A Billing Scheme of Tollbooth in Service Oriented Vehicular Network

Thiagarajan
Research scholar, Anna university chennai,
Assistant Professor, Prathyusha Engineering College, Chennai, Tamil Nadu, India.

Dr.Moorthi
Professor, Prathyusha Engineering College, Chennai, Tamil Nadu, India.

Abstract – In this paper we have proposed to billing scheme of tollbooth in service oriented vehicular network It is an emerging technology is built and improve the safety. The VANETs – vehicular Ad-hoc network is a most important role for commercial services. The vehicular network is works with an ore effective and good approach. I toll requirement is essential to control fine grained, I our main aim is clear the billing issue and address with safely, privacy using VANETs, in proposed scheme to long access delay of the centralized novel AAA architecture. In high security billing and control access for encryption ensure fine- grained the valid electronic currency are to authorized to access the requested services, in our system to high security non fraud electronic currency prevention, analysis and simulated with demonstrate using AAA architecture with centralized and decentralized method for scalability improve for service orientation VANETs.

Index Terms – Secure billing, VANETs, Electronic currency, Security, Access control devices.

Introduction

The VANETs - vehicular Ad-hoc networks is one of the most popular networks for access with security and privacy notation used for industry and academic as well as researcher. It's the Dedicated short range protocol to communication using standard IEEE802.11p worked with group communication protocol, the VANETs is used for communication is classified in to two various types one is V to V- vehicle to vehicle and another is V to I- Vehicle to infrastructure, in purpose Road access unit(RAU) is function to transferred the data to gateway. VANETs application is referred to service in vehicular network for commercial, access to vehicular network into practice emerging challenges must be consider. In VANET address in security issue is standard IEEE609.2 for security and vehicular network such as includes billing process and authentication.

The novel based AAA architecture is widely adopted for high secure and authentication in standard IEEE EAP /802.1X based for authorization "New research challenges, especially in the aspects of security, user privacy, and billing. In this article we first identify the key requirements of authentication, privacy preservation, and billing for service delivery in vehicular networks"[1]. "The standard covers methods for securing WAVE management messages and application messages, with the exception of vehicle-originating safety messages" [2]. "Lightweight authenticated key establishment scheme with privacy preservation to secure the communications between mobile vehicles and roadside infrastructure in a VANET is proposed" [3]. We are proposed a portable billing machine with fine-grained control to access with privacy and security to use of E-coin to achieve location authentication.

Motivation of Research

The current security mechanisms in VANETs are used in service oriented VANETs to access centralized billing system. The security is the important criteria for billing system and identification in road side units. He hole authentication is described in standard IEEE802.1x its required for delay up to 750-1200 Ms for long time authentication due to the long roundtrip passing signal between the AAA server to RAU. The final end of the problem if any other occurs in the common server to large scale vehicular network (8). Centralized AAA architecture it is one of the lead a high packet low loss ratio and lower customer satisfaction in this disadvantage overcomes to utilize our localized security scheme in VANETs.

The managing of service provider (SP) et the offer from service resources like security and privacy issue because is belong to government in GSB trusted, in service provider (SP) to offer some services to vehicle including location based service, multimedia and content services. The government is maintained information storage units with well equipped to subordination with RAU. The RAU is the gateway for information delivering in particular vehicle with use of SPs and GSB. Every vehicle having he separate onboard unit (OBU) to communicate with RAU for the purpose of moving vehicle identification. The DSRC protocol is majorly used for communication.

System model and security objective

I our proposed system model for Service oriented VANETs is shown in fig1 in following network model we assume that work as four roles.

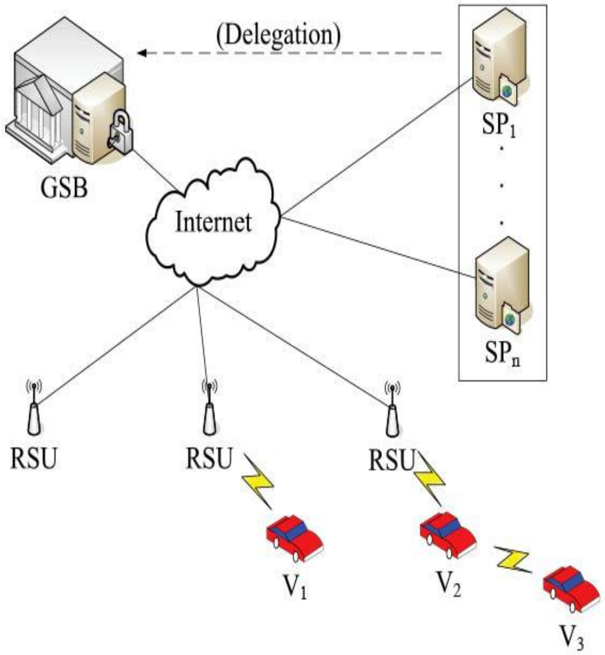

Fig1. System model of service oriented vehicular networks

Security Intention

In major service oriented vehicular network is having some security objectives to e follow.

- Non repudiated billing
- Avoidance authentication ad key agreement
- Avoidance of double spending problem
- Avoidance of Fraud E-currency
- Privacy
- Fine grain access control.

Proposed system

The proposed system are mainly two advantages of the public broadcasting services are given bellow, it allows fine grained control access over file service and E-currency acceptable to resolve he bill issue it has used novel cryptography technique ABE-KP adopted, Each vehicle having unique access structure under cryptography technique that each E-coin is exclude to its own vehicle. The flow chart of proposed system is shown in fig2. This system is based on service order and protocol to handoff clearance.

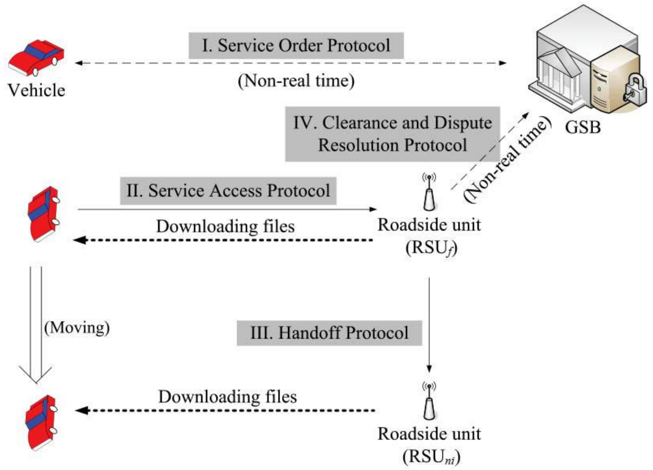

Fig 2. Proposed public broadcast service.

The system initialize with GSB service provider (SP), RAU, vehicle. First we have ensure with the every vehicle is well equipped with tamper proof device that is secure that identification of compromise attempt under any condition. It is assume that no data to be stored in the device for TPD. The TPD is the performance of device to real identity with password, TPD device is activate using PWD and user to be verified and secure to make the E-coin payment at the any circumstance. In order to access the service the system must to do two procedures E-coin purchase and service registration.

System architecture

The architecture involves the processing of data in the Road side environment. The vehicle wants to send the request query to intermediate nodes in order to collect the information from the vehicle.

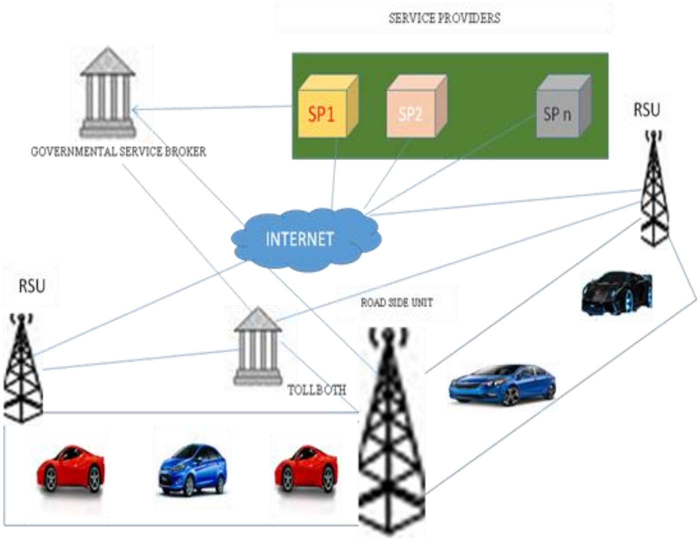

Fig 3. System architecture using DSRC protocol

Distributed public key voiding

In order to service oriented vehicle networks (VAVENTs) is high security V2V communication is based on public key authorized. The efficiency of service provider represents the ajor change. In certificate authority o issue the certificate to public owner identity with password, “In traditional public key infrastructure (PKI) architecture, the most commonly adopted certificate revocation scheme is through a certificate revocation list (CRL), which is a list of revoked certificates stored in central repositories prepared in CAs. In the context of VANETs, the CA adds the identification of the revoked certificate(s) to a CRL. The CA then publishes the updated CRL to all VANET participants, instructing them not to trust the revoked certificate”. To achieve the encountered vehicle roa crossing is successful.

Conclusion

This study main objective to resolve privacy, security and billing issue of service-oriented vehicular network, fin grained control access if full supported and satisfy the customer. The vehicular network is works with an ore effective and good approach. I toll requirement is essential to control fine grained, I our main aim is clear the billing issue and address with safely, privacy using VANETs, in proposed scheme to long access delay of the centralized novel AAA architecture. In high security billing and control access for encryption ensure fine- grained the valid electronic currency are to authorized to access the requested services, in our system to high security non fraud electronic currency prevention, analysis and simulated with demonstrated.

References

[1] H.Zhu et.al.,“Security in service-oriented vehicular networks”, IEEE wireless comm. Vol.16, issueno.4, PP16-22 2009.

[2] X.Shen et.al.,“Trial-Use Standard for Wireless Access in Vehicular Environment-Security Services for Applications and Management Message”, IEEE standard 1609.2-2006- Jul 2006.

[3] C.T.Li et.a., ,“A secure and efficient communication scheme with authenticated key establishment and privacy perserving for vehicular ad hoc networks,” compt.comm.v-31,no.12 2008.

[4] C.W.Wang et.l.,“A novel secure communication scheme in vehicular ad hoc networks,” compt.comm. v-31, no12 2008.

[5] M.ray et.al., “Securing vehicular ad hoc networks,”J.Comput.secure vol.15 no.1 pp-39-68, 2007.

[6] H.Zhu et.al., ,“SLAB: A secure localized authentication and billing scheme for wireless mesh networks,”IEEE Trans. Wireless com. Oct.2008.

[7] L.Zhang et.al.,“A scalable robust authentication protocol for secure vehicular communications,” ,”IEEE Trans. Wireless com. May.2010.

Authors

Mr.Thiagarajan working as an Assistant Professor in computer Science and Engineering Department at Prathyusha Engineering College also doing part time research in Anna University in the domain on MANET

Dr.Moorthi working as a Associate Professor in Electronics and Communication Engineering Department at Prathyusha Engineering College