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. 5, Issue 3, March 2016

Implementing a Billing Scheme with Fine Grained Distributed Access Control for Service Oriented Vehicular Networks

R.Balamurugan[1], S.Kungumavathi[2]

Assistant Professor, Department of CSE, Adhiparasakthi Engineering College, Melmaruvathur, India [1]

PG Scholar, Department of CSE, Adhiparasakthi Engineering College, Melmaruvathur, India[2]

ABSTRACT: VANETs are wireless network technology used to improve road safety. To meet the diverse requirements of different users, fine grained distributeddata access control is essential. This paper aims to address security, privacy and billing issues in service oriented vehicular networks. Taking advantage of a portable electronic currency, the proposed scheme mitigates the long authentication delay of the centralized AAA architecture. Variant attribute based encryption ensures fine grained distributed data access control and secure billing. Only vehicles possessing the proper service attributes and valid electronic currency are authorized to access the requested service file. The security properties of entity authentication, session key agreement, privacy, fraud electronic currency prevention, double spending prevention, and non-repudiated billing are achieved.

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) are created by applying the principles of mobile ad hoc networks (MANETs) the spontaneous creation of a wireless network for data exchange to the domain of vehicles. They are a key component of intelligent transportation systems (ITS). While, in the early 2000s, VANETs were seen as a mere one to one application of MANET principles, they have since then developed into a field of research in their own right. By 2015, the term VANET became mostly synonymous with the more generic term inter vehicle communication (IVC), although the focus remains on the aspect of spontaneous networking, much less on the use of infrastructure like Road Side Units (RSUs) or cellular networks.

To evaluate VANET protocols and services, the first step is to perform an outdoor experiment. Many wireless technologies such as GPRS, IEEE 802.11p and IEEE 802.16 have been proposed for reliable traffic information. Before the technology hits the ground and can meet the expectations, a series of experiments should be performed to test it. These experiments could be expensive and highly complex to inherit all kinds of situation.

VANET relies on and is related to two other simulations for its smooth functioning, namely traffic simulation and network simulation. Network simulators are used to evaluate network protocols and application in a variety of conditions. The traffic simulators are used for transportation and traffic engineering. These simulations work independently but to satisfy the need of VANET, a solution is required to use these simulators together. Numerous traffic and network simulations have been tried to resolve the issues with VANET but every solution has had its shortcomings. There are a large number of traffic and network simulator and they need to be used together into what can be called VANET simulator. There are few tools for VANET simulation but most of them have the problem of proper 'interaction'. Thus a proper selection of a simulator is also a question for simulation. Therefore, we will debate on present tools and will suggest the choice with proper 'interaction'.

In this thesis we present NCTUns (National Chiao Tung University) simulator, a powerful network and traffic simulator freely available for the research community. NCTUns replaced Harvard simulators in 2002 and after the release of version 4, it greatly supports the simulation of ITS (Intelligent Transpiration System) network.

VANET is a widely discussed area of wireless communication at present. VANET is a subset of MANET where nodes represent vehicles moving at high pace and vehicle traffic determined regularity. This technology enables communication between vehicles and nearby road-side infrastructure and is made possible through a wireless sensing device installed in the vehicles. With the inception of VANET, new opportunities and related technologies like applications for traffic jam, accident control and weather updates have appeared.

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. 5, Issue 3, March 2016

VANET performance can be tested in real situations but factors like cost, inaccurate results and protocol evaluation of complex environment may contribute towards a disappointing end. An automated tool called simulation can imitate the protocol and yield a similar result to that of the real world. VANET differs from MANET (mobile ad-hoc network) because in VANET the nodes strictly follow the traffic rules and their pattern of movement is very complex.

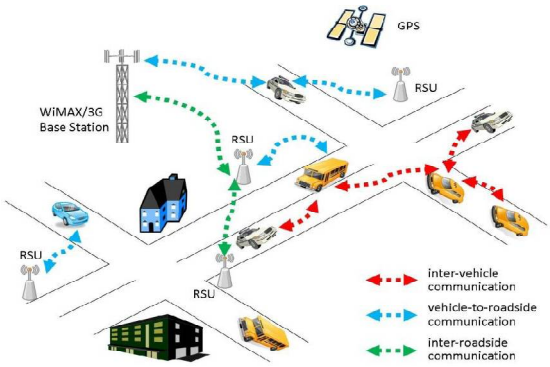

Fig. 1.1 VANET (Vehicular Adhoc Networks)

Characteristics of VANET

- High mobility of nodes
- Unreliable wireless channel
- One dimensional nature of roads
- The structure of lanes
- The group mobility of vehicles
- Equipped on vehicles
- Unbounded Network Size
- Better Physical Protection

II. LITERATURE SURVEY

D. Niyato and E. Hossain (2010) described a unified framework for optimal wireless access for data streaming over vehicle-to-roadside communications for the wireless access through vehicle-to-roadside (V2R) communications can be used in public transportation vehicles for streaming applications, e.g., video and interactive advertisements. A hierarchical optimization framework is presented to obtain both short- and long term optimal decisions on wireless access for streaming applications in a public transportation system. This framework considers the application requirements, the cost of wireless connectivity for transit service provider, and the revenue of the wireless network service provider. The onboard unit in a vehicle makes a short term decision on whether to download streaming data while it is in the coverage area of a roadside unit (RSU). The objective of this decision is to minimize the cost of wireless connectivity while satisfying the application quality of service (QoS) requirement in terms of the maximum buffer under run probability. **Y. Cao, K. - C. Leung, and V. O. K. Li (2010)** described bandwidth guaranteed fair scheduling with effective excess bandwidth allocation for wireless networks for Traffic scheduling is key to the provision of quality of service (qos) differentiation and guarantees in wireless networks. Unlike its wireline counterpart, wireless communications pose special channel-specific problems such as time-varying link capacities and location dependent errors. These problems make designing efficient and effective traffic scheduling algorithms for wireless networks very challenging. Although many wireless packet scheduling algorithms have been proposed in recent years, issues such as how to improve bandwidth efficiency and maintain goodput fairness with various link qualities for power-constrained mobile hosts remain unresolved.

S. Yu, K. Ren , and W. Lou (2011) described FDAC: Toward Fine-Grained Distributed Data Access Control in Wireless Sensor Networks for a distributed sensor data storage and retrieval have gained increasing popularity in recent years for supporting various applications. While distributed architecture enjoys a more robust and fault tolerant wireless sensor network (WSN), such architecture also poses a number of security challenges especially when applied in mission critical applications such as battlefield and e-healthcare. As sensor data are stored and maintained by individual

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. 5, Issue 3, March 2016

sensors and unattended sensors are easily subject to strong attacks such as physical compromise, it is significantly harder to ensure data security. In many mission critical applications, fine-grained data access control is a must as illegal access to the sensitive data may cause disastrous results and/or be prohibited by the law. Last but not least, sensor nodes usually are resource-constrained, which limits the direct adoption of expensive cryptographic primitives .To address the above challenges, we propose, in this paper, a distributed data access control scheme that is able to enforce fine-grained access control over sensor data and is resilient against strong attacks such as sensor compromise and user colluding.The proposed scheme exploits a novel cryptographic primitive called attribute based encryption (ABE), tailors, and adapts it for WSNs with respect to both performance and security requirements.

S. Yu, C. Wang, K. Ren, and W. Lou (2010) described for Achieving secure, scalable, and fine grained data access control in cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents.

III. SYSTEM ARCHITECTURE AND DESIGN

Design is a meaningful engineering representation of something that is to be built. Software design is a process through which the requirements are translated into a representation of the software. Design is the place where quality is fostered in software engineering. Design is the perfect way to accurately translate a customer's requirements into a finished software product. Design creates a representation or model, provides detail about software data structure, architecture, interfaces and components that are necessary to implement a system. This chapter discusses the design part of the project. Here in this document the various UML diagrams that are used for the implementation of the project are discussed.

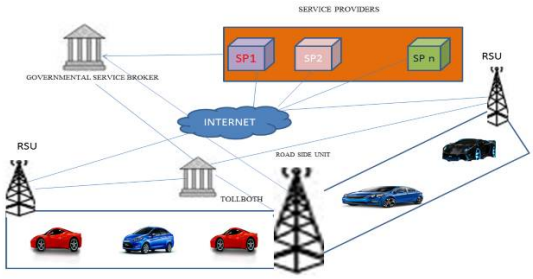

Fig. 1.2 System Architecture

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.The communications made possible by VANETs can be classified as either vehicle to infrastructure (V2I) or vehicle-to-vehicle (V2V). The dedicated short-range communication (DSRC) protocol standardized by the IEEE 802.11p working group serves as the communicationprotocol. VANETs' primary function is to improve road safety. In general, roadside units (RSUs) function as gateways for transferring data. Unfortunately, RSUs cannot provide coverage in all areas. In these cases, V2V transmission plays a vital role in relaying messages. As more vehicles take part in VANETs, more of VANETs' advantages are realized. Consequently, the DSRC standard also provides commercial applications to encourage customers to take part in VANETs.

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. 5, Issue 3, March 2016

NODE DEPLOYMENT

The number have been created depends upon the user, following nodes are Governmental Service Broker (GSB):The GSB belongs to the government and is trusted. The GSB's responsibility is to issue security parameters and manage the service resources offered by service providers (SPs). The GSB also serves as the arbitrator if there are disputes between the vehicles and SPs.Service Providers (SPs): SPs offer many services to vehicles, including multimedia content services and location-based services. SPs may periodically update popular service files for the RSUs. Roadside Units (RSUs): RSUs are subordinated by the government and equipped with storage units for storing information. The RSUs function as gateways for delivering data among vehicles, SPs and the GSB.Vehicles (Vs): Vehicles move along roads and are installed with onboard units (OBUs) to communicate with each other and with RSUs. Communication is based on the DSRC protocol.

Mobile Node is the basic nsNode object with added functionalities like movement, ability to transmit and receive on a channel that allows it to be used to create mobile, wireless simulation environments. The class Mobile Node is derived from the base class Node. Mobile Node is a split object. The mobility features including node movement, periodic position updates, maintaining topology boundary etc. are implemented in C++ while plumbing of network components within Mobile Node itself (like classifiers, dmux , LL, Mac, Channel etc.) have been implemented in Otcl.

SECURITY OBJECTIVES

Entity authentication and key agreementthe validity of the requesting vehicle should be authenticated, and a session key agreement is also demanded for subsequent communications.Fine grained access controlThe SPs should be able to enforce fine-grained access control on service files while differentiated services are provided.Privacy

A secure service-oriented vehicular network should protect individual vehicles' identities against anyone except the GSB.Prevention of fraud electronic currencyIn case a vehicle picks up or illegally purchases electronic currency, referred to as fraud electronic currency, RSUs should not grant a service request using fraud electronic currency.

Prevention of double spending problem

No vehicle can overuse its electronic currency. Each RSU should be able to detect the occurrence of a double spending event and refuse to offer services.

Non repudiated billing

Non repudiation is an important property in electronic commerce. Each vehicle should possess unique credentials that cannot be tampered with or counterfeited by attackers; these credentials can serve as evidence to settle commercial disputes.

We assume that sensor nodes are similar to the current generation of sensor nodes, e.g., MicaZ or Telos motes, in their computational and communication capabilities and power resources, while BS is a laptop class device supplied with long-lasting power. We assume that BS cannot be compromised and it uses a protocol such as μTesla to authenticate its broadcast messages to the network nodes. We also assume each node shares a pair-wise key with BS. Let the key of the node with ID X be denoted as KX . To authenticate a message to BS, a node X sends a MAC (Message Authentication Code) generated using the key KX. We further assume that each pair of neighboring nodes has a pairwise key to authenticate its mutual communication.

One is a cryptographically secure pseudo-random function H that uniformly maps the inputs (the node id and Sg) into the\ range of [0, 1]; the other is a grouping function Fg that takes the local node's count value as the input and outputs a real number between [0, 1]. More specifically, each node, say x, decides if it is a leader node by checking whether H(Sg|x) <Fg(c)where c is the count value of node x. If this inequality is true, node x becomes a leader. Once a node becomes the leader, all the nodes in its sub tree that have not been grouped yet become members of its group. The function Fg() is constructed such that Fg(c) increases with the count value c. This ensures that nodes with more descendants have a higher probability of becoming group leaders.

PERFORMANCE METRICS

Performance metrics is used to measure the performance of centralized AAA service oriented vehicular network with fine grained distributed access control in the form of graph.

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. 5, Issue 3, March 2016

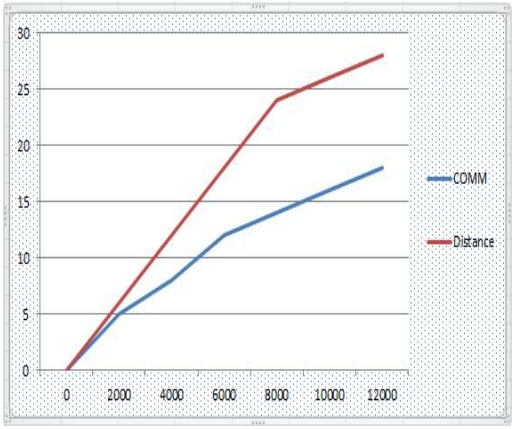

Fig. 1.3 The performance of communication delay

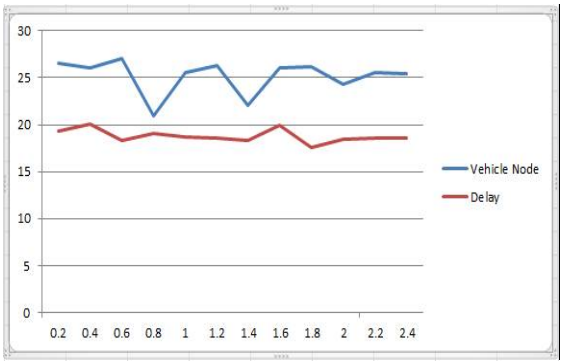

Fig. 1.4 The performance of communication throughput.

IV. ALGORITHMS

SIGN PRIVATE KEY GENERATION ALGORITHM

To fulfill the requirement of privacy protection, each SP periodically receives a pseudo identity tID and the corresponding signing private key generation algorithm is used. User choose the real identity as [0,1] and then requestor id check with the government service broker id, if equal then id is set as a pseudo identity as public, finally private key is generated.

VERIFICATION ALGORITHM

This algorithm is used to verifying the validity of transaction The GSB creates the E coin signature σGSB using the sign algorithm. The E coin = <Cred, d, ExpDate, σGSB>, ek1E and ek2E are then loaded into the vehicle. After receiving the E coin, the vehicle first verifies σGSB using the verification algorithm. When the integrity is valid, the TPD further checks whether both Cred and d adhere to the purchase contract using e(T1E , ek1E)ˆd?= Cred, where d is the face value in the purchase contract, as verified below. If one verification fails, the E coin payment is denied. If all the values are authenticated, the TPD stores ek1E and ek2E and keeps track of the face value and compute the credit.

ECDSA ALGORITHM

The proposed algorithm uses ECDSA (Elliptic Curve Digital Signature Algorithm) scheme to sign the message and thus it forms the message signature scheme. ECDSA uses random number generator, to obtain different random numbers that serve as private keys. With respect to the private key, the public key is computed by the sender. The private public key pairs are renewed once they are used to sign a message. The Public Key Infrastructure (PKI) is responsible for distribution of these public keys to any node, which is in the radio range of the source node. This is used to signature, verifying and obtaining authentication.

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. 5, Issue 3, March 2016

V. RESULTS

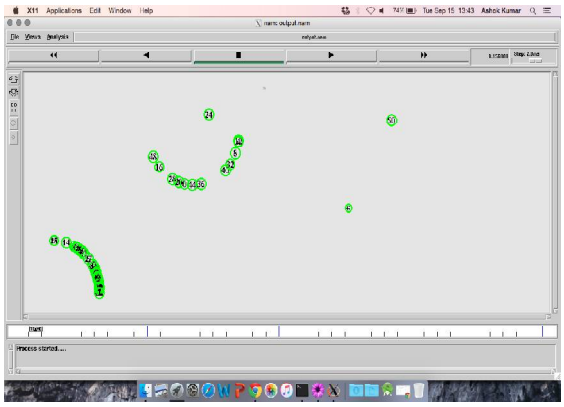

Fig. 1.5 Creating number of nodes

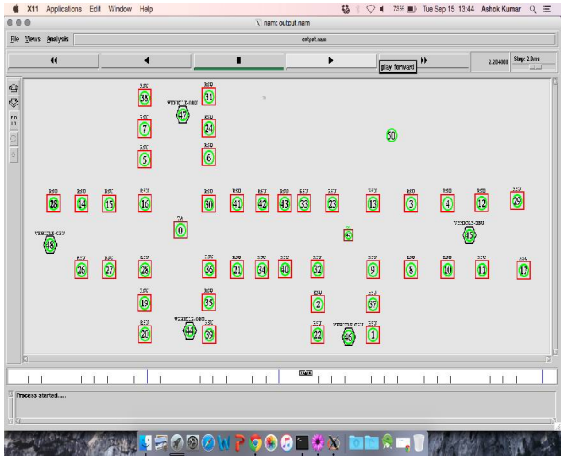

Fig. 1.6 Deployment of nodes as vehicle, RSU, Toll both , OBU.

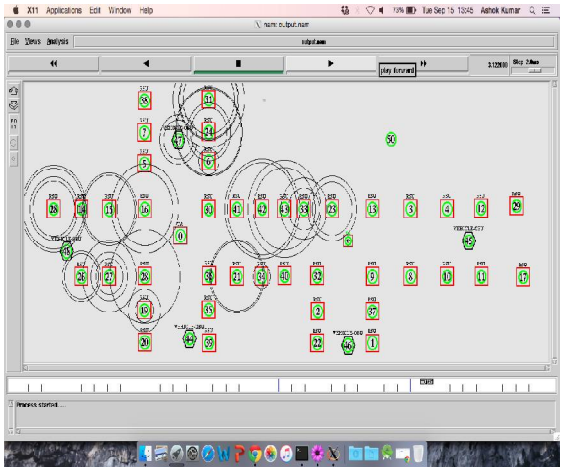

Fig. 1.7 Moving of vehicle form vehicle to vehicle and vehicle to infrastructure.

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. 5, Issue 3, March 2016

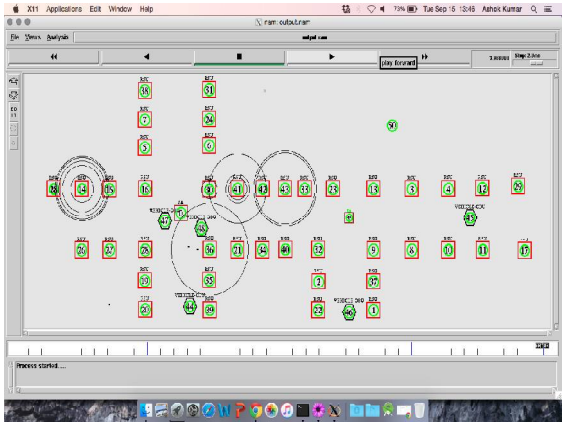

Fig. 1.8 Access of Toll booth service in VANET

VI. CONCLUSION AND FUTURE WORK

To resolve the security, privacy and billing issues of service oriented vehicular networks. Fine grained Access control is also supported to fit the diverse requirements of different consumers. A portable electronic currency is utilized to eliminate communications between RSU and AAA servers and to diminish authentication delay. Electronic currency fraud prevention, double spending Prevention and non repudiated billing properties are also achieved. To the best of our knowledge, this work is the first attempt to simultaneously address the billing and fine grained access control issues of service oriented vehicular Networks.

To investigate how best to address efficient user revocation issues, dynamic attribute addition, and secure V2V transmissions and also try to improve the scalability of our scheme in order to access secure service. Vehicular Communication (VC) systems cannot escape from this ongoing trend towards multi-service environments accessible from anywhere. To meet the diverse requirements of vehicle operators and Service Providers (SPs), SEROSA, a service oriented security and privacy preserving architecture for VC. By synthesizing existing VC standards and Web Services (WS), our architecture provides comprehensive identity and service management while ensuring interoperability with existing SPs. It significantly extends the state of the art and serves as a catalyst for the integration of vehicles into the vast domain of Internet based services.

REFERENCES

1.H. Zhu, R. Lu, X. Shen, and X. Lin, “Security in service-oriented vehicular networks, Aug. 2009
2.C.-T. Li, M.-S. Hwang, and Y.-P. Chu, “A secure and efficient communication scheme with authenticated key establishment and privacy perserving for vehicular ad hoc networks, 2008.
3.C.-W. Wang, Y.-M. Huang, and W.-M. Chen, “A novel secure communication scheme in vehicular ad hoc networks”, 2008.
4.M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” 2007.
5.H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, “SLAB: A secure localized authentication and billing scheme for wireless mesh networks,” Oct. 2008.
6.L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, “A scalable robust authentication protocol for secure vehicular communications,” May 2010.
7.C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, “An efficient identity-based batch verification scheme for vehicular sensor networks,”2008.
8.R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, “ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications”,2008.
9.A Wasef and X. Shen, “EMAP: Expedite message authentication protocol for vehicular ad hoc networks”,2013.
10.S. Yu, K. Ren, and W. Lou, “FDAC: Toward fine-grained distributed data access control in wireless sensor networks”,2011.