IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661 Volume 2, Issue 2 (July-Aug. 2012), PP 01-08
www.iosrjournals.org

Efficient Data Delivery For Secured Communication in Vanet

[1]Neha Verma, [2]Rakesh Kumar
[1]*Department of Information Technology, Maharishi Markandeshwar University,Mullana, India*
[2]*Assistant Professor, Department of Information Technology, Maharishi Markandeshwar University, Mullana, India.*

Abstract-*As Vehicular networks become popular, it will provide the communication between Vehicle to Vehicle (V2V) and between Vehicles to Road side unit (V2R). Security is the main issue in VANET. As there are many aspects to improve security in VANET, but still security remains the delicate research. In this paper two methods have been proposed for maintaining the security. One method is Combo algorithm and other method is the Global System for Mobile computing (GSM) technique. The objective of combo algorithm is to achieve the principle of confidentiality, integrity, authentication and non-repudiation. This algorithm is designed by combining the two cryptography mechanism i.e. symmetric and asymmetric key; with the help of this technique we can solve the key distribution/exchange problem. The speed of encryption/decryption process is very fast in symmetric key cryptography so the process will not take much more time and the time complexity reduces. With the use of GSM technique, the authentication and confidentiality services have been achieved. Also, data transmitted in the form of voice and packets, and secure communication will takes place.*

Keywords: *Algorithm, GSM, RSU, V2R, V2V.*

I. Introduction

Vehicular communication system consists of many exciting application which will make driving safer, efficient and comfortable and also it is a core of various industries whose aim is to enhance safety and efficiency of transportation system. Vehicular communication allows vehicle to vehicle communication and vehicle to roadside unit communication to form a vehicular ad hoc network. VANET divided the nodes into two categories i.e. on board units and RSU. On board units are installed on vehicles and they are the radio devices where as RSU are installed along the road which is controlled by a network operator. There are many applications of ITS but the main application is to provide safety message. Security also plays a very vital role in VANET. Good security management practices will take care of security policy and also which in turn good security policy takes care of four key aspects i.e. affordability, functionality, cultural issue and legality. Affordability deals with cost and effort in security implementation. Functionality provides the security mechanism. Cultural issue deals with people expectations, working style and beliefs. And the last is the legality which ensures that whether the policy meets the legal requirement. Security is the most significant challenges in network perspective. Attackers will send the bogus information to the vehicles, drivers etc. Different types of attacks have been taken place, which is discussed in this paper. Safety applications must be protected to avoid malicious manipulation, potentially causing harm to the vehicle driver, and commercial applications must be protected to prevent loss of revenue. So the safety will be provided to drivers, vehicles and passengers are very important in VANET. So it is very essential to secure VANET against abuse. In this paper we proposed a combo algorithm, which provide the security services such as authentication, non repudiation, confidentiality and integrity. Also a new technology i.e. GSM has been introduced in this paper. With the use of this technique the data transmitted in the form of voice and packets. A completely secure communication takes place between vehicles to vehicle.

GSM technology [15] is a cellular network, which means that cell phones connect to it by searching for cells in the immediate vicinity. There are five different cell sizes in a GSM network—macro, micro, pico, femto and umbrella cells. The coverage area of each cell varies according to the implementation environment. Macro cells can be regarded as cells where the base station antenna is installed on a mast or a building above average roof top level.

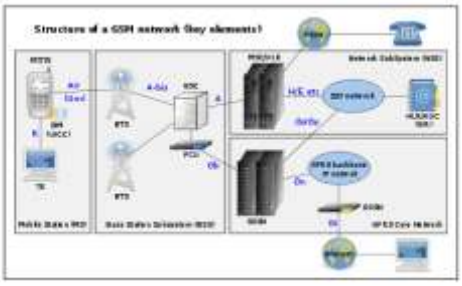


Figure 1. Network structure of GSM [15]

The network is structured into a number of discrete sections:
The Base Station Subsystem (the base stations and their controllers).

- The Network and Switching Subsystem (the part of the network most similar to a fixed network). This is sometimes also just called the core network.
- The General Packet Radio Service (GPRS) Core Network (the optional part which allows packet based Internet connections).
- The Operations Support System (OSS) for maintenance of the network.GSM uses GPRS for data transmissions like browsing the web.

The main challenge in providing security in VANET depends on privacy, trust, cost and gradual deployment. Figure 2 shows the representation of VANET and the position of GSM in vehicle where it has been placed. And the rest of this paper is organized as follows: Section 2 describes the literature work. Section 3 describes the Security approaches and use of GSM technology in VANET Section 4 gives the idea of proposed scheme that is used in this paper. Performance Evaluation is presented in section 5. Section 6 concludes this paper.

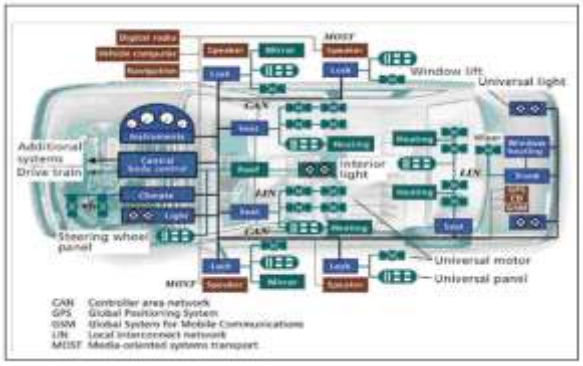


Figure 2. Schematic Representation of a Vehicular Ad hoc Network [16]

II. Literature Work

Paolo and Roberto propose the protocol VIPER: a Vehicle-to-Infrastructure communication Privacy Enforcement pRotocol. VIPER [1] combines in two existing solutions i.e. mix and universal re-encryption. The mix is well known in the Internet context while the universal is a recent proposal in cryptography. But the main problem in this protocol is that it required extra bits, computations, time delay and number of dummy messages sent, are feasible even for increasing requirements on the security of the underlying cryptographic mechanisms. For secure infrastructure of VANET, there are some security challenges that propose the secure scheme for vehicular communication on VANET [3]. The author of this paper provides both confidentiality and non-repudiation services in the secure communications by using session keys and also analyze the robustness. Before the successful deployment of VANET there are many challenges such as designing of security mechanisms to secure VANET against abuse and efficient medium access control (MAC) [4]. So the Kejie Lu and others propose a secure MAC protocol for VANET and to access DSRC channels. Stavrou and Pitsillides had surveyed the state-of-the-art of secure multipath routing protocols in WSNs and number of security issues related to multipath routing itself [5]. The security framework for VANET, using identity-based cryptography, to provide confidentiality, authentication, message integrity, non-repudiation and also it provides security and privacy using short-lived [6]. In VANET, better communication efficiency and security are very important and VANET cannot get started without either of them. Use of message aggregation and group communication is the main idea and the solution of first class is based on asymmetric cryptographic primitives, the second class uses symmetric ones, and the third one mixes the two [7]. In VANET aggregation increases not only efficiency but also security. Different challenges for security, privacy and authentication schemes in wireless LAN, VANET

are discussed. Proxy re encryption scheme and new proxy re encryption scheme [8] are compared which shows that better privacy can be maintained by using new proxy re encryption. In a VANET, there is also a certificate authority which issues keys and certificates to vehicles [9]. Author of this paper proposes a method for car-to-car epidemic distribution of certificate revocation lists which is quick and efficient. Samara, Al-Salihy, W.A.H. proposes that need for a robust VANET networks is strongly dependent on their security and privacy features [10]. The need for a robust VANET networks is strongly dependent on their security and privacy features [11]. The design of SDAP is based on the principles of divide-and-conquer and commit-and –attest [12]. M.Y. Hsieh indicates that the proposed design can prevent and detect malicious nodes with a high probability of success by neighbor monitor mechanisms and cluster-based [13].

III. Security Approaches in VANET

Different approaches for security purpose have been used in VANET. In this section the approaches which are used in our proposed algorithm i.e. Combo algorithm has been discussed. Also what key size should be used for encryption purpose?

3.1 Principles of Security

Different principles of security have been discussed which are very essential for secure communication between V2V or between V2R.

1. Confidentiality: This service specifies that only the sender and receiver can access the contents of message. As confidentiality guarantee the privacy of message against the unauthorized access.
2. Authentication: In this service we ensure that the origin of message is correctly identified. The sender who sends the message is authorized or not and the communication is authentic in nature. This service help establish the proof of identities. And the protocols for authentication and key establishment are the foundation for security of communications [14].
3. Integrity: This service ensures that the message is not changes in transit when the sender sends it. Integrity assures that messages are received by the receiver without modification, insertion, deletion or replacing of message.
4. Non-repudiation: In this security service a sender or receiver can not repudiates the fact having sent the message.
5. Availability: Availability defines that the resources or the information must be available only to the authorized parties.
6. Access Control: In access control we can assign the roles and privileges to all the nodes in the network. Access control specifies and control who can access what.
7. Privacy: It ensures that the unauthorized users are not allowed to view the information. Only the authorized user can access the data.

3.2 Types of Attacks

The attacker will create the different types of attacks which have discussed below:

1. Interception: Interception causes loss of confidentiality service. When an unauthorized party will access the resources such as copying of data or programs and listening to the network traffic.
2. Fabrication: When there is no proper authentication mechanism, the type of attack is called as fabrication and the attacker may add the fake records to a system.
3. Modification: The loss of message integrity is known as modification and the attacker may modify the values in a system.
4. Interruption: A kind of attack in availability is called as interruption which puts the availability of resources in danger.
5. Passive attacks: In this type of attack the attacker only monitors the data transmission but not perform any modifications to data. This type of attack only prevented rather than detection or correction.
6. Active attacks: In this type of attack the attacker can modify the content of message and this type of attack can not be prevented easily.
7. Masquerade attack: When the attacker are trying to pose as another entity.
8. Replay attack: In this type of attack the attacker captures a sequence of events and then it resends them.
9. Alteration of message: In this the attacker involves some change to the original message.
10. Denial of service (DoS): Fabrication causes loss of this type of attack. DoS attacks are mounted by physically jamming the communication channel to block any communication.

3.3 Cryptography Mechanism

There are two types of cryptographic mechanism:

1. Symmetric Key Cryptography: In this mechanism the same key is used for encryption and decryption of message. In symmetric key cryptography there is a problem of key distribution or key exchange.
2. Asymmetric Key Cryptography: In this type of mechanism the two different keys are used for encryption and decryption of message. One key is used to encrypt the message and another key is used to decrypt the message.

3.4 Key Range and Key Size

In data security the knowledge about the key size is very important. For the attacker the actual value of key remains a challenge. If the attacker found a key than it can easily access the plain text data. To overcome from this problem we have to increase the key range to a size which requires attacker to work for more than five years to crack the key. Our key range should be from 0 to 100 billion billion billion billion. Key range leads us to the principle of key size and we measure the key size in bits such as 40 bits, 56 bits, 128 bits and so on. A 40-bit key takes about 3 hours to crack and 41-bit key would take 6 hours and so on which means that every additional bit doubles the amount of time required to crack the key. Increase in the key size increases the key range and therefore, complexity for the attacker.

3.5 Use of GSM Technology in VANET

GSM have three key aspects to security i.e. subscriber identity authentication, signaling data confidentiality and user data confidentiality. One of the key features of GSM is the Subscriber Identity Module, commonly known as a SIM [15] card. The SIM is a detachable smart card containing the user's subscription information and phone book. This allows the user to retain his or her information after switching handsets. Each subscriber is identified with a unique International Mobile Subscriber Identity (IMSI). Each subscriber has a unique subscriber authentication key, Ki. GSM authentication and encryption work in such a way that this sensitive information never transmitted across the mobile network.

IV. Proposed Scheme

In this scheme the two different techniques have been used for secure data communication in VANET i.e. Combo algorithm and GSM technique. Let us explain these techniques in detail.

4.1 Issue a Digital Certificate

Digital certificate simply signifies the associate between a user and their public key. Digital certificate are issued by trusted agency known as certification authority (CA).

- Vehicle requests for digital certificate to CA.
- CA will check if the vehicle has Electronic License Plate (ELP) which is issued by the govt.
- If the vehicle has ELP then only CA will issue the certificate.

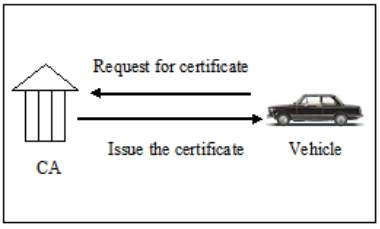


Figure 3. Trusted CA signs on each vehicle public key and Issue a certificate

- CA will sign on vehicle public key and issue the certificate.
- Now the vehicle consists of ELP and digital certificate then only it will communicate with RSU and other vehicles.

ELP is the electronic license plate which is an electronic identity issued by a Government. Some existing security tools in some countries include ELP, which are cryptographically verifiable numbers equivalent to traditional license plates and help in identifying stolen cars and also keeping track of vehicles crossing country border. Tamper proof hardware is essential for storing the cryptographic material like ELP for decreasing the possibility of information leakage.

4.2 Certificate Verification

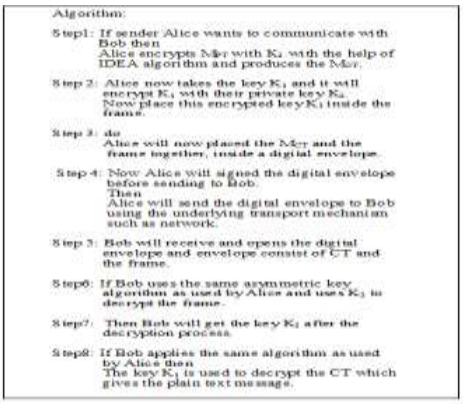
Before starting the secure communication vehicle and RSU exchange their certificates. Verification of certificates is required by all the protocols. We use the $CHECK_{CERT}$ to verify the certificates. Let us take C(A) is either a certificate Cert(A) or a certificate digest which is truncated output of H(cert(A)) where H is a hash function. The time required for $CHECK_{CERT}$ is given by T_{CC}. CRL is the certificate revocation list where the certificates are placed after their identification.

Algorithm:
Step1: if Cert (A) is a certificate Then
Step2: verify ver (Cert (A)) is valid
Step3: store Cert (A) with a validity flag and its digest
Step4: else if Cert (A) is a certificate digest then
Step5: verify whether Cert (A) is stored and valid
Step6: end if
Verify the CRL for Cert (A)

4.3 Proposed Combo Algorithm

Combo algorithm takes place between vehicle to vehicle communication and we use the combination of two cryptography mechanism i.e. symmetric key cryptography and asymmetric key cryptography. This method is completely secure and the cipher text generated in this is compact in size.

Notations:
K_1: one time symmetric key
$M_{PT:}$ plain text message
M_{CT}: cipher text message
K_2: sender private key
K_3: receiver private key
CT: cipher text


Algorithm:

Step1: If sender Alice wants to communicate with Bob then
Alice encrypts M_{PT} with K_1 with the help of IDEA algorithm and produces the M_{CT}.

Step2: Alice now takes the key K_1 and it will encrypt K_1 with their private key K_2.
Now place this encrypted key K_1 inside the frame.

Step3: do
Alice will now placed the M_{CT} and the frame together, inside a digital envelope.

Step4: Now Alice will signed the digital envelope before sending to Bob.
Then
Alice will send the digital envelope to Bob using the underlying transport mechanism such as network.

Step5: Bob will receive and opens the digital envelope and envelope consist of CT and the frame.

Step6: If Bob uses the same asymmetric key algorithm as used by Alice and uses K_3 to decrypt the frame.

Step7: Then Bob will get the key K_1 after the decryption process.

Step8: If Bob applies the same algorithm as used by Alice then
The key K_1 is used to decrypt the CT which gives the plain text message.

Figure 4. Combo algorithm

4.4 Proposed Algorithm Uses GSM Technology

Security is distributed in three different elements of the GSM infrastructure i.e. SIM which is a plastic card inside a mobile phone, GSM handset and GSM network. SIM contains the IMSI, Ki, the ciphering key generation algorithm (A8), authentication algorithm (A3) as well as personal identification number (PIN).

In GSM the transmission are encrypted with the help of a temporary, randomly generated ciphering key, Kc. The GSM handset contains the ciphering algorithm (A5). Authentication center (AUC) which is a part of GSM network, contains the encryption algorithms (A3, A5 and A8) as well as database for identification and authentication information about the subscribers. For the communication in GSM technology the driver must contains the GSM handset.
Here some notation have been defined which are used in the network.

Notations:
Node A: It is considered as GSM network
Node B: It is considered as Subscriber or driver in vehicle which consists of handset.
A3: Authentication Algorithm
A5: Ciphering Algorithm
A8: Ciphering Key Generation Algorithm
Ki: Vehicle Authentication Key
Kc: 64 Bit Ciphering Key
RAND_No: Random Number

Figure 5. GSM message authentication

With the help of algorithm 1 the authentication service has been achieved.

* A3, A5 and A8 are the standard algorithms.
* SEC_ENC: It is used for secured encryption.

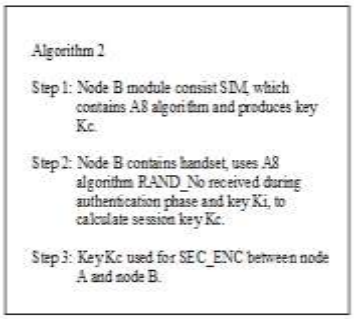


Figure 6. GSM message confidentiality

Algorithm 2 provides the data confidentiality service between the Node A and Node B.

* ENC (M): It is used for encrypting the message

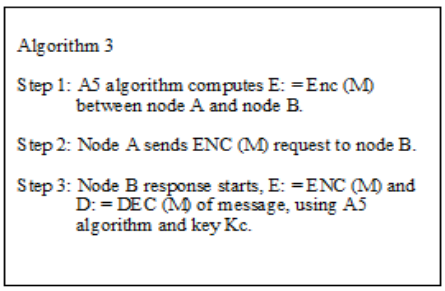


Figure 7. Secure communication of Voice and Data

V. Performance Evaluation

In this section simulation and analysis have been presented to show the performance, results of the proposed secure algorithms. The needed Parameters to carry out the simulation and their corresponding values for both protocols are specified below:

Table 1. Simulation Parameters

Parameter	Value
Number of Nodes	40
Topography Dimension	800 m x 800 m
Traffic Type	TCP
Radio Propagation Model	Two-Ray Ground Model
MAC Type	802.11.Mac Layer
Routing Protocol	DSDV
Antenna Type	Omni directional

There are two scenarios of the VANET: V2V based VANET, and V2R based VANET. In vehicle to vehicle communication there is no road side unit and each on board unit (OBU) on a vehicle has to carry its own communication with other vehicles. OBU has to broadcast all messages to the nearby nodes. Figure 8 shows vehicle to vehicle communication.

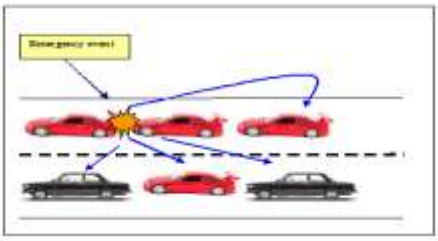


Figure 8. Vehicle to Vehicle Communication

Figure 9 shows vehicle to road side communication. But in vehicle to road side unit the vehicular communication is controlled by RSU. Every RSU acts as an access point which broadcasts all the messages received from one vehicle to all others vehicle in the range.

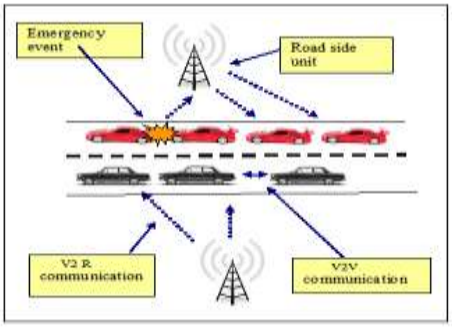


Figure 9. Vehicle to Roadside communication

Figure 10 shows that the efficiency of messages is increasing. If the message generation rate is 40 and the time required to generate 40 messages is very less i.e. 10-12 ms. so it shows that the efficiency of our method is increasing.

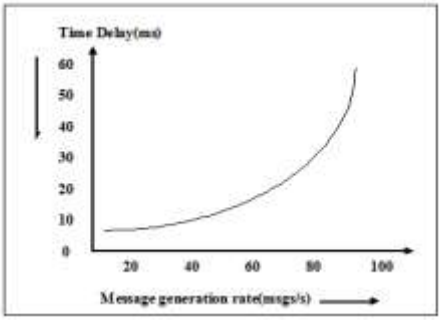


Figure 10. Increasing the Efficiency of proposed method

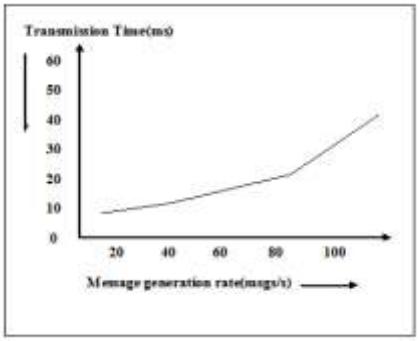


Figure 11. Reduces Time Complexity in Proposed Method

Figure 11 shows that the amount of time required, by the process during encryption and decryption is less. Our proposed method reduces the time complexity.

VI. Conclusion and Future Work

VANET is a wireless communication technology for improving highway safety and also providing safety to the drivers and passengers. In this paper combo algorithm had been proposed which solves the key distribution problem and provides the security services such as confidentiality, integrity, authentication and non-repudiation. As, algorithm involves the two techniques i.e. symmetric and asymmetric key cryptography and the encryption and decryption process takes place efficiently in case of symmetric key cryptography. So in combo algorithm the time complexity reduces and privacy has been maintained. One new approach has been used i.e. GSM technology in security issues of VANET. It provides the authentication and confidentiality services. Secure communication for voice and data has been provided by the GSM technology. In future work we can provide the access control services in V2V and V2R communication. And also we have to improve the efficiency of GSM technology in VANET.

References

[1] Paolo Cencioni and Roberto Di Pietro, "A mechanism to enforce privacy in vehicle-to-infrastructure communication", Elsevier, *International Journal of computer communication, 31(12),* 30 July 2008, 2790-2802.

[2] Neng-Wen Wang, Yueh-Min Huang and Wei-Ming Chen, "A novel secure communication scheme in vehicular ad hoc networks", *International Journal of computer communication, 31(12),* 30 July 2008, 2827-2837.

[3] Yi Qian, Kejie Lu, and Nader Moayeri, "A Secure VANET Mac Protocol for DSRC Applications", *Proc. of Global Telecommunications Conference, IEEE GLOBECOM*, Dec. 2008,1-5.

[4] Eliana Stavrou and Andreas Pitsillides, "A survey on secure multipath routing protocols in WSNs", Elsevier, Volume 54, Issue 13, 15 September 2010, Pages 2215–2238.

[5] Pandurang Kamat, Arati Baliga and Wade Trappe "An identity-based security framework For VANET", *Proc. of the 3rd international workshop on Vehicular ad hoc networks*, 2006, 94-95.

[6] Raya, Maxim; Aziz, Adel; Hubaux and Jean-Pierre, "Efficient secure aggregation in VANET", *Proc. of 3rd international workshop on Vehicular ad hoc networks*, September 2006.

[7] Surabhi Mahajan and Alka Jindal, "Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks", *International Journal of Computer Applications, 1(20),* February 2010, 17-21.

[8] Kenneth P Laberteaux, Jason J Haas, Yih-Chun Hu, " Security certificate revocation list distribution for VANET", *Proc. of fifth ACM international workshop on Vehicular Internetworking VANET*, 2008, 88-89.

[9] Samara, G., Al-Salihy, W.A.H., Sures, "Security issues and challenges of Vehicular Ad Hoc Networks", *Proc. of 4th International Conference on New Trends in Information Science and Service Science (NISS) ,* May 2010, 393-398.

[10] H. Chan, A. Perrig, and D. Song, "Secure hierarchical in-network aggregation in sensor networks," *Proc. of 13th ACM conference on Computer and Communications Security*, November 2006, 278-287.

[11] Y. Yang, X. Wang, and S. Zhu, "SDAP: a Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks", *ACM Transactions on Information and System Security (TISSEC), 11(4),* July 2008, 18:1-18:43.

[12] M.Y. Hsieh, Y.M. Huang, H.C. Chao, "Adaptive security design with malicious node detection in cluster-based sensor networks", *Computer Communications, 30 (11–12),* September 2007, 2385–2400.

[13] C. Boyd, A. Mathuria, "Protocols for Authentication and Key Establishment", *Information security and cryptography series*, September 2003.

[14] Chung-Ming Huang and Yuh-Shyan Chen, Telematics communication technologies and vehicular networks: wireless architectures and applications (Information science reference Hershey, New York, 2010).

[15] www.en.wikipedia.org/wiki/GSM.

[16] www.pcquest.ciol.com/content/technology/ 2009/109020101.asp.