VANET BASED SECURED NAVIGATION SYSTEM

P.Saravanan[1], Dr.P.Marikkannu[2]

[1]PG Scholar, [2]Head of Department, Dept of Information Technology,
Anna University, Coimbatore (India)

ABSTRACT

Generally today navigation systems are most useful to all the people, from drivers to ordinary persons. But few decades back atlas maps are used to find route to a destination. As it is a hardcopy day to day and time to time changes will not be reflected in the atlas map. Other complication to the system is accuracy and there is no assurance we are following the rite route to reach the destination. In the last decade GPS (Global Position systems) are become familiar in the navigation system due to less cost, easy to use, high assurance and accuracy of the application. Still these GPS systems are inefficient in finding the suitable destination route by considering the current dynamics of the situation. A GPS system finds the best route depends on the distance but I don't consider the dynamics of the conditions. So this paper proposes the Efficient navigation system with privacy preserving of the requester and request location by using the Anonymous credential scheme.

Key Terms: GPS, VANET, MANET, RSU, C2C, ECC

I. INTRODUCTION

Vehicular Ad hoc Networks (VANET) is part of Mobile Ad Hoc Networks (MANET), this means that every node can move freely within the network coverage and stay connected, each node can communicate with other nodes in single hop or multi hop, and any node could be Vehicle, Road Side Unit (RSU). The basic application of a VANET is to allow arbitrary vehicles to broadcast safety messages (e.g. road condition, traffic accident information) to other nearby vehicles and RSU such that other vehicles may adjust their travelling routes and RSU may inform the traffic control center to adjust traffic lights for avoiding possible traffic congestion. This paper focuses on inter-vehicle communications. Other recent efforts for making authentication in VANET more efficient include and In the authors propose to use the physical property of a transmitting signal to discriminate one transmitter from others because physical measurement is more efficient than software computation. On the other hand, aims at enhancing the efficiency of any certificate-based authentication scheme. In terms of secure VANET applications, and are two representatives. proposes a secure navigation scheme for locating parking lots in a car park while proposes a secure and privacy preserving road toll calculation scheme under the principle of multi-party computation. The process in which exchange of information via some transmission media takes place is known as network. VANETs are used for V2V and V2I communication considering all the aspects required by the process of cryptography. In Safety and non-safety applications of VANET, there is a requirement of V2V & V2I communication The security policy should define acceptable encryption algorithms for use within the VANET System. The security policy should also specify the required procedures for key management. In order to successfully gain access to the information transmitted over the VANET, an attacker must capture the entire session and use a substantial amount of computer power and time to bruteforce the key and decrypt the traffic. Unless the information is exceedingly valuable, any well known, strong algorithm is appropriate for use in the VANET System. Vehicular ad-news networks (VANETs) are distributed selforganizing and highly mobile networks based on wireless car-to-car-communication (C2C).VANETs have recently won a great deal of attention from industry and academe. The ultimate goal is to diminish the number and severity of accidents by holding out the driver's view of perception beyond what is visible locally is possible. Nevertheless, these active safety applications depend on a certain level of dissemination of C2C communications systems. To help increase market penetration, a second class of applications has to be developed that offer an immediate benefit to possible customers: the so-called deployment applications. These applications are accepted from the fields of entertainment, information access and increased riding comfort.

The primary agents that would determine the adoption of VANET architecture for future vehicular applications would be-

1) Low latency requirements for safety applications.

2) Extensive growth of interactive and multimedia Applications.

3) Increasing concerns about privacy and security.

While there are strong reasons to adopt the VANET architecture as pointed above, there are also several research challenges that needs to be addressed before VANETs could become widespread. They include -Data dissemination techniques, Security and Privacy concerns, Lack of simulators for protocol evaluations, Bootstrapping/Market penetration issues, Automatic incident detection and collision avoidance capability and Driver distribution studies. Vehicular communications (VC) will take on a key part in this endeavor, enabling a mixture of applications for safety, traffic efficiency, driver assistance, and infotainment. For instance, warnings of environmental hazards (e.g., ice on the pavement) or abrupt vehicle kinetic changes (e.g., emergency braking), traffic and route conditions (e.g., congestion or construction sites), and tourist information downloads will be offered by these arrangements. Vehicular networks, protocols will allow nodes, that is, vehicles or roadside infrastructure units, to communicate with each other over single or multiple hops. In other words, nodes will act both as end points and routers, with vehicular networks emerging as the first commercial instantiation of the *mobile ad hoc networking technology*.

II. RELATED WORKS

The proposed system has the advantage of using real-time road conditions to compute a more honest path and at the same time, the information source can be properly authenticated. To protect the secrecy of the drivers, the query (destination) and the driver who issues the query are guaranteed to be unthinkable to any party including the trusted authority. We build use of the idea of anonymous credential to achieve this end. In addition to authentication and privacy preserving, our scheme fulfills all her necessary requirements. Two kinds of roles exist in the proposed scheme: the first is the trusted third party named Authorization server (*AS*) in the VANET, the second is the VANET user, Vehicle. Each vehicle registers at *AS* before joining the network. The authorization server can recover the real identity of any broadcaster when needed. If there is a malicious vehicle broadcasting wrong messages or something else malicious such that the validity of the vehicle needs to be broken, the authorization server is able to revoke that specific vehicle. The lower layer is composed of vehicles and RSUs. The communication among them is based on the DSRC protocol. Each vehicle has its own public keys and private keys, with which all messages are signed and then sent to its neighboring RSU.

Each RSU receiving the traffic related information is responsible for verifying the digital signatures of the messages. In general, the top layer is comprised of application servers (such as traffic control analysis center), and a Trust Authority (TA). The RSUs communicate with an application server and TA using a secure transmission protocols, such as the wired Transport Layer Security (TLS) protocol. The road to a successful introduction of vehicular communications has to pass through the analysis of potential security threatsand the design of a robust security architecture able to cope with these threats. In addition to providing a survey of related academic and industrial efforts, we also outline several open problems.

Message Suppression Attack, An attacker selectively dropping packets from the network, these packets may hold critical information for the receiver, the attacker suppresses these packets and can use them again in another time. The goal of such an attacker would be to prevent registration and insurance authorities from learning about collisions involving his vehicle and/or to avoid delivering collision reports to roadside access points. The GPS location information of the nodes is used to connect new nodes to the physically closest node. In this way, the communication cost is reduced by localizing the group operation. PPGCV preserves the privacy of the users. Finally, PPGCV provides conditional full statelessness property compared to the partial statelessness property of the GKMPAN protocol. the RAISE protocol was suggested for vehicle-to-vehicle communications. The protocol is software-based. It permits a vehicle to verify the signature of another with the assistance of a nearby RSU. Still, no batch verification can be made out and the RSU has to verify signatures, one after another.

VANETs have mainly two types of application provisioned by two models first is a push model (communication in terms of broadcast nature) and second is a pull model (communication in terms of on demand nature). When communication in VANETs in the sort of broadcast nature.Thus along the basis of communication this network needs group communication.The principal applications of VANETs can be divided platooning and co-operative driving.These cases of applications required mainly privacy location and identity, both, non- repudiation.

III. SYSTEM ARCHITECTURE

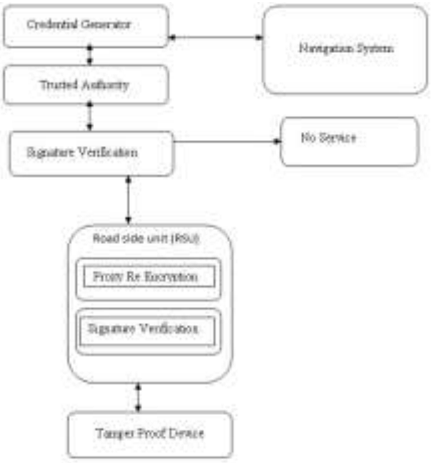

Fig 3.1 System Architecture

Finding a route to a certain destination is a common experience for all drivers. In the old days, a driver usually refers to a hard copy of the atlas. The drawbacks are quite obvious. With the founding of Global Positioning System (GPS), fig 3.1 System Aritecture GPS-based navigation systems become popular, for example In such a scheme, a small hardware device is installed on a vehicle. By receiving GPS signals, the device can define its current location and then find the geographically shortest route to a certain destination based on a local map database. Nevertheless the route searching procedure of these systems is based on a local map database and real-time road conditions are not taken into account.

To read about real-time road conditions, a driver needs another system known as Traffic Message Channel (TMC), which has been taken up in a number of developed nations. TMC makes use of the FM radio data system to transmit real-time traffic and weather information to drivers. Special equipment is taken to decipher or to filter the info obtained. Nevertheless, only special road conditions (e.g., severe traffic accident) aredistributed and a driver cannot obtain information like the general smoothness of a road from TMC. Recently, vehicular ad hoc network (VANET) has become more and more popular in many rural areas. It is an important component of the Intelligent Transportation Systems (ITSs). In a typical VANET, each vehicle is presumed to have an onboard unit (OBU) and there are road-side units (RSU) installed along the roads.

A trusted authority (TA) and possibly some other application servers are set up in the hind end. The OBUs and RSUs communicate using the Dedicated Short Range Communications (DSRC) protocol over the wireless channel while the RSUs, TA, and the application servers communicate using a secure fixed network (e.g., the Internet). The basic application of a VANET is to allow arbitrary vehicles to broadcast safety messages (e.g., vehicle speed, turning direction, traffic accident information) to other nearby vehicles (denoted as vehicle-vehicle or V2V communications) and to RSU (denoted as vehicle-infrastructure or V2I communications) regularly, such that other vehicles may adjust their traveling routes and RSUs may inform the traffic control center to adjust traffic lights for avoiding possible traffic congestion. As such, a VANET can also be read as a sensor network because the traffic command center or some other key servers can collect tons of useful info about road conditions from vehicles. It is natural to investigate how to utilize the collected real-time road conditions to offer useful applications.

IV. STEPS IN NAVIGATION SYSTEM

TA sets up parameters and generates anonymous credentials. Vehicle Vi’s tamper-proof device starts up and requests for the master secret s from RSU Rc. Vehicle Vi’s tamper-proof device requests for a navigation credential from RSU Rj. RSU Rj verifies Vi’s identity and sends its tamperproof device an anonymous credential. After a random delay or after traveling for a random distance, Vi’s tamper-proof device sends out its navigation request to RSU Rk. RSU Rk forwards the navigation request to its neighbors. This procedure iterates until the request reaches RSU Rd is covering the destination.

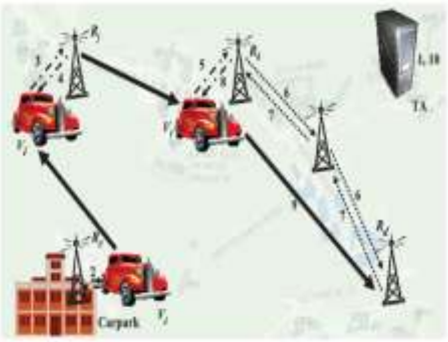

Fig 4.1 Navigation System

RSU Rd constructs the navigation reply message and sends it along the reverse route. Each hop along the path attaches the corresponding hop information (with signature). RSU Rk forwards the navigation reply message to

Vi's tamper-proof device which then verifies the messages from all RSUs along the route in a batch. By presenting the navigation session number, each RSU along the route guides Vi to reach the next RSU closer to the destination. Based on Vi's pseudo identity received from RSU Rj, TA reveals Vi's real identity for billing purpose

V. NETWORK INITIALIZATION

In this module, Network elements like TA Trusted authority, RSU Road side unit, On board unit OBU are deployed in the NS2 for the functioning. These objects are set in the positions and mobile nodes mobility are set for the movements. Finally this do the process of discovering the network elements used in the workspace for the initialization process.

5.1 Key Generation

Key Generation module generates the anonymous credentials in the trusted authority for the distribution of key for the tamper proof device in the vehicle every node when it switch on the tamper proof device Vehicle send the identity to the TA through the RSU. Once identity is verified TA distribute the key which is generated in the initialization of network.

5.2 Key Distribution

Anonymous credentials generated and Diffie Hellman Cryptographic system is used for the key generation every node will have the private key and public key for the transmission of the route request and route response. These keys are used to check the user identity and privacy of user query and user location. In every transition node moves from the one RSU coverageto other RSU pseudorandom numbers are generated and used as a key for the key distribution.

5.3 Proxy Re-Encryption

Every query passes to TA through the RSU are in need to do the proxy re encryption to transmit the packet and process the packet securely. This method brings the privacy preserving system for the request and response. This scheme is enhanced to the all the mobile node.

5.4 Query System

This module sets up the random generation of the query from the mobile unit to the TA. This random generation of queries justifies about the performance of the system, considering various network parameters performance.

5.5 Routing

This module describes the various routing functionality of the entire system. Mobile host and RSU are connected in the wireless pattern. TA and RSU are connected through the wired network. so this modules sets up routing models to route the credentials and route request & route response.

VI. PERFORMANCE MEASURE

X-graph tool is used in the NS2 to draw the performance measure of the system. Various network performances are measured in the network.

6.1 Algorithm

Elliptic curve cryptography is an approach to public key cryptography based on the algebraic structure of elliptic curve over finite fields. Elliptic curve is applicable for encryption, digital signature, pseudo-random generators and other tasks.

Selection of elliptic curve is standard called FIPS 186-2 has 10 which recommended finite fields: 5 prime fields, and the binary fields F2163 , F2233 , F2283 , F2409 ,and F2571 . For each of the prime fields, one randomly selected elliptic curve was recommended, while for each of the binary fields one randomly selected elliptic curve and one Koblitz curve was selected. The fields were selected so that the bit lengths of their orders are at least twice the key lengths of common symmetric-key block cipher this is becauseexhaustive key search of a k-bit block cipher is expected to take roughly the same time.

Another important advantage is to improve the computational power, this disparity should get rapidly bigger and uses a negligible amount of storage.

6.2 Digital Signature Schemes

A digital signature is the electronic equivalent of a handwritten signature. When attached to an electronic document, it provides authentication of the signer, date and time of signature and contents of the signed document. Furthermore, the signature must be verifiable to ensure that the signer cannot deny signing the document afterwards. Therefore, a digital signature algorithm needs to be able to generate keys for the signature, sign a document and verify the signature.

6.3 Encryption Schemes

In this section, the ElGamal encryption and decryption algorithms will be compared to its elliptic curve version. Comparisons will be made on cryptosystems with the same level of security. Thus, a 768-bit conventional ElGamal should be compared to a 151-bit ECC ElGamal, while a 1024-bit conventional ElGamal should be compared to a 173-bit ECC-ElGamal. However, for key sizes of 151 and 173 bits on the ECC ElGamal, there does not exist trinomial in polynomial bases (PB) nor optimized normal basis in normal bases (NB) [23], hence 155 and 183-bit key sizes will be used instead. Note, however, that there is slight improvement in security levels in the ECC versions of ElGamal.

VII. CONCLUSION

VANET based secure and privacy-preserving navigation scheme in this theme. We utilized speed data and road conditions collected by RSUs to guide vehicles to desired destinations in a diffused way. Our scheme adopts some security primitives in a nontrivial way to supply a number of security features: 1) Vehicles are authenticated by means of fake identities. 2) Navigation queries and results are protected from eavesdroppers. As well, with the thought of anonymous credential, no one including TA can link up a vehicle's navigation query and its individuality. 3) Information provided by RSUs can be properly authenticated before the route is really being applied.Besides meeting all security and privacy requirements, our solution is efficient in the sensory faculty that a vehicle can complete the whole navigation querying process and receive urgent notification in a very little time. On the other hand, the route turned backby our strategy can contribute to savings of traveling time compared with the offline map data searching approach. Our system also makes the lower route blocking rate in practice.Notice that our VSPN scheme can apply to the state of affairs where the route searching process is managed by a central server, which gathers and verifies speed data and route conditions from RSUs.The authentication process at vehicles can be even simpler because a vehicle only needs to check against the central server's signed on the processed result. However, such a centralized approach is not scalable, especially for large cities.

REFERENCE

[1] C. Zhang, R. Lu, X. Lin, P.H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," Proc. IEEE INFOCOM '08, pp. 816-824, Apr. 2008.

[2] E. Aimeur, H. Hage, and F.S.M. Onana, "Anonymous Credentials for Privacy-Preserving E-learning," Proc. IEEE MCETECH Conf. e-Technologies (MCETECH '08), pp. 70-80, July 2008.

[3] G. Samara, W. Al-Salihy, and R. Sures, "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)," Proc. IEEE Fourth Int'l Conf. New Trends in Information Science and Service Science (NISS '10), pp. 393-398, May 2010 1457, May 2008.

[4] A. Wasef and X. Shen, "PPGCV: Privacy Preserving Group Communications Protocol for Vehicular Ad Hoc Networks," Proc. IEEE Int'l Conf. Comm. (ICC '08), pp. 1458-1463, May 2008.

[5] T. Chim, S. Yiu, L.C. Hui, and V.O. Li, "SPECS: Secure and Privacy Enhancing Communications for VANET," Elsevier Ad Hoc Net- works, vol. 9, no. 2, pp. 189-203, Mar. 2010.

[6] R. Hwang, Y. Hsiao, and Y. Liu, "Secure Communication Schem of VANET with Privacy Preserving," Proc. IEEE 17th Int'l Conf. Parallel and Distributed Systems (ICPADS '11), pp. 654-659, Dec.2011.

[7] B.K. Chaurasia, S. Verma, and S.M. Bhasker, "Message Broadcast in VANETs Using Group Signature," Proc. IEEE Fourth Int'l Conf. Wireless Comm. Sensor Networks (WCSN '09), pp. 131-136, Dec. 2008.

[8] M. Scott, "Efficient Implementation of Cryptographic Pairings, "http://ecryss07.rhul.ac.uk/Slides/Thursday/mscottsamos07.pdf, 2007.

[9] "Topologically Integrated Geographic Encoding and Referencing System (TIGER)," http://www.census.gov/geo/www/tiger/,2009.