Message Authentication in VANET

Preetham

Department of Mathematics
Hochschule Mittweida

10 January 2017

INTRODUCTION

- The Multidimensional Knapsack Problem (MKP) is a NP-hard problem which has many practical applications, such as processor allocation in distributed systems, cargo loading, or capital budgeting. The goal of the MKP is to find a subset of objects that maximizes the total profit while satisfying some resource constraints.

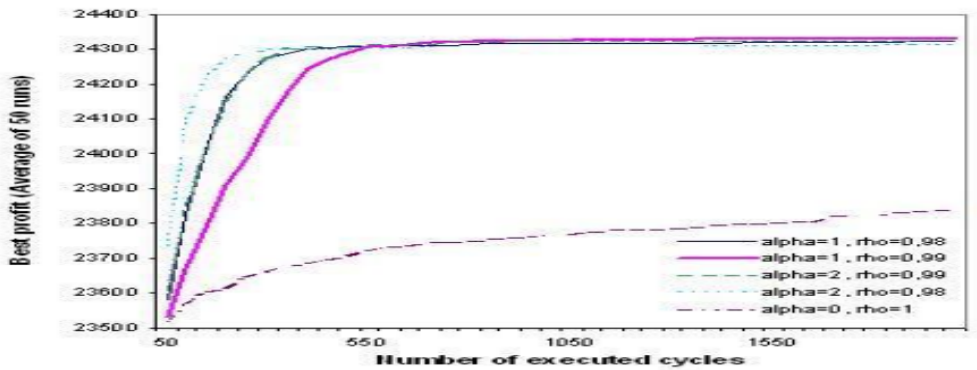


Figure: Influence of and on solution quality: each curve plots the evolution of the profit of the best solution when the number of cycles increases, for a given setting of and . The other parameters have been set to = 5, nbAnts = 30, min = 0.01, and max = 6.

Vehicular Ad-hoc Network(VANET)

- Vehicular Ad Hoc Network (VANET) is an application of mobile ad hoc network (MANET)

Vehicular Ad-hoc Network(VANET)

- Vehicular Ad Hoc Network (VANET) is an application of mobile ad hoc network (MANET)
- VANET is self-organised network , used for communicating between vehicles

Vehicular Ad-hoc Network(VANET)

- Three types of communication are available in the VANET

Vehicular Ad-hoc Network(VANET)

- Three types of communication are available in the VANET
- Network infrastructure

Vehicular Ad-hoc Network(VANET)

- Three types of communication are available in the VANET
- Network infrastructure
- Inter-vehicular communication

Vehicular Ad-hoc Network(VANET)

- Three types of communication are available in the VANET
- Network infrastructure
- Inter-vehicular communication
- Hybrid vehicular network communication

Vehicular Ad-hoc Network(VANET)

- Network infrastructure: Vehicles connect to a centralized server or a backbone network such as the Internet, through the road-side infrastructure, e.g., cellular base stations, IEEE 802.11p RSUs

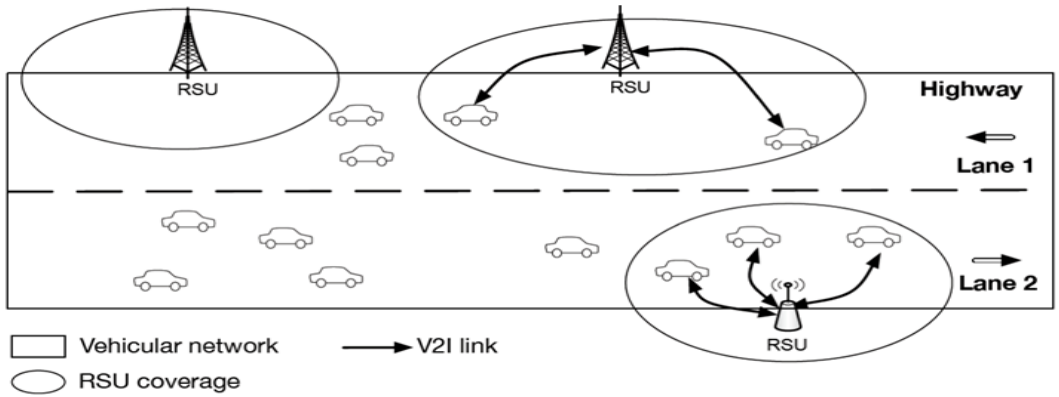


Figure: Network infrastruture traffic model

Vehicular Ad-hoc Network(VANET)

- Inter-vehicular communication:Use of direct ad-hoc connectivity among vehicles via multihop for applications requiring long-range communications (e.g., traffic monitoring), as well as short-range communications (e.g., lane merging)

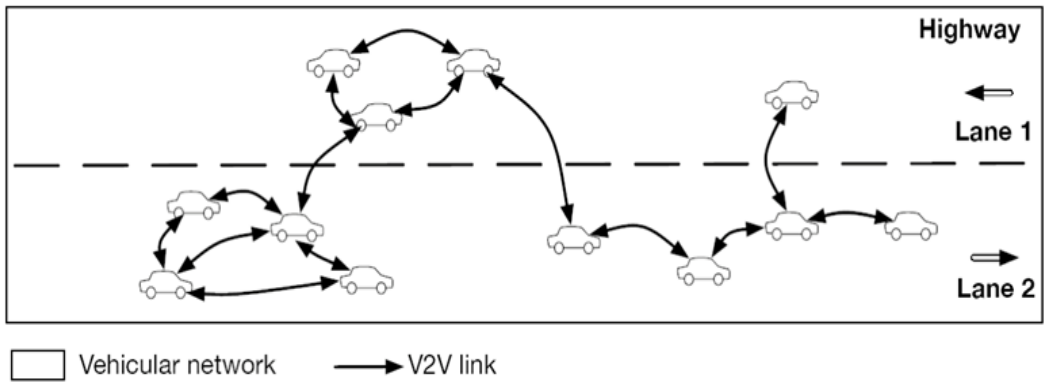


Figure: Inter-vehicular traffic model

Vehicular Ad-hoc Network(VANET)

- Hybrid vehicular network communication:Use of a combination of V2V and V2I. Vehicles in range directly connect to the road-side infrastructure, while exploit multi-hop connectivity otherwise

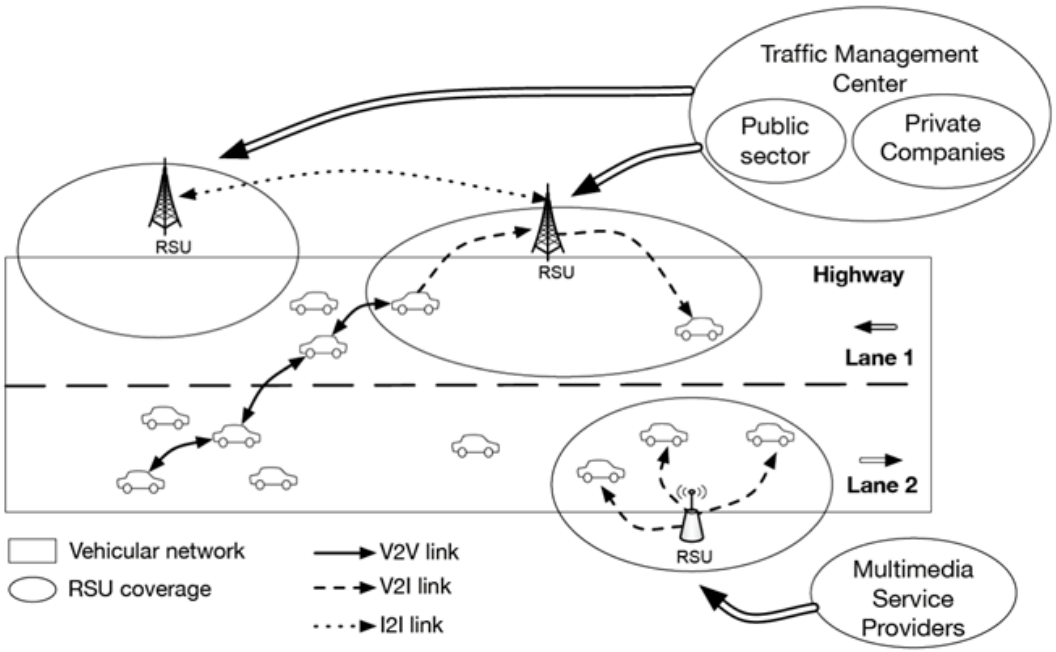


Figure: Hybrid vehicular network traffic model

Vehicular Ad-hoc Network(VANET)

Application

- Collision Avoidance:If a driver get a warning message on time collision can be avoided.

Vehicular Ad-hoc Network(VANET)

Application

- Collision Avoidance:If a driver get a warning message on time collision can be avoided.
- Cooperative Driving: Drivers can get signals for traffic related warnings like curve speed warning, Lane change warning etc. These signals can co-operate the driver for an uninterrupted and safe driving

Vehicular Ad-hoc Network(VANET)

Application

- Collision Avoidance:If a driver get a warning message on time collision can be avoided.
- Cooperative Driving: Drivers can get signals for traffic related warnings like curve speed warning, Lane change warning etc. These signals can co-operate the driver for an uninterrupted and safe driving
- Traffic optimisation: Traffic can optimised by the use of sending signals like jam, accidents etc. to the vehicles so that they can choose their alternate path and can save time

Application

- Peer to peer application: These application are useful to provide services like sharing data among the vehicles in the network.

Application

- Peer to peer application: These application are useful to provide services like sharing data among the vehicles in the network.
- Internet Connectivity: People always want to connect with the Internet all the time. Hence VANET provides the constant connectivity of the Internet to the users.

Application

- Peer to peer application: These application are useful to provide services like sharing data among the vehicles in the network.
- Internet Connectivity: People always want to connect with the Internet all the time. Hence VANET provides the constant connectivity of the Internet to the users.
- Other services: VANET can be utilised in other user based application such as payment service to collect the toll taxes, to locate the fuel station, restaurant etc.

Attack

- Denial of service attack:This attack happens when the attacker takes control of the vehicle resources or jam the communication channel used by the vehicular network

Attack

- Denial of service attack:This attack happens when the attacker takes control of the vehicle resources or jam the communication channel used by the vehicular network
- Message suppression attack:Attacker drops message from the network,which have critical information to the receiver

Attack

- Denial of service attack:This attack happens when the attacker takes control of the vehicle resources or jam the communication channel used by the vehicular network
- Message suppression attack:Attacker drops message from the network,which have critical information to the receiver
- Fabrication attack: Attacker transmits false information in to the network

Attack

- Alteration attack: The attacker alters an existing data, like delay in the transmission, replaying earlier transmission, or altering the data transmitted.

Attack

- Alteration attack: The attacker alters an existing data, like delay in the transmission, replaying earlier transmission, or altering the data transmitted.
- Replay attack: Here an attacker replay the transmission of earlier information to take advantage of the situation of the message at time of sending.

Attack

- Alteration attack: The attacker alters an existing data, like delay in the transmission, replaying earlier transmission, or altering the data transmitted.
- Replay attack: Here an attacker replay the transmission of earlier information to take advantage of the situation of the message at time of sending.
- Sybil attack: This attack happens when an attacker creates large number of pseudonymous, e.g.: jam ahead and force them to take alternate route.

Technical challenges

- High Mobility: The vehicle in VANET's usually are moving at high speed. This makes harder to predict a vehicles position and making protection of vehicle privacy

Technical challenges

- High Mobility: The vehicle in VANET's usually are moving at high speed. This makes harder to predict a vehicles position and making protection of vehicle privacy
- Rapidly changing network topology: Due to high vehicle mobility and random speed of vehicles, the position of vehicle changes frequently. As a result of this, network topology in VANETs tends to change frequently.

Technical challenges

- High Mobility: The vehicle in VANET's usually are moving at high speed. This makes harder to predict a vehicles position and making protection of vehicle privacy
- Rapidly changing network topology: Due to high vehicle mobility and random speed of vehicles, the position of vehicle changes frequently. As a result of this, network topology in VANETs tends to change frequently.
- Time Critical: The information in VANET must be delivered to the vehicle with in time limit so that a decision can be made by the vehicle and perform action accordingly.

Security

- Authentication: Authentication ensures that the message is generated by the legitimate user. In VANET a vehicle reacts upon the information came from the other vehicle hence authentication must be satisfied.

Security

- Authentication: Authentication ensures that the message is generated by the legitimate user. In VANET a vehicle reacts upon the information came from the other vehicle hence authentication must be satisfied.
- Privacy: The privacy of a vehicle against the unauthorised vehicle should be guaranteed. This is required to eliminate the message delay attacks

Security

- Authentication: Authentication ensures that the message is generated by the legitimate user. In VANET a vehicle reacts upon the information came from the other vehicle hence authentication must be satisfied.
- Privacy: The privacy of a vehicle against the unauthorised vehicle should be guaranteed. This is required to eliminate the message delay attacks
- Data Verification: A regular verification of data is required to eliminate the false messaging.

Message Authentication in VANET

ECDSA Approach

- Reasons for ECDSA used in VANET

- Reasons for ECDSA used in VANET

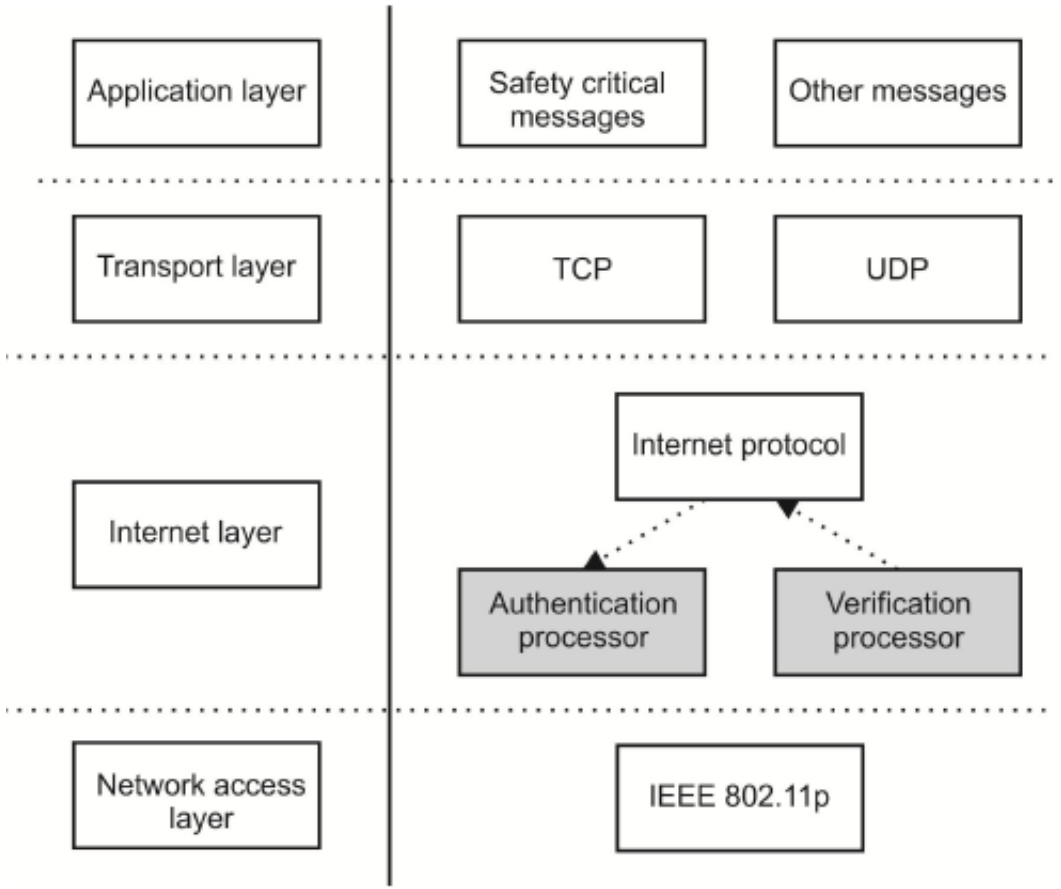
	Key	Private	Public	Sign [s]	Verify [s]
RSA	512	73148	789777	0.000137	0.000013
RSA	1024	13272	254362	0.000747	0.000039
RSA	2048	2045	64246	0.004873	0.000155
RSA	4096	268	17040	0.037068	0.000574
DSA	512	74480	68644	0.000134	0.000145
DSA	1024	24869	21805	0.000401	0.000459
DSA	2048	6469	5545	0.001533	0.001802
ECDSA	160	92305	24595	0.0001	0.0004
ECDSA	192	73776	18892	0.0001	0.0005
ECDSA	224	57669	14097	0.0002	0.0007
ECDSA	256	47598	10836	0.0002	0.0009
ECDSA	384	22111	4551	0.0005	0.0022
ECDSA	521	11311	2122	0.0009	0.0047

Figure: comparison of rsa,dsa and ecdsa

Message Authentication in VANET

ECDSA Approach

- Two types of messages
  safety critical messages
  event driven messages



- shared secret key
- Signature Generation
- Signature Verification

Shared Secret Key

- Let (d_A, Q_A) be the private key - public key pair of A
- Let (d_B, Q_B) be the private key - public key pair of B

Shared Secret Key

- Let (d_A, Q_A) be the private key - public key pair of A
- Let (d_B, Q_B) be the private key - public key pair of B
- A computes $S_k = d_A * Q_B$

Shared Secret Key

- Let (d_A, Q_A) be the private key - public key pair of A
- Let (d_B, Q_B) be the private key - public key pair of B
- A computes $S_k = d_A * Q_B$
- B computes $S_k = d_B * Q_A$

Shared Secret Key

- Let (d_A, Q_A) be the private key - public key pair of A
- Let (d_B, Q_B) be the private key - public key pair of B
- A computes $S_k = d_A * Q_B$
- B computes $S_k = d_B * Q_A$
- $S_k = (X_s, Y_s)$

Signature Generation

- m be the message by sender A using private d_A

Signature Generation

- m be the message by sender A using private d_A
- calculate $e = HASH(m)$

Signature Generation

- m be the message by sender A using private d_A
- calculate $e = HASH(m)$
- select the random integer k from $[1, n-1]$

Signature Generation

- m be the message by sender A using private d_A
- calculate $e = HASH(m)$
- select the random integer k from $[1, n-1]$
- calculate $r = x_1(modn)$ where $(x_1, y_1) = k$
  if $r = 0$ select the random integer k

Signature Generation

- m be the message by sender A using private d_A
- calculate $e = HASH(m)$
- select the random integer k from $[1, n-1]$
- calculate $r = x_1(modn)$ where $(x_1, y_1) = k$
  if $r = 0$ select the random integer k
- calculate $s = k^{-1}(e + d_A r)(modn)$
  if $s = 0$ select the random integer k

Signature Generation

- m be the message by sender A using private d_A
- calculate $e = HASH(m)$
- select the random integer k from $[1, n-1]$
- calculate $r = x_1(modn)$ where $(x_1, y_1) = k$
  if $r = 0$ select the random integer k
- calculate $s = k^{-1}(e + d_A r)(modn)$
  if $s = 0$ select the random integer k
- the signature pair (r, s)

Signature Verification

- for B to authorise A's signature, B must have A's public key Q_A

Signature Verification

- for B to authorise A's signature, B must have A's public key Q_A
- firstly, verify that r and s are integers in $[1, n-1]$
  if not the signature is invalid

Signature Verification

- for B to authorise A's signature, B must have A's public key Q_A
- firstly, verify that r and s are integers in $[1, n-1]$
  if not the signature is invalid

Signature Verification

- for B to authorise A's signature, B must have A's public key Q_A
- firstly, verify that r and s are integers in $[1, n-1]$
  if not the signature is invalid
- calculate $w = s^{-1}(mod n)$

Signature Verification

- for B to authorise A's signature, B must have A's public key Q_A
- firstly, verify that r and s are integers in $[1, n-1]$
  if not the signature is invalid
- calculate $w = s^{-1}(mod n)$
- calculate $u_1 = ew(mod n)$ and $u_2 = rw(mod n)$

Signature Verification

- for B to authorise A's signature, B must have A's public key Q_A
- firstly, verify that r and s are integers in $[1, n-1]$
  if not the signature is invalid
- calculate $w = s^{-1}(mod n)$
- calculate $u_1 = ew(mod n)$ and $u_2 = rw(mod n)$
- calculate $(x_1, y_1) = u_1 G + u_2 Q_A$

Signature Verification

- for B to authorise A's signature, B must have A's public key Q_A
- firstly, verify that r and s are integers in $[1, n-1]$
  if not the signature is invalid
- calculate $w = s^{-1}(mod n)$
- calculate $u_1 = ew(mod n)$ and $u_2 = rw(mod n)$
- calculate $(x_1, y_1) = u_1 G + u_2 Q_A$
- the signature is valid if $x_1 = r(mod n)$, otherwise invalid

Network Algorithm

- consider A and B are two vehicles

Network Algorithm

- consider A and B are two vehicles
- if A and B are in the coverage area of the infrastructure unit

Network Algorithm

- consider A and B are two vehicles
- if A and B are in the coverage area of the infrastructure unit
- then update the Table with identity,speed and direction of vehicle

Network Algorithm

- consider A and B are two vehicles
- if A and B are in the coverage area of the infrastructure unit
- then update the Table with identity,speed and direction of vehicle
- encrypted message are sent between A and B

Network Algorithm

- consider A and B are two vehicles
- if A and B are in the coverage area of the infrastructure unit
- then update the Table with identity,speed and direction of vehicle
- encrypted message are sent between A and B
- if A or B moved out of coverage area

Network Algorithm

- consider A and B are two vehicles
- if A and B are in the coverage area of the infrastructure unit
- then update the Table with identity,speed and direction of vehicle
- encrypted message are sent between A and B
- if A or B moved out of coverage area
- update the table

Network Algorithm

- consider A and B are two vehicles
- if A and B are in the coverage area of the infrastructure unit
- then update the Table with identity,speed and direction of vehicle
- encrypted message are sent between A and B
- if A or B moved out of coverage area
- update the table
- check for the new vehicle in the coverage area

key generation

- key generation delay:It is the total time taken by sending vehicle for key generation

key generation

- key generation delay:It is the total time taken by sending vehicle for key generation

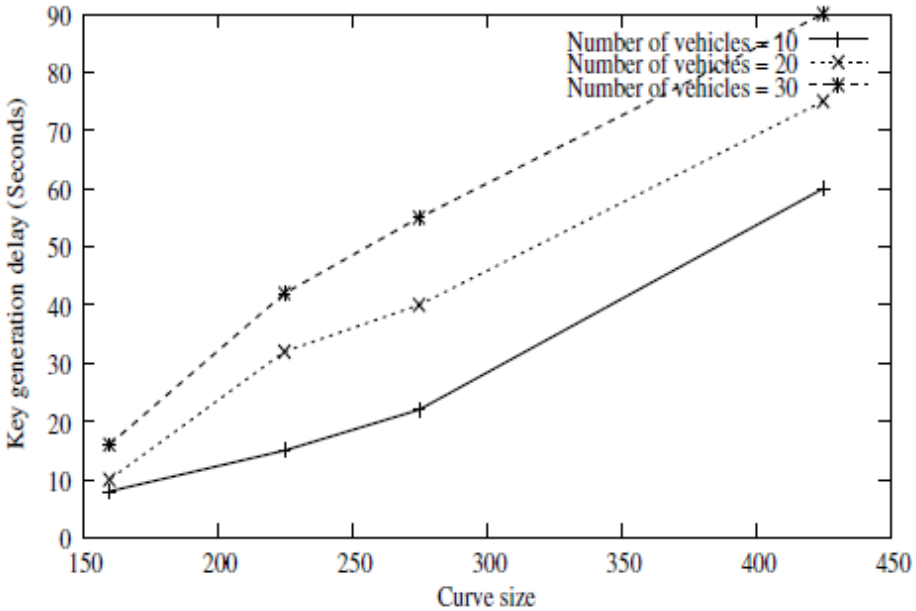


Figure: key generation delay vs curve size

signature generation

- signature generation delay:It is the total time taken by sending vehicle for signature generation

signature generation

- signature generation delay:It is the total time taken by sending vehicle for signature generation

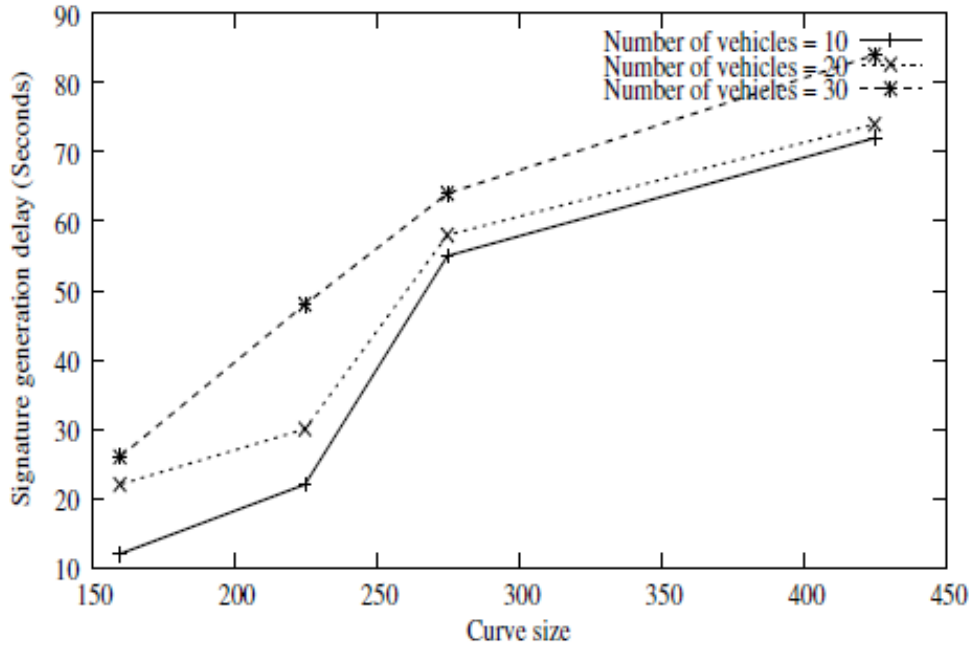


Figure: signature generation delay vs curve size

signature verification

- signature verification delay:It is the total time taken by receiving vehicle for signature verification

signature verification

- signature verification delay:It is the total time taken by receiving vehicle for signature verification

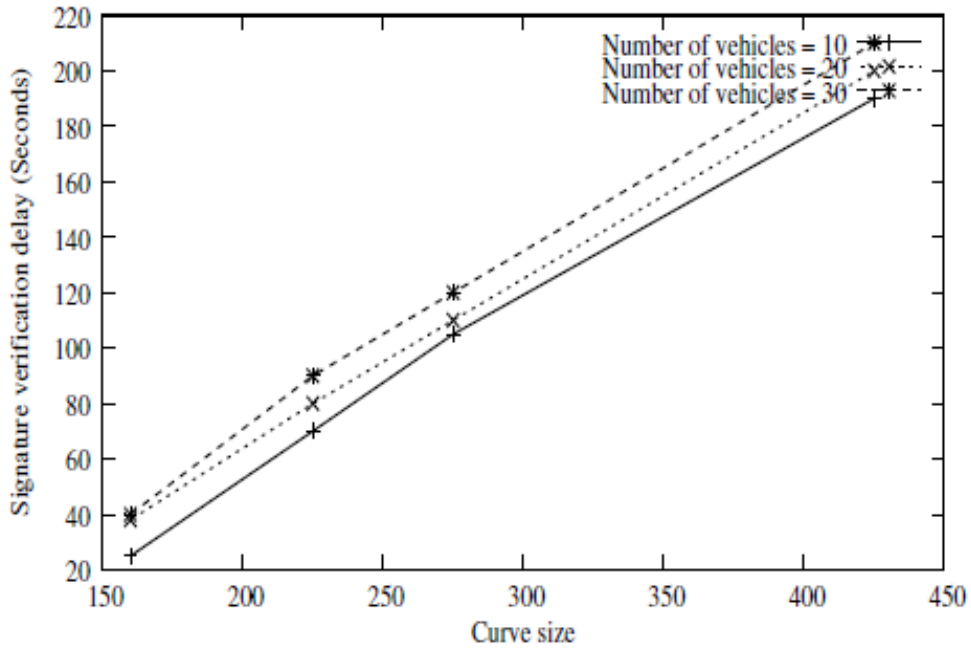


Figure: signature verification delay vs curve size

Conclusion

- Security is the major issue to implement in the VANET.
- As the number of vehicles increases the message delay increase to reduce the delay we need add more number of infrastructure unit

Reference I


S.S.Manvi, M.S.Kakkasageri,D.G.Adiga
Message Authentication in Vehicular Ad hoc Networks:ECDSA Approach.
International Conference on Future Computer and Communication ,2009


Ram shringar Raw, Manish Kumar ,Nanhay Singh
Security Challenges, Issues And Their Solutions For VANET
IJINSA ,vol.5, No.5,2013


Jan Durech, Maria franekova ,Peter Holecko ,Emilia Bubenikova
Modelling of security principles within Car-to-car communication in modern cooperative intelligent transportation system
AEEE.v14il.1279