ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

The Smart Transportation using IoT and Intelligent Transport System in GPS Localization

Elavarasi T[1], Kuppusamy P[2]

M.E Student, Dept. of Computer Science and Engineering, Gnanamani College of Technology, Namakkal, India[1]

Head of the Department, Dept. of Computer Science and Engineering, Gnanamani College of Technology, Namakkal, India[2]

ABSTRACT: Internet of things (IoT) a real world things or objects are connected each other for communicate anytime anywhere. Large numbers of real world objects are connected to internet that generated large amount of data. The major objectives for the IoT are creation of smart environments on transportation, home automation, education, agriculture on cities and villages. The IoT offers many number of solutions in transport sector like toll systems, traffic management, vehicle tracking, vehicle to vehicle communication, smart parking, accident prevention infrastructure monitoring

KEYWORDS: Internet of things (IoT), Transportation, RFID, Regional Transport Office, Arduino UNO, Aadhaar's card, Vehicle registration

I. INTRODUCTION

Consider the problem of check post and toll gate they just check the documents such as Driving License, RC book, Insurance documents and leave the vehicle. The documents submitted by the persons not aware either original or duplicate .In this case some people provide wrong documents for illegal transactions. This project proposed to avoid the problem such as illegal transaction, vehicle theft.The vehicle entered in to the check post or toll gate the information's of vehicle will be checked from the system. Weight sensor is employed in this project for calculate the weight of the vehicle. Bio metric readers used for scan the thumb of driver and check the details of the person from data base of aadhaar data and verify the vehicle number for reference. These three details are stored on the system. If any details are wrong then the vehicle is not allowed to cross the check post. Every day the vehicle details of crossing the check post or toll gate will be stored in data storage. Cluster connectivity established with nearest toll gate, check post for communicate each other for share the details of crossed vehicles.

II. RELATED WORK

In existing system check post officers just check the documents and leave the vehicle. So the over loaded vehicle, illegal transition vehicles can be allow them to enter in check posts. Officers check the documents such as Driving License, RC book, Insurance documents and leave them. The documents provided by the person who drives the vehicle was original or duplicate. In this case some people provide wrong documents for illegal transactions. To avoid this problems using Smart Transportation using IoT. Some problems are illegal object transition, over loaded vehicles, money laundering by official, duplicate vehicles documents.

Disadvantages

- Time Delay
- Weight will be not accurate
- Illegal object transition

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

- Over loaded vehicles
- Money laundering by official
- Duplicate vehicles with same permit

III. PROPOSED ALGORITHM

In Smart Transportation project is used to overcome the problem of illegal transaction. Using this project easily finding the documents provided by the driver is correct or not. And also the exact weight of Vehicle will be measured by the weight sensor. During illegal transaction the vehicle numbers are changed. So the registration numbers of the vehicles in tamilnadu will be get from Regional Transport Office(RTO) registration department and the numbers are not in database easily stop the illegal transitions or vehicle theft. Also the alert message will send to related departments. In this project, consider the problem of check post and toll gate they just check the documents. The documents provided by the person who drives the vehicle was original or duplicate. In this case some people provide the wrong documents for illegal transactions. To avoid this problems using Smart Transportation using IOT. The vehicle entered in to the check post or toll gate the information's of vehicle will be checked from the system. The details of the vehicle where send to the every check posts by the owners during the vehicle is started from the source location. Details are required by application on website is first the transport company need to sign up with the transport details such as registration id, VAT tax number, CST number , address of the transport, owner details.After signup each data's where verified using the transport data's and provides login id and password for each user. Suppose vehicle was travel from one location to another location owner need to login in to the transportation web site and enter the source of the vehicle started from, destination to deliver the product, which type of item where loaded on vehicle, who drives the vehicle, weight of the vehicle when it was loaded, traveling path of the vehicle from source to destination. After enter all the details the verification barcode will send to user.Weight sensor is employed here for calculate the weight of the vehicle. Bio metric readers used for scan the driver thumb and check the details of the person from Data base of Aadhaar's card data. Also check the vehicle number for reference. These three details are stored on the system. If any details are wrong means the vehicle was not allowed to cross the check post. Every day the vehicle details of crossing the check post or toll gate will be stored in data storage.

INTELLIGENT TRANSPORTATION SYSTEM USING GPS LOCALIZATION:

A challenging issue in intelligent transportation systems (ITS) is to accurately locate moving vehicles in urban area. Considerable efforts have been made to improve the localization accuracy of standalone GPS receivers. However, through empirical study, found that the latitude and longitude values generated by GPS receivers fluctuate significantly because of the multipath effect in urban areas. The relative distances between neighboring vehicles with similar GPS signal data in terms of satellite sets and signal strength are much more stable in such a scenario. cooperative localization algorithm, Networking-GPS, to improve the accuracy of location information for vehicular networks in urban area using commodity GPS receivers. First, atom redundantly rigid graphs of vehicles are constructed according to the similarity of neighboring GPS data.Based on real-time exchange of their individual GPS position coordinates, and then propose a novel system solution for achieving the same (relative positioning functionality) during persistent GPS outages. Based on survey results, also qualitatively assess various radio based ranging and relative positioning techniques, experimentally evaluate the received signal strength based ranging technique, and comment on their suitability for our proposed solution.

1) Vehicles in geographical proximity often share redundant information such as road and traffic conditions. Hence, in V2I based applications, such as probe vehicle data, where the vehicles respond to requests received from the infrastructure, not all vehicles need to send replies. 2) As observed in, the mobility of vehicles is spatially restricted and spatially dependent. Hence, vehicles in geographical proximity can navigate as a group, with the same average velocity due to the spatial dependency, and with similar direction due to the spatial restrictions, over a period of time. The above observations, and propose to enable vehicles to form a group. In order to form a group, restrict the vehicles to be in a group if each group member can hear broadcasts of every other group member. Since vehicles in a group will move relative to each other, and on average have the same velocity, a group can be represented by a single vehicle that refer to as the group leader. Then for most of the V2I communication based VANET applications, it is sufficient if only the group leader communicates on behalf of the group.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

DIFFERENTIAL GLOBAL POSITIONING SYSTEM (DGPS)

Differential GPS (DGPS) consists of two receivers observing the same GPS satellites. One of these receivers is stationary and the other one is roving. The stationary receiver resides at a known location and obtains the pseudo-range from the satellite signals, so it identifies a global error by comparing the measurements with its location. The stationary receiver transmits the global error correction to the roving receiver so that the roving one can correct its measurements. DGPS takes advantage of correlated errors by installing a GPS receiver in an already known fixed location. This GPS receiver can compute its position using the information from the satellites and compare the computed position with its already known physical location. The difference between these two positions can be broadcasted and all nearby GPS receivers can correct their computed positions based on the broadcasted differential information. This is why this technique is known as Differential GPS. A drawback of this technique is that fixed ground-based reference stations must be used to broadcast this differential information. On the other hand, DGPS can lead to a sub-meter precision, which is sufficient for most VANET critical applications.

EXTERNAL HARDWARE REQUIREMENTS

- Arduino UNO board
- RFID tag
- Bio-metric Reader- for find the driver details from database
- Weight Sensor – for measure exact weight of vehicle
- Ethernet shield – for network connectivity
- RSU,GPS tracker

DEVICE CONNECTIVITY WITH ARDUINO UNO BOARD

On arduino uno board the devices like RFID, sensor, Biometric reader, and Ethernet shield are connect to board. Each device is used to find some important details in this project. Sensor is employed here for calculate the exact weight of the vehicle. And finger print reader used to find the driver data from the database. And Ethernet shield used to establish the internet connection for data sharing and communication with the server device and nearest tollgate or check post on high ways.
RFID tags are used to store smart vehicle number data storage.

THRESHOLD LIMIT FOR WEIGHT SENSOR

Weight sensor is used to calculate the exact weight of vehicle .suppose the threshold weight will cross the limit means vehicle not allowed to go and put fine to the driver. And the weight within the limit on threshold limit value means go for the next step of checking the documents provided by the driver.

AADHAAR'S CARD, VEHICLE REGISTRATION DATA STORAGE

The details of aadhaar card and vehicle number details are stored in the database for verification. Verify the name and photo of the driver from aadhaar database. With the use of finger print reader. The finger print reader scan the drivers thump and get the correct match of the thump from aadhaar's card data stored on system. The officer enter the vehicle number on system means the data of vehicle details such as registered distract and name of the owner, address, phone number of the owner and all the data's are shown on the system. These details are wrong means the system shows the alert message. Also all the details will be stored in data storage.

ESTABLISH THE CLUSTER CONNECTIVITY WITH NEAREST CHECK POST AND TOLL GATES:

Cluster connectivity established between the nearest check post and toll gate. Cluster means a group of similar things or people connect together throw internet. If the check post and toll gate are in between the particular district or state or particular distanced areas will connect together for getting vehicle details that cross the first check post and toll gate. It just for verifying the data. Suppose in between the distance of two check post and toll gate it may have a chance

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

to change driver or illegal activities like vehicle theft, illegal object transaction. So the data's of vehicles are shared to next check post and toll gate with in particular distance.

IV. SIMULATION RESULTS

1. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure

In this Module, the two basic communication modes, which respectively allow OBUs to communicate with each other and with the infrastructure RSUs. Since vehicles communicate through wireless channels, a variety of attacks such as injecting false information, modifying and replaying the disseminated messages can be easily launched.

A security attack on VANETs can have severe harmful or fatal consequences to legitimate users. Consequently, ensuring secure vehicular communications is a must before any VANET application can be put into practice. A well-recognized solution to secure VANETs is to deploy Public Key Infrastructure (PKI), and to use Certificate Revocation Lists (CRLs) for managing the revoked certificate[fig1]. In PKI, each entity in the network holds an authentic certificate, and every message should be digitally signed before its transmission. A CRL, usually issued by a Trusted Authority (TA), is a list containing all the revoked certificate. In a PKI system, the authentication of any message is performed by first checking if the sender's certificate is included in the current CRL, i.e., checking its revocation status, then, verifying the sender' certificate, and finally verifying the sender's signature on the received message.

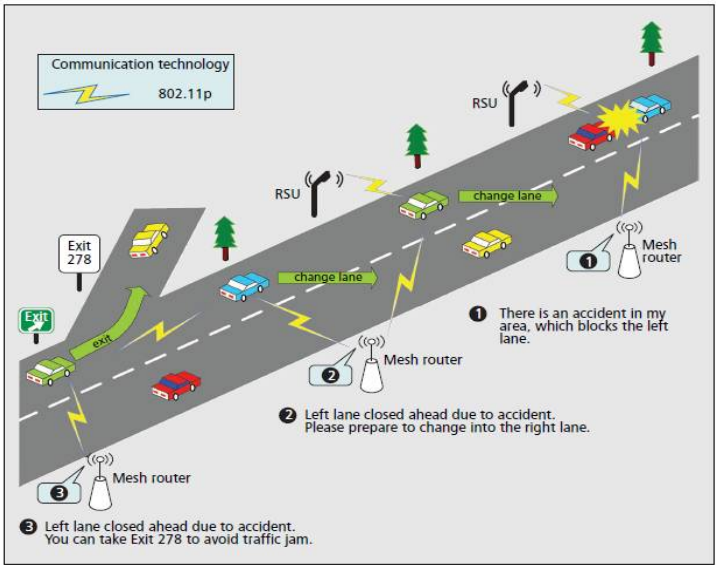

Fig:1 System architecture

2. Expedite Message Authentication Protocol

A Trusted Authority (TA): This is responsible for providing anonymous certificate and Distributing secret keys to all OBUs in the network.

Roadside units (RSUs): which are fixed units distributed all over the network. The RSUs Can communicate securely with the TA.

On-Board Units (OBUs): which are embedded in vehicles? OBUs can communicate either with other OBUs through V2V communications or with RSUs through V2I communications [Fig2].

3. Security Analysis

a. *Hash Chain Values*

The values of the hash chains are continuously used in the revocation processes, and hence, the TA can consume all the hash chain values. As a result, there should be a mechanism to replace the current hash chain with a new one.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

b. ***Resistance of forging attacks***

To forge the revocation check of any on board unit an attacker has to find the current problem. And find the TA secret key and signature. To the revocation check and TA message and signature are unforgeable.

c. ***Forward* secrecy**

The values of the hash chain included in the revocation messages are released to non-revoked OBUs starting from the last value of the hash chain, and given the fact that a hash function is irreversible, a revoked OBU cannot use a hash chain value received in a previous revocation process to get the current hash chain value, a revoked OBU cannot update its secret key set.

d. ***Resistance to replay attacks***

Each message of an OBU includes the current time stamp in the revocation check value check an attacker cannot record REV check at time T and replay it at a later time process as the receiving OBU compares the current time.

e. ***Resistance to colluding attacks***

A legitimate OBU colludes with a revoked OBU by releasing the current secret key such that the revoked vehicle can use this key to pass the revocation check process by calculating the correct HMAC values for the transmitted messages. All the security materials of an OBU are stored in its tamper-resistant.

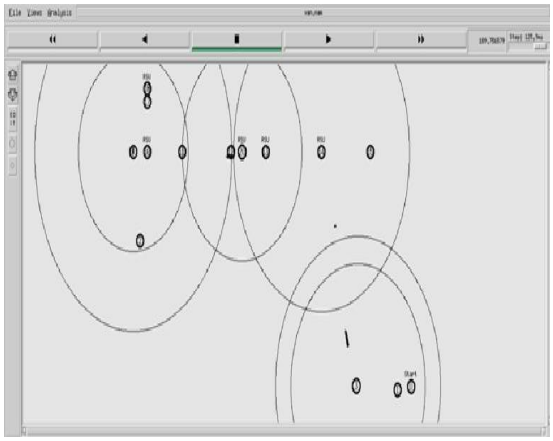

Fig2:Vehicle to RSU GPS signal broadcasting

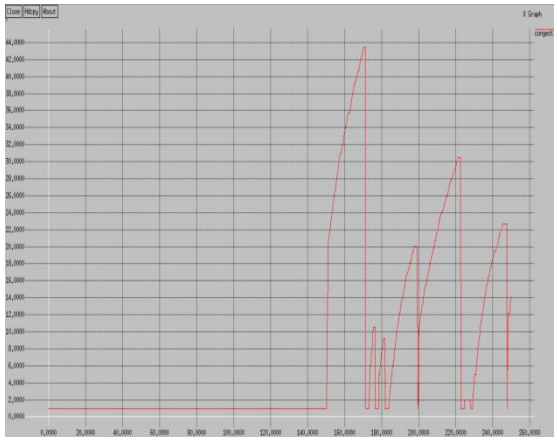

Fig3: communication graph of devices

V. CONCLUSION AND FUTURE WORK

Security and efficiency are two crucial issues in vehicular ad hoc networks. Many researchers have devoted to these issues. However, we found that most of the proposed protocols in this area are insecure and can't satisfy the anonymous property. Due to this observation, we propose hardly method to resolve the problems. After analysis, we conclude that our scheme is the most secure when compared with other protocols proposed so far.

The future of this research concerns the use of numerical model of terrain in order to provide a height estimate for purpose of reliability improvement. In the same way, the benefits of using SBAS corrections and future GNSS improvement for accuracy and precision of the estimated position will be studied.

REFERENCES

[1] P. Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, "Privacy and Identity Management for Vehicular Communication Systems:A Position Paper," Proc. Workshop Standards for Privacy in User-Centric Identity Management, July 2006.
[2] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura,and K. Sezaki, "CARAVAN: Providing Location Privacy for VANET," Proc. Embedded Security in Cars (ESCAR) Conf., Nov.2005.
[3] A. Wasef, Y. Jiang, and X. Shen, "DCS: An Efficient Distributed Certificate Service Scheme for Vehicular Networks," IEEE Trans.Vehicular Technology, vol. 59, no. 2 pp. 533-549, Feb. 2010.
[4] M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks," J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.
[5] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Preservation for Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.
[6] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in Vanets," IEEE Trans. Vehicular Technology, vol. 61, no. 1, pp. 86-96, Jan. 2012.
[7] US Bureau of Transit Statistics, http://en.wikipedia.org/wiki/ Passenger_vehicles_in_the_United_States, 2012.
[8] J.J. Haas, Y. Hu, and K.P. Laberteaux, "Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET," Proc. Sixth ACM Int'l Workshop VehiculAr InterNETworking, pp. 89-98, 2009.
[9] IEEE Std 1609.2-2006, IEEE Trial-Use Standard for Wireless Access inVehicular Environments - Security Services for Applications and Management Messages, IEEE, 2006.
[10] "5.9 GHz DSRC," http://grouper.ieee.org/groups/scc32/dsrc/ index.html, 2012.