An Essential of Security in Vehicular Ad hoc Network

K P Tripathi
Lecturer
Bharati Vidyapeeth University
Institute of Management, Kolhapur, India.

ABSTRACT
Vehicular Ad-Hoc Networks (VANET) are a specific type of wireless ad-hoc networks, formed with short range wireless communication devices, each one representing a vehicle on the road or a static device. Developing applications and protocols for Vehicular Ad-Hoc Networks (VANETs) poses unique security challenges, induced by the devices being used, the high speed and sporadic connectivity of the vehicles, the high relevance of their geographic location combined with the absence of adequate/reliable means of determining it.

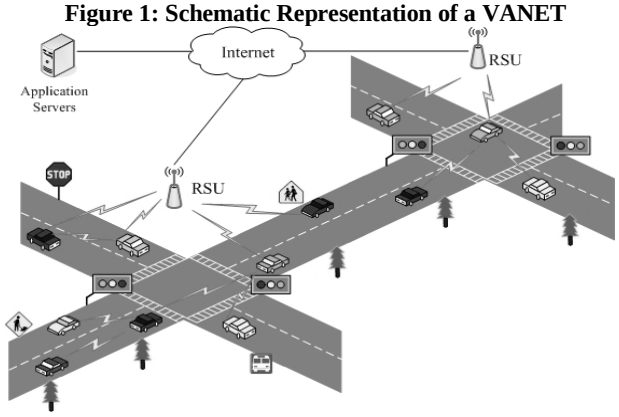
Since the last few years VANET have received increased attention as the potential technology to enhance active and preventive safety on the road, as well as travel comfort. Security and privacy are indispensable in vehicular communications for successful acceptance and deployment of such a technology. Generally, attacks cause anomalies to the network functionality. A secure VANET system, while exchanging information should protect the system against unauthorized message injection, message alteration, eavesdropping. This paper is an attempt to highlights the problems occurred in Vehicle Ad hoc Networks and security issues.

Keywords
VANET, ITS, RSU, PKI, DSRC, Attacks on Vehicular Network, Security Architecture.

1. INTRODUCTION
A Vehicular Ad-Hoc network is a form of Mobile ad-hoc Networks, to provide communication among nearby vehicles and between vehicles and nearby fixed equipment i.e. roadside equipment. The main goal of VANET is providing safety and comfort for passengers. Each vehicle equipped with VANET device will be a node in the Ad-hoc network and can receive & relay other messages through the wireless network. Collision warning, Road signal arms and in place traffic view will give the driver essential tool to decide the best path along the way. VANET or Intelligent Vehicular Ad-Hoc Networking provides an intelligent way of using vehicular Networking. With the sharp increase of vehicles on roads in the recent years, driving becomes more challenging and dangerous. Roads are saturated; safety distance and reasonable speeds are hardly respected. The leading car manufacturer decided to jointly work with govt. agencies to develop solution aimed at helping drivers on the roads by anticipating hazardous events or bad traffic areas. One of the outcomes has been a novel type of wireless access called wireless access for vehicular environment (WAVE) used for vehicle to vehicle and vehicle to road side communication. [2]

Vehicular ad hoc network (VANET) can offer various services and benefits to VANET users and thus deserves deployment effort. VANETs with interconnected vehicles and numerous services promise superb integration of digital infrastructure into many aspects of our lives, from vehicle-to-vehicle, roadside devices, base stations, traffic lights, and so forth. A network of a huge number of mobile and high-speed vehicles through wireless communication connections has become electronically and technically feasible. Safety information exchange enables life-critical applications, such as the alerting functionality during intersection traversing and lane merging, and thus plays a key role in VANET applications. The attractive features of VANETs inevitably incur higher risks if such networks do not take security into account prior to deployment. For instance, if the safety messages are modified, discarded, or delayed either intentionally or due to hardware malfunctioning, serious consequences such as injuries and even deaths may occur. Unlike traditionally wired networks are protected by several lines of defense such as firewalls and gateways, security attacks on such wireless networks may come from any direction and target all nodes. Therefore, VANETs are susceptible to intruders ranging from passive eavesdropping to active spamming, tampering, and interfering due to the absence of basic infrastructure and centralized administration. Moreover, the main challenge facing vehicular ad hoc networks is user privacy. Whenever vehicular nodes attempt to access some services from roadside infrastructure nodes, they want to maintain the necessary privacy without being tracked down for whoever they are, wherever they are and whatever they are doing.

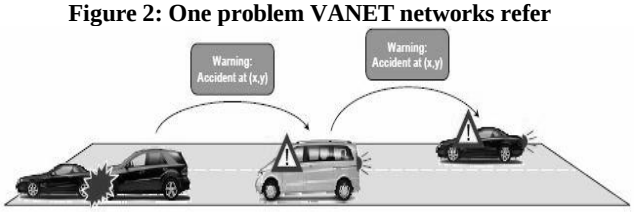
Figure 1: Schematic Representation of a VANET



2. PROBLEMS OCCURRED IN VEHICULAR NETWORK

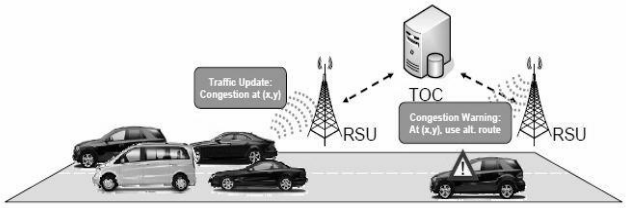
One problem which VANET networks refer to is increasing the traffic safety. This thing is possible because of the permanent transfer of messages which refers to any possible threats, as figure 2 show.

Figure 2: One problem VANET networks refer



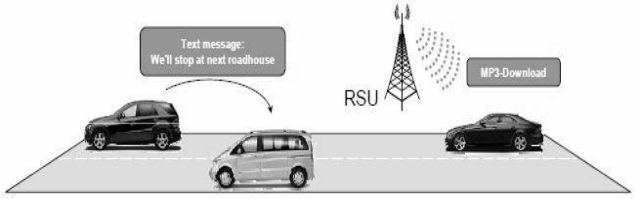
Another problem which VANET networks refer to is a more efficient traffic. Figure 3 presents a situation where, when a blocking occurs in the traffic, the vehicles which detects the blocking broadcasts information to near RSUs (Road Side Unit). Then, RSUs broadcasts the information about blocking too, so other vehicles can choose alternative routes.

Figure 3: One problem VANET networks refer



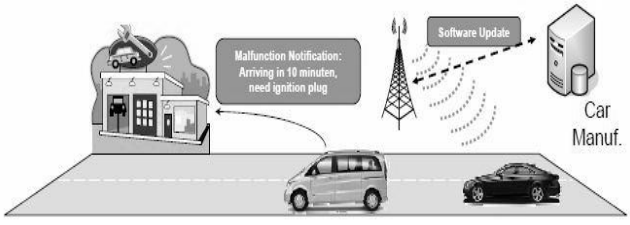
Since people need entertainment more often, this cannot be missing from VANET networks (figure 4).

Figure 4: One problem VANET networks refer



Daily problems can now be solved with VANET networks help. Auto service scheduling or getting necessary information are some of the benefits of this kind of network.

Figure 5: One problem VANET networks refer



Considering the tremendous benefits expected from vehicular communications and the huge number of vehicles (hundreds of millions worldwide), it is clear that vehicular communications are likely to become the most relevant realization of mobile ad hoc networks. The appropriate integration of on-board computers and positioning devices, such as GPS receivers along with communication capabilities, opens tremendous business opportunities, but also raises formidable research challenges. One of these challenges is security. Limited attention has been devoted so far to the security of vehicular networks, although security is crucial. For example, it is essential to make sure that life-critical information cannot be inserted or modified by an attacker. Likewise, the system should be able to help establishing the liability of drivers. But at the same time, it should protect as far as possible the privacy of the drivers and passengers.

These concerns may look similar to those encountered in other Communication networks, but they are not. Indeed, the size of the network, the speed of the vehicles, the relevance of their geographic position, the very sporadic connectivity between them, and the unavoidably slow deployment make the problem very novel and challenging. [10] [12]

3. VANET SECURITY NECESSITIES

The security design of VANET should guarantee following:

1. Message Authentication, i.e. the message must be protected from any alteration.
2. Data integrity does not necessarily imply identification of the sender.
3. Entity Authentication, so that the receiver is not only ensured that sender generated a message.
4. Conditional Privacy must be achieved in the sense that the user related information, including the driver's name, the license plate, speed, and position and traveling routes.
5. In some specific application scenarios, Confidentiality, to protect the network against unauthorized message injection, message alteration, and eavesdropping, respectively.

An important feature of VANET security is the Digital Signature as a building block [7]. Whether in inter-vehicle communications or communications through infrastructure, authentication (using signatures) is a fundamental security requirement since only messages from legitimate senders will be considered. Signatures can also be used to guarantee data integrity (i.e., the message being sent is not modified). For instance, safety-related messages do not contain sensitive information and thus encryption is not needed [7].

4. VANET APPLICATIONS

VANET application can be categorized into following categories:

1. VANET provide ubiquitous connectivity on the road to mobile users
2. It provides efficient vehicle to vehicle communications that enables the Intelligent Transport System (ITS). ITS includes variety of applications like cooperative traffic monitoring, control of traffic flows, blind crossing and collision prevention.
3. Comfort application are the application to allow the passenger to communicate with other vehicles and with

internet hosts, which improves passengers comfort. For example VANET provides internet connectivity to vehicular nodes while on the movement so that passenger can download music, send emails, watch online movies etc.

4. The VANET also provide Safety, Efficiency, Traffic and road conditions, Road signal alarm and Local information etc.

5. ATTACKS ON VEHICULAR NETWORK

The attacks on vehicular network can be categorized into following categories:

5.1 ATTACKERS MODEL

5.1.1 Insider vs. Outsider: The insider is an authenticated member of the network that can communicate with other members. This means that he possesses a certified public key. The outsider is considered by the network members as an intruder and hence is limited in the diversity of attacks he can mount (especially by misusing network-specific protocols).

5.1.2 Malicious vs. Rational: A malicious attacker seeks no personal benefits from the attacks and aims to harm the members or the functionality of the network. Hence, he may employ any means disregarding corresponding costs and consequences, whereas a rational attacker seeks personal profit and hence is more predictable in terms of the attack means and the attack target.

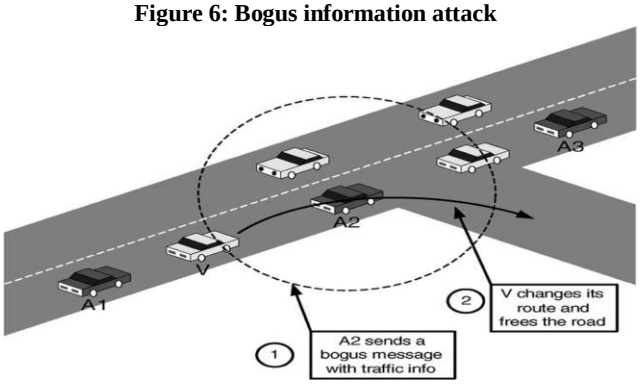
5.1.3 Active vs. Passive: An active attacker can generate packets or signals, whereas a passive attacker contents himself with eavesdropping on the wireless channel.

5.1.4 Local vs. Extended: An attacker can be limited in scope, even if he controls several entities (vehicles or base stations), which makes him local. An extended attacker controls several entities that are scattered across the network, thus extending his scope. This distinction is especially important in privacy-violating and wormhole attacks that we will describe shortly. [3] [12]

5.2 BASIC ATTACKS

Attackers disseminate wrong information in the network to affect the behavior of other drivers (e.g., to divert traffic from a given road and thus free it for themselves). In this example bogus information attack, colluding attackers (A2 and A3) disseminate false information to affect the decisions of other vehicles (V) and thus clear the way of attacker A1

Figure 6: Bogus information attack



5.2.1 Cheating with sensor information: Attackers use this attack to alter their perceived position, speed, direction, etc. in order to escape liability, notably in the case of an accident. In the worst case, colluding attackers can clone each other, but this would require retrieving the security material and having full trust between the attackers.

5.2.2 ID disclosure of other vehicles in order to track their location: In this scenario, a global observer can monitor trajectories of targeted vehicles and use this data for a range of purposes (e.g., the way some car rental companies track their own cars). [6]

5.2.3 Denial of Service: The attacker may want to bring down the VANET or even cause an accident. Example attacks include channel jamming and aggressive injection of dummy messages.

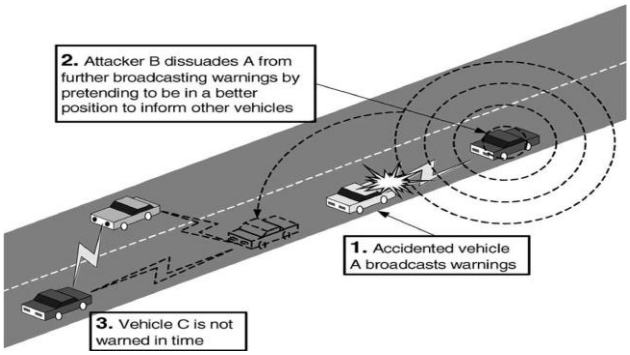
5.2.4 Masquerading: The attacker actively pretends to be another vehicle by using false identities and can be motivated by malicious or rational objectives.

5.3 SOPHISTICATED ATTACKS

Sophisticated attacks are more elaborated variants or combinations of the above attacks. They are examples of what an adversary can do.

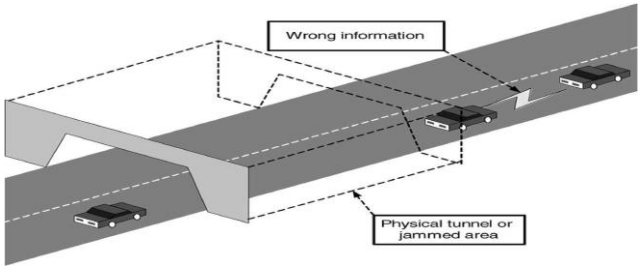
5.3.1 Hidden vehicle: This is a concrete example of cheating with positioning information. It refers to a variation of the basic safety messaging protocol. In this version of the protocol, a vehicle broadcasting warnings will listen for feedback from its neighbors and stop its broadcasts if it realizes that at least one of these neighbors is better positioned for warning other vehicles. This reduces congestion on the wireless channel. As picture below illustrates, the hidden vehicle attack consists in deceiving vehicle A into believing that the attacker is better placed for forwarding the warning message, thus leading to silencing A and making it hidden, in DSRC terms, to other vehicles. This is equivalent to disabling the system.

Figure 7: Hidden vehicle attack



5.3.2 Tunnel: Since GPS signals disappear in tunnels, an attacker may exploit this temporary loss of positioning information to inject false data once the vehicle leaves the tunnel and before it receives an authentic position update as figure below illustrates. The physical tunnel in this example can also be replaced by an area jammed by the attacker, which results in the same effects.

Figure 8: Tunnel attack



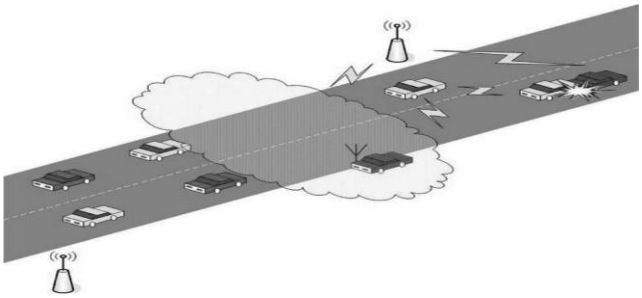
5.3.3 Wormhole: In wireless networking, the wormhole attack [13] consists in tunneling packets between two remote nodes. Similarly, in VANETs, an attacker that controls at least two entities remote from each other and a high speed communication link between them can tunnel packets broadcasted in one location to another, thus disseminating erroneous (but correctly signed) messages in the destination area.

5.3.4 Bush telegraph: This is a developed form of the bogus information attack. The difference is that in this case the attacker controls several entities spread over several wireless hops. Similarly to the social phenomenon of information spreading and its en-route modification, this attack consists in adding incremental errors to the information at each hop. While the errors are small enough to be considered within tolerance margins at each hop and hence accepted by the neighbors. Bush telegraph stands for the rapid spreading of information, rumors, etc. As this information is propagated along a human chain, it is frequently modified by each person in the chain. The result may sometimes be completely different from the original.

5.4 OTHER ATTACKS

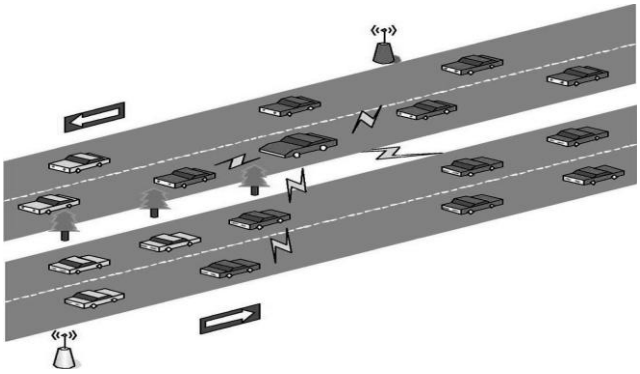
5.4.1 Jamming: The jammer deliberately generates interfering transmissions that prevent communication within their reception range. As the network coverage area (e.g., along a highway) can be well-defined, at least locally, jamming is a low-effort exploit opportunity. As the figure illustrates, an attacker can relatively easily, without compromising cryptographic mechanisms and with limited transmission power, partition the vehicular network.

Figure 9: Jamming



5.4.2 Forgery: The correctness and timely receipt of application data is a major vulnerability. The figure illustrates the rapid "contamination" of large portions of the vehicular network coverage area with false information where a single attacker forges and transmits false hazard warnings (e.g., ice formation on the pavement), which are taken up by all vehicles in both traffic streams. [5]

Figure 10: Forgery



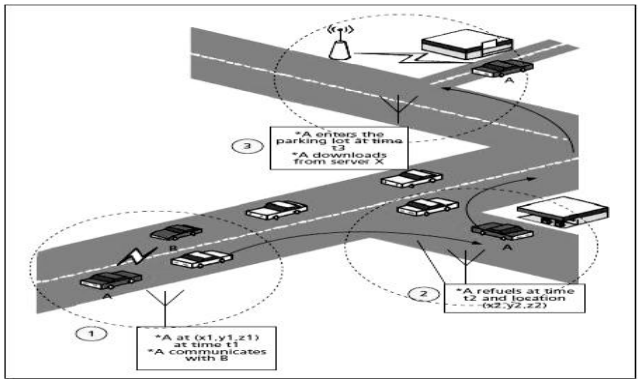
5.4.3 In-transit Traffic Tampering: Any node acting as a relay can disrupt communications of other nodes: it can drop or corrupt messages, or meaningfully modify messages. In this way, the reception of valuable or even critical traffic notifications or safety messages can be manipulated. Moreover, attackers can replay messages (e.g., to illegitimately obtain services such as traversing a toll check point). In fact, tampering with in-transit messages may be simpler and more powerful than forgery attacks.

5.4.4 Impersonation: Message fabrication, alteration, and replay can also be used towards impersonation. Arguably, the source of messages, identified at each layer of the stack, may

be of secondary importance. Often, it is not the source but the content (e.g., hazard warning) and the attributes of the message (freshness, locality, relevance to the receiver) that count the most. However, an impersonator can be a threat: consider, for example, an attacker masquerading as an emergency vehicle to mislead other vehicles to slow down and yield; or an adversary impersonating roadside units, spoofing service advertisements or safety messages.

5.4.5 Privacy Violation: With vehicular networks deployed, the collection of vehicle specific information from overheard vehicular communications will become particularly easy. Then inferences on the drivers' personal data could be made, and thus violate her or his privacy. The vulnerability lies in the periodic and frequent vehicular network traffic: safety and traffic management messages, context-aware data access (e.g., maps, ferryboat schedules), transaction based communications (e.g., automated payments, car diagnostics), or other control messages (e.g., over-the-air registration with local highway authorities). In all such occasions, messages will include, by default, information (e.g., time, location, vehicle identifier, technical description, trip details) that could precisely identify the originating node (vehicle) as well as the drivers' actions and preferences.

Figure 11: Privacy violation



5.4.6 On-board Tampering: Beyond abuse of the communication protocols, the attacker may select to tinker with data (e.g., velocity, location, status of vehicle parts) at their source, tampering with the on-board sensing and other hardware. In fact, it may be simpler to replace or by-pass the real time clock or the wiring of a sensor, rather than modifying the binary code implementation of the data collection and communication protocols.

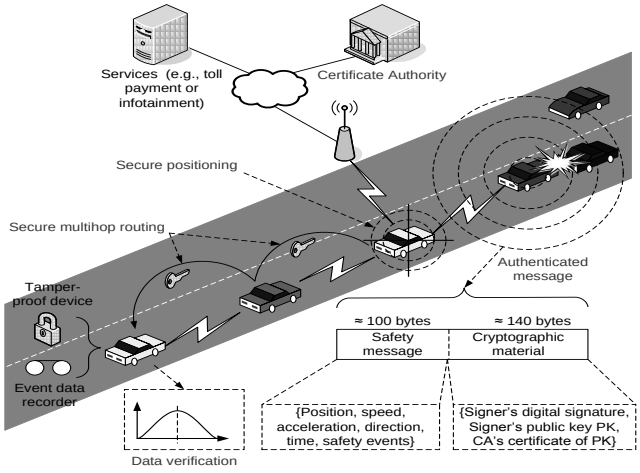
6. SECURITY REQUIREMENTS

1. Authentication: React only to legitimate events. Authenticate senders of messages.
2. Verification of data consistency: Legitimate senders can send false data (attack / unintentional). Can cause immense damage even fatalities.
3. Availability: Network should be available under jamming attacks.
4. Non-repudiation: Drivers causing accidents should be reliably identified
5. Privacy (conflicts with authentication): Privacy of drivers against unauthorized observers.
6. Real-time constraints: High speed means constraints on time

7. SECURITY ARCHITECTURE

VANET applications imply different security and privacy requirements with respect to the protection goals integrity, confidentiality and availability. Nevertheless, there is a common need for a security infrastructure establishing mutual trust and enabling cryptography. Simply using digital signatures and a public key infrastructure (PKI) to protect message integrity is insufficient taking into account multilateral security and performance requirements.

Figure 12: Security Architecture Overview



The main challenge in providing security in VANET depends on privacy, trust, cost and gradual deployment. Some existing security tools in some countries include electronic licence plates (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, vehicular public key infrastructure (VPKI) in which a certification authority manages security issues of the network like key distribution, certificate revocation etc., event data recording by which important parameter can be registered during abnormal situation like accidents etc. Tamper proof hardware is essential for storing the cryptographic material like ELP and VPKI keys for decreasing the possibility of information leakage. To keep a tap on bogus information attack, data correlation techniques are used. To identify false position information, secure positioning techniques like verifiable multilateration is commonly used.

8. CONCLUSION

VANET is a promising wireless communication technology for improving highway safety and information services. In this paper both security concerns and the requirements of potential VANET applications are taken into account. I also study several enabling technologies for the design framework. These enabling technologies include security management, key management, secure routing and network coding. Securing VANETs communication is a crucial and serious issue, since failure to do so will delay the deployment of this technology on the road. All vehicles' drivers want to make sure that their identity is preserved while exchanging messages with the other entities on the road. On the other hand the governments want to guarantee that the deployment of such system will not cause more accidents due to security flows. I believe that my study can provide a guideline for the design of a more secure and practical VANET.

9. FUTURE SCOPE

VANET is definitely something to lookout for in the future. A lot of theoretical work has been put into realizing these networks and few experiments has been performed to validate this theory as cost of setting up this architecture is high, but more such efforts can be expected in near future. A successful vehicular network will open up a plethora of services to a huge number of audiences which will turn out to be life saving as well as fun.

10. REFERENCES

[1] D. Shaw and W. Kinsner, Multifractal modelling of radio transmitter transients for classification, in: Proceedings of WESCANEX'97: Communications, Power and Computing, 1997.

[2] Jochen Schiller, "Mobile Communication", Second Edition, Pearson Education Ltd., 2003.

[3] Kevin,Uichin Lee, Mario Gerla, "Survey of Routing Protocols in Vehicular Ad Hoc Networks in Car 2 Car communication consortium.

[4] K. Plossl, T. Nowey, C. Mletzko, "Towards a security architecture for vehicular ad hoc networks", in: The First International Conference on Availability, Reliability and Security, 2006.

[5] Maxim Raya and Jean-Pierre Hubaux "Securing vehicular ad hoc networks", Journal of Computer security, IOS Press Amsterdam, The Netherlands, Volume 15, Issue 1(January 2007), pages 39-68

[6] M. Raya, A. Aziz and J.-P. Hubaux, Efficient secure aggregation in VANETs, in: Proceedings of VANET'06, 2006.

[7] M. Raya, J. P. Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security 15 (1) (2007) 39–68. Special issue on Security of Ad Hoc and Sensor Networks

[8] M. Raya, J.P. Hubaux, "Security aspects of inter-vehicle communications", in: Proceedings of the 5th Swiss Transport Research Conference (STRC 2005), Ascona, Switzerland, 2005

[9] Maxim Raya, Panos Papadimitratos and Jean-Pierre Hubaux "Securing Vehicular Communication", IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular communication, Vol 13, num. 5, 2006, p. 8-15

[10] Sascha Schnaufer, Holger Fuisler, Matthias Transier, Wolfgang Effelsberg, "Unicast Ad-hoc Routing in Vehicular City Scnarios" in "Network on wheels" project under contract no. 01AK064F and Matthias Transier.

[11] S. Eichler, F. Dotzer, C. Schwingenschlogl, F.J.F. Caro, J. Eberspacher, "Secure routing in a vehicular ad hoc network", in: IEEE 60th Vehicular Technology Conference, 2004, pp. 3339–3343.

[12] Yu Wang and Fan Li, "Vehicular Ad Hoc Networks" in Guide to Wireless Ad Hoc Networks, Computer communication and Networks, DOI 10.1007/978-1-84800-328-6_20

[13] Y. C. Hu, A. Perrig and D.B. Johnson, Packet leashes: A defense against wormhole attacks in wireless networks, in: Proceedings of IEEE Infocom'03, 2003.