ISSN 23499842(Online), Volume 1, issue 1 March 2015

International Journal of Innovative Trends and Emerging Technologies

ACCIDENT AVOIDENCE BASED ON PREDECESSOR AND SUCCESSOR VEHICLE SPEED WITH PRIVACY PRESERVING NAVIGATION USING CHORD ALGORITHM

C. AROKIA MARY[1], A.M. ARULRAJ[2],

[1]ME Student, Associate Professor, [1,2] Department of Computer Science and Engineering,

[1,2]Dhaanish Ahmed College of Engineering, Chennai,

[1]arockyamary90@gmail.com, [2]arulrajphd@gmail.com

***Abstract*— Computing real-time road condition is really tough and it is not achieved using GPS. Initially A vehicle should be authenticated by Trusted Authority (TA) via RSU, only then the navigation query sent to RSU through tamper proof device (in the Vehicle) for identifying best destination route. After authentication, TA generates a re-encryption key to requested vehicle for encrypting the query. Based on vehicle request, contacted RSU identifies the shortest path to reach the destination RSU by passing the vehicle request to neighboring RSU's. After identification of shortest path, it sends the encrypted message to requested vehicle using re-encryption key. Finally it decrypts the message using its own private key. In the modification process, network checks each vehicle speed for avoid accident based on predecessor and successor vehicle's speed using chord algorithm. We also implementing priority based vehicle movement. Network gives high priority in emergency vehicle, it gives medium priority for registered vehicle and it gives low priority for unregistered vehicle.**

***Keywords*— Trusted Authority; Roadside Unit; Onboard Unit; Traffic Message Channel; VANET.**

I. INTRODUCTION

In this paper, Vehicular ad-hoc network 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 Broad cast real-time traffic and weather information to drivers. Special equipment is required to decode or to filter the information received.

However, only special road 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 onboard unit (OBU) and there are road-side units (RSU) installed along the roads. A trusted authority (TA) and May be 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

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 and to RSU 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.

II. INTRODUCTION TO VANET

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 onboard unit (OBU) and there are road-side units (RSU) installed along the roads. A trusted authority (TA) and May be 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.

This is in comparison with roadside sensors such as loop detectors that can only detect the presence or absence of vehicles and, at best estimate, the size of vehicle queues. Furthermore, it is cheaper to equip vehicles with wireless devices than to install roadside equipment. Traffic adaptive signal control has been widely studied.The VANET-based vehicle-actuated traffic method is based on the study presented with additional enhancements that take advantage of the finer grain information enabled by a VANET. These enhancements take advantage of the ability of the VANET infrastructure to estimate when a vehicle is going to approach the stop line.

The controller uses this information to extend the GREEN time by an appropriate amount so that the vehicle can pass through the intersection. Another example of VANET-based traffic signal control is Traffic View. This work modified the Webster's method to leverage VANETs to communicate with the traffic signal controller. VANETs have also been used to enhance other traffic control and management applications. The study in presents a VANET-based method for variable speed limits to improve the flow of vehicles in freeways.

In VANETs are used to detect highway incidents and broadcast this information to drivers. In an extension to this work, examines the "memory" that platoons of vehicles can keep to more efficiently broadcast freeway incident messages. VANETs have also been used in many driver experience improvement applications. For example, VANETs have been used to monitor road conditions. In addition to VANET, cellular communications have been used to design a system that estimates traffic delays.

The speed and location information on vehicles that can be disseminated to the traffic signal controller using VANETs are both spatially and temporally fine-grained. Such precise per vehicle speed and location information can enable additional capabilities such as being able to predict the time instance when vehicles will reach the stop line of the intersection.

The speed and location information on vehicles that can be disseminated to the traffic signal controller using VANETs are both spatially and temporally fine-grained. Such precise per vehicle speed and location information can enable additional capabilities such as being able to predict the time instance when vehicles will reach the stop line of the intersection.

III. EXISTING WORKS

Vehicle Ad Hoc Networks (VANETs) have been received particular attention both in industrial and academic levels. Searching for a vacant parking space in a congested area or a large parking lot and preventing auto theft are major concerns to our daily lives. In this paper, an efficient parking scheme for large parking lots through vehicular communication is described. The proposed scheme can provide the drivers with real-time parking navigation service, and friendly parking information dissemination. Performance analysis via extensive simulations demonstrates its efficiency and practicality. The system is designed, developed and tested using network simulator NS-2. AODV protocol is used for implementation and found that the system works satisfactory.

Deploying roadside access points (APs) or an infrastructure can improve data delivery. Our empirical results from real trace driven simulations show that deploying APs produces up to 5x performance gain in delivery ratio and reduces delivery delay by as much as 35% with simple routing. However, we also find that buffer resources at the APs become a critical factor and poor buffer allocation leads to marginal performance gain for inter-vehicle routing. Motivated by this important observation, we investigate the optimal infrastructure-assisted routing for inter- vehicle data delivery.

IV. PROPOSED MODEL

A vehicle should be authenticated by Trusted Authority (TA) via RSU, only then the navigation query sent to RSU through tamper proof device (in the Vehicle) for identifying best destination route. After authentication, TA generates a re-encryption key to requested vehicle for encrypting the query. Based on vehicle request, contacted RSU identifies the shortest path to reach the destination RSU by passing the vehicle request to neighboring RSU's. After identification of shortest path, it sends the encrypted message to requested vehicle using re-encryption key for security purpose. Finally it decrypts the message using its own private key. In the modification process, network checks each vehicle speed for avoid accident based on predecessor and successor vehicle's speed using chord algorithm.

Route has many numbers of vehicles and their details. It maintains the vehicle connection details also. Vehicles are connecting with other vehicles in all the route ways. All vehicles registered in a trusted authority. Trusted Authority will maintain the revocation list for vehicle details and status each and every vehicle movement required. TA generates the re-encryption key and secret key for each vehicle and it secures vehicle query.

After verification of vehicle id, RSU receives vehicle re-encryption key for encrypt the vehicle query form trusted authority. In this module, destination RSU finds the best and shortest path based on query travelling path. Then it sends the required path to vehicle through neighbor RSU's. Finally vehicle receives the encrypted query then it decrypts the query based on its private key. After decryption, vehicle moves one network to another one.

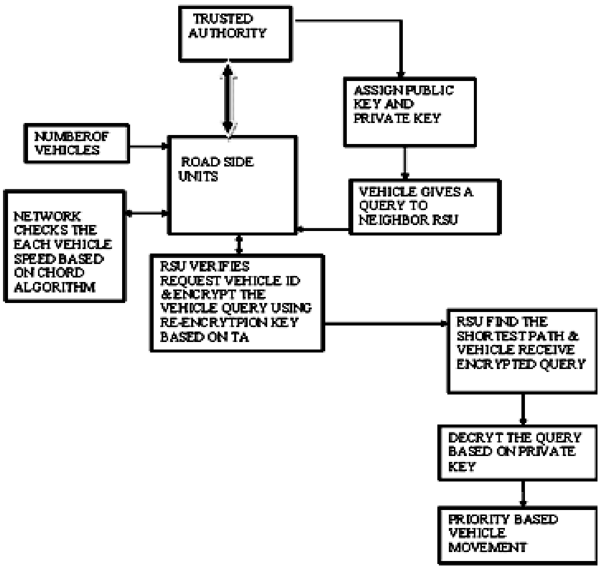
TRUSTED AUTHORITY
ASSIGN PUBLIC KEY AND PRIVATE KEY
NUMBEROF VEHICLES
ROAD SIDE UNITS
VEHICLE GIVES A QUERY TO NEIGHBOR RSU
NETWORK CHECKS THE EACH VEHICLE SPEED BASED ON CHORD ALGORITHM
RSU VERIFIES REQUEST VEHICLE ID &ENCRYPT THE VEHICLE QUERY USING RE-ENCRYTPION KEY BASED ON TA
RSU FIND THE SHORTEST PATH & VEHICLE RECEIVE ENCRYPTED QUERY
DECRYT THE QUERY BASED ON PRIVATE KEY
PRIORITY BASED VEHICLE MOVEMENT

Fig 1. Proposed System Architecture

A. *Construction of Chord Algorithm for Proposed Model*

Support of just one operation: given a key, Chord maps the key onto a node.The consistent hash function assigns each node and each key an m-bit identifier using SHA 1 (Secure Hash Standard).

a. m = any number big enough to make collisions improbable
b. Key identifier = SHA-1(key)
c. Node identifier = SHA-1(IP address)

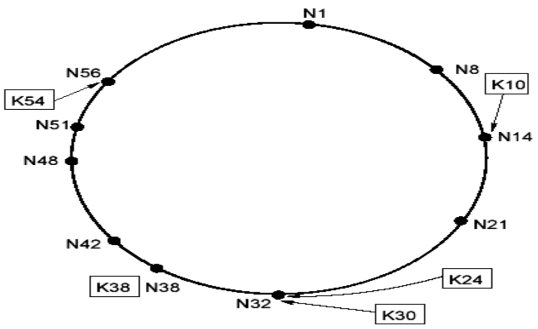

Fig 1. Process of Chord Algorithm

```
ask node n to find the successor of id
n.find_successor(id)
  if (id    (n; successor])
     return successor;
  else
forward the query around the circle
    return successor.find_successor(id);
```

STEP 1: Each node stores information about only a small number of nodes (m)

STEP 2: Each nodes knows more about nodes closely following it than about nodes farer away.A finger table generally does not contain enough information to directly determine the successor of an arbitrary key k.

V. CONCLUSION AND FUTURE WORKS

In the paper, 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. Our scheme also gives lower route blocking rate in practice.

The authentication process at vehicles can be even simpler because a vehicle only needs to check against the central server's signature on the processed result. However, such a centralized approach is not scalable, especially for large cities. We are implementing our VSPN scheme on a test bed to further verify its performance.

In the future, we will extend our efforts to investigate how best to address efficient user revocation issues, dynamic attribute addition, and secure V2V transmissions. Therefore, we will also try to improve the scalability of our scheme.

REFERENCES

[1]. VANET–based secure and privacy-preserving Navigation"t.W.Chim,s.M.Yiu,lucas c.K.Hui,senior MEMBER,IEEE,AND VICTOR o.K.Li,fellow" february 2014.
[2]. "Papago! Z-Series Navigation System," http://www.papago.com.hk/, 2009.
[3]. "Traffic Message Channel (TMC)," http://www.tmcforum.com/, 2011.

[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. 2010.

[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. 2011.

[6]. I.Leontiadis, P. Costa, and C. Mascolo, “Extending Access Point Connectivity through Opportunistic Routing in Vehicular Networks,” 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 VANETBased Smart Parking Scheme for Large Parking Lots,” Proc. IEEE INFOCOM ’09, pp. 1413-1421, Apr. 2009.

[9]. D. Chaum, “Security without Identification: Transaction Systems ssto Make Big Brother Obsolete,” Comm. ACM, vol. 28, pp. 1030-1044, 2012.

[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]. Global Positioning System Standard Positioning Service Signal Specification. Navtech GPS Supply, 2010.