Vehicluar Ad-hoc Network

Tobias Glocker
University of Vaasa
Tobias.Glocker@uwasa.fi

January 11, 2011

1 INTRODUCTION

Nowadays Vehicular Ad-hoc Networks (VANETs) are becoming more and more important. It is a technology that uses moving vehicles as nodes to create a mobile network. A VANET offers benefits to vehicle and insurance companies. One of the main benefits is Vehicle to Vehicle (V2V) communication. Vehicles can send warning messages once an emergency event happens. This results that many accidents can be avoided. Besides the benefits of a VANET it is to mention that it is quite challenging to establish and to handle a mobile network. To the most challenging parts belong the routing techniques, security and power control. Before the challenging parts can be solved it is very important to observe the traffic in the city and on the country side. The movement of different vehicles, like buses, taxi and cars play an essential role. This report focuses mainly on the routing techniques and security options for a VANET.

2 TRAFFIC OBSERVATION

It is very important to observe the traffic before suitable routing or security algorithms can be applied or developed. The traffic flow and the traffic density in an urban area is not the same as on a highway. Traffic lights and the road size have a great influence on the vehicle movement. In the city, vehicles that move in the same direction are close to each other like clusters. According to Luo, Gu, Zhao

& Yan (2010) the expectation distance between two clusters can be computed with the following formula.

$$expected\_distance = min(T * V, L); \tag{1}$$

The road segment length is L, the period of the red traffic light is T and the velocity is V. Besides the movement of the vehicles it is also important to know the percentage of different vehicles. In urban areas there are at least two types of vehicles which are ordinary cars and buses. In comparison to a car a bus is much longer and more powerful. This leads to the advantage that a bus can carry a much better wireless equipment with a larger communication range. (Luo, Gu, Zhao & Yan 2010.)

3 ROUTING PROTOCOLS

To forward packets to their destination a routing protocol is required because not all the vehicles that should receive a certain message are inside the communication range. Messages sent inside a VANET should be forwarded in a fast and reliable way. Abedi, Barangi & Azgomi (2009) introduce a method that improves the stability and overhead of the Ad-hoc On Demand Distance Vector (AODV) protocol so that it is usable for VANETs. AODV finds routes for a destination only if there is a packet to transmit. Many improvements have been made on this protocol. SAODV is a further developed protocol that contains additional security functions. It protects the routing messages of the original AODV protocol by using digital signatures.

A stable routing is very important for VANETs. Stable routing can be achieved by mobility prediction. The Prior AODV (PAODV) protocol proposed by Abedi et al. (2009) improves the routing stability by decreasing the routing overheads. In this protocol the routing overhead is decreased by dividing the communication range of a node/vehicle into two zones. One of them is the overhead zone which is the zone between node/vehicle and a defined threshold distance. The prior zone of the node/vehicle is the zone between the threshold distance and the transmission range. Before a node/vehicle starts broadcasting a Route Request (RREQ) packet to the destination it waits for a certain time to find its neighbors. After this step is completed, the node/vehicle broadcasts RREQ packets only to the nodes/vehicles that are located in the prior zone.

4 SECURITY

Security in VANETs plays an essential role to reduce the risk of a network attack. According to Samara, Al-Salihy & Sures (2010a) a VANET can be attacked by Denial of Service, Message Suppression, Fabrication, Alteration, Replay or Sybil attack. The Denial of Service Attack happens when the Attacker jams the network so that critical information packets can not be received. Another dangerous attack is the so called Message Suppression attack in which the attacker is selectively dropping packets from the network that contain critical information. Furthermore, an attacker can send wrong information to the network which is known as Fabrication attack. The manipulation of data, delaying the transmission of information or replaying earlier transmissions can lead to a dangerous situation when the car driver receives a message that the road is clear instead of congested. This attack is the so called Alteration Attack. There is also the risk of a replay attack in which the attacker replays the transmission of earlier information. The Sybil Attack happens when an attacker convinces other vehicles to take another road by pretending a traffic jam.

A high security standard is required to keep the risk of an attack in a VANET low. Wagan, Mughal & Hasbullah (2010a) have proposed a security framework for a VANET that is based on a combination hybrid cryptography scheme. It also supports the Trusted Platform Module (TPM) chip.

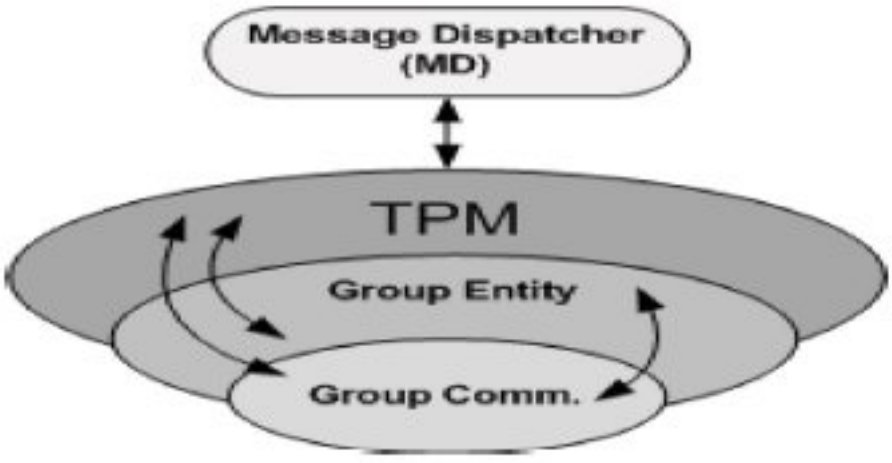

Figure 1. VANET Security Framework (Wagan, Mughal & Hasbullah 2010a.)

The framework consists of three basic components: Hardware Entity (TPM chip), Group Entity and Group Communication. The target of this framework is to create a trusted connection between a group of vehicles by using default Public Key Infrastructure (PKI) mechanism. **Figure 1** shows the security frame work.

To remove duplicated information collected from different sensors a Message Dispatcher is used. Besides removing duplicated information, the Message Dispatcher is also used to send the received information to concerned applications. The Trusted Platform Module takes care of the security features during the transmission of safety messages. It is necessary to specify how the group leader is going to be selected and how the group is formed. This is the task of the Group Entity. There are already several approaches of how groups can be formed. One approach is to form a group by dividing a road into segments. Another approach is to build groups on the fly by using different clustering techniques. Before a group of vehicles can exchange data it must be defined how the vehicles communicate with each other. This is defined in the Group Communication. (Wagan, Mughal & Hasbullah 2010b.)

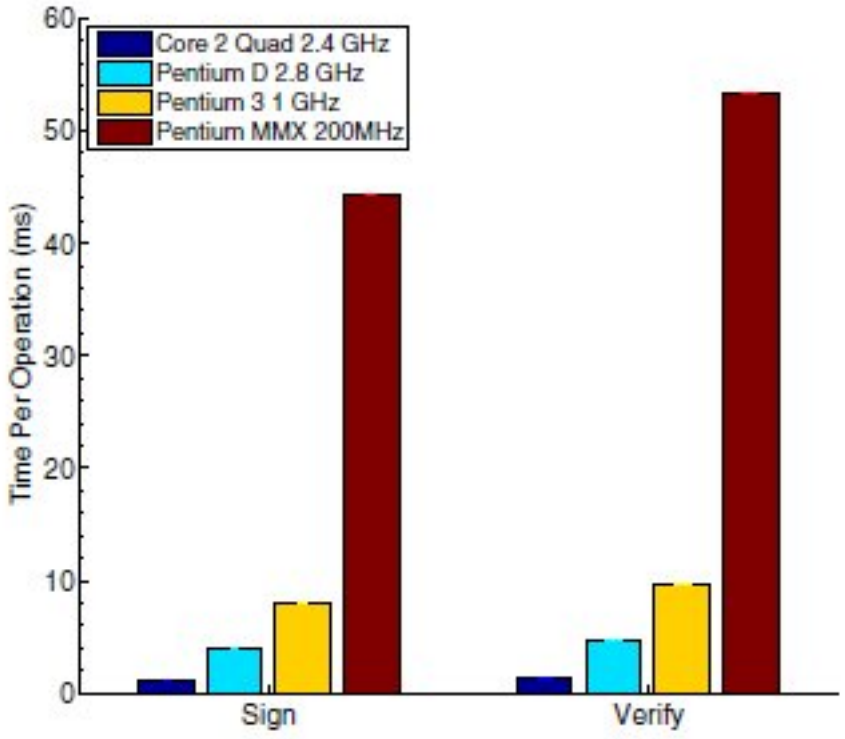

Figure 2. Authentication mechanism verification latency for ECDSA (Haas, Hu & Laberteaux 2009.)

The Security Protocol Performance is very important because the authentication process should be fast, so that a vehicle which joins the network will not miss many important packets before it is authenticated. For this reason, a fast authentication mechanism must be used that provide also a high security standard. In the paper proposed by Haas, Hu & Laberteaux (2009) there are two authentication mechanisms compared. **Figure 2** and **Figure 3** illustrate the verification latency for various hardware. By comparing both figures it can be seen that the TESLA authentication mechanism is much more efficient than the Elliptic Curve Digital Signature Algorithm (ECDSA).

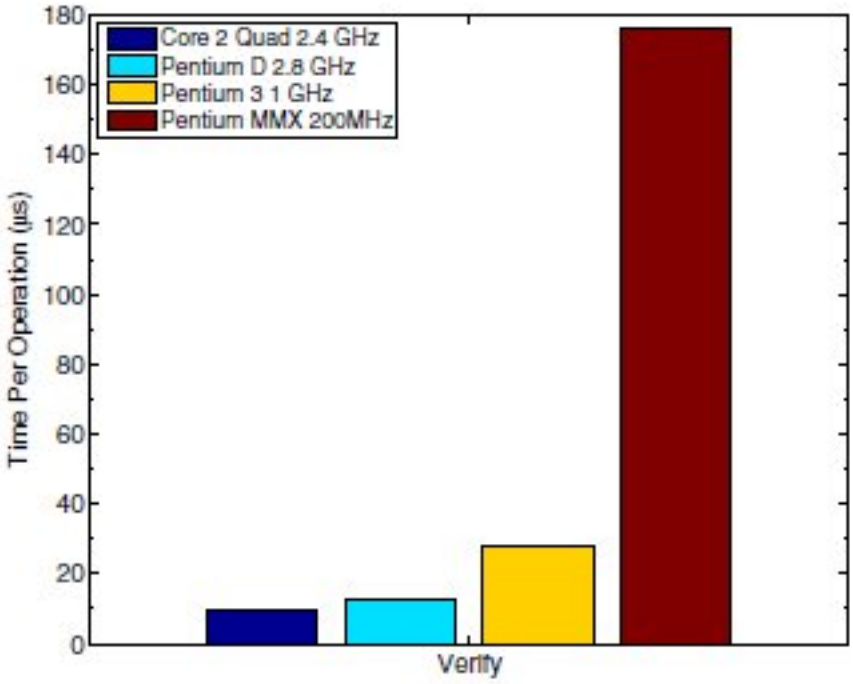

Figure 3. Authentication mechanism verification latency for TESLA (Haas, Hu & Laberteaux 2009.)

5 CONCLUSION

In this report the routing and security requirements for VANETs were discussed. Before the algorithms for routing and security can be developed, the observation of the traffic is important to find out how the vehicles in an certain area are distributed.

Nowadays VANETs are becoming more and more important. One of the main reasons is that the security can be increased by sending warning messages in case an emergency happens or the car approaches a common crossing. A VANET is quite complicated to create and to manage. Vehicles are leaving and joining the network continuously. Besides the group leader selection it is also challenging to share the keys needed for the encryption and decryption. Nowadays and in the future there are plenty of challenges to conquer.

6 BIBLIOGRAPHY

Luo, Jie, Xinxing Gu, Tong Zhao & Wei Yan (2010). A Mobile Infrastructure Based VANET Routing protocol in the Urban Environment. International Conference on Communications and Mobile Computing. 978-0-7695-8/10 ©2010 IEEE.

Samara, Ghassan, Wafaa A.H. Al-Salihy & R. Sures (2010). Security Analysis of Vehicular Ad Hoc Networks (VANET). Second International Conference on Network Applications, Protocols and Services. 978-0-7695-4177-8/10 ©2010 IEEE.

Wagan, Asif Ali, Bilal Munir Mughal & Halabi Hasbullah (2010a). VANET Security Framework for Trusted Grouping using TPM Hardware: Group Formation and Message Dissemination. 978-1-4244-6716-7/10 ©2010 IEEE.

Wagan, Asif Ali, Bilal Munir Mughal & Halabi Hasbullah (2010b). VANET Security Framework for Trusted Grouping using TPM Hardware 978-0-7695-3961-4/10 ©2010 IEEE.

Haas, Jason J., Yih-Chun Hu & Kenneth P. Laberteaux (2009). Real-World VANET Security Protocol Performance. 978-1-4244-4148-8/09 ©2009.

Abedi, Omid, Reza Barangi & M. Abdollahi Azgomi (2009). Improving route stability and overhead of the AODV routing protocol and making it usable for VANETs. 1545-0678/09 ©2009 IEEE.