ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Special Issue 6, May 2015**

# Efficient Authentication and Congestion Control for Vehicular Ad Hoc Network

Deivanai.P[1], K.Sudha[2], K.Radha[3]

Department of CSE, Muthayammal Engineering College, Rasipuram, India[1]

Assistant Professor, Department of CSE, Muthayammal Engineering College, Rasipuram, India[2]

Assistant Professor, Department of CSE, Muthayammal Engineering College, Rasipuram, India[3]

**ABSTRACT:** VANET is a subclass of MANET in which each vehicle acts as a node. In VANET Road Side Units (RSUs) are responsible for distributing group private keys and managing vehicles in a localized manner for every 100 to 300 m. Then, use a Hash Message Authentication Code (HMAC) to avoid time consuming CRL checking and to ensure the integrity of messages. Cooperativemessage authentication scheme is mainly used for reducing the authentication burden. The scheme is more efficient in terms of authentication speed and privacy. Congestion control scheme is introduced to monitor and regulate the traffic levels, So with the help of this approach whenever there is a problem of congestion and emergency message occurs, the congestion control can reserve time slots by dynamically partitioning the beacon interval without the expense of beacons for reducing the traffic.

**KEYWORDS:**Certificate revocation list, Hash message authentication code, Vehicular Ad Hoc Network, Road side units.

## I. INTRODUCTION

A Vehicular Ad Hoc Network (VANET) uses vehiclesas mobile nodes in a MANET to create a mobile network. In VANETs, vehicles communicate with Each other, as well as with RSUs, and onboard units are responsible for distributing the security related materials to all the vehicles.Tamper proof device also fixed for every vehicle that are presented in the road side environment.

Everyvehicle in the road acts as a wireless router or node,and allowing vehicles approximately 100 to 300 meters of each other to connect, in turn, to create a network with a wide range. Each RSU is responsible for maintaining the vehicles for that particular distance on the road side.Intelligent vehicular ad hoc networks (In VANETs**)** use Wi-Fi IEEE 802.11p (WAVE standard) and WiMAX IEEE 802.16 effective communication between vehicles in the road side infrastructure with dynamic mobility.

**Figure I: VANET infrastructure**

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Special Issue 6, May 2015**

**COMMUNICATION IN VANET**

- Vehicle to Vehicle communication (V2V)
- Vehicle to Infrastructure communication (V2I)
- Vehicle to Roadside Communication (V2R)

**HYBRID MODELS OF VANET**

- Vehicle to Vehicle message passing
- Vehicle to Vehicle (V2V) & Vehicle to Roadside message passing (V2R)

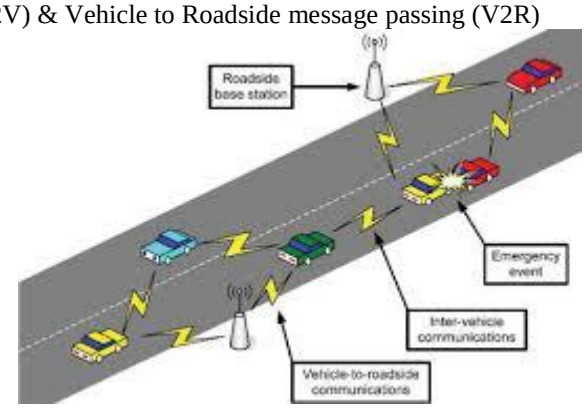


**Figure II: Communication between vehicles**

**VEHICLE TO VEHICLE COMMUNICATION (V2V)**

Vehicle to Vehicle communication method is well suited for short range vehicular communication networks. It is responsible for providingfast, reliable communication and real time safety. Road side infrastructure units are not involved here.

In V2V communicationthe vehicles are moving at different velocities due to the quick network topology changes.

Periodic broadcasts from each vehicle is happened for every 300 ms and it inform the direct neighbors about its address, but the address-position map may change frequently due to relative movements among vehicles in the road side environment.

**VEHICLE TO INFRASTRUCTURE /ROADSIDE COMMUNICATION (V2I/V2R)**

- Vehicle to Infrastructure communication is responsible for longer-range vehicular networks
- Road side units are acts as a wireless access points
- Vehicles and Road side units are communicated by using Vehicle-to-Infrastructure (V2I) and Vehicle-to-Roadside (V2R) protocols for safety

## II.LITERATURE REVIEW

A novel group signature based security framework for vehicular communication is proposed. Compared to the traditional digital signature scheme, the new scheme achieves authenticity, integrity, anonymity, accountability at the same time. Furthermore, describe a scalable role-based access control approach for vehicular networks. Finally, present a probabilistic signatureverification scheme that can efficiently detect the tampered messages from an unauthorized node. A group signature scheme allows members of a group to sign messages on behalf of the group members. Signatures can be verified with respect to a single group public key, but they do not reveal the identity of the signer of that message. Furthermore, it is impossible to decide whether two signatures have been issued by the same group member [1].

A novel RSU-aided message authentication scheme named RAISE has been proposed. With RAISE, RSUs are responsible for verifying the authenticity of messages sent by vehicles and notifying the authentication results back to

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Special Issue 6, May 2015**

all the associated vehicles. The RAISE scheme has many advantages because of its lower computation and communication overhead [3].
An efficient pseudonymous authentication scheme with strong privacy preservation, such as PASS used for vehicular communications. In traditional pseudonymous authentication scheme, thesize of Certificate Revocation List (CRL) in PASS is linear with the number of revoked vehicles and it is unrelated to how many pseudonymous certificates are held by the revoked vehicles.
Furthermore, PASS provides strong privacy preservation to the vehicles so that the adversaries cannot trace any vehicle even all Roadside Units have been compromised [4].

## III.METHODOLOGY

VANETs come with several challenging characteristics, such as large scale and high mobility. Nodes in the vehicular environment is more dynamic because most vehicles usually are at a high speed and changing their position constantly over the network. The high mobility leads to a dynamic network topology, when the links between nodes connect and disconnect very often. And VANETs have a potentially large scale which can include many participants and extend over the entire road network environment.
VANET routing approaches are mainly divided into three types:
I Geocast
Ii Broadcast
IiiUnicast
vehicular communication systems are more effective in avoiding accidents and traffic congestions .

Basically, vehicular networks are considered to contain two types of nodes and one authority: vehicles, roadside stations and central trust authority. Both vehicle and Road side unitsare dedicated short-range communications (DSRC) devices. And it works with the approximate range of 1000 m. The network is suitable for both private data communications and public (mainly safety) communications but higher priority is given to public communications. Vehicular communication is developed as a part of intelligent transportation systems (ITS) in ad hoc networks.

### 3.1 EXISTING METHODOLOGY

#### 3.1.1 ROADSIDE COMMUNICATION

The Road side communication of VANETs consists of Trusted authority, fixed Road side units at the road side, and Onboard unit equipped in vehicles.

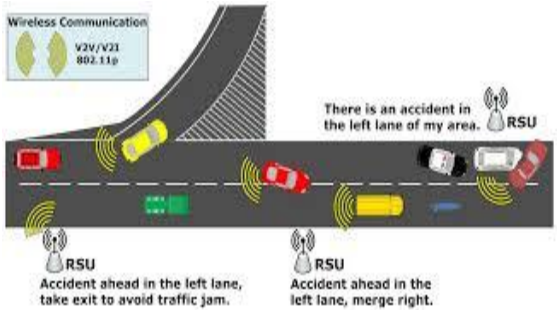


**Figure III: Road side communication for VANET**

TA is a trusted management center of the vehicular network. And it providesregistration, certification for all the Road side units and onboard units when they join the network. It divides precinct into several domains, and generates the group key and group signature materials for every domain, and then sends these materials to the RSUs in the domain. As usual, assume that TA is powerful enough in terms of communication, computation, and storage capability in terms of VANET.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Special Issue 6, May 2015**

RSUs are responsible for managing and communicating with vehicles in their communication range. They are bridges between TA and vehicles, in which connect with TA by wire and OBUs by a wireless channel.
Onboard units are fixed inside of the vehicle and periodically broadcast traffic-related status information such as its location, speed, and direction to improve the road environment, traffic safety, and multimedia infotainment dissemination for drivers and passengers. Each vehicle has a tamper-proof device (TPD) to store Security-related materials. Integrity by attaching a message authentication code (MAC) to the message, which is accomplished by a cryptographic keyed hash function.

HMAC is mainly used for two purposes: 1) Ensuring the validity of sender's identity, since only valid users can generate correct HMACs; and 2) Checking the integrity of messages before batch verification.

### 3.2 PROPOSED SYSTEM

VANET provide the communication channel for transmission of safety messages such as beacons and emergency messages. Primarily, emergency messages are transmitted with higher priority over beacons. But under the high density situations communication channel observes asignificant network load due to the frequently exchanged beacons. The MAC protocol suffers from a large number of packet collisions. Greater number of solutions has been proposed for increasing beacon performance based on the priority of incoming messages.
Congestion in communication leads to packet loss,reduction of throughput and degradation of channelquality. It is necessary to regulate and monitor the traffic level.
An OBU receives large number of messages for every 300 msecwhen large number of vehicles transmits beacons at a higher frequency then bandwidth can be exhausted very easily. In result significant number of packet collision occurs. And in a scenario of emergency message, if the channel is already congested then highly life-critical even-driven message which will be deprived of channel access will either get lost or delivered to its intended recipients with a much higher delay. Thus loss of beacons and emergency message will severely affect the safety of a vehicle in road side environment.
The proposed approach is to design a scheme which will allot time slots for beacons andemergency messages. Even if the vehicledensity increases and the channel gets exhausted easily ,this scheme will allow vehicles to broadcast messages by dynamically partitioning the beacon interval and increasing the transmission duration of messages. So, with the help of this scheme vehicles are allowed to broadcast emergency messages without the expense of beacons. And it is mainly based on the priority.

Algorithm:
Packet Queue (Pq) =Priority (P) + Deadline (D) (1)
Deadline (D) =Packet Arrival (Pt) + Max Latency (Mx) (2)
Where Pq is a packet queued to serve.
The proposed congestion control will be expressed with pseudo code below:

```
If (event-driven safety message is locally generated) or (event-driven safety message detected)
{
 Freeze all MAC queues except for the event-driven safety message
 }
Else {
          If (Packet Queue > 5)
         {
                  Discard extra incoming beacon messages in CCH channel
         }
         Else
   {
If (event-driven messages detected >1)
                  {
                           Freeze all MAC queues except for the event-driven safety messages queue based on priority-based EDF scheduling
                  }
```

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Special Issue 6, May 2015**

}
}

**3.2.1 Performance measure**

The security and performance analysis show that this scheme is efficient in terms of authentication speed, mobility while keeping conditional privacy in networks. To analyze the average end-to-end transmission delay with different number of vehicles in the communication range.

## IV.CONCLUSION

HMAC scheme is used in our scheme to replace the time-consumingin CRL checking and to ensure the integrity of messages before verification, reducing the number of invalid messages in the batch. The security andperformance analysis show that our scheme can achieve efficient groupsignature based authentication while keeping conditional privacy for VANETs.

Congestion Control Scheme will be introduced to design a scheme which will allot time slots for beacons and emergency messages. Even if thevehicle density increases and the channel gets exhausted easily ,this scheme will allow vehicles to broadcast messages by dynamically partitioning the beacon interval and increasing the transmission duration of messages. So, with the help of this scheme vehicles will be allowed to broadcast emergency messages without the expense of beacons, which are also equally important in vehicular communications. This Scheme is used to reduce the congestion in VANET and provides safety to the road side infrastructure.

## REFERENCES

[1] J. Guo, J. P. Baugh, and S. Wang," Agroup signature based secure and privacy-preserving vehicular communication framework," in Proc. Mobile Netw.Veh.Environ., Anchorage, AK, USA, May 2007, pp. 103–108.

[2] Y. Hao, Y. Cheng, and K. Ren, "Distributed key management with protection against RSU compromise in group signature based VANETs," in Proc. IEEE GLOBECOM, New Orleans, LA, USA, Dec. 2008, pp. 1–5.

[3] 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, Nov. 2008.

[4] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," IEEE Trans. Veh. Technol., vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

[5] A.Wasef and X. Shen, "Efficient group signature scheme supporting batch verification for securing vehicular networks," in Proc. IEEE ICC, Cape Town, South Africa, May 2010, pp. 1–5.