A Cooperative Dual message Authentication and Group key Management in VANET

M.Padma Priya¹, P.Jayaselvi², R.Valarmathi³

¹, ², ³ Assistant Professor, Department of CSE, Sri Sairam Engineering College, Chennai, 600044, India.

¹padmapriya.cse@sairam.edu.in, tel-9840708360
²jayaselvi.cse@sairam.edu.in, tel-9894861337
³valarmathi.cse@sairam.edu.in, tel-9444778710

Abstract

VANET has become an active area of research and development. This technology has been used to improve vehicle and road safety by exchanging information regarding traffic congestion and road condition during emergency to comfort the drivers and passengers. But such environments are more prone to security threats. Thus the major concern in such environment is to provide authentication services and to maintain confidentiality among users. For this purpose a trustworthy authority (TA) is created which provides services to users and authentication of messages that is exchanged between trusted authorities and VANET nodes. Firstly a cooperative dual authentication method is used to issue an effective and noteworthy security in order to block the vehicles which are uncertified. Next we use a group key technique to distribute key among group of users and a key pair is assigned to them. Keys are updated periodically after every join or leave operations. This scheme allows users to send and receive messages to and from the trusted authority and through road side units (RSU’s) in a secured manner.

Keywords: VANET, trusted authority, dual authentication, RSU

I Introduction
An ad-Hoc network is an infrastructure less network and self-organizing networks. It extends mobile concepts to vehicular environment. The mobile nodes act as the routers. The routers transmit, receive and also relay information. VANET uses equipped vehicles as network nodes. VANET promises safer roads and assures no accidents. VANET helps driver of the vehicle to know about the traffic. Communication types in VANETS include Vehicle to Vehicle communication (V to V) and vehicle to Infrastructure communication (V to I). V to V communication is used for limited range of vehicular networks. They do not require any road side infrastructure whereas V to I communication or vehicle to roadside communication is used for long range vehicular network and uses the pre-existing network infrastructure.

![Fig 1. VANET Environment](image)

VANET is an emerging technology that incorporates the potentiality of wireless networks to vehicular environment. It is used to share information about road conditions, traffic and collision detection. It acts as a powerful Ad-Hoc network between vehicles and RSU’s. VANET’s uses group communication to establish a communication among nearby vehicles and RSU’s. Information from one user to other users needs to be broadcasted. An effective communication can be achieved between mobile nodes by using different networking technology such as WiMAX, Bluetooth etc.

The main components of VANET includes the trusted authority(TA) ,Road side units(RSU), On Board units(OBU). A TA authenticates all the users of VANET environment and manages the keys for all those users. RSU are used to route the messages between the users and authority. Each user has OBU in their vehicle, contains the sensors for communicating with other users.

Main motto of this paper is to authorize the OBU’s(On board unit) and the authority in both sides and to control key for reliable and efficient data transmission in VANET.

II Background & Related Work

Many literature surveys are conducted on VANETs which worked on the schemes that provide authentication only. One of the approach used in existing system Anonymous Batch authentication which provides value-Added Services to VANET’s [5].This scheme was introduced to verify miscellaneous requests which are forwarded from distinct vehicles. It authenticates multiple requests efficiently by a single authentication operation. The main issue with this system was scalability problem. Another approach was to provide secure group communication using key graphs[13].Here key graphs are introduced to specify secure groups. Three strategies are defined for distributing rekey messages securely after a join/leave. The Group key management service is scalable to large groups with frequent joins and leave operations. The major drawback with this system is the usage of user-oriented rekeying on the sever side and group oriented rekeying on the client side which effects the performance.

Next approach is a Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework. It achieves authenticity, data integrity, anonymity, and accountability at the same time. It
provides authenticity and ensures secrecy of the data. Here Vehicles use their own identity. A Scalable Robust Authentication protocol for Secure Vehicular Communications [15] is another technique proposed by Lei Zhang. In this system each RSU maintains and manages an on-the-fly group within its communication range. Here vehicles broadcast V to V messages, which are verified instantly by the vehicles in the same group. It uses an ID-based cryptography which actually increases storage space.

Co-operative Message Authentication (CMAP) [12] is another approach which identifies malicious information that is being broadcasted by a malicious user. The main disadvantage of this system is that if no verifier is present then the malicious information can be broadcasted to legitimate users also.

Yet another approach [10] Certificate Management Scheme for Vehicular Networks which offers a flexible way of certificate management as well as provides a way for OBU’s to update the certificate anywhere at any time. This system can reduce the complexity of certificate management and can achieve excellent security. Major drawback of this system is long delay incurred in checking the revocation status of a certificate.

### III Existing Model

Existing system used an elliptic Curve Digital Signature Algorithm (ECDSA). It used a key pair (public and private key) to authenticate. Also digital certificates management techniques were used which includes the concept of a Public Key Infrastructure (PKI). Here each vehicle is provided with a certificate for a short duration which is further updated frequently from any RSU in order to preserve privacy. As there are no verifiers to validate the messages, a malicious and unauthorized message can penetrate into the network and can be received by the vehicles. The major drawback of the system is that an additional overhead is created to identify the malignant messages that are being transmitted by the unauthorized users.

### IV Proposed System

We propose a group key technique in order to reduce the computational cost of TA and the re-keying operation. To implement this, the Trusted Authority is allowed to perform addition and subtraction operations to upgrade the group key of its users. Vehicles of a group performs multicast group operation i.e. requires one modulo operation to recover the key when the group members are changed.

- A secure authentication technique is proposed which helps in blocking the malign vehicles to penetrate into the VANET environment.
- A group key management approach is also introduced to spread the data from the Trusted Authority to the class of users in a reliable way.
- Authentication is done twice between the user and the authority.
- Malicious vehicles or intruders will not be allowed into the network because authentication will be done while the vehicles enter into the network.
- Vehicles are classified as primary and secondary users to distribute group keys for communication between them.
Figure 2 shows the overall system model which depicts the information flow and services offered by RSU to users.

V Network formation

An authority is created for monitoring the network. Then the RSU’s and OBU’s are created for establishing communication among the vehicles. The OBU’s are the equipment’s which are integrated into the vehicles. Services are forwarded from OBU via RSU. The OBU’s which are under the span of RSU will be the vehicles in its range.

The figures 3(a),(b),(c) shows the creation of trusted authority, RSU and OBU as per distance and range calculation.
VI Vehicle user’s authentication

Here authentication of the vehicle user is done with a secret key of vehicle in order to verify the authority of the users. In the proposed system the authority will not allow the unauthorized user to enter the network and a hash code is used to validate the user. The User, who needs to enter the VANET, does the authentication using a smart card. A hash code gets generated after authenticating using smart card. This hash code is encrypted with the user’s key and sent to the trusted authority through the RSU’s. The TA receives it and decrypts and finally compares this hash code with one stored in its database. Authentication is successful when it matches and the user is added to the VANET. Otherwise vehicle is identified as unauthorized and does not allow to enter into the VANET.

VII Group key management

In this module, two keys for authentication are managed for the road side unit which includes the primary and secondary user key. Here the primary users are linked directly to the authority and the secondary user links with the primary user for getting the information related to the temperature and road conditions etc. The information which is broadcasted by the authority will be encountered only by the primary user.
Fig. 5. Group key management

The above figure 6 shows the generation of primary and secondary user OBU list and authentication of vehicle using secret key. Then allocating group key both for primary and secondary users.

VIII V2R and V2V Communication

This module represents communication between vehicle to road side unit and vehicle to other vehicles. Here information transaction is done between services. At first RSU and PU interacts with each other. Prior of accepting the information that is being transmitted by the PU (Primary user), it has to be verified by the authority to identify whether its from an authorized primary user. After verifying the identity it will forward the information to the SU (secondary user). It will also be validated by the PU with the group key.

Fig. 7. Sending services from primary user to secondary user

Figure 7 shows the services and information forwarded from RSU to primary user and then to secondary user. Primary and secondary user group key has to be entered to receive the information.

IX Conclusion and Future Work

Dual authentication and group key management is implemented for secure data transmission using a smartcard device in vehicular Ad-Hoc networks. The vehicles are authenticated while entering into the region, group keys are provided when the vehicles enter into a new region. As malicious vehicles are not allowed to enter into the network false messages are not transferred between vehicles, eavesdropping is also controlled. The attacks are prevented by authenticating the users two times.
As evaluating VANET environment is expensive, simulation technique has to be refined and improved in order to show the impact of VANETs on traffic, road conditions, and accident. In future work the Road Side Units can communicate with the secondary user directly without the help of the primary user. The range of coverage of Road Side Units can be increased.

References


