Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs)

Patrice Seuwou, Dilip Patel, Dave Protheroe, George Ubakanma

Centre for Information Systems and Management
Department of Informatics,
London South Bank University,
London SE1 OAA
{seuwoup, dilip, prothed, ubakang}@lsbu.ac.uk

Keywords: Vehicular Ad hoc Network, Efficiency, Security, Traceability, Authentication.

Abstract

As the application of computer technology continues to proliferate and diversify, vehicles are becoming increasingly intelligent and it is expected that in the near future they will be equipped with radio interfaces for short range communications. This will enable the formation of vehicular networks, commonly referred to as VANETs, an instance of mobile ad hoc networks with vehicles as mobile nodes. Vehicular networks are receiving a lot of attention due to the wide variety of services they can provide and are likely to be deployed commercially in coming years. Security is a fundamental issue because such networks will provide the necessary infrastructure for various applications that can help improve the safety of road traffic. Effective security of vehicular ad hoc network is an ill-defined problem as most existing security mechanisms available for VANET do not combine efficiency, security and traceability. They tend to score well in one or two qualities, but not all three because of the potential contradictions between some of their attributes. In this paper, we give an overview of VANETs and the security challenges related to their deployment. We identify and analyse current security limitations, then an effort is made to show that efficiency, security and traceability are the key qualities to consider while implementing an effective security mechanism. Therefore the most suitable way to achieve this goal is by identifying the intersection point connecting their attributes.

1 Introduction

A Vehicular Ad hoc Network (VANET) is an emerging technology that uses moving cars as nodes in a network to create mobile networks. VANETs enable vehicles to communicate amongst themselves (V2V communications) and with road-side infrastructure (V2I communications). Every participating car is turned into a wireless router or node, allowing connection between other cars in a radius approximately of 100 to 300 meters, thus creating a network with a wide range [9]. Such networks present various functionalities in terms of vehicular safety, traffic congestion reduction, location based service (LBS) applications [7] and many other services to drivers but they are also exposed to a variety of risks while carrying out these functions.
Information technology has gained central importance for many new automotive scope applications services [12] and despite significant amount of research carried out in order to protect drivers within a VANET environment, none of the published solutions guarantee a complete security [2]. Existing security mechanisms leave a lot of improvements to be made as there are still many issues in relation to authentication left unaddressed. This report will define our perception of Effective Security for vehicular networks, analyses some existing security mechanisms, and discuss potential limitations and paradoxes related to their properties.
Furthermore, an effort will be made to show that effective security in VANET can be achieved by identifying the most suitable intersection point connecting Efficiency, Security and Traceability.
The main contributions of this paper are as followed: (1) We have classified attacks into broad categories; (2) existing contradictions in regards to security in Vehicular network systems have been highlighted. Furthermore, (3) an effective security model for VANETs systems has then been proposed.

The rest of the paper is organised as follows. In Section 2, we gave a brief overview of VANET technology, followed by a security analysis in Section 3. Section 4 details the proposed model for an effective security system in Vehicular Networks and Section 5 presents our conclusion and future work.

2 Overview of VANET

Until very recently, road vehicles design was a field dominated by mechanical engineers. Factors including the dropping cost of electronic components and the enduring enthusiasm of the car manufacturers to boost road safety and to distinguish themselves from their contestants, has led to vehicles becoming “computers on wheels”, or rather “computer networks on wheels” embedded with technologies such as collision avoidance systems, parking assistance and others [6]. VANET can then be defined as communication network composed of vehicles (cars, buses, trucks and so on) and road side base stations with the purpose to provide ubiquitous connectivity while on the road to mobile users,

who are otherwise connected to the outside world through other networks. Vehicular Ad hoc Network (VANET) is regarded as the first commercial version of Mobile Ad hoc Networks (MANETs) as well as one of its most promising application scenarios [8,14]. The roots of ad hoc network could be traced back as far as 1968 [3] with early project in 1972 developed by the Defence Advanced Research Projects Agency (DARPA).
Figure 1 shows a graphical depiction of a Vehicular Ad hoc network. The unloading vehicle blocks a route and the surrounding vehicles can adopt alternative routes to avoid disruption.

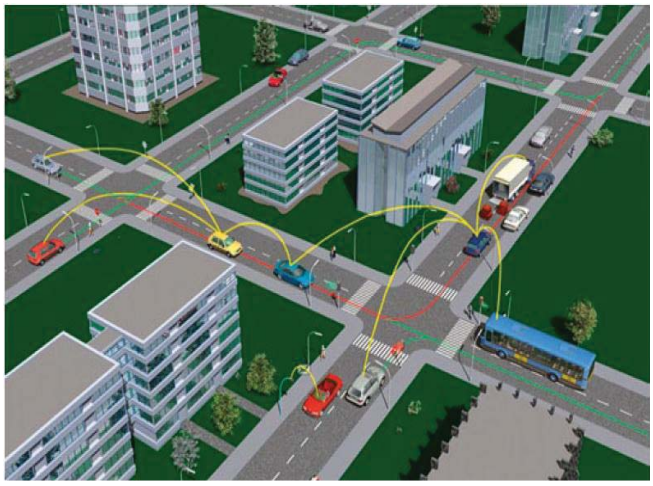

Figure 1: A graphical depiction of a Vehicular Ad hoc NETwork (VANET). (Image Extracted from CAR 2 CAR Communication Consortium at www.car-to-car.org/).

Before analysing security aspects related to VANETs systems, it will be necessary to define the following terminologies:

- **Effective Security in VANET.** This is a VANET security system that combines efficiency, security and traceability.
- **Ill-defined Problem.** This is a problem with existing definitions not taking into consideration all required specifications.
- **Traceability.** This is the ability to trace the location and history of vehicle activity by means of recorded data.
- **Efficiency.** This is the ability to produce a desired effect with a minimum amount of effort or waste.

3 Security Analysis

In recent years, there have been an excessive number of contributions related to security in vehicular networks. Most of these researches were based on different techniques designed to improve security and protect communicating members against a number of potential attacks. An effective security mechanism should be able to handle threats targeting the availability, the confidentiality and the authenticity of data in regards to communication between vehicles and infrastructures in a VANET enabled environment. Indeed most security mechanisms available for VANET do not combine Efficiency, Security and Traceability [1]. They tend to score well in their provision of one or two qualities, but not all three because of the potential contradictions between some of their properties, therefore Effective Security is still an ill-defined problem. Security plays an essential role in Vehicular Ad-hoc Networks and in the absence of an effective security mechanism, malicious parties could inject bogus information within the network, causing serious accidents.

Secure data communication is a well-researched area in Information Technology, despite the significant volume of devastating attacks that still occur. VANET technologies pose different security threats and requirements therefore create a new research challenge preventing the use of existing network security solutions [14].
This section explores various network security problems, analyses key security requirements and demonstrates that an effective security mechanism should be rigorous and should ensure that the information received is correct, the source is who he claims to be and that privacy of the user sending messages can be preserved.
Before reviewing the potential attacks that can be mounted in vehicular networks, it is important to comment on possible attackers.

3.1 Attackers

Effective security in VANETs is vital as the reason of their very existence relates to significant life threatening situations. The ideal solution should allow drivers to distinguish genuine members of the network from malicious individuals by determining the liability of each driver while maintaining their privacy. The motivation behind VANET was to merge various disciplines involving engineers, computers scientists, psychologists, legislators and others professionals together with car manufacturers in order to make driving more secured and comfortable. Attackers also have their own role to play and predicting their dynamic behaviour is very difficult. An advantage of VANETs over other ad hoc network systems is that they can provide sufficient computational and power resources. Indeed a typical vehicle will be able to host numerous microprocessors [6].

In [6], Raya and Hubaux classify attackers as having four dimensions and characterize them by ***Membership .Motivation.Method.Scope***, where *Membership* represent an Insider or an Outsider, *Motivation* for Malicious or Rational, *Method* for Active or Passive and *Scope* for Local or Extended.

3.2 Possible Attacks

Vehicular Ad hoc NETworks may suffer from a high number of attacks although it can be difficult to envisage all possible attack scenarios that will be launched in the future. Therefore it is critical to have a clear understanding of the different ways in which VANET technologies could be attacked. In this paper, attacks have been grouped into two broad categories (Logical and Physical) as illustrated in Figure 2.

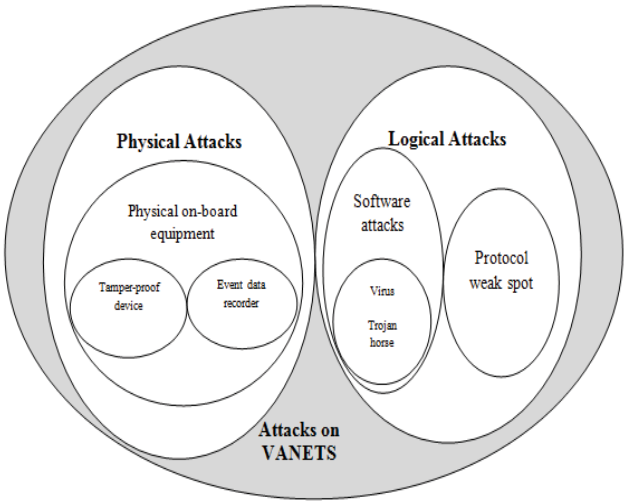

Figure 2: Broad categories of attacks in VANETs

3.2.1 Logical Attacks

Logical attacks typically involve sending messages to a device and observing its responses. Attackers exploit weaknesses or bugs in the overall architecture as well as limitations in the design of security mechanisms in order to trick a device into revealing keys or allowing them to run malicious piece of code.
In [6], Raya and Hubaux Considering attacks perpetrated against messages sent between nodes rather than those targeting physical equipment. Attacks on VANETs were outlined as Basic attacks and Sophisticated attacks.

Further attacker behaviours were discussed by Sumra et *al* [11] where a number of new possible attacks in vehicular networks were identified as illustrated below:

Distributed Denial of service (DDOS) in vehicle to vehicle communication
Timing Attack
Home Attack
Man in the Middle Attack (MiMA)
Social Engineering Attack
Broadcast spam message in Network
Traffic Analysis
Packet Capturing in network

Figure 3: New possible attacks in VANETs

While concentrating our efforts on attacks perpetrated against the message itself, it appears that most threats to VANET systems could be organised into three main groups:

a. Threats to Availability

The following threats to the availability of V2V and V2I have been identified:

- Malware
- Spamming
- Denial of Service (DoS)
- Black Hole Attack
- Broadcast Tampering

b. Threats to Confidentiality

The most prominent VANET attack in this group is Eavesdropping [4]. In this scenario, internal or external attackers can be located in moving or motionless vehicles attempting to collect private information from other road users during the transmission of broadcast messages without the sender/receiver knowledge and authorisation.

c. Threats to Authentication

Authentication is the core security requirement in VANET. It provides message integrity in order to avoid message manipulation over the network. Most applications using this technology will require authentication. This may involve protecting legitimate nodes from attackers penetrating the network using a false identity, revealing spoofed GPS signals, suppressing vital information, fabricating, altering or replaying legitimate messages and injecting incorrect material to damage and affect communication amongst vehicles within the network. In this group, threats may include the following:

- Replay attack
- Position Faking
- Global Positioning system (GPS) Spoofing
- Masquerading
- Sybil attack
- Certificate replication / Key management
- Message Tampering / Manipulation
- Tunneling

3.2.2 Physical Attacks

Physical attacks refer to attacks that exploit the system implementation by identifying its properties. This involve getting access to pieces of equipment such as the Tamper-Proof Device (TPD) and the Event Data Recorder (EDR) to observe, manipulate and interfere with the system internals. This category of attack may be harder to deploy due to the relatively expensive infrastructure required.

3.3 Discussion on Existing security Mechanisms

We live in a society where information is ubiquitous. Data are all around us and due to the fast advancement and invasive deployment of Information Technologies in the automobile industry, both modern high-speed motorways and recently designed vehicles are becoming increasingly intelligent. Intelligent Transport Systems (ITS) are advanced applications which aim to provide innovative services relating to different modes of transport and traffic management and enable various users to be better informed and make safer, more coordinated use of transport networks. **ITS** is a system in which information and communication technologies are applied in the field of road transport. In one aspect, due to commercial implications of VANET enabled system deployment, many organisations are committed to its rapid development although it is estimated that the first systems that will integrate this technology are military, police and fire vehicles to communicate with each other for safety purposes. In the other aspect, road traffic injuries are predicted to rise from their current position as the ninth leading cause of death to become the fifth leading cause of death by 2030 if further actions are not taken, as highlighted on the Global status report on road safety. Therefore a number of organizations such as the World Health Organization, the World Bank, the United Nations and many other are joining forces to address the problem.

In recent years there has been a plethora of contribution in VANET security. This section provides an analysis of some existing security mechanisms.

a. PKI (Public Key Infrastructure)

Based on asymmetric cryptography concepts requiring two separate keys, PKI is widely used in VANET systems. This authentication mechanism uses Public key and Private Key to secure users identification and location while avoiding backtracking by unauthorized. For private key security, a Tamper-proof device is needed in each vehicle, allowing secret information storage and outgoing messages to be signed. However, this scheme requires a large key and certificate posing storage concerns.

b. TESLA (Timed Efficient Stream Loss-Tolerance Authentication)

TESLA was used as an authentication mechanism for multicast and broadcast network communications. In this scheme, symmetric cryptography was used instead of asymmetric cryptography while providing the necessary asymmetric elements. Though TESLA was vulnerable to storage based Denial of Service (DoS) attacks.

c. TESLA++

To overcome TESLA weaknesses, a more advanced authentication mechanism was developed yet raises other concerns. Despite all improved functionalities including prevention of memory based DoS attacks, better authentication techniques, TESLA++ could offer neither **non-repudiation** nor **multi-hop authentication**. Therefore also failed to meet the utmost Security mechanism requirements.

d. ECDSA (Elliptic Curve Digital Signature algorithm)

ECDSA was accepted worldwide as a standard to provide secure and faster dissemination of information after user authentication. Although ECDSA scheme performed well by reducing the scope of attacks, we had more wireless errors and less packets received.

e. VAST (VANET Authentication using Signatures and TESLA++)

VANETs require an effective mechanism which provides more than just packet authentication, but also Non-repudiation, multi-hop communication, DoS resilience, real - time guarantee as discussed above. VAST using a combination of ECDSA signatures and TESLA++ techniques to verify each packet fulfils many of these requirements were met in [10], maintaining acceptable authentication delays with a worst case of 107ms. Despite all efforts, there is still no published work able to guarantee a full effective security.

3.4. Paradoxes and Contradictions

Authentication is the core security requirement in VANET and is strong using Digital signature. It provides message integration in order to avoid message manipulation. Furthermore, Asymmetric ciphers are fantastic for encrypting small amounts of random data, such as session keys and message digests. They are also used for digital signature which is typically much slower than a Symmetric ciphers. While it is possible to use a symmetric cipher for message authenticity, a symmetric cipher cannot provide non-repudiation which creates the paradox within Authentication mechanism with the speed able to vary significantly from one scheme to the other. Existing systems available for VANET sill do not fully combine Efficiency, Security and Traceability despite the number of robust systems been proposed in recent years. This is because Effective security was still an ill-defined problem in VANETs. Therefore, securing effectively a vehicular network is still an unsolved problem.

3.5 Effective Security Mechanism Requirements

Security and privacy issues are fairly common to most mobile and wireless network settings [13]. Indeed, security is amongst the essential user's requirement in VANET and it will be difficult to convince drivers to use this emerging technology unless they have a guaranty of its effectiveness. Therefore, an Effective security system could not be achieved if attributes such as traceability, unlinkability, anonymity in addition to the existing security measures are not taken into consideration. This section includes a list of critical VANET requirements for an effective security mechanism.

3.5.1 Logical Security

A number of authentication mechanisms have been introduced in recent years, aiming to authenticate the validity of users while increasing security and privacy in a VANET enabled environment. Such techniques includes Pseudonymous certificates, Public Key Infrastructure (PKI), Vehicular Public Key Infrastructure (VPKI) composed by a set of Trusted Third Parties (TTPs) in charge of managing pseudonymous certificates with a single root Certificate Authority (CA) in each administrative domain (e.g. Country) with a delegated CA in each region within that domain. In other instance, Symmetric as well as Asymmetric Cryptography concepts were used sometime in combination with Digital Signature algorithm (DSA). Below are some widely used protocols.

- **Authentication.** This service is concerned with assuring that the origin of a message is correctly identified. Vehicles reactions to events should be based on legitimate messages. This attribute is the core security requirement in VANET.
- **Integrity.** This service assures that system assets and information transmitted over the network cannot be altered by unauthorised parties. Indeed these modifications may include writing, deleting or changing the status of transmitted messages.
- **Confidentiality.** In VANET, vehicles send and receive safety as well as non-safety messages from either vehicle to vehicle (V2V) or vehicle to infrastructure (V2I). This service ensures that the transported information is kept secret from all unauthorised parties and cannot be eavesdropped on its way between the sender and the receiver.
- **Privacy.** Recognised as an important factor for the public acceptance and for the successful deployment of this developing technology. Individuals are increasingly concerned about Big Brother enabling technologies. This property is achieved when two related goals are satisfied (**traceability** and **unlinkability**). This service ensures that user is able to maintain control of personal data and his/her location. This service also secures other information related to the vehicle from unauthorised parties. These facts may include driver identity, their driving behaviour, Electronic License Plate (ELP), vehicle's speed, internal car sensors, past and present location of the vehicle.
- **Availability.** This service requires all nodes to be able to send information at any time. The main purpose of VANET was to use technology to serve users by making driving more secure and comfortable. As a result, if the network is not available for communication, then VANET become useless. Information should be omnipresent and the network must be available at all times as many applications require real-time communication with fast response time. Any form of delay may make a specific message become meaningless, leading to terrible accidents or much bigger disasters.
- **Access control.** This service provides users with the ability to restrict access to resources reserved for privileged entities. Access control policies can be implemented on Road Side Unit (RSU) allowing limited access to other vehicles infrastructure and application data through communication channels.
- **Non-repudiation.** This requirement also called **auditability** [5] is a service that prevents the sender or receiver from denying reception of a transmitted message. Moreover they can prove that a particular message has been received or sent.
- **Multi-hop communication.** Applications of VANETs technologies will occur in situations like battlefields, major disaster areas and outdoor assemblies. Therefore, being characterized by an unpredictable mobility, Vehicle should have the properties allowing them to communication in a multi-hop fashion.
- **Real-time Guarantee.** A high volume of messages broadcast within this context have real-time requirements and some delays in response time may be disastrous. But due to the high mobility of nodes and the dynamic nature of the network topology, managing real time constraints is a very challenging task. Safety and non-safety applications are time sensitive as users need the right information at the right time. The system should be designed to serve users while allowing applications to send and receive signals with a minimal level of delay.

3.5.2 Physical Security

Securing hardware components involved in vehicular communication is also an important requirement for an effective security mechanism. Devices such as Event Data Recorder (EDR), Tamper-Proof Device (TPD), vehicle sensors, Global Positioning System (GPS), radars and computing platform embedded in smart vehicles were initially designed to work separately. Therefore to have a secured and reliable vehicular network, the designed effective security mechanism must be carefully planned and all above equipment properties must be considered despite the great challenges to prevent highly motivated adversary from launching robust attacks. The process of vehicle identification should be performed by both vehicle manufacturers and legal authorities. Manufacturers will assign a special identification number (VIN) to each vehicle and an Electronic License Plate (ELP) will be provided by transportation authorities as a legal requirement. Furthermore, relying only on physical security measures would not be sufficient for an effective security mechanism.

4. Proposed Model towards an Effective Security Mechanism in VANETs

After introducing our broad categories of attacks model, this section outlines an Effective Security Model for VANETs.
In the field of Information Technology, it is argued that a guaranteed 100% security is not realistic. Therefore the best approach to tackle existing issues left unaddressed and achieve an acceptable level of security will depend on

balancing the technologies deployed. Schemes such as TESLA++ and VAST presented in earlier publications [10] were characterized by a combination of a number of Authentication and cryptographic techniques. In [6] Raya and Hubaux classified the safety messages into three classes, based on their properties related to privacy and real-time constraints. As shown on Figure 4, Physical and logical security should be considered during the scheme design process. And the way forward will be to determine the most suitable intersection point able to satisfy effectively all key security properties as discussed above. The designed mechanism could then be tested using existing simulation tools.

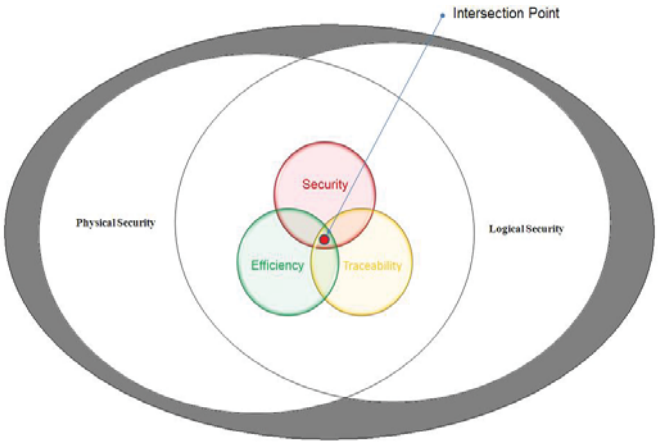

Figure 4: Effective Security Model for VANETs

5. Conclusion and Future work

In this paper, we investigate the issue of Effective Security in vehicular Ah Hoc Networks. We start our study by giving a clear definition of effective Security in the context of Vehicular ad hoc networks and the reason it was still and ill-defined problem. We then analyse security issues, possible attackers and classified attacks into broad categories. Furthermore, Security requirements were discussed and an Effective Security Model for VANETs was then proposed.
In future work, we can identify a suitable intersection point connecting an effective security requirement. Suggest an enhanced security mechanism which will then be tested with a suitable simulation tools under a number of mobility scenarios.

References

[1] H. K. Choi, I. H. Kim and J. Yoo. "Secure and Efficient Protocol for Vehicular Ad Hoc Network with Privacy Preservation", *EURASIP Journal on Wireless Communications and Networking, Hindawi Publishing Corporation*, **Volume 2011**, pp. 1-15, (2011).
[2] H. Dok, H. Fu, R. Echevarria and H. Weerasinghe. "Privacy Issues of Vehicular Ad-Hoc Networks", *International Journal of Futur Generation Communication and Networking,* **volume 3**, pp. 17-31, (2010).
[3] M. Frodigh, P. Johansson,P. Larsson, "Wireless ad hoc networking", *The art of networking without a network,* Ericsson Review, No. 4. (2000).
[4] J. Fuentes, M. D. Gonz´alez-Tablas, A., I. and A. Ribagorda, "Overview of Security Issues in Vehicular Ad-hoc Networks", *in Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts.* IGI Global, pp. 894–911 (2011).
[5] F. Kargl, Z. Ma, E. Schoch, "Security Engineering for VANETs" *fourth Workshop on Embedded Security in Cars,* (2006).
[6] M. Raya, and J. P. Hubaux. "Securing vehicular ad hoc networks", *Journal of Computer Security*, **volume 15** , pp. 39-68, (2007).
[7] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura and K. Sezaki. "CARAVAN: providing location privacy for VANET", *in Proceedings of the Workshop on Embedded Security in Cars (escar)*, (2005).
[8] E. Schoch, F. Kargl, T. Leinmuller, S. Schlott, and P. Papadimitratos, "Impact of Pseudonym Changes on Geographic Routing in VANETs", *in Proc. of the European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS)*, pp. 43–57, (2006).
[9] P. K. Singh, K. Lego, T. Tuithung. "Network Centric Approach using MOVE & Application Centric Approach using TraNS for protocols and safety in VANET", *International Journal of Research and Reviews in Computer Science(IJRRCS),* **volume** 2, p. 104, (2011).
[10] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication", *6th Conference on Embedded Security in Cars (Escar),* Hamburg, Germany, pp. 22. (2008).
[11] I. A. Sumra, I. Ahmad, B. A. Hasbullah, J. L. Manan, "Behavior of Attacker and Some New Possible Attacks in Vehicular Ad hoc Network (VANET)" *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 3rd International Congress,* (2011).
[12] A. Weimerskirch, J. J. Haas, Y. C. Hu and K. P. Laberteaux. "Data Security in Vehicular Communication Networks", *VANET Vehicular Applications and Inter-Networking Technologies*, (2010).
[13]Zarki, M., E., Mehrotra, S., Tsudik, G. and Venkatasubramanianm, N. (2002) *Security issues in a future vehicular network*, in: *Proceedings of European Wireless'02*.
[14] L. Zhang, "Research on Security and Privacy on Vehicular ad hoc Networks", (2010).