A Survey on VANET based Secure and Privacy Preserving Navigation

S.Kathirvel, D.Gautham Chakravarthy, Dr.S.Gunasekaran,

Abstract— VANET is collected of vehicles and roadside infrastructure units (RSUs). Vehicles are equipped with wireless communication devices, which are called On-Board Units (OBUs). The wireless communication devices enable vehicles to exchange traffic related information with each other and with RSUs. VANETs raise many security and privacy concerns at the same time. Malicious users can take advantage of VANET and disturb the whole system. In the previous researchers introduced many techniques and methods, Road information collected to provide navigation service to drivers. Based on the destination and the current location of the driver the system can automatically search for a route that yields minimum traveling delay in a distributed manner using the online information of the road condition. . In this survey discuss various VANET security techniques and algorithms to detect and prevent the malicious users in the roadways.

Index Terms— anonymous credential, Batch verification ,GPS, pseudo identity ,secure vehicular sensor network, signature verification,VANET.

1 INTRODUCTION

A GPS navigation device is a device that accurately calculates geographical location by receiving information from satellite. The Global Positioning System (GPS) is a gathering of satellites that orbit the earth twice a day, transmitting precise time and position latitude, longitude and altitude information. With a GPS Receiver, users can determine their location anywhere on the Earth. GPS is a space-based satellite navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites. The system provides critical capabilities to military, commercial user's position, steering to destination, and city guide software and tourism attraction around the city. It is maintained by the United States government and is freely accessible to anyone with a GPS receiver.

In Vehicular sensor network [1] has attracted people's attention in recent years with the vision that it can provide crucial information, such as traffic conditions, to interested parties. The vehicular network architecture is mainly composed of inter-vehicular communications, and communication between vehicles and the roadside sensors. Although the picture is very exciting, we do not expect the technology to be mature in the next couple of years for very practical deployment. This is due to the hurdles along the way the standardization of the network communications, the effort associated with the deployment of the roadside sensors, and the maturity of the hardware. These processes can be both expensive and time consuming. A public-key based Scheme ECC of the schemes can be implemented efficiently on sensor platforms. Taking a closer look at the problem

- *S.Kathirvel is currently pursuing masters degree program inComputer Science Enginering in CIET, India, PH-8807188052. E-mail:kathirvel91cbe@gmail.com*
- *D Gowtham Charavarthy is currently working as Assistant Professor in CIET, India, PH-9994222724. E-charavarthy.gowtham@mail.com*

in a real experimental study, we found that authentication takes about one to two seconds in many cases, which is non-negligible for a car traveling at high speed. A car may rush out of a sensor's transmission range after the authentication is conducted.

Intelligent spaces [3] are environments that can continuously monitor what's happening in them, communicate with their inhabitants and neighborhoods, make related decisions, and act on these decisions. Embedding such intelligence in an automobile would be a natural next step for intelligent vehicles. Current in-vehicle applications of GPS, ad hoc networks, and sensor networks have already led the way. Future cars will behave more like intelligent agents traveling in intelligent spaces. For example, traffic control at intersections could employ cooperative driving technologies implemented over ad hoc networks, instead of relying on traffic lights.

In set of specifications to allow interoperability between wireless devices on board of vehicles (On-Board Unit, OBU) and devices located near the roads (Road Side Unit, RSU). the coverage area of a RSU/OBU, and messages related to traffic information, road conditions, local utility information and so forth, which should be disseminated in an area of several kilometers, but having less stringent delay requirements (seconds or tens of seconds). Spreading messages originating from the RSU in a service area that is larger than the RSU coverage one. This fact means that only a fraction of vehicles can be reached directly in a single hop. Multi-hop, inter-vehicle communications is necessary to reach vehicles in the whole area. The OBUs moving in the area define a graph, where an arc between two nodes exists if they are within coverage of each other. so that each node is potentially reachable.

In this survey focused on VANET each vehicle is assumed to have an onboard unit (OBU) and there is road-side units (RSU) installed along the roads. A trusted authority (TA) and maybe some other application servers are installed in the back end. Traffic Message Channel (TMC), Pseduo identity, signature verification, Identity-based public key, Dedicated Short

Range Communications.

1.1 Features of VANET

•The nodes in a VANET are vehicles and road side units.
•The movement of these nodes is very fast.
•The motion patterns are restricted by road topology.
•Vehicle acts as transceiver i.e. sending and receiving at the same time while creating a highly dynamic network, which is continuously changing.
•The vehicular density varies from time to time for instance their density might increase during peak office hours and decrease at night times.

2 Traffic Message Channel

The Traffic Message Channel (TMC) is a standard designed for delivering real-time traffic information to drivers on the move through TMC compliant devices. It is an increasingly popular technology commonly used in dynamic route navigation, where TMC traffic information enables Global Positioning Systems (GPS) navigation devices to route the driver around congestion and road incidents. A TMC message, comprising a defined location and an event code, is transmitted over-the-air to the navigation device or radio receiver in the vehicle. A Location Table (LT) stores the location codes and referencing rules that include road links, intersections and other useful travel information such as car park locations. Because of its low bandwidth the TMC protocol is a cost effective means of disseminating traffic information. This benefits not only motorists but also adds value to the whole business chain. The TMC standard is widely accepted globally and has been adopted by many countries in Europe and America. In recent years, many countries in Asia Pacific and Middle East have also started adopting and providing TMC services to motorists. TMC information is broadcasted through the FM – Radio Data System (FM-RDS) communications protocol.

3 Dedicated Short Range Communications

Jinhua Guo and Nathan Balon [6] suggested that dedicated short-range communication (DSRC) technology implemented in vehicle-to-vehicle and vehicle-to-roadside communication, the effectiveness of this technology is highly dependent on cooperative standards for interoperability. DSRC technology, for the vehicular communication including insights into why specific technical solutions are being adopted, and key challenges remaining for successful DSRC deployment. The radio communication interface between a Land Mobile Station OBU and a Base Station RSU for the Dedicated Short Range Communication system, RSU performs land mobile radio communication with OBU. The system configuration for the OBU and RSU, the Base Station (RSU) is composed of radio equipment with antenna (e), a transmitter and receiver, a control unit and a display unit. Mobile Station (OBU) performs land mobile radio communication with Base Station. The Mobile Station consists of radio equipment with antenna (e), a transmitter and receiver, and optional equipment such as an IC card, a control unit and a display unit The system is duplex short range and small zone communication which connects between Base Station (RSU) and Mobile Stations (OBEs) with high speed radio wave and is capable of being used for multiple applications. System requirements of RSU and OBU characteristics performs are multiple application use, Effective use of frequency by small zone, Capable of transmitting fast and large amount of information to moving vehicles, Service connecting internet, Use for Electronic Toll Collection and other means of electronic payment.

4 Temporary Anonymous Certified Keys (TACKs)

Ahren Studer and Elaine Shi and Fan Bai [5] suggested that in the TACKs system, roadways are divided into geographic regions with Regional Authorities (RAs) acting as certificate authorities for their region. Within a region, a RA certifies vehicle generated temporary keys which are used to authenticate vehicles. As traffic enters a region, each vehicle anonymously requests a certificate from the RA. If the requesting vehicle has not been revoked, the RA responds with a certificate. Since in the system, all vehicles entering the region change keys simultaneously, the TACK update provides unlink ability between prior and current keys. In the TACK s system it perform most expensive operation is for an OBU to update its short-term key with an RA it requesting OBU sign a group signature, and that RA verify the group signature, OBU its has a limited processing power.

5 Pseudonymous certificates from RSUs

Bharati Mishra1 and Saroj Kumar [7] suggested that an RSU aided message authentication scheme, has been proposed in which shall also provide conditional privacy preservation. When a vehicle shall come in the range of an RSU, it shall request the RSU for a temporary ID known as pseudo ID which will be valid till the vehicle moves to another RSU's range. This pseudo ID will be used by the sender vehicle for its identity instead of its actual identity. When the vehicle wants to send a message, the vehicle shall sign the message with its private key using ECDSA signature and append its temporary ID in place of sender address. The vehicle which receives the message shall query the RSU for the public key of the sender vehicle and provides the sender's pseudo ID in the request. The RSU shall find out the actual ID from the pseudo ID and broadcast the corresponding public key of the sender vehicle. The interested vehicles shall verify the sender vehicles signature and thus authenticate the message but the sender's identity remains anonymous to the receiving vehicles.

6 Signature verification Schemes

Bharati Mishra1 and Saroj Kumar [7] suggested that Elliptic curve digital signature algorithm (ECDSA) which generates secure signatures that is to be used by the participating nodes. The vehicles are provided with temporary identities that are generated using secure cryptographic techniques. These temporary identities are used during any sort of communication,

thereby preserving privacy and provide anonymity to the user. ECDSA is a variant of the Digital Signature Algorithm (DSA) that operates on elliptic curve groups an efficient message authentication scheme that is based on elliptic curve digital signature algorithm (ECDSA). It claimed to overcome some inherent drawbacks of existing authenticating and security schemes like more processing delay for authentication at sender and receiver, computational and communicational overheads, storage requirements .

7 CONCLUSION

In this survey investigated VANET security requirements and authentication. VANET each vehicle is assumed to have an onboard unit (OBU) and there is road-side units (RSU) installed along the roads. A trusted authority (TA) and maybe some other application servers are installed in the back end. Traffic Message Channel (TMC), Pseduo identity, signature verification, Identity-based public key, Dedicated Short Range Communications. In a road vehicles are traveling they periodically broadcast traffic related information that could be extremely vital and life-critical information for neighboring vehicles. To ensure the integrity of the messages, each message sent by a vehicle should be signed and verified when being received. The Message based batch verification achieves high performance a vehicle receives traffic related messages from other vehicles; the vehicle has to verify the signatures of the messages.

REFERENCES

[1] Ahren Studer, Elaine Shi, Fan Bai, Adrian Perrig TACKing , "Together Efficient Authentication, Revocation, and Privacy in VANETs"Carnegie mellon university,PA-15213,cmu-cylab-08-011,march 2008.

[2] Bharati Mishra1, Saroj Kumar Panigrahy, "A Secure and Efficient Message Authentication Protocol for VANETs with Privacy Preservation",International journal of information and communication Technologies (ijict),vol.11,no.14.,December 2011.

[3] Chenix Zhang,Xiaodong Lin,Rongxing Lu,Pin-Han Ho,Xuenmin, "An Efficient Message Authentication Scheme for Vehicular Communications"IEEE Transaction on Vechicluar Technology,Vol.57, no.6,November 2008.

[4] Fengh hong qu, Fei-yuewang, Liuqing yang , " Intelligent Transportation Space: vehicle,Traffic,communication," IEEE Pervasive Computing, vol.48, no. 11, pp. 136-142, Dec. 2010.

[5] Ghassan samara,Wafaa A.H.AI-salihy,R.sures, "Security Issues and Challenges of Vehicular AdHoc Networks (VANET)",universiti sanins Malaysia, IEEE xplore-june 28,2010.

[6] Harry Gao, Seth Utecht., " High Speed Data Routing in Vehicular Sensor Networks" , Department of computer science , college of William and mary , Journal Of Communication, vol.5 , No.3 ,March 2010.

[7] Mohammad Saiful Islam Mamun and Atsuko Miyaji, "An Optimized Signature Verification System for Vehicle Ad hoc Network", japan advanced institute of science and technology(jaist).

[8] Jinhua Guo and Nathan Balon , "Vehicular Ad Hoc Networks and Dedicated Short-Range Communication" University of Michigan – Dearborn, june26,2006.