Secure Authentication in Vehicular Ad Hoc Networks (VANET)

Shreya Singh
Supervisor:Keith Mayes

ABSTRACT

Many schemes already exist such as the public-key infrastructure models. Two new basic approaches to secure authentication in VANETs are described. Kerberos based scheme is based on the Kerberos authentication model whereas the token based scheme used a challenge-response protocol for authentication and also has a simple reputation based node blacklisting technique. The token based scheme provides reliable authentication with the use of a smart card and tokens. A basic model describing both these approaches is presented.

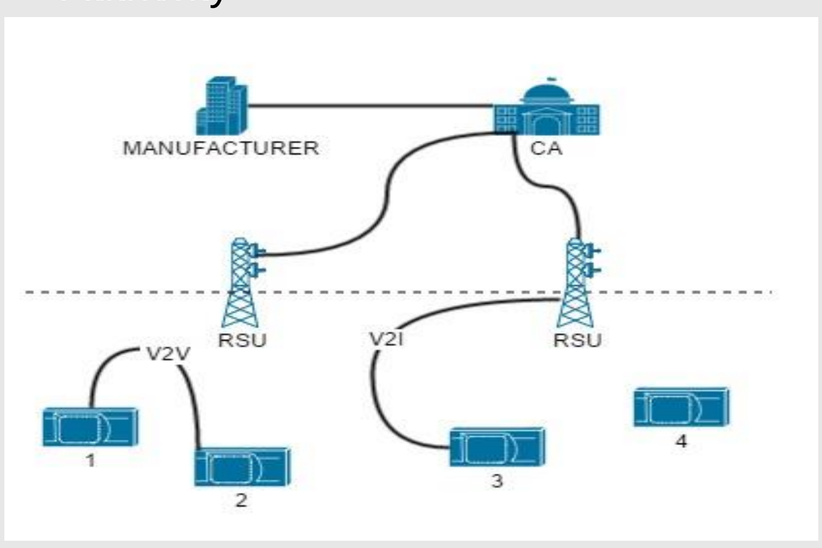
PROBLEM

With continued development in the field of ad hoc networks, its importance with relation to vehicular networks was realised. Vehicular networks are here to transform the future of the automobile industry by providing safety and comfort applications. These networks will provide safety applications including the transmission of traffic information related safety messages between vehicles which is designed for optimization. By making use of the advantages provided by these networks, a vehicle can be gifted the power of intelligence. Unfortunately such applications also need to be highly secured in order to prevent attacks. Attacks on these systems can prove to be very dangerous and can lead to loss of life or revenue.

Vehicular Ad Hoc Networks

Structure

- Road-side unit
- On-board unit
- Application unit
- Manufacture
- Authority

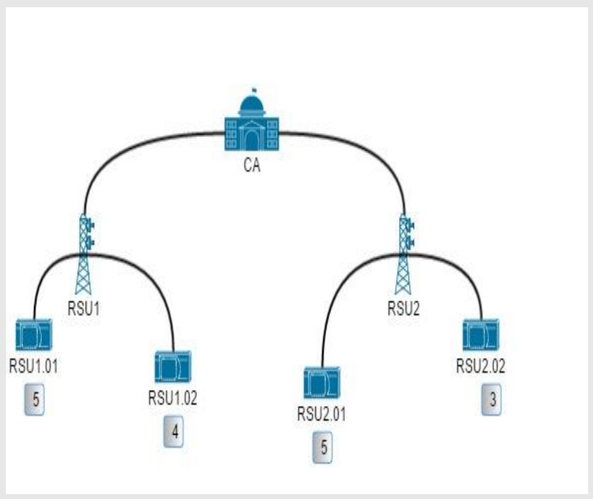


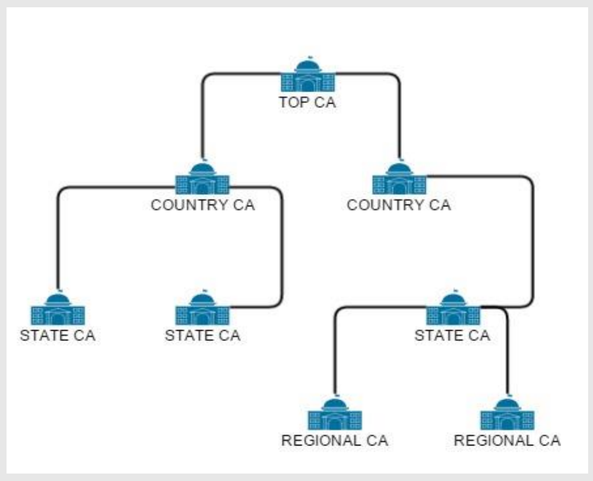
Token based authentication scheme in VANETs

1- Level 0 or the certification authority
2- Level 1 or the RSU
3- Level 2 or nodes
Vehicle Identification number (VIN)-

The VIN will be stored inside the smart card. This VIN is generally issued by the manufacturer of the vehicle and is unique in nature. The VIN will correspond to crucial information like-

- The manufacturer name
- The manufacturer serial number
- Vehicle serial number





STEPS IN TOKEN APPROACH

The OBU will send a request to the RSU with the purpose of registering itself with that particular RSU. Note that there can be two circumstances-

- *Case 1* - When a vehicle node is registering itself with a RSU for the first time. This can be possible in the case of a new vehicle.
- *Case 2*- When a vehicle has already registered itself with an RSU and is now trying to register itself with another RSU.

OBU → RSU: Request

RSU → CA: Challenge Request

CA → RSU: challenge

OBU→ smart card: Challenge

Smart card → OBU: E_k {RESPONSE||CHALLENGE}

OBU → RSU: Response

RSU → CA: Response

CA → RSU: First token

RSU → OBU: Second Token

Token characteristics

The token issued by the CA to the RSU will have these features-

- ***PROPERTY 1-*** The token individually authenticates the node.
- ***PROPERTY 2-*** A new token will be generated for every node that is identified.
- ***PROPERTY 3-*** The node corresponds to a particular vehicle, whose identity is only known to the CA and not the RSU.
- ***PROPERTY 4-*** The token issued to the RSU will identify the CA that issues it and will have a CA identifier along with a random number.
- ***PROPERTY 5-*** The CA will maintain a database in which it will make an entry when a token is issued. This entry will be the token number which will correspond to the particular VIN. Thus only the CA has knowledge about the identity of the vehicle. Using this privacy of the vehicle can be guaranteed.

The token issued by the RSU to the node will have certain distinguished features-

PROPERTY 1- The token will individually authenticate the node.

PROPERTY 2- The token will be valid only for that particular VANET. This means that when a vehicle that is part of a VANET leaves it to go and join some other VANET, then the vehicle will need to go through the authentication process again using which it will have to obtain a new token from the respective RSU to start communicating with the other nodes in the network

PROPERTY 3- The token will uniquely identify the RSU. The token number will contain the identifier of the RSU that issued the token.

PROPERTY 4- The token will bind itself to the OBU.