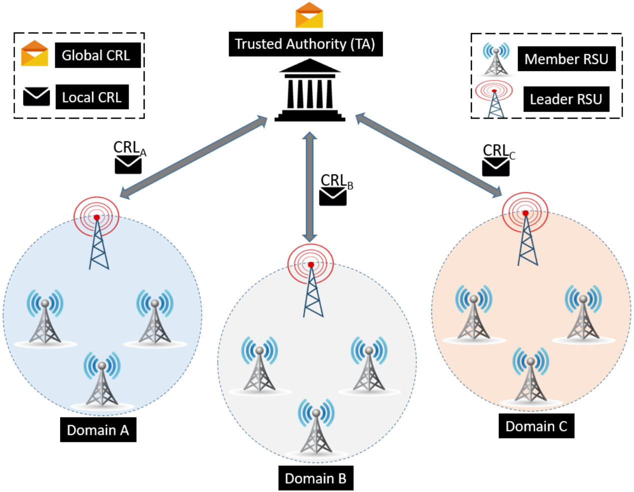
- **2.5 MBytes** is the size of the certificates for one vehicle.
- If the vehicle is malicious, all the certificates held by the vehicles are required to be revoked.
- What if thousands of such vehicles has to be revoked ?
- According to FBIs Uniform Crime Reports, a total of **4.3 million motor vehicles were reported stolen between 2011 to 2016**. Inserting all the identifiers of these vehicles would result of a CRL of **431 MBytes**.
- Managing large CRL is a challenging issues in VANETs.

Motivation

Is it really necessary to store all the CRL list in one vehicle ?

Proposed Model

CRL distribution in Hierarchical VANETs



Proposed Model

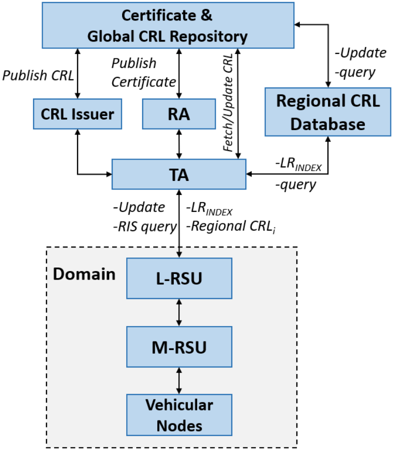
CRL distribution in Hierarchical VANETs

- Vehicles are registered and the certificates are issued by the **trusted authority (TA)**.
- A group of RSUs forms a **domain**.
- A domain size is defined as the desired number of vehicles that can be accommodated by the number of RSUs within a geographic region.
- RSUs are further classified into **leader RSUs (L-RSU)** and **member RSUs (M-RSU)**.
- The L-RSU is the leader of a regional domain.
- **Global** and **local CRL** separation.

Proposed Model

Modified PKI in hierarchical VANETs

- Updated version of the Public Key Infrastructure in hierarchical VANETs from **RFC 5280**.
- The $L\text{-}RSU$ is distinguished by the unique identifier called leader RSU index (LR_{INDEX}).
- When a vehicle enters a domain, a query about the revocation status information **(RIS)** is sent to TA by the $L\text{-}RSU$.
- The TA provides the LR_{INDEX} of the $L\text{-}RSU$ on the basis of which the regional CRL database constructs the regional CRL.
- The TA can query about the regional CRLs and global CRL for any malicious nodes.



Proposed Model

Regional CRL

$\star$ The appropriate regional CRL size can be achieved by considering the required number of vehicles in a domain.

$$\text{Average } N_D = \frac{\text{total \# of vehicles}}{\text{total \# of domains}}$$

N_D : No. of vehicles inside a domain

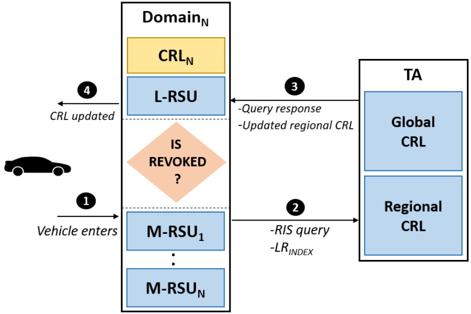
$$\text{CRL}_{Regional_1} + \text{CRL}_{Regional_2} + \ldots = \text{CRL}_{Global}$$

The total segmented regional CRLs can formulate the global CRL.

Proposed Model

Synchronization between Global and Regional CRL

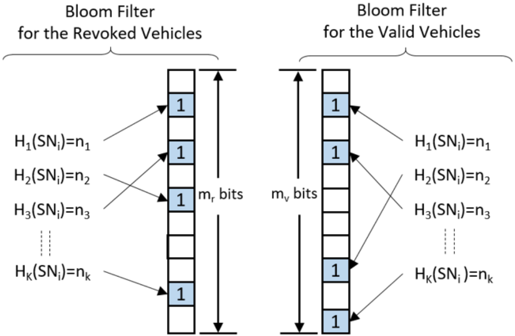
- Vehicle enters and initiates for the connection setup sending the certificate. The $M\text{-}RSU$ forwards the request to the $L\text{-}RSU$.
- The $L\text{-}RSU$ sends its LR_{INDEX} and its RIS query about vehicle certificate to the TA.
- The TA then inquires global CRL database and updates the regional CRL with respect to the LR_{INDEX}
- After receiving the response from the TA, the $L\text{-}RSU$ then checks if the certificate of the vehicle is revoked or not.
- If the certificate is revoked, the $L\text{-}RSU$ then distributes the updated regional CRL inside the domain and aborts the communication initiation process with the revoked vehicle.



Proposed Model

Utilizing two bloom filter

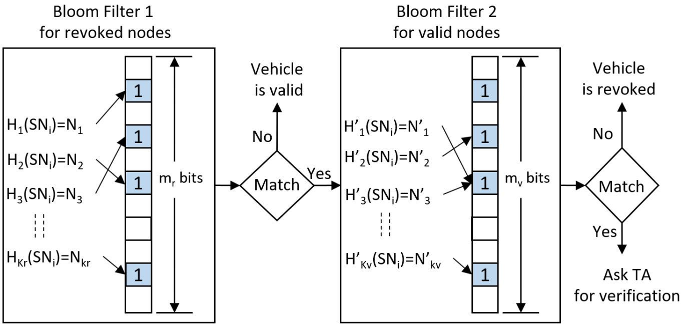
- **Bloom filter** can reduce the CRL size by compressing, however, it suffers from the **false positive rate (FPR)**.
- My proposed scheme adopts the **two bloom filter** to address the FPR issue.



Proposed Model

Utilizing two bloom filter

- **No false negative**.
- When certificates matches in the first bloom filter, then it is compared to the second bloom.



Proposed Model

Table: Notations

Notation	Description
K_v	Hash value for valid vehicle
K_r	Hash value for revoked vehicle
N_r	Number of revoked vehicles in a domain
N_v	Number of valid vehicles in a domain
m_r	bit vector length for revoked vehicles
m_v	bit vector length for valid vehicles
FPR_r	False Positive Rate for revoked vehicles
FPR_v	False Positive Rate for valid vehicles
$CVFP$	Certificate Verification Failure Probability

Proposed Model

Utilizing two bloom filter

- Equations 1,2 shows false positive rate of the dual bloom filter for the revoked certificate (FPR_r) and valid certificates (FPR_v).
- Equations 3 provides the Certificate Verification Failure Probability ($CVFP$) of the dual bloom filter.

$$FPR_r = \left(1 - \left(1 - \frac{1}{m_r}\right)^{K_r N_r}\right)^{K_r} \quad (1)$$

$$FPR_v = \left(1 - \left(1 - \frac{1}{m_v}\right)^{K_v N_v}\right)^{K_v} \quad (2)$$

$$CVFP = P_r\,(\text{the certificate is revoked}) \times FPR_v + P_r\,(\text{the certificate is valid}) \times FPR_r \quad (3)$$

Certificate Revocation List Size

CRL Size in a new modified PKI

- Modified CRL format contains additional fields.
- Highlighted fields are added due to the use of hierarchical VANET and utilization of dual bloom filter.
- The size of the CRL in this approach is $(\mathbf{126.5} + K_r + K_v + m_r + m_v)$ bytes.

FIELD	DESCRIPTION			SIZE(bytes)
Version		Certificate	Uint8	2
craca_id		CA_id field	SIZE(8)	8
Issue Date		CRL issued time stamp	Uint32	8
Next CRL		Next Expected CRL	Uint32	8
PriorityInfo		CRL Priority	Uint8	2
LR_Index	Unsigned	***L-RSU index Id***	***Uint5***	***2.5***
Hash_functions		***For revoked and valid certificate***	***Domain Variable***	***K_r***
				K_v
Two Bloom Filter		***Revoked bit vector***	***Domain Variable***	***m_r***
		Valid bit vector		***m_v***
Signature (ECDSA)		r	Data encryption	32
		s		32
Certificate	Signed	Public Key of TA	Authentication	32

Certificate Revocation List Size

Assumptions

- Five different SHA-256 hash functions for both bit vectors $\rightarrow K_r = K_v =$ **160 bytes**.
- For CVFP=0.05 $\rightarrow m_r$=8×N_r & m_v=3×N_v
- For CVFP=0.1 $\rightarrow m_r$=8×N_r & m_v=1.5×N_v
- 10% of the total certificates (N) are revoked $\rightarrow N_r =$ 0.1×N and valid certificates are $N_v =$ 0.9×N
- One certificate assigned per vehicle.

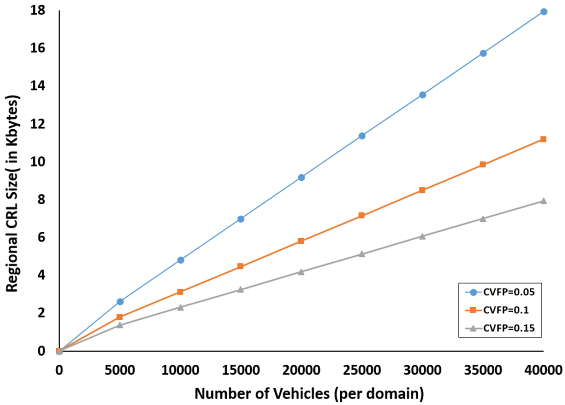
Certificate Revocation List Size

CVFP vs Regional CRL Size

- Totol of 40,000 vehicle:
- CFVP=0.05, CRL size is 18 Kbytes
- CFVP=0.1 has CRL size 11 Kbytes;
- And, CFVP=0.15 CRL size is 8 Kbytes.

⋆ **It is observed that the least CFVP has the highest size of CRL.**

⋆ **Trade-off between the least CVFP and high CRL size, however, high CVFP is undesirable.**



Certificate Revocation List Size

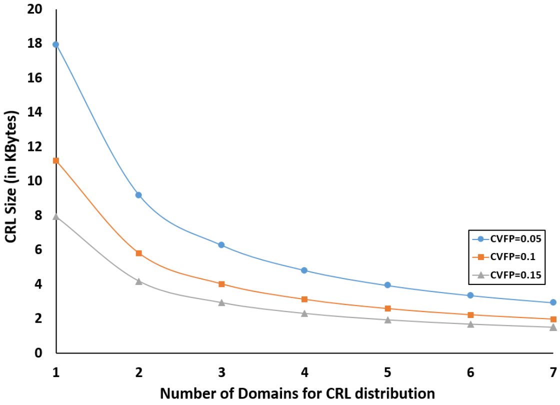
Performance Evaluation with proposed scheme

- The average number of car sale in the U.S. is **6.3 million every year**.
- 63 million cars are sold for last 10 years.
- With **CFVP of 0.1**, revocation probability=10%, the global CRL size will be **17 Mbytes**.
- With the same parameter, if we assume that each domain contains only **10,000 vehicles** then the regional CRL will be only **11 Kbytes**.
- The CRL size is thus reduced by a factor of **1600 times**.

Certificate Revocation List Size

Regional CRL Size vs Number of Domains

- Regional CRL sizes can vary with the domain size.
- With the increase in the number of the domain, we can get the small CRL size.
- $LR_{INDEX} = 2.5$ Bytes $\rightarrow (2^{20})$ possible number of domains.
- Desired Number of domains can be set.
- The CRL size and the number of domains with three CVFP values 0.05, 0.1 and 0.15. We select total vehicles N=40,000 and assumed 10% probability for the revocation.



Secret Key Distribution

Secret Key Distribution

Motivation

- It is difficult to store/manage all keys in a vehicle.
- Centralized trusted authority has high burden of generating and managing the group public/private keys.
- Another challenge in VANETs is delivering group private keys securely from the key generator to vehicular nodes.
- A group is confined to the coverage of a road side unit (RSU).
- Thus, the goal is to mitigate frequent key updates requirement and to make the key management process more efficient and scalable.

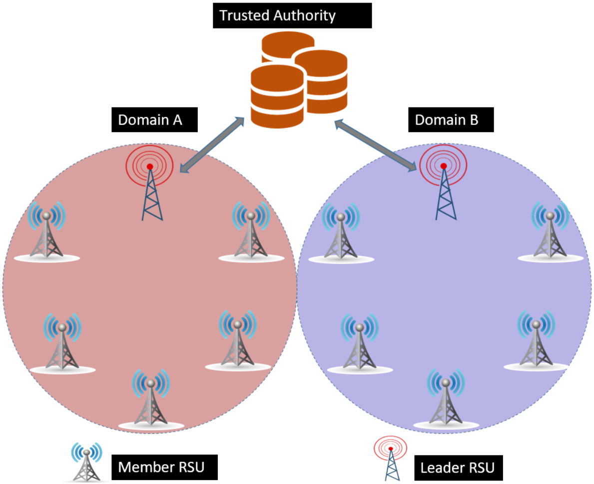
Motivation

Related Work

- Chaum et al. introduced group signatures for anonymous authentication, which employs several group keys corresponding to one group public key.
- Sun et al. proposed a pseudonymous authentication for vehicular communication to provide anonymity and traceability.
- A distributed key management framework distributes the group key with the help of RSUs.
- However, frequent key establishment has not been addressed.
- Also, delivering the group keys in a secure manner is crucial.

System Model

Overview of the System Model



System Model

Trusted Authority (TA)

Vehicles are registered by the trusted authority and provided the certificates. TA and RSUs are securely connected by the stable backbone network. TA can help RSUs to identify the real identity of vehicles on request.

Vehicular nodes

Vehicular nodes are vehicles on the road which are equipped with an on-board unit (OBU) for computation and communication, a global positioning system (GPS) for location service, and an interface for interacting with drivers.

System Model

Road Side Units (RSU) and Domain

⋆ RSUs are the infrastructure deployed along the road side which play an important role in key management, message authentication/verification, and message dissemination.

⋆ A group of RSUs forms a domain. The number of RSUs within a domain can be determined based on the geographical status, infrastructure capacity, deployment plan and vehicle demography.

⋆ RSUs are further classified into member RSUs (M-RSU) and leader RSUs (L-RSU).

System Model

Leader Road Side Units (L-RSU)

⋆ The L-RSUs coordinate with the trusted authority and generates the group private keys and group public keys for the vehicles. The L-RSUs also manage and maintain the database of the group keys. Upon detecting suspicious behavior, the L-RSUs communicate with the TA to reveal the identity of the malicious vehicle.

Member Road Side Units (M-RSU)

⋆ M-RSUs do not perform the key generation and management process, but help vehicles to obtain the group keys from a leader RSU. M-RSUs are semi-trust with the medium security level. Once the vehicle gets the group key, it can communicate with any M-RSU inside a domain with the same key.

Proposed Scheme

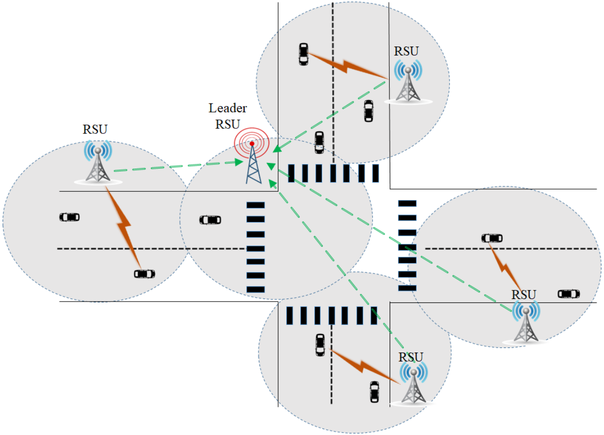
Secure Key Distribution Protocol

- The proposed protocol utilizes short group signature protocol to generate a group private key.
- The leader RSU as a key generator issues group private keys within a domain.
- In a domain which consists of multiple RSUs, there are one group public key and many corresponding group private keys so any member of a domain can sign messages.
- A vehicle can use the same group key with multiple RSUs within a domain without having to initiate a key establishment process.

Proposed Scheme

Secure Key Distribution Protocol

⋆ Figure illustrates how vehicles can request a group private key to the leader RSU within a domain.



Proposed Scheme

Secure Key Distribution Protocol

- As a vehicle enters an area of a domain, it can communicate with any RSU to securely obtain group public/private key pair.
- The secure key distribution scheme is based on the Diffie-Hellman key agreement protocol for mutual authentication and sharing a symmetric key.
- Vehicles and $M\text{-}RSU$ shares the related parameters to get the symmetric key.
- g_{ab} serves as the secret key K_{Vi_MR} between V_i and $M\text{-}RSU$.

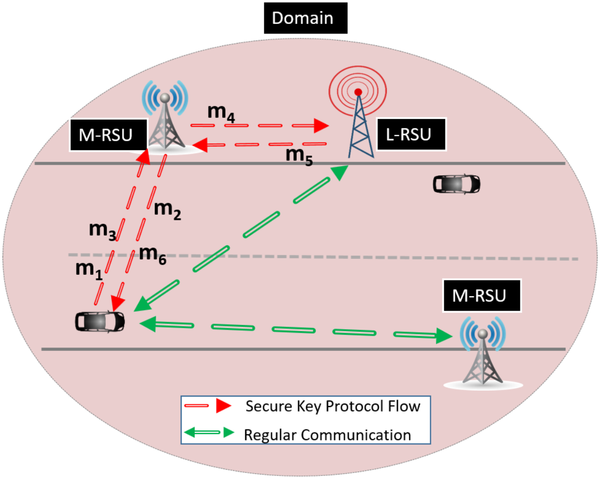
Proposed Scheme

Secure Key Distribution Protocol

- After establishing a symmetric key, vehicle requests for the group keys to M-RSU.
- M-RSU forwards the request to the L-RSU.
- L-RSU replies to M-RSU with the group keys for the vehicle.
- Finally, M-RSU transmits the group keys to vehicle using the shared symmetric keys.

Proposed Scheme

Secure Key Distribution Protocol



Proposed Scheme

Secure Key Distribution Protocol

TABLE II: Key Establishment Process

Vehicle V		Member RSU($M\text{-}RSU$)		Leader RSU ($L\text{-}RSU$)
1. Sends message m_1 to $M\text{-}RSU$ $g, p, A, \{g, p, A \| T_s\}_{SK_{V_i}}, C_{V_i}$	$\rightarrow$	2. Sends message m_2 to V_i $(B)_{PK_{V_i}}, \{A \| B \| T_s\}_{SK_{MR}}, C_{MR}$		
3. Sends m_3 (Ack. and Request) to $M\text{-}RSU$ $(B \| T_s)_{SK_{V_i}}, (Req)_{K_{V_i - MR}}$	$\leftarrow$ $\rightarrow$	4. Forwards request to $L\text{-}RSU$ in msg m_4 $ID_{LR}, ID_{MR}, \{Req, C_{V_i}, T_s\}_{PK_{LR}}$	$\rightarrow$ $\leftarrow$	5. Issues a group key and send msg m_5 $ID_{LR}, ID_{MR}, \{gpk, gsk[v_i], T_s, dgt_L\}_{PK_{V_i}}$
7. V_i receives the group key and can use it	$\leftarrow$	6. Sends message m_6 to V_i m_5, $HMAC(m_5)$		

Evaluation and Analysis

Simulation Setup

- Manhattan Grid environment simulated in the Network Simulator.
- NS-2 and the mobility simulator SUMO.
- NS-2 is TCL based scripting language that provides Network Animation and X-graph tools.
- SUMO provides the real world map with desired number of vehicles and its mobility.
- Mobility from SUMO can be used in NS-2 to generate trace file.
- Trace file provides vehicle location with time stamp on simulation time.
- Map of 3600*3600 square meters has been considered in this case.

SUMO mobility generator

After fetching Open Street Map helps to generate mobility

Example (SUMO mobility generator)

```
Commands:
1. polyconvert --osm - files manhattan.net.xml --type - file
osmPolyconvert.typ.xml -o manhattan.poly.xml
2. python /usr / local /src/sumo -0.25.0/ tools / randomTrips.py
-n manhattan.net.xml -r manhattan.rou.xml -e 50 -l
3. python /usr / local /src/sumo -0.25.0/ tools / traceExporter.py --
fcd - input manhattan.sumo.xml --ns2config - output manhattan.
tcl --ns2mobility - output mobility.tcl --ns2activity - output
activity.tcl
```

NS-2 Simulator

NS-2 supports different protocols. The vehicle mobility can be attached to get the simulation and trace file.

Example (NS-2 network configuration code)

```
#TN means Total number of wireless node
global TN
set TN 100
set god_ [create -god $TN]
# global node setting
$ns node - config - adhocRouting AODV \
-llType LL \
-macType Mac /802 _11 \
-ifqLen 100 \
-ifqType Queue / DropTail / PriQueue \
-antType Antenna / OmniAntenna \
...
```

Trace-File Sample

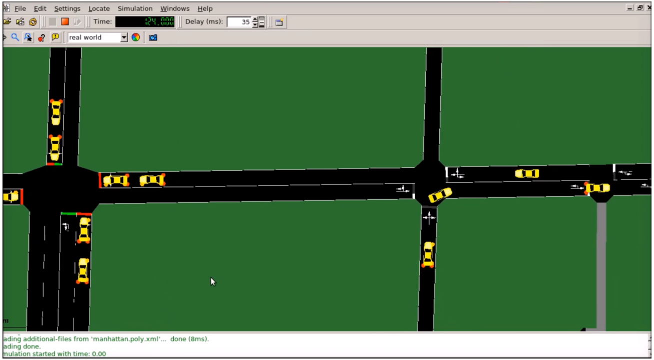
Example (Trace-File)

```
$node_(0) set X_ 4567.59
$node_(0) set Y_ 2539.32
$node_(0) set Z_ 0
$ns_ at 0.0 "$node_(0) setdest 4567.59 2539.32 0.00"
$ns_ at 1.0 "$node_(0) setdest 4566.24 2538.81 1.44"
$node_(1) set X_ 1577.62
$node_(1) set Y_ 2291.6
$node_(1) set Z_ 0
$ns_ at 1.0 "$node_(1) setdest 1577.62 2291.6 0.00"
$ns_ at 2.0 "$node_(0) setdest 4563.33 2537.69 3.12"
$ns_ at 2.0 "$node_(1) setdest 1575.15 2292.2 2.54"
```

Evaluation and Analysis

Simulation Setup

⋆ Vehicles are on the road. Task is to fix the infrastructure lay out with the desired size of domain.



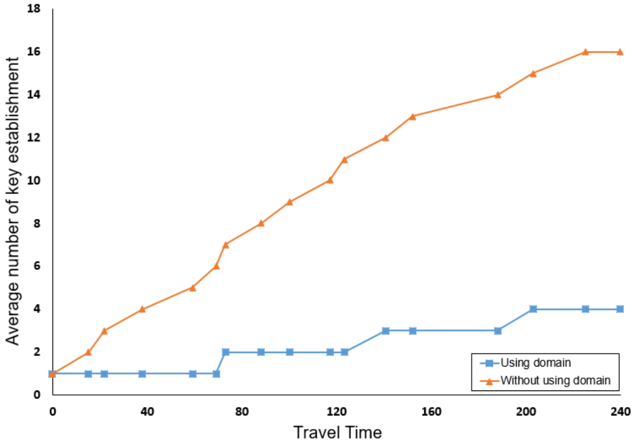
Evaluation and Analysis

Key Establishment

- When the domain of multiple RSUs is not considered, vehicles have to perform the key exchange procedure with each and every RSUs separately.
- The figure shows how the average number of key establishment changes as the vehicles are moving with/without using domains.
- Here, domain has the area covered by four RSUs with the vehicles moving randomly.

Evaluation and Analysis

Key Establishment



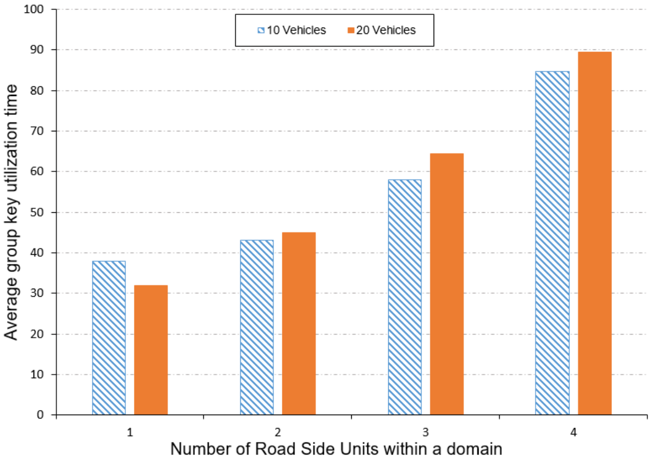
Evaluation and Analysis

Group Key Utilization

- Group key utilization time is the time that the vehicle travels inside the domain after establishing the key.
- Group key utilization time can be used to consider the frequency of the group key usage in domains and get idea about average travel time of the vehicles in various.
- The Figure shows the group key utilization time for different size of vehicles after receiving the group keys under the different size of domain.

Evaluation and Analysis

Group Key Utilization



Evaluation and Analysis

Group Key Utilization

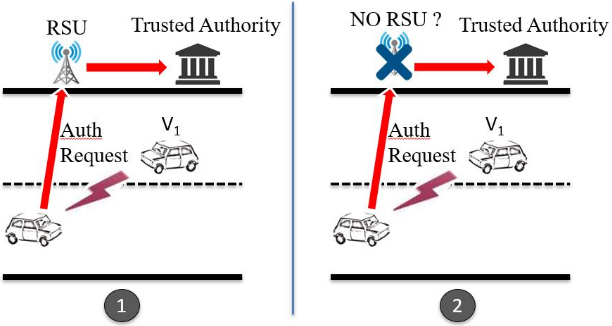
- It is observed that the vehicles spends around 30-40 seconds in one RSU on average.
- And the average travel time is continuously increasing as the size of the domain increases.
- When there are four RSUs within a domain, it is observed that the moving vehicles utilize the group key about 200% more than the moving vehicles without having a group key for the domain.

Future Works

Authentication/Revocation with NO infrastructure!

Motivation

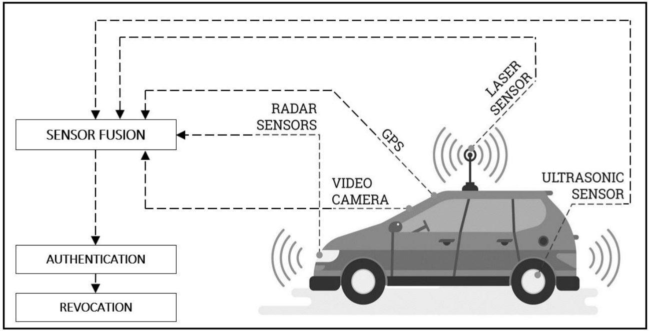
- The **US Department of Transportation (DOT)** has conducted connected vehicle (CV) **pilot deployment program** for real-world feasibility on 2017 in NY City.
- It is likely to **take a while to fully deploy the infrastructure**. Further, in **rural area** context, **V2V will be dominant over V2I**.
- The previous **approach of authentication and revocation will not function in the infrastructure-less environment** where only V2V communications are prevalent.



Authentication/Revocation using ADAS sensors

Sensor Fusion

- The sensor data that can provide the **fingerprint of the surrounding objects** and can be utilized to match the existence of the target vehicle in the proximity of its periphery.
- This method will utilize the existing sensors of the vehicles **without the additional hardware cost**.
- This method will **not require PKI certificates for authentication** which will beneficial as the huge packet size is one of the drawback of PKI system.



Conclusion

Conclusion

VANET Introduction

⋆ Introduction ⋆ Application ⋆ Autonomous Vehicles ⋆ Security

Certificate Revocation

⋆ Introduction ⋆ Motivation ⋆ Proposed Scheme ⋆ Evaluation

Secure Key Distribution

⋆ Motivation ⋆ System Model ⋆ Proposed Scheme ⋆ Evaluation

Future Work

⋆ Summary/Goals

Thanks

Special Thanks

Thesis Committee Members

- ⋆ Dr. Kiho Lim (Thesis Committee Chair, Supervisor)
- ⋆ Dr. Santosh KC (Thesis Committee Member)
- ⋆ Dr. Ahyoung Lee (Thesis Committee Member)
- ⋆ Dr. Jose Flores (Thesis Committee Member)

Department of Computer Science

- ⋆ Awarded Travel Grant 2018, IEEE EIT 2018 Conference Proceedings

And, Thank you all for attending !

IEEE Xplore® Digital Library

> Institutional Sign In

Conferences > 2018 IEEE International Confe...

Efficient and Scalable Certificate Revocation List Distribution in Hierarchical VANETs

Conferences > 2017 IEEE 8th Annual Ubiquito...

A scalable and secure key distribution scheme for group signature based authentication in VANET