Privacy and Energy Preserving Parallel Machine Intelligence Based VANETs with Path Relocation

R.SHARMILA, S.SUMITHRA

Abstract---**In this paper, we propose a navigation scheme that utilizes the online road information collected by a vehicular ad hoc network (VANET) to guide the drivers to desired destinations in a real-time and distributed manner. The proposed scheme has the advantage of using real-time road conditions to compute a better route and at the same time, the information source can be properly authenticated. To protect the privacy of the drivers, the query (destination) and the driver who issues the query are guaranteed to be unlinkable to any party including the trusted authority. We make use of the idea of anonymous credential to achieve this goal. In addition to authentication and privacy preserving, our scheme fulfills all other necessary security requirements.**

Index Terms--**Navigation, secure vehicular sensor network, signature verification, pseudo identity, anonymous credential, proxy re-encryption.**

1. INTRODUCTION

A vehicular ad hoc network (VANET) uses cars as mobile nodes in a MANET to create a mobile network. A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.

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 introduction of Global Positioning System (GPS), GPS-based navigation systems become popular, for example. In such a system, a small hardware device is installed on a vehicle. By receiving GPS signals, the device can determine its current location and then find the geographically shortest route to a certain destination based on a local map database. However, 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 learn about real-time road conditions, a driver needs another system known as Traffic Message Channel (TMC), which has been adopted in a number of developed countries. TMC makes use of FM radio data system to broadcast real-time traffic and weather information to drivers. Special equipment is required to decode or to filter the information received. However, only special road conditions (e.g., severe traffic accident) are broadcasted and a driver cannot obtain information like the general fluency of a road from TMC. Recently, vehicular ad hoc network (VANET) becomes increasingly popular in many countries. It is an important element of the Intelligent Transportation Systems (ITSs). In a typical VANET, each vehicle is assumed to have an on- board unit (OBU) and there are road-side units (RSU) installed along the roads.

A trusted authority (TA) and maybe some other application servers are installed in the back 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 interpreted as a sensor network because the traffic control center or some other central servers can collect lots of useful information about road conditions from vehicles. It is natural to investigate how to utilize the collected real-time road conditions to provide useful applications.

Vehicular Ad Hoc Network (VANET) is the most important component of Intelligent Transportation System (ITS), in which vehicles are equipped with some short-range and medium-range wireless communication. In VANET two kinds of communication are supposed: Vehicle-to-Vehicle and Vehicle-to-road side units, where the road side units might be cellular base station for example. From the definition of VANET, a salient challenge is obvious. Suppose at the mid-night in some rural area, a vehicle has a very important data packet (i.e. detection of an accident) which should be forwarded to the following vehicles immediately. The probability of low density of vehicles in the rural areas at mid-night is very high. Consequently, in this situation the packet will be lost due to lack of presence of other vehicles to receive and broadcast it, and arrival of the following vehicles in the accident area is unavoidable.

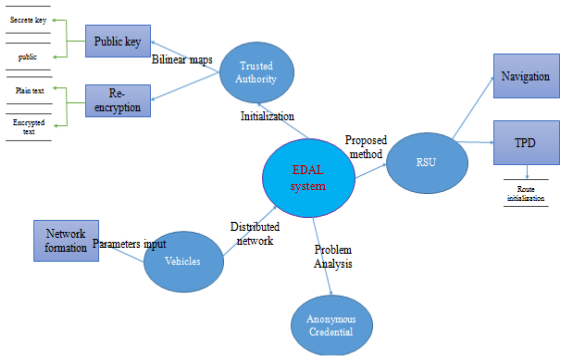
Both of them can address the security requirements well, such as authentication, non-repudiation, identity revocation, and conditional anonymity. In the group-signature-based schemes, utilizing group signatures,

ISSN: 2278 – 7798

any public entity will not reveal the originator identity of a routine traffic message. However, one limitation is that the cost for signing and verifying messages is far more than adopting the traditional public-key based signature. To reduce these overhead A. Wasefet propose the Hybrid scheme, wherein a vehicle can issue a certificate for itself by using a group key and then signing its messages using the public key-based signature.

2. PROPOSED SYSTEM

The proposed scheme has the advantage of using real-time road conditions to compute a better route and at the same time, the information source can be properly authenticated. To protect the privacy of the drivers, the query (destination) and the driver who issues the query are guaranteed to be unlinkable to any party including the trusted authority. We make use of the idea of anonymous credential to achieve this goal. In addition to authentication and privacy preserving, our scheme fulfills all o necessary security requirements.



3. MODULES

- Network Formation
- Trusted Authority
- Road side units
- Vehicles
- Performance Analysis

3.1. Network Formation:

TA sets up parameters and generates anonymous credentials. Vehicle V_i's tamper proof device starts up and requests for the master secret s from RSU Rc.

Vehicle V_i's tamper-proof device requests for a navigation credential from RSU R_j. RSU R_j verifies V_i's identity and sends its tamper proof device an anonymous credential.

After a random delay or after traveling for a random distance, V_i's tamper-proof device sends out its navigation request to RSU R_k. RSU R_k forwards the navigation request to its neighbors.

This process repeats until the request reaches RSU Rd covering the destination. RSU Rd constructs the navigation reply message and sends it along the reverse path.

Each hop along the path attaches the corresponding hop information (with signature). RSU R_k forwards the navigation reply message to V_i'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 V_i to reach the next RSU closer to the destination. Based on V_i's pseudo identity received from RSU R_j, TA reveals Vi's real identity for billing purpose.

3.2. Trusted Authority:

Generation of Anonymous Credentials by TA

TA performs two simple operations:

TA computes the credential for the current period as $C_T = <$ NVC; T; $TSIG_{TSK}$ (NVC || T)>, where the keyword NVC is used to denote that it is a navigation credential and $TSIG_{TSK}$ (NVC ||T) = H (NVC || T)^{TSK}.

TA sends S_ENC_s (C_T) to all RSUs securely via a fixed infrastructure.

3.3. Road side units:

Guiding to Destination by RSUs

Having the returned route, if V_i has GPS device installed and it can receive GPS signals for current location, it can simply search for each RSU based on the list of RL_i.

However, GPS device is not an assumption of our scheme. Even if V_i does not have GPS device installed, our scheme can make use of the VANET to guide Vi to the destination.

To use the guiding service, Vi first generates a random number rand and sends <$RRID_k$; AS_ENC_{RRIDk} (rand, nsn)> to R_k.

Here, nsn is the navigation session number generated earlier and R_k is the first RSU along the route.

Urgent Change of Rout e Initiated by RSU

Road conditions vary abruptly. A road which is initially in good condition may become blocked in a second.

Thus, our scheme is designed in such a way that the querying vehicle V_i will be informed about important changes in road conditions along the returned route.

Assume RSU R_b is an RSU along the returned route.

Now, if a road within its range is blocked, it immediately composes the road blocking notification message that is defined as M_b = f{ROAD_BLOCKED} and sends {M_b, nsn, $RRID_b$, RL_b, RC_b, $RSIG_{RRIDb}(M_b)$} to the next RSU hop along the reverse path.

The message is propagated along the reverse path until an RSU that is currently in contact with V_i is reached.

That RSU forwards the message to V_i. Again that RSU includes nsn into its message for V_i so that other vehicles nearby know that they do not need to process the message.

3.4. Vehicles:

Activation and Requesting for Master Key by Vehicle Tamper-Proof Device:

When the vehicle Vi starts, the driver enters the real identity VRIDi and password V PWDi into the tamper-proof device to activate it. Here, only simple hardware checking is involved. Two cases are possible and the tamper-proof device reacts accordingly:

If either the real identity or the password, or both are incorrect, the tamper-proof device refuses to perform further operations. .

If both the real identity and the password are correct, the tamper-proof device signs a master key request message as $SIG_{CSK}i$ (MK_Req). It then sends < RRIDc; V C_i; SIG_{CSKi} (MK_Req) > to an RSU R_c (with identity $RRID_c$).

Verification of RSUs' Hop Information by Vehicle Tamper-Proof Device

ISSN: 2278 – 7798

Recall that the reply contains a set of identities, a set of locations, a set of certificates, and a set of hop information (average speed and road condition together with signatures), each corresponding to an RSU along the route returned.

To verify the average speed and road condition provided by an RSU, its signature is verified using its identity.

In turn, to verify an RSU's real identity, its certificate has to be verified using TA's identity.

Note that the verification process may take excessive amount of time if carried out by a tamper-proof device with today's technology.

As such, this part can be relaxed to be carried out by a conventional car computer device to speed up the process.

Requesting for Anonymous Credential by Vehicle Tamper-Proof Device:

To obtain anonymous credentials, Vi's tamper-proof device performs the following steps:

It first generates a pseudo identity $VPID_i$, which is composed of two parts $VPID_{i\ 1}$ and $VPID_{i\ 2}$ (or denoted as ($VPID_{i1}$; $VPID_{i2}$)). It then composes the navigation credential request message M_i = {NVC_ REQ}.

It also picks a random number rand and encrypts it using R_j's identity as AS_ ENC_{RRIDj}(rand). This random number becomes a shared secret between itself and RSU R_j. R_j will use it to encrypt the credential at a later stage.

Next, it generates the signing key VSK_i as (VSK_{i1}; VSK_{i2}) = ($VPID^s_{i1}$; HP_i^s), where $HP_i = H(VPID_{i1}||VPID_{i2})$.

Requesting for Navigation Service by Vehicle Tamper-Proof Device:

Next, let us come to the core part of our scheme requesting for navigation service.

Note that if V_i obtains the credential CT from RSU R_j and if it sends out its navigation query to R_j immediately, its real identity and its query may be linked up if R_j colludes with TA (since TA can always recover Vi's real identity from its pseudo identity based on our traceability requirement), especially when Vi is the only vehicle which requests credential from R_j.

3.5. Performance Analysis:

Our scheme adopts some security primitives in a nontrivial way to provide a number of security features: 1) Vehicles are authenticated by means of pseudo identities. 2) Navigation queries and results are protected from eavesdroppers. Besides, with the idea of anonymous credential, no one including TA can link up a vehicle's navigation query and its identity.

4. ROUTING ALGORITHM FOR PATH RELOCATION

Ad hoc On-demand Distance Vector (AODV)

The AODV routing protocol builds on top of the DSDV protocol that was previously described. AODV is an improvement of DSDV as it minimizes the number of required broadcasts since it creates routes in an on-demand basis, in contrast to DSDV which maintains a complete set of routes. It utilizes destination sequence numbers to ensure loop-freedom at all times and to avoid the count-to-infinity problem associated with classical distance-vector protocols.

Route tables are used in AODV to store applicable routing information. AODV utilizes both a route table for unicast routes and a multicast route table for multicast routes. The unicast route table includes information about the destination, the next-hop IP address and its sequence number. For each destination a node maintains a list of precursor nodes, which route through it in order to reach the destination. This list is maintained for the purpose of route maintenance in case of a link breakage. When an entry's lifetime attribute expires because it was not frequently used it is removed from the routing table and if there is a need for this route again it is reacquired through a route discovery process. AODV is able to maintain both unicast and multicast routes even for nodes with mobility. Also it provides a quick detection mechanism of invalid routes through the use of route errors (RERR) messages. The protocol is able to respond to topological changes that affect the active routes in a quick and timely manner. Finally, because it does not use source routing it does not introduce additional overhead since it requires only the next-hop routing information.

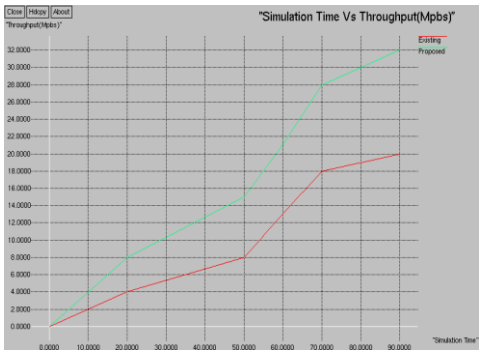
If the entry satisfies these two conditions then it unicast a RREP back to the source of the RREQ by incrementing the hop count by one. The structure of the RREP and the fields it contains are presented in figure 3.3. If none of the intermediate nodes is able to reply, the RREQ eventually reaches the destination node. When the destination node sends the RREP it places its current sequence number in the packet, initializes the hop count to zero and places the length of time this route is valid in the RREP's Lifetime field. It is possible that the destination node will receive more than one RREP from its neighbours. In this case it uses the first RREP that it receives and upon the reception of another reply it checks if the later packet contains a greater destination sequence number or if it has a smaller hop count, meaning that it provides a fresher or sorter route. In this case it updates the route entry with the new values; otherwise the reply packet is discarded. Once the route between the source and the destination nodes is established it is maintained for the source node as long as it remains active. If the source node moves during an active session, it can simply reinitiate a route discovery process and establish a new route to the destination and continue communication. However, if either the destination or an intermediate node moves a RERR packet is sent to the source affected nodes.

5. SIMULATION RESULT

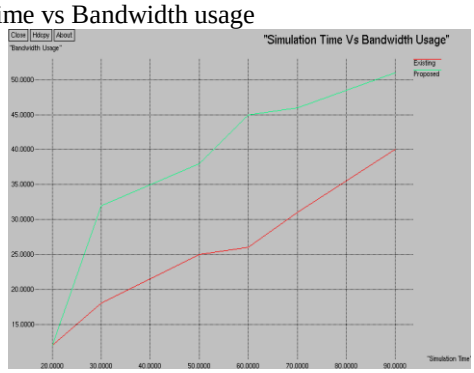
We evaluate the Routing algorithm of our Network simulator. Specifically, The proposed scheme has the advantage of using real-time road conditions to compute a better route and at the same time, the information source can be properly authenticated. To protect the privacy of the drivers, the query (destination) and the driver who issues the query are guaranteed to be unlinkable to any party including the trusted authority. we simulate the throughput of the signal and bandwidth usages, packet delivery ratio, end-end delay. Fig (a) Relationship between the throughput and time is shown in fig. Fig (b) the use of the routing algorithm to provide the security based on encryption will provide considerable increase in bandwidth usage is shown in fig. Fig (c) The considerable reduction in loss will causes the better performance by increase the end-end delay which can be shown in fig. Fig (d)relationship between the packet delivery ratio with time and increases the security and energy efficiency.

(a)Throughput vs time

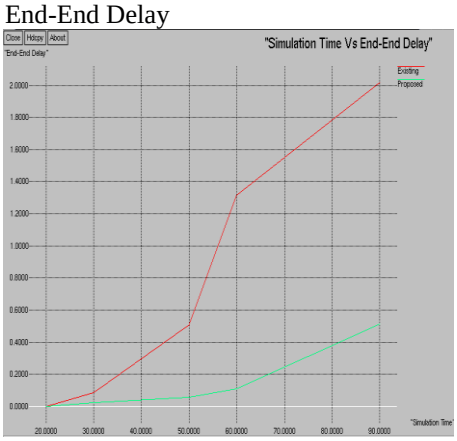
ISSN: 2278 – 7798



(b) Time vs Bandwidth usage



(c) Time vs End-End Delay



(d) Packet Delivery Ratio vs Time

CONCLUSION

We proposed a VANET-based secure and privacy-preserving navigation scheme in this paper. We utilized speed data and road conditions collected by RSUs to guide vehicles to desired destinations in a distributed manner. Our scheme adopts some security primitives in a nontrivial way to provide a number of security features: 1) Vehicles are authenticated by means of pseudo identities. 2) Navigation queries and results are protected from eavesdroppers. Besides, with the idea of anonymous credential, no one including TA can link up a vehicle's navigation query and its identity. 3) Information provided by RSUs can be properly authenticated before the route is actually being used. Besides satisfying all security and privacy requirements, our solution is efficient in the sense that a vehicle can complete the whole navigation querying process and receive urgent notification in a very short time.

REFERENCES

[1] Global Positioning System Standard Positioning Service Signal Specification. Navtech GPS Supply, 1995.

[2] "Papago! Z-Series Navigation System," http://www.papago. com.hk/, 2009.

[3] "Traffic Message Channel (TMC)," http://www.tmcforum.com/, 2004.

[4] F. Wang, D. Zeng, and L. Yang, "Smart Cars on Smart Roads: An IEEE Intelligent Transportation Systems Society Update," IEEE Pervasive Computing, vol. 5, no. 4, pp. 68-69, Oct.-Dec. 2006.

[5] H. Oh, C. Yae, D. Ahn, and H. Cho, "5.8 GHz DSRC Packet Communication System for ITS Services," Proc. IEEE VTS 50th Vehicular Technology Conf. (VTC '99), pp. 2223-2227, Sept. 1999.

[6] I. Leontiadis, P. Costa, and C. Mascolo, "Extending Access Point Connectivity through Opportunistic Routing in Vehicular Net- works," Proc. IEEE INFOCOM '10, Mar. 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," Proc. IEEE INFOCOM '08, pp. 816-824, Apr. 2008.

[8] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANET- Based Smart Parking Scheme for Large Parking Lots," Proc. IEEE INFOCOM '09, pp. 1413-1421, Apr. 2009.

[9] D. Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete," Comm. ACM, vol. 28, pp. 1030- 1044, 1985.

[10] 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.

[11] 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.

[12] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET," IEEE J. Selected Areas in Comm., vol. 25, no. 8, pp. 1569-1589, Oct. 2007.

ISSN: 2278 – 7798

BIOGRAPHY

R.SHARMILA,
DEPARTMENT OF ECE,
PAVENDAR BHARATHIDASAN
COLLEGE OF ENGINEERING
AND TECHNOLOGY,
THIRUCHIRAPALLI.
TAMILNADU, INDIA.

S.SUMITHRA,
HEAD OF THE DEPARTMENT OF
ECE,
PAVENDAR BHARATHIDASAN
COLLEGE OF ENGINEERING
AND TECHNOLOGY,
THIRUCHIRAPALLI.
TAMILNADU, INDIA.

ISSN: 2278 – 7798