Volume 5, Issue 9, September 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Study on Security of IoT in Intelligent Transport Systems Applications

[2]Anitha Chepuru, [2]Dr. K.Venugopal Rao
[1]Associate Professor IT Dept, [1]Professor ,HOD ,CSE Dept
[1, 2] G.Narayanamma Institute of Technology and Science (for women),
Shaikpet, Hyderabad, Andhra Pradesh, India

Abstract: In this paper ,We study the Internet of things in Intelligent transport system (IoT- ITS) existing methods for IOT –ITS and the results with different parameters . The Radio Frequency IDentification (RFID) technology is one of the core technologies of IoT deployments in the ITS. To satisfy the various security requirements of RFID technology in IoT, many RFID authentication schemes have been proposed in the past decade. Recently, Elliptic Curve Cryptography (ECC)-based RFID authentication schemes have attracted a lot of attention and have been used in the ITS .As Security will be fundamental enabling factor of most Internet of things (IoT) our proposed system can implemented in Intelligent transport (ITS) applications as existing system Study analyses the existing work done in IoT –ITS using RFID Technology. we propose a new method for obtaining more security by reducing attacks and also to decrease the communication time ,computation time, Encryption Time and communication overhead .

Key words: IoT, ITS, Security, RFID, ECC

I. INTRODUCTION

Information technology develops fastly on the nowadays, a new concept comes out and develops the Inter-net of things. In the past decade, there were various techniques and algorithms developed the Intelligent Traffic System by using AVL and APC data [1]. Intelligent Traffic System now, because the accuracy of this algorithm is better than others. However, many re-searchers cannot realize the algorithms on the Intelligent Traffic System based on the Internet of things.

In the future, the Internet of things will be more popular on the intelligent transportation system. The Internet of things has provided a very fine platform for intelligent traffic studies, it exchanges public transit vehicle information by the network and without people's disturbance, thereby the information of the public transit vehicle be-come especially intelligence. ITS effectively used in advanced technology in the field of IoT. With introduction of the IoT the service mode of intelligent transport system and system architecture has changed dramatically."Internet of things is an internet which is connected with things" through RFID technology, infrared, sensors positioning information of vehicles using GPS technology .Research done in ITS application areas are - Advanced public transport system: (APTS) Advanced Traveler Information System: (ATIS) Advanced Traffic Management System: (ATMS) Vehicle-to-infrastructure Integration (VII) and Vehicle-to-vehicle (V2V) Integration. ITS based on IoT has number of advantages such as low cost ,high reliability ,never effected by adverse weather.

II. EXISTING

Advanced Traveler Information System (APTS)fleet management system, travelers information system and electronic payment system.

Saeed Samadi author [2] proposed Radio Frequency
Identification (RFID) Technology in Intelligent Transportation Systems In fig. 1 shows the main architecture of the system in which fare payment using "My Card" is also anticipated. The RFID technology will identify each vehicle and driver and facilitate the dispatch of taxis by agents using handheld devices linked to a wireless network. It is believed that RFID-based technologies can be extensively exploited to improve transportation safety and security, increase the efficiency of the transportation system, ultimately save costs, and improve people lives. Also, Smartcard-based fare payment provides convenience for passengers and efficiency gains for transport service providers.

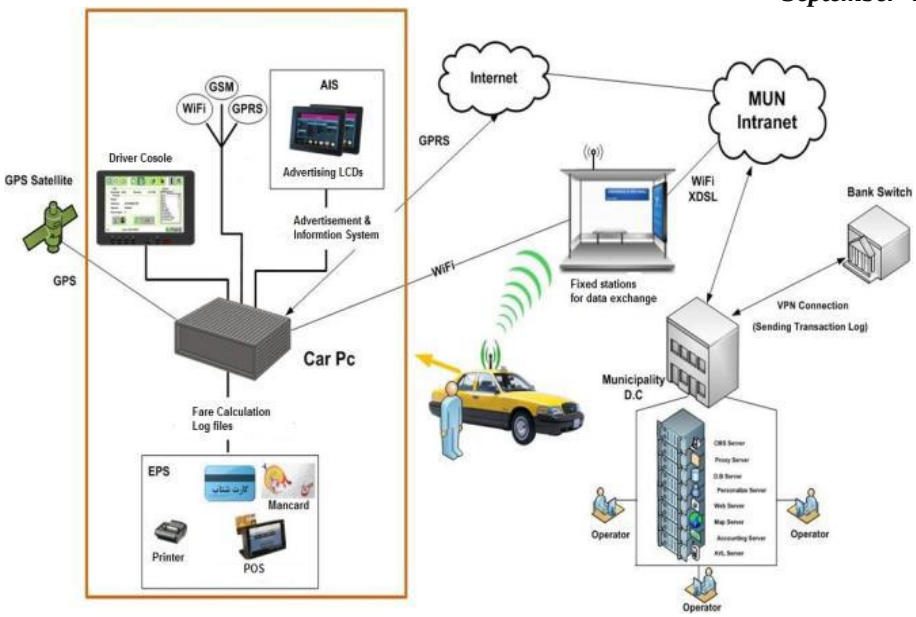


Fig 1. Architecture of Mashhad taxi fleet management system using " My Card" payment

In Fig 2.The system also provides important management information for planning and statistics. Some important outcomes of the system are:

- Rapid and accurate tracking of Taxi sign out and activity history
- Effective real-time updates on fleet inventory and activity records
- Rapid check in/check out for reduced turn-around time and client wait
- Accurate information on vehicle use and activity history for maintenance and purchasing decisions
- Current record of vehicle availability for efficient management
- Reduction in labor to manually record data and update system
- Reduced theft and increased safety

An interesting benefit of this project is the ability of checkpoints to gather real-time travel data .Based on this information, traffic management authorities could help predict travel times and optimize their traffic plans. This is an inexpensive way and eliminates the need to probe vehicles for traffic data gathering management system

Fig. 2. Tags, readers and checkpoints used in Mashhad Taxi fleet

Advanced Traffic Management System Application-Intelligent traffic monitoring

Laisheng Xiao and Zhengxia Wang [3] author proposed Constructing an intelligent traffic monitoring system firstly depends on automatic identification for vehicles.At present, automatic identification technology based on image and vehicle license plate is going to fall in the trap due to its low recognition rate and affection by adverse weather. Fig.3 shows the vehicles with RFID Thus it is necessary to apply new technologies to solve this problem, and technologies based on Internet of Things provide a new approach for it. In this paper, explored this issue and proposed a feasible scheme. At first, taking global unique EPC code as identity identification of vehicles instead of vehicle license plate and utilized RFID reader to read EPC code by RF electromagnetic wave, which completely solved the problem of no all-weather operations. Secondly, by obtaining positioning information of vehicles by using GPS technology. Thirdly,

because GPRS provides high-speed wireless IP services for mobile users, fully supports the TCP/IP, we took wireless GPRS scheme to transmit data of mobile objects. The realization of automatic detection and transmission of data provided a fundamental guarantee for constructing an intelligent traffic monitoring system. And then, designing intelligent decision-making module. Each vehicle is equipped a RFID tag in which a global unique EPC code is taken as its identity identification. When it comes by a fixed monitoring station or a mobile monitoring station, the RFID reader will read the EPC information in RFID tag on it. In such a way, a mobile vehicle can be identified.

Synchronously, a GPS receiver installed in a monitoring station can communicate with GPS satellites to obtain its position information that is taken as a position parameter of the vehicle. So with this method the position data of mobile vehicle is also captured. To solve the third problem, we take wireless GPRS scheme to transmit data of mobile objects. GPRS provides high speed wireless IP services for mobile users, fully supports the TCP/IP, dynamically allocates IP addresses for the mobile sites and achieves mobile Internet functions, so it can be connected with Internet seamlessly[4][5][6].

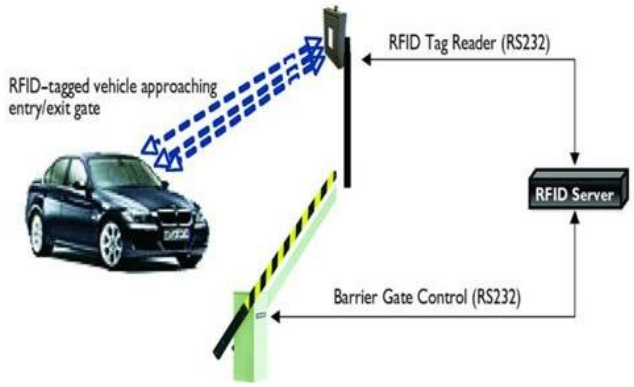
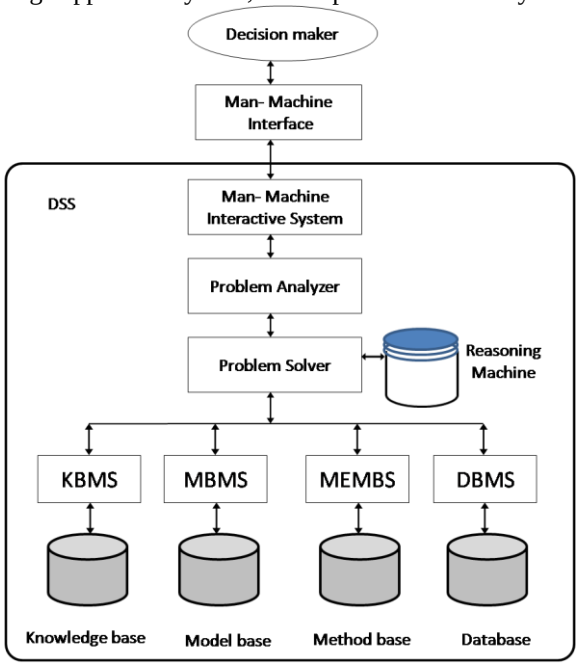


Fig.3 RFID tagged vehicle and Reader

Software of monitoring center: Intelligent monitoring includes two implications. At first, automatic identification and automatic transmission in front-end should be actualized. The other implication is that automatic managements in back-end should be realized too, where construction of traffic decision-making support system for traffic management is the core of the all problems. Because of finite length of the paper, here we introduce a module of traffic decision-making support subsystem for intelligent traffic monitoring system. The software structure of traffic decision-making support subsystem is shown in Figure 4.Traffic decision-making support subsystem consists of man-machine interactive system, problem analyzer, problem solver, KBMS, MBMS, MEBMS, DBMS etc. A reasoning machine of problem solver for highway congestion control and scheduling, which is based on the data of EPC code, GPS positioning and vehicle speed, is designed in traffic decision-making support subsystem, which provides the subsystem a very highly intelligence.



KBMS –Knowledge Base Management System
MBMS- Model Base Management System
MEBMS- Method Base Management System
DBMS- Data Base Management System

Fig. 4 Software Structure of traffic decision making support subsystem

Advanced Traveler Information System Application-Public transit problem

Yuqi Wang, Hui Qi [7] author proposed public transport problem solution based on the Internet of things frame Intelligent transportation system. That system collects data by vehicle terminal and uploads data to the server through the network and makes data visible to the consumer passing an algorithm in the server. One aspect, the consumer may inquire about public transit vehicle information by Web. On another aspect, the consumer can know public transit vehicle information by station terminal. The experiments have tested that the Intelligent transportation system can offer public transit vehicle information to many consumers with convenient way thereby this system can solve the city mass transit problem in the picture

As is shown in Fig. 5, before the bus bears off the station 0th, the arithmetic need to match the bus current longitude and latitude coordinate with the station 0th (bjut0) longitude and latitude coordinate. Because actual longitude and latitude coordinate is different from longitude and latitude coordinate of Google Maps labeling and the GPS module acquisition data has some certain inaccuracy. The arithmetic must correct the bus current longitude and latitude coordinate to close to the station 0th (bjut0) longitude and latitude coordinating and up- loading the departure to corresponding database. In order to correct bus current longitude and latitude coordinate and realize that bus demonstrates on the map every time, the arithmetic blend bus's information with the departure after system extracts current bus longitude and latitude data every time. Many times experiment data analysis indicates the above-mentioned coordinate departure happening change only in one day, so the arithmetic can concentrate initializessystem

Fig .5 Not corrected effect.

Fig.5 is the picture without algorithm processing. The bus obviously appears in deflecting the rough 10 meters place of station 0th (bjut0) in the picture.

Fig. 6 is the picture with algorithm correction of deviation. The bus appears in station 0th (bjut0) and there is correction numerical value in the map below. Observing the effect correcting the front and back can explain that the correcting algorithm is successful which make bus appearing on accurate field in reality [8].

In the process of system operation, GPS module drift will be able to lead to bus being away from actual vehicle orbit, will is more obvious especially during bus corner ing. This phenomenon has greatly affected public transit system platform's visualization. The visibility correction algorithm can be adopted specifically for four kinds of driving and four corners.

The four kinds of driving are: driving from west to east, driving from east to west, driving from north to south, driving from south to north. Four kinds of curved condition are respectively: cornering from west to east, cornering from east to west, cornering from north to south, cornering from south to north. Bus makes judgment according to different driving situation to keep running on the road all the time. Bus also makes judgment ac- cording to different cornering situation. When bus drives into the range of cornering (the inflection point as the center and radius of the circular area of 5 meters), With the development of intelligent traffic application and technology of the Internet of things, based on the Internet of things frame intelligent transportation system can provide public transit vehicle information for resident and dispatching point [9]. This system will have an effect to improve the traffic resources utilization ratio and make travel much more convenient. It is the most important to resolve problem about vehicle location information in the Intelligent Transportation System. On one aspect, the resident can inquire about the public transit vehicle's information in the internet and find out which circuit they want to choose. The system not only economizes waiting time and rise travel efficiency but also provides the technology guarantee for punctually arriving at the destination. On another aspect, public transit controller stand strengthens public transit vehicle controller ability according to public transit vehicle information. The public transit controller stand can depend on public transit vehicle information to dis- patch bus during the peak time. When bus appears state of emergency, the system can provide vehicle location and accurate time for rescue workers. Therefore, based on the Internet of things frame Intelligent transportation system has very big prospect and space on intelligent traffic field.

Figure 6. Correction effect.

As is shown in Fig.7, when bus runs away from the actual vehicle orbit, the algorithm can make bus return to orbit. The red circle is the range of cornering judgment [10,11].

Fig 7. Visualization effect.

Vehicle to vehicle Application-securing user authentication

Mrs. Arzoo Dahiya [12] author proposes securing user authentication. In Fig 8. Also, VANET introduces the concept of „Distributed database" in Inter Vehicular Communication. VANET was developed mainly to provide safety and comforts to the passengers. With large number of accidents claiming precious lives, it became necessary to develop a system which could prevent accidents by developing an efficient communication system between vehicles. The earliest works in VANET the earliest works in VANET was started in 1980s when organizations like JSK in Japan, PATH in California and Chauffeur in EU came into existence. These organizations provided the coupling of two or more vehicles. With further research, VANET was not confined to avoidance of accidents but also preventing traffic congestion and providing comforts to the passengers. Recent research has extended uses of VANETs to provide a pool of services to the users.

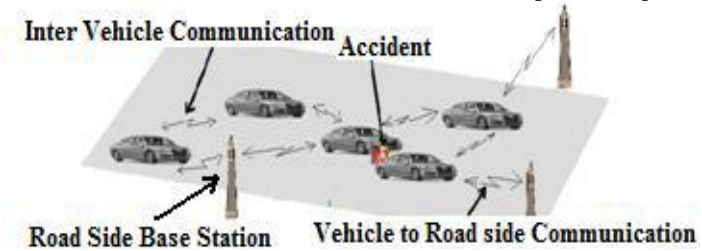


Fig 8 communication in Vehicle 2Vehicle

ECDSA- The Elliptic Curve Digital Signature Algorithm (ECDSA) is a mathematically derived form of Digital Signature Algorithm (DSA). It is a mathematical representation for the elliptic curve analogue of the DSA. It has been accepted as a standard worldwide. The strength per key bit is significantly greater in an algorithm using elliptic curves because elliptic curve discrete logarithm problem has no sub exponential-time algorithm. Being a mathematical entity, the security of elliptic curve can be described in mathematical terms only. The computational intractability and

mathematical hardness of the ECDLP contributes towards its security. It is advantageous to use ECDSA to provide secure and faster dissemination of information after authenticating the users in environments where amount of storage offered is less and lesser response time is allocated for user authentication. Asymmetric ECDSA key pair is used in VANET systems to provide User authentication. ECDSA can also be used to generate and verify signatures.

Don Johnson and others gave a complete account of ECDSA in [13]. This was the first paper that explained ECDSA to minute details. We have provided an account of important findings of that paper related to User Authentication. As per the words of the authors, „ECDSA uses an asymmetric key pair of a public key and a private key. The public key is a random multiple of the base point, while the private key is the integer used to generate the multiple. An entity's key pair is associated with a particular set of EC domain parameters". We present a brief outline of User Authentication using both the public keys and the private keys of ECDSA as explained by Don Johnson and others: User validation follows two steps. First, the public key of sender is validated. The public key validation prevents chances of attacks arising from use of invalid public keys and detects transmission errors. Then, the second step involves authentication of user by validating his private key. The private key of the sender is validated to ensure that no other malicious attacker is using the identity of a valid user to transmit faulty information. After validating the public key, the sender is asked to sign the message using his private key. This provides high levels of reliability. Even after providing such high levels of security, attacks can be made mainly using the following two methods: (i) Attacks on Elliptic Curve Discrete Logarithmic Problem(ECDLP) (ii) Attacks on the hash function. Though ECDSA reduces the scope of attacks from malicious users, but still we need to dedicate a lot of research efforts to further improve the security of the ECDSA system.

Security Issues. User Authentication should not pave the way to his identification, unless he permits. „Backtracking" tricks to obtain user identification should be prevented at any cost. The user authentication schemes should be highly reliable and very safe. No data should be counterfeited while establishing authentication. Confidentiality of User should not be compromised. The „location privacy" of user should not be revealed under any circumstances. The working of Digital Signatures has been shown diagrammatically in Fig.9

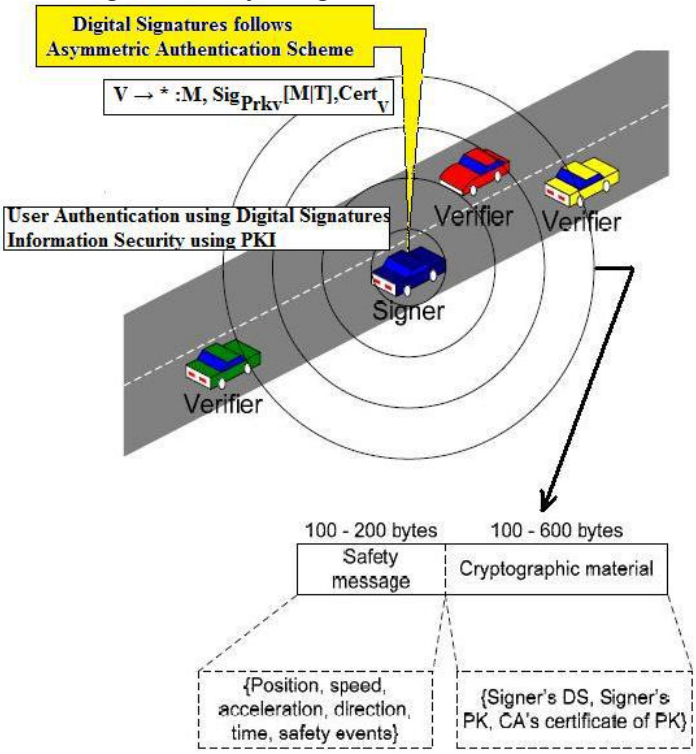


Fig.9. Diagrammatic Representation of working of Digital Signatures authenticating a user.

III. PROPOSED

As the Performance in ITS applications is lagging in Security, attacks like Mutual authentication, Availability, Forward security, Unauthorized tracking of tag, Eaves dropping attack, Impersonation attack ,Replay attack, Anonymity. We need to focus on the following

Security Requirements

When designing an authentication scheme, the security requirements of an RFID implant system need to be well defined. The security requirements can be defined in terms of mutual authentication, confidentiality, integrity, availability, and forward security.

Mutual Authentication: mutual authentication is a scheme where both sides, a tag and a reader, authenticate each other. Unlike the most common authentication schemes, where just a party authenticates another party, mutual authentication is critical if each of the parties is involved in a communication. Without having mutual authentication in an RFID system, either of the parties can falsify their identities.

Confidentiality: all of the secret information concerning the RFID implant system are securely transmitted during all communications. To ensure the confidentiality, one of the two parties, either the tag or the reader, transmit the encrypted information and just the other one can decrypt it.
Data Integrity: the data collected and stored by a device must be protected from tampering by unauthorized parties.
Availability: the device should be resilient to Denial of Service (DoS) attacks, and a malicious entity should not be able to affect the operational capabilities of the device in any way.
Forward Security: The property of forward security ensures that the revelation of the tag's secret information will not threaten the security of previously transmitted information.
Pairing Attacks. GHS attacks. Zero Value Point Attack. Exceptional Procedure Attack are also not minimized in any research

Threat Models

In the following, some of the most relevant attack models concerning the RFID implant systems.
Unauthorized Location Tracking: such an attack is directed against the privacy of tagged people in order to track their activities. For example, the activity of a person who is implanted with an RFID tag can be tracked by any
unauthorized person. This will happen if an adversary pretends to be a trusted component of an RFID implant system. By doing so, the adversary will be able to track an implanted person and access his/her confidential information, or implement a counterfeiting attack to probing the information that he captured from the tag.
Eavesdropping Attack: in an RFID implant system, with an eavesdropping attack the adversary can capture the communications conveyed between the tag and the reader. In this type of attack the adversary does not need to communicate with the RFID tag. He/she only captures the transmitted signals using Radio Frequency (RF) equipment. The information gained by the adversary can be utilized later against the privacy of the implanted users.
Impersonation Attack: to impersonate either a tag or a reader in an RFID implant system. In this system, when there is no authentication scheme to prove that the tag/reader is authentic, it is possible that the adversary implements the impersonation attack against the whole system and utilizes the gained information (e.g. medical history of a patient) in malicious ways. As a result, such a system requires a robust and secure authentication scheme to verify that the tag/reader is valid.
Replay Attack: all messages transmitted between a tag and a reader can be captured and saved by an adversary. Then, he/she can transmit the intercepted information in an attempt to deceive an authorized device and pass the authentication phase. For example, an illegal reader may listen and capture the information transmitted between a tag and an unauthorized reader.

IV. CONCLUSION

The development of security primitives for vehicle to vehicle is an area that has not received lot of attention to till date. We believe it is worthwhile to consider the potential threat associated with an increased reliance on wireless communication for the smooth flow of traffic.
A new method can be developed by Enhancing ECDSA to overcome all the security attacks, Reduce Encryption time, Communication overhead, Computation overhead and key size. This paper surveys some User Authenticating Techniques and explains them in detail. It performs a review of all the work done by earlier researchers in this direction. We discuss some threats to privacy in Vehicle to vehicle and explain why privacy is important. Although this paper presents non technical results but we believe this paper can be helpful for future researchers to do more research on the concepts of privacy in vehicular networks.

REFERENCES

[1] Q. Qian, "Google Earth/Maps/KML Kernel Development Technology," *Proceedings of Google Earth/Google Maps the Use of Basic*, Public House of Electronics Industry, Beijing, 2010, pp. 23-57.
[2] Applications and Opportunities for Radio Frequency Identification (RFID) Technology in Intelligent Transportation Systems: A Case Study*International Journal of Information and Electronics Engineering, Vol. 3, No. 3, May 2013*
[3] Laisheng Xiao and Zhengxia Wang JOURNAL OF NETWORKS, VOL. 6, NO. 6, JUNE 2011 887 Internet of Things: a New Application for Intelligent Traffic Monitoring System
[4] Carlos J. Bernardos, Ignacio Soto a, Marı□a Caldero□n, Fernando Boavida, Arturo Azcorra, VARON: Vehicular Ad hoc Route Optimisation for NEMO, Computer Communications 30 (2007) 1765–1784
[5] M.-C. Chen et al., Android/OSGi-based vehicular network management system, Comput. Commun. (2010), doi: 10.1016/ j.comcom.2010.03.032 [6] M. Gerla, L. Kleinrock, Vehicular networks and the future of the mobile internet, Comput. Netw. (2010), doi: 10.1016/j.comnet. 2010.10.015
[7] *Wireless Engineering and Technology*, 2012, 3, 160-166 http://dx.doi.org/10.4236/wet.2012.33023 Published Online July 2012 (http://www.SciRP.org/journal/wet) Research of Intelligent Transportation System Based on the Internet of Things Frame Yuqi Wang, Hui Qi
[8] Mike Burmester, Emmanouil Magkos and Vassilis Chrissikopoulos. Strengthening Privacy Protection in VANETs. In proceedings of the 2008 IEEE International Conference on Wireless & Mobile Computing, Networking & Communication.

[9] W. Li, M. W. Koendjbiharie, R. C. Juca, Y. Yamashita, and A. Maciver, "Algorithms for Estimating Bus Arrival Times Using GPS Data," *IEEE* 5*th International Confer- ence on Intelligent Transportation Systems*, Singapore City, 3-6 September 2002, pp. 868-873.

[10] Wikipedia, 2012. http://www.wikipedia.org/

[11] R. Jeong and L. R. Rilett, "Bus Arrival Time Prediction Using Artificial Neural Network Model," *IEEE* 7*th Intel- ligent Transportation Systems Conference*, Washington DC, 11-15 January 2004, pp. 988-993

[12] A survey on securing user authentication in vehicular ad hoc networks, Mrs. Arzoo Dahiya, Google PDF

[13] Don Johnson, Alfred Menezes and Scott Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA). Published in International Journal of Information Security, Vol. 1 (2001) pp. 36-63.

