International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT206497

Monitoring Vehicle Communication and Road Condition in VANET

Saravanakumar S
Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamil Nadu, India

Article Info
Volume 6, Issue 4
Page Number : 530-537
Publication Issue :
July-August-2020

Article History
Accepted : 20 Aug 2020
Published : 27 Aug 2020

ABSTRACT

The connected vehicular ad-hoc network (VANET) and cloud computing technology allows entities in VANET to enjoy the advantageous storage and computing services offered by some cloud service provider. However, the advantages do not come free since their combination brings many new security and privacy requirements for VANET applications. In this article, we investigate the cloud-based road condition monitoring (RCoM) scenario, where the authority needs to monitor real-time road conditions with the help of a cloud server so that it could make sound responses to emergency cases timely. When some bad road condition is detected, e.g., some geologic hazard or accident happens, vehicles on site are able to report such information to a cloud server engaged by the authority. We focus on addressing three key issues in RCoM. First, the vehicles have to be authorized by some roadside unit before generating a road condition report in the domain and uploading it to the cloud server. Second, to guarantee the privacy against the cloud server, the road condition information should be reported in ciphertext format, which requires that the cloud server should be able to distinguish the reported data from different vehicles in ciphertext format for the same place without compromising their confidentiality. Third, the cloud server and authority should be able to validate the report source, i.e., to check whether the road conditions are reported by legitimate vehicles. To address these issues, we present an efficient RCoM scheme, analyze its efficiency theoretically, and demonstrate the practicality through experiments

Keywords : Data privacy, vehicular ad hoc networks, VANET, cloud computing, authentication, audit ability.

I. INTRODUCTION

In the growing needs for increased safety and efficiency of road transportation system have promoted automobile manufacturers to integrate wireless communications and networking into vehicles. The wirelessly networked vehicles naturally form Vehicular Ad-hoc Networks (VANETs), in which vehicles cooperate to relay various data messages through multi-hop paths, without the need of centralized administration. VANETs(have the prospective to transform the way people travel

through creations of exchanging and making use of information wireless communications network .In VANETs, various nodes, such as vehicles and Roadside Units (RSUs), are generally equipped with sensing, processing, and wireless communication capabilities. Both Vehicle-to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication enable safety applications that provide warnings regarding road accidents, traffic conditions (e.g., congestion, emergency braking, and icy road) and other relevant transportation events. However, VANETs are vulnerable to threats due to increasing reliance on communication, computing and control technologies. The unique security and privacy challenges posed by VANETs include integrity (data trust), confidential, non repudiation, access control, real- time operational constraints demands, availability, and privacy protection.VANET technology with Machine Learning to create a system which can notify drivers of dangerous conditions such as forward collisions and over speeding which and lead to a potential accident. The data collected by the system can be used to take actions for preventing accidents.

VEHICULAR AD HOC NETWORKS

The majority of the data transmitted in the vehicular ad hoc network (VANET) supporting traffic safety applications will be broadcasted (one-to-many communication) and no acknowledgements (ACK) will be sent in response if messages are received successfully. Many ITS stations are typically interested in receiving the broadcasted messages and if everyone sent an ACK the communication channel would be flooded. In the VANET using 802.11p (with no central coordination), there will be a set of predetermined frequency channels for communication, and the only way to state the presence of an ITS station is to broadcast CAM/BSM on one these channels.

The network establishment has been removed in 802.11p, i.e., a station is allowed to communicate outside the context of a basic service set (the smallest building block of an 802.11 network). This implies that whenever a station has a message to send it can transmit directly under the condition that the MAC protocol allows it. Ad hoc topologies without prior network establishment has advantages such that a lower average delay can be achieved and no coverage by base stations is necessary – if there is someone to communicate with information exchange can take place. On the other hand, the ad hoc structure entails specific requirements for the communication protocols operating in this scenario. Specifically, the MAC protocol used in a VANET must be decentralized. It must cope with few stations as well as many stations without collapsing. Further, it should minimize simultaneous transmissions in an attempt to keep the interference at an acceptable level for receiving stations. The MAC protocol is a key component in cooperative systems because if channel access is not granted in a timely fashion, cooperation cannot be achieved.

MEDIUM ACCESS CONTROL

The MAC method decides when a station has the right to access the shared communication channel. The regulation is made by scheduling transmissions in time, frequency, space or by using unique codes, constellations or interleaves to distinguish different stations. The type of MAC method to use in a particular communication network is selected based on network topology and application. Since all communications in a centralized network must traverse the AP/BS, it has knowledge of all nodes within range. A centralized network can therefore use a centralized MAC protocol that distributes available resources (frequencies, time slots or orthogonal codes) among all nodes currently within range. This implies that the AP/BS can use the MAC protocol to optimize performance based on specific

requirements. In ad hoc networks it is more difficult find such a resource efficient MAC method, especially since the number of stations can drastically vary from time to time. In a C-ITS operating in a VANET context, the requirements on the MAC method stem from three different parts namely (i) the ad hoc topology, (ii) road traffic safety applications, and (iii) the overall C-ITS

VEHICULAR NETWORKS

In recent years, most new vehicles come already equipped with GPS receivers and navigation systems. Car manufacturers such as Ford, GM, and BMW have already announced efforts to include significant computing power inside their cars and Chrysler became the first car manufacturer to include Internet access in a few of its 2009 line of vehicles . This trend is expected to continue and in the near future, the number of vehicles equipped with computing technologies and wireless network interfaces will increase dramatically. These vehicles will be able to run network protocols that will exchange messages for safer, entertainment and more fluid traffic on the roads. Standardization is already underway for communication to and from vehicles. The Federal Communication Commission (FCC) in the United States has allocated a bandwidth of 75MHz around the 5.9GHz band for vehicle to vehicles and vehicles to road side infrastructure communications through the Dedicated Short Range Communications (DSRC) services.

COMMUNICATIONS THROUGH CELLULAR NETWORK

The first method connects vehicles to the Internet through cellular data networks using any of the following technologies: EV-DO, 3G, GPRS, etc. This service is already commercially available from car manufacturers and from other third-parties. In most commercially available solutions, the vehicle is transformed into a IEEE 802.11 (WIFI) hotspot and the Internet connection can be shared by many computers in the car. Usually, a limit is set on the amount of data transfer (e.g., 1GB or 5GB maximum per month). The main advantage of this method of connection is that the vehicle will have Internet access wherever cellular coverage is available. The main drawbacks are the dependence on the cellular operator coverage network and the limited available data rates (rates vary around 500Kbps – 800Kbps).

VEHICLE TO ROADSIDE INFRASTRUCTURE COMMUNICATIONS

The second method uses roadside infrastructure. Here, vehicles connect to other vehicles or to the Internet through roadside access points positioned along the roads. Two main variants can be found in the literature: the access points could be installed specifically for the purpose of providing Internet access to vehicles or the latter could make use of open 802.11 (Wi-Fi) access points encountered opportunistically along city streets. The advantage of this method of connection is that vehicles will be able to connect to the Internet using much higher data rates (e.g., 11Mbps) than through the cellular network. The drawbacks include the cost related to installing access points along the roads to obtain reasonable coverage. Additionally, in the case where open access points are used, the access point's owners' consent would legally be required before such a service is deployed

Characteristics of vehicular ad hoc networks

VANETs are characterized by (a) high node mobility, (b) constrained nodes movements (c)obstacles-heavy deployment fields, and (d) large number of nodes, which all add to the communication challenges. First, vehicles are continually moving along the roads at higher speeds than in a MANET. Thus a VANET will present a continually changing structure, and

communication links are expected to be valid for few minutes or seconds. Next, the movements of vehicles are constrained on roads; hence the existing roadmaps put a limit to the topologies available in VANETs, when compared to MANETs. Then, the presence of high- rise buildings and houses between streets impacts the propagation of wireless waves through reflections and refractions. Finally, VANETs have the potential to contain a very large number of nodes as any vehicle can be part of the network. It is assumed that each vehicle is equipped with a Geographical Positioning System (GPS), digital maps or navigation system and an ad hoc wireless communication device.

II. EXISTING METHODOLOGY

- In an existing system a new privacy- preserving signature scheme for inter- vehicle communication has been implemented using bloom filters.
- Data authentication and integrity protection in automatic dependent surveillance-broadcast system has been implemented.
- A Bloom Filter (BF) is a type of probabilistic data structures that is used to store a set of n elements and test a membership of an element.
- A lightweight authentication scheme using Timed Efficient Stream Loss- Tolerant Authentication (TESLA) scheme and Bloom Filters that not only prevents active attacks but also adds a privacy-preserving feature to make the scheme have better performance.
- In addition, the expected anonymity set sizes have significant drops on both proposed scheme and no scheme installed scenario when the value of k increased. Because it is less probability of finding greater or identical k neighboring vehicles when the value of k is getting bigger.

DRAWBACKS

- External sources for destination location
- Delay
- Increasing the network congestion
- Flooding in route discovery initial phase

PROPOSED METHODOLOGY

- In this project road monitoring scheme implemented based on RCoM algorithm.
- Different types of feature implemented based on different kind of features a root authority (RA), many sub-authorities (SAs), many roadside units (RUs), a cloud server, and many vehicles.
- RCoM algorithm trained based on these features. And it's used to monitoring road vehicles.
- This paper proposes a privacy-preserving cloud-based road condition monitoring system with source authentication.

ADVANTAGES

- Public safety
- Traffic management
- Traffic coordination and assistance

III. RELATED WORK

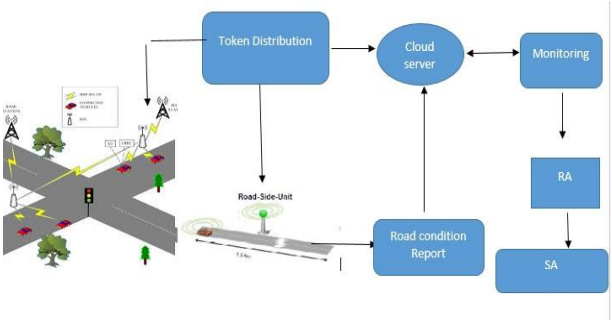
The RCoM system consists of five types of entities that is, a root authority (RA), many sub-authorities(SAs), many roadside units (RUs), a cloud server, and many vehicles. A platform is the hardware or software environment in which a program runs. We've already mentioned some of the most popular platforms like Windows 2000, Linux, Solaris, and MacOS. Most platforms can be described as a combination of the operating system and hardware. The Java platform differs from most other platforms in that it's a software-only platform that runs on top of other hardware-based platform.

JDBC

In an effort to set an independent database standard API for Java; Sun Microsystems developed Java Database Connectivity, or JDBC. JDBC offers a generic SQL database access mechanism that provides a consistent interface to variety of Rdbms.

This consistent interface is achieved through the use of "plug-in" database connectivity modules, or drivers. If a database vendor wishes to have JDBC support, he or she must provide the driver for each platform that the database and Java run on.

To gain a wider acceptance of JDBC, Sun based JDBC's framework on ODBC. on a variety of platforms. Basing JDBC on ODBC will allow vendors to bring JDBC drivers to market much faster.than developing a completely new connectivity solution.



Initially, to join the system, all vehicles must be authorized by RA, in this way to get private keys extracted from their respective identities. Note that
the number of vehicle may be significantly large. Thus, RA needs to delegate SAsto authorize vehicles and roadside units. In practice, each SA has a disjoint management region, which is only responsible for authorizing vehicles in its region. Also, each vehicle can
only be authorized by one SA. Every vehicle can collect
and report real-time road condition if a dangerous road condition is detected. Similarly, every RU also gets a private applications, SAs can be separated into two categories to respectively deal with the registration of vehicles and RUs. In RCoM, all roads are divided into disjoint sections. For ease of presentation, each road section is represented by the identity of its administrative RU in this paper. When some vehicle gets into a new section, the administrative RU issues
a token which enables the vehicle to report the detected road condition information in this section.

IV. SYSTEM SETUP

The root authority RA generates a bilinear mapping ^e : G_G ! GT , where G and GT are cyclic groups with prime order p, and g; h are two distinct generators of G. RA then selects random values x; z 2R Z_key msk = (x; z), and computes y = gx and w = gz. RA also picks seven cryptographic hash functions such as Hi : f0; 1g_ ! Z_p for 1 _ i _ 5, H6 : G ! f0; 1g_ru+_I+2 log p and H7 : f0; 1g_ ! G, where _ru and _I denote the length of the identities of RU and road condition information I, respectively.

RA also generates an alert threshold _ (e.g., _ =10) such that when _ or more vehicles report the same road condition at the same place, it would be looked as an emergency case and need fast response from RA. Finally, RA sets the public system parameters par =(^e; G;GT ; g; h; p; y;w;H1;H2; _ _ _ ;H7; _).

VEHICLE REGISTRATION

In the registration phase, every vehicle Vj gets the authorization (e.g., a secret key) from its administrative subauthority SAi. SAi picks a random value ri;j 2R Z_p , calculates the secret key vskj = (vskj;1; vskj;2; vskj;3) where,
vskj;1 = sski;1; vskj;2 = gri;j

vskj;3 = sski;2 _ hri;jH2(SAikVjkvskj;1kvskj;2)

and gives vskj to Vj securely. Vehicle Vj is able to verify vskj as follows

^e(vskj;3; g) ?=^e_h; vskj;1 _ yH1(SAikvskj;1)
_vskH2(SAikVjkvskj;1kvskj;2)
j;2
_

ROADSIDE UNIT REGISTRATION

As in the vehicle registration phase, every roadside unit RUl obtains a secret key from its Administrative sub-authority SA`. That is, SA` picks a random value r`;l 2R Z_p , calculates the secret key rskl = (rskl;1; rskl;2; rskl;3) rskl;1 = ssk`;1; rskl;2 = gr`;l and

rskl;3 = ssk`;2 _ hr`;lH2(SA`kRUlkrskl;1krskl;2)
and gives rskl to RUl securely. Roadside unit RUl can validate rskl as follows
^e(rskl;3; g) ?=^e_h; rskl;1 _ yH1(SA`krskl;1)

METHODOLOGIES

1. Registration module and Contacts details

2. VANET

3. Accident intimation

4. Weather forecast

5. MongoDB

6. Trace module

REGISTER AND CONTACT MODULE

- User can view the details about the all other users.
- It's processed by user module get all the user information's.
- Web system is connected with local host.
- The user enter the personal details for registering in the web system.

VANET

- Vehicular ad-hoc networks (VANETs) include vehicle-to-vehicle and vehicle-to infrastructure communication.
- In this, a novel smartphone integrated driving safety application along with a traffic signal priority control method is an effort to clear the path for emergency vehicles is modeled.
- Management of Road Traffic through Data Retrieval In VANET Environment),a server and Road Side units.

ROADSIDE UNIT REGISTRATION

- An accident management system that make use of VANET coupled with systems that employ cellular technology in public transport.
- It provides systems ensures the possibility of real time communication among vehicles, ambulances, Management of Road Traffic through Data Retrieval In VANET Environment).

WEATHER FORECAST

- Weather forecast system that make use of VANET coupled with systems that employ cellular technology in public transport.
- The provides systems ensures the possibility of real time communication among vehicles, ambulances, hospitals, road side and cloud servers.
- It is intimate the weather condition to the vehicles

MongoDB

- MongoDB is a document database with the scalability and flexibility that you want with the querying and indexing that you need.
- Here it is used to show the speed level of vehicles and performance chart.
- It is used to track the vehicle particular location

V. CONCLUSION

Common system to manage accidents so that vehicles are able to avoid congested areas within an ITS. Initially, we established an accident management system which employs cellular systems of the public transportation systems and VANETs to make efficient real-time communication between vehicles possible, including ambulances, hospitals, RSUs, and central servers. We subsequently propose a real-time algorithm for planning routes with the aim of improving the overall use of space while at the same time reducing the cost of travelling, through vehicles' ability to avoid congested road segments.

The path planning algorithm to propose will reduce the time taken by ambulances to be alerted and dispatched to a scene of accident through being able to avoid road segments that are congested and will increase the chance of saving the lives of accident victims.We considered the problem of privacy-preserving cloud-based road condition monitoring with source authentication (RCoM). There are two levels of authorities such that the root authority delegates sub-authorities to perform registration for vehicles and RUs. RA monitors real-time road conditions through a third party intermediary, that is, vehicles report the detected road conditions to the cloud server for verification and processing, in this way, only the valid information sent from legitimate vehicles will be picked out for RA to make response. To protect the privacy against the cloud server, the road condition report should be uploaded in cipher text format, which brings another challenge for the cloud server to distinguish the same road condition for the same place from lots of reports. In response to these functionalities and security and privacy requirements in RCoM, we presented an efficient scheme and compared it with related techniques. A Road Accident Prevention (RAP) scheme for instant EWM dissemination to the vehicles is proposed in order to prevent them from highway road traffic accidents. Thereby the death and injury rates can be reduced in Indian four lane highways. In RAP scheme, once the RSU predicts the possibility of occurrence of an accident or emergency situation, instantly it generates EWM, forms a VBN structure and disseminates EWM to the vehicles which have high reception priority.

The performance evaluation of RAP schemes is done by using NS-2 simulator. From the simulation results, it is noticed that RAP scheme with VBN structure outperforms RAP scheme without VBN structure by providing better EWM dissemination performance in terms of (i) reducing the S-D distance, (ii) improving notification by 19 percent and (iii) reducing end-to-end delay by 14.38 percent. Further, the number of RSUs required is reduced due to the usage of VBN structure in VANET. But, the network processing overhead of RAP scheme with VBN structure is found to be higher.

VI. REFERENCES

[1]. L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B.Qin, "Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response," IEEE Transactions on Computers, vol. 65, no. 8, pp. 2562–2574, Aug. 2016.

[2]. Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," IEEE Transactions on Vehicular Technology, vol. 59, no. 2,pp. 559–573, Feb 2010.

[3]. F. Qu, Z. Wu, F. Y. Wang, and W. Cho, "A security and privacy review of vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985-2996, Dec 2015.

[4]. "IEEE Standard for Wireless Access in Vehicular Environments Security Services for

Applications and Management Messages,"IEEEStd 1609.2-2016 (Revision of IEEE Std 1609.2-2013), pp. 1-240, March 2016.

[5]. "L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 516–526, March 2017.

[6]. L. Chen, S. L. Ng, and G. Wang, "Threshold anonymous announcement in vanets," IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp.605 -615, March 2011.

[7]. Y. Liu, J. Ling, Q. Wu, and B. Qin, "Scalable privacy-enhanced traffic monitoring in vehicular ad hoc, networks," Soft Computing, vol. 20, no.8, pp.3355-3346, Aug 2016.

[8]. R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, "Toward cloud based vehicular networks with efficient resource management,"IEEE Network, vol. 27, no. 5, pp. 48–55, September 2013.0

[9]. J. A. Guerrero-ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies," IEEE Wireless Communications, vol. 22, no. 6, pp. 122–128, December 2015.

[10]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,"A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp.50–58, Apr. 2010

Cite this article as :

Saravanakumar S, "Monitoring Vehicle Communication and Road Condition in VANET", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 4, pp. 530-537, July-August 2020. Available at doi : https://doi.org/10.32628/CSEIT206497
Journal URL : http://ijsrcseit.com/CSEIT206497