# Analysis of authentication protocols in vehicular networks

Could computers be used to help drivers avoid road traffic accidents? **Abdul Kalam Aboobaker** and **Stephen Wolthusen** explain the theory behind Vehicular Ad Hoc Networks and some of the challenges they have to overcome to be effective.

# SECURE MESSAGING AND TRAFFIC SAFETY

**TRAFFIC SAFETY** is a major challenge recognised by governments and automotive companies around the world. On an average day in United States and Europe, vehicular collisions kill more than 100 and injure thousands [5, 20]. To further improve traffic safety and efficiency, significant research efforts [13] have been undertaken to integrate computing and communication technologies into vehicles. This enables vehicles to alert each other with information like speed, position, acceleration and road conditions over short and medium range wireless networks. Such a network of communicating vehicles makes a Vehicular Ad Hoc Network (VANET).

Traffic incidents are often a result of the driver's inability to assess quickly and correctly the driving situations at high vehicular speeds. Normally a driver is forced to make decisions like braking and lane changing without the benefit of complete information about road and vehicles around them.

In the case of a VANET, if a driver needs to brake or change lanes, he will periodically broadcast/receive warning messages to/from neighbouring vehicles. This helps him and other drivers react faster, thereby avoiding the likelihood of accidents.

If a malicious driver could falsely report that a road is heavily congested, or could impersonate other vehicles or traffic signals in order to trigger false safety hazards, this could result in traffic confusions or accidents. Therefore authentication is an important aspect of safety messaging that helps detect and prevent participants spreading wrong information in the network.

Factors like vehicle mobility (speed, topology and traffic density), need for low message delays, and message size etc induce challenges that make conventional wireless technologies and protocols unsuitable for VANETs. This article analyses the security requirements of safety messaging, the impact of message size on security and on the performance of secure messaging (authentication) protocols.

## 1. INTRODUCTION TO VANETS

In a Mobile Ad Hoc Network (MANET), wireless nodes operate in a peer to peer mode independent of any infrastructure or a centralised administration. To communicate with nodes beyond wireless range, intermediate nodes forward messages to destination node over multiple hops. Each node acts as an independent router and generates independent data. Fault detection and network management becomes distributed and hence more difficult.

*To communicate with nodes beyond wireless range, intermediate nodes forward messages to destination node over multiple hops. Each node acts as an independent router and generates independent data.*

Nodes in MANETs are mobile causing the network topology to change frequently and unpredictably. This causes nodes to move in and out of wireless range resulting in node unavailability, changes in packet routes, and possibly loss of packets.

Since MANETs do not rely on any form of central administration or control, nodes in the wireless range dynamically discover each other and establish connection with each other.

We hope that the ad hoc network will be maintained even in situations where nodes keep moving in and out of each other's wireless range. Some MANET applications are given in TABLE 1.1.

VANETs are expected to be the largest commercial application of MANETs, envisioned to

TABLE 1.1

**MANET APPLICATIONS**

| MANET APPLICATION | DESCRIPTION |
|---|---|
| Tactical networks | Military communication and operations |
| Commercial and Civilian environment | Dynamic database access, mobile offices • Vehicular Ad Hoc Networks (VANET) |
| Emergency services | Search and rescue operations • Policing and fire fighting |
| Entertainment | Multi-user games • Wireless P2P networking |
| Education | Universities and campus settings • Virtual classrooms |

achieve considerable market penetration in the next decade [11, 18].

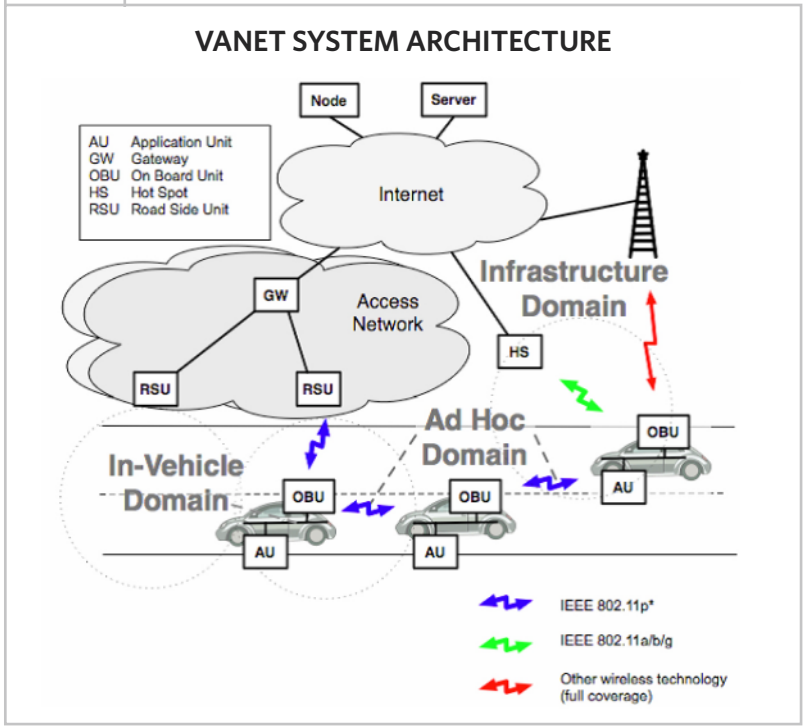
## 1.1 VANET SYSTEM ARCHITECTURE

A VANET system architecture (FIGURE 1.1 [4]) consists of in-vehicle, ad hoc, and infrastructure domains.

The in-vehicle domain consists of an on-board unit (OBU) and one or more applications units (AU) inside a vehicle. An OBU is at least equipped with a (short range) wireless communication device dedicated for road safety, and potentially with other optional communication devices (GSM , GPRS , etc). The AU executes a set of applications utilising the communication capability of the OBU.

An ad hoc domain is composed of vehicles equipped with OBUs communicating with each other or with road-side units (RSUs). The infrastructure consists of RSUs and wireless hotspots (HS) that the vehicles access for safety and non-safety applications. RSUs and HS may be connected to the Internet.

FIGURE 1.1




## 1.2 VANET APPLICATIONS

VANET applications can be divided into two major categories: safety and non-safety applications [17].

**1. SAFETY APPLICATIONS:** Safety applications have the ability to reduce traffic accidents and to improve general safety. These can be further categorised as safety-critical and safety-related applications.

**a) Safety-critical:** These include applications where the danger is high or imminent (e.g.

collisions, lane change). In this case message delay/latency, i.e. the time interval between the generation and reception of a message (M100 ms), and reliability of messages play an important role in realising the safety function. Safety-critical applications involve communication between vehicles (V2V) or between vehicles and infrastructure/infrastructure and vehicles (V2I/I2V).

**b) Safety-related:** These include safety applications where the danger is either low (curve speed warning) or elevated (work zone warning), but foreseeable.

In safety-related applications, the latency requirements are not as stringent as in the case of safety-critical ones. Safety-related applications can be V2V or V2I/I2V.

**2. NON-SAFETY APPLICATIONS:** These are applications that provide traffic information and enhance driving comfort.

Non-safety applications mostly involve a V2I or I2V communication. Non-safety applications include applications for traffic information and recommendations, enhanced route guidance, internet access, media downloading, instant messaging, electronic toll collection, parking management etc.

## 1.3 CHALLENGES IN A VANET ENVIRONMENT

For safety applications, the wireless system needs to maintain definite quality of service with respect to message latency and reliability (acceptable channel throughput and packet reception rates) in the sending and receiving of messages. This brings up the need for new multi-channel architectures like North American IEEE P1609 (WAVE), and European C2C-CC Communication System based on 802.11p wireless system [8].

*Once an emergency situation occurs, it is critical to update the surrounding vehicles as soon as possible.*

Once an emergency situation occurs, it is critical to update the surrounding vehicles as soon as possible. Because the driver reaction time (the duration between when an event is observed and when the driver actually applies the brake) to traffic warning signals can be in the order of 700 milliseconds or longer, the update interval of safety message should be less than 500 milliseconds [10].

Mobility is an important factor that induces challenges to VANET communication [19]. One of the most important aspects of mobility in

VANETs is the potential node velocity.

Node velocity may range from zero to over 200 km per hour on highways. In case of very high node velocities, the mutual wireless communication window is very short. For example, if two cars are driving in opposite directions with 90 km/h each, and if we assume a theoretical wireless transmission range of 300m, communication is only possible for 12 seconds.

Moreover, the routes discovered by conventional topology-based routing protocols may get invalidated (due to changing topology and link failures at high speeds) even before they are fully established. Slow movements usually give rise to a stable topology, but a very high vehicle density, which gives rise to high levels of interference, medium access problems, etc. For such reasons, scalable communication solutions are required.

Vehicles do not move around arbitrarily, but use predefined roads, usually in two directions. But unpredictable changes in the direction of vehicles can occur at intersections of roads.

These movement scenarios pose special challenges particularly for the routing. Even on a highway, that gives smooth traffic in one direction, frequent communication disruptions are encountered. Studies have revealed that a link lifetime of only about 1 minute can be achieved even when driving in the same direction (assuming 500 ft radio range) [14].

In case of very low traffic density, immediate message forwarding becomes impossible. In this case, more sophisticated information dissemination techniques are necessary, which can store and forward selected information when vehicles encounter each other. In this case, the same message may be repeated by the same vehicle multiple times. In high density situations, the opposite must be achieved. Here, a message should be repeated only by selected nodes, because otherwise this may lead to an overloaded channel.

## 2. SECURITY AND PERFORMANCE ANALYSIS

The purpose of this work is to study the security requirements of safety-critical V2V communication and the impact of message size on security and performance on VANET system [7, 16].

Security and performance analysis involves

- Identifying suitable safety-critical VANET applications having maximum latency constraints [1, 7].
- Identifying basic attacks against VANET systems [17].
- Identifying security and performance requirements for the applications [7, 16].
- Mobility patterns: VANET performance varies

with vehicle mobility. Hence we consider two traffic models for analysis - highway (normal traffic) and congestion (city traffic) scenarios [16].

• Identifying the required wireless system: The North American 5.9 GHz DSRC (dedicated short-range communications) is used in this case, specially designed for vehicular safety communication [8].

• Identifying suitable secure authentication protocols for the purpose of analysis [3, 9, 12].

## 2.1 IDENTIFYING SAFETY-CRITICAL APPLICATIONS

• **Pre-crash sensing:** This application can be used to prepare for imminent, unavoidable collisions. Based on position information obtained by messaging, the car can determine whether a crash is about to occur. This application could use communication in combination with other sensors to mitigate the severity of a crash. Counter-measures may include pre-tightening of seatbelts, airbag pre-arming, front bumper extension, etc. Allowable latency: ~20 ms. Broadcast frequency: 50/sec.

• **Cooperative (forward) collision warning:** The vehicle receives data regarding the position, velocity, heading, yaw rate, and acceleration of other vehicles in the vicinity. Using this information along with its own position, dynamics, and roadway information (map data), the vehicle will determine whether a collision with any vehicle is likely. Allowable latency: ~100 ms. Broadcast frequency: 10/sec

• **Emergency electronic brake lights:** When a vehicle brakes hard, the Emergency Electronic Brake light application sends a message to other vehicles following behind.

*When a vehicle brakes hard, the Emergency Electronic Brake light application sends a message to other vehicles following behind.*

This application will help the driver of following vehicles by giving an early notification of lead vehicle braking hard even when the driver's visibility is limited (e.g. a large truck blocks the driver's view, heavy fog, rain). This information could be integrated into an adaptive cruise control system. Allowable latency: ~100 ms. Broadcast frequency: 10/sec.

• **Lane change:** The application receives periodic updates of the position, heading and speed of surrounding vehicles via vehicle-to-vehicle communication. When the driver signals a lane change intention, the application uses this communication to predict whether or not there is an adequate gap for a safe lane change, based on the position of vehicles in the adjacent lane. If the gap between vehicles in the adjacent lane will not be sufficient, the application determines that a safe lane change is not possible and will provide a warning to the driver. Allowable latency: ~100 ms. Broadcast frequency: 10/sec.

## 2.2 IDENTIFYING BASIC ATTACKS

A VANET can be compromised by an attacker manipulating either the physical security of vehicles or messages. The following basic kinds of attacks can be visualised against messages:

**1. Message Forgery:** An attacker can pretend to be another vehicle by using false identities and can be motivated by malicious or rational objectives. Or attackers diffuse wrong information in the network to affect the behaviour of other drivers (e.g., to divert traffic from a given road and thus free the road for themselves).

Attackers can also alter their sensor values to change perceived position, speed, direction, etc. in order to escape liability, notably in the case of an accident. For example, in the case of a hit and run accident, the guilty driver can manipulate sensor information to avoid prosecution.

**2. In-transit traffic tampering:** Any node acting as a relay can disrupt communications of other nodes: it can replay (e.g., to illegitimately obtain services such as traversing a toll check point), 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. In fact, tampering with in-transit messages may be simpler and more powerful than forgery attacks.

**3. Privacy violation:** With vehicular networks deployed, the collection of vehicle-specific information from overheard vehicular communications will become particularly easy. 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. Then inferences on the drivers' personal data could be

made, and thus violate her or his privacy.

**4. Denial of Service (DoS):** The attacker may want to bring down the VANET or even cause an accident. There are many ways to perform this attack, either by sending messages that would lead to improper results or by jamming the wireless channel so that vehicles cannot exchange safety messages.

## 2.3 IDENTIFYING SECURITY REQUIREMENTS

Security requirements are the measures that are put in place in order to secure the Vehicular Communication (VC) system from the effects of possible attacks. In identifying the security

TABLE 2.1

**SECURITY REQUIREMENTS OF SELECTED SAFETY-CRITICAL APPLICATIONS**

| APPLICATION | PROPERTY AUTHENTICATION | LOCATION AUTHENTICATION | INTEGRITY | ENTITY AUTHENTICATION | ID PRIVACY | AVAILABILITY | AUDITABILITY |
|---|---|---|---|---|---|---|---|
| Pre-crash sensing | 2 | 2 | 2 | 2 | 2 | 2 | 0 |
| Cooperative forward collision warning | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| Electronic brake lights | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| Blind spot/Lane change warning | 1 | 2 | 2 | 2 | 2 | 2 | 2 |

0=IRRELEVANT 1=IMPORTANT 2=VERY IMPORTANT

requirements (TABLE 2.1 [7]) for selected applications, application requirements and the basic attacks on VC system were considered.

**1.** Property authentication is a security requirement that allows verifying properties of the sender, e.g. that the sender is a car, a traffic sign etc. For applications using location information,

**2.** Location authentication allows for the verification of the sender's claimed position, or a message's location claim.

**3.** Integrity requirements demand that the information from the sender to the receiver must not be altered, replayed or dropped.

**4.** Entity Authentication ensures that the recently received authenticated message is fresh and live. It ascertains that a message was sent and received in a reasonably small time frame.

**5.** ID privacy specifies how much the identity (licence plate, chassis number or ownership) of the sender should be kept secret. Privacy may be overridden by public authorities (law enforcement, department of transport) wishing to have access to the identity or location information of vehicles.

**6.** Availability of communication systems is critical in VC. The wireless channel has to be continuously available so that approaching vehicles can still receive the warning messages. If the radio channel gets jammed by an attacker, then the warning cannot be broadcast and the application itself becomes useless.

**7.** Auditability is the non-repudiation requirement by which senders or receivers can prove that messages have been received or sent respectively. In some applications, messages may only be stored for a very limited time (e.g. the last 10 seconds in a ring buffer) and made permanent only in case of an incident (e.g. crash).

## 2.4 IDENTIFYING PERFORMANCE REQUIREMENTS

Performance of a VANET messaging system depends on wireless channel throughput, message latency, and message processing delay. This is determined by factors like vehicle mobility, message rate (messages/second), message size (bytes/message), messaging range (meters), and density of messaging vehicles. These factors vary with vehicle environment (highway or congestion scenarios).

Raya et.al in [17] has explored symmetric keys (pairwise keys, group keys), TESLA [15] protocols and asymmetric cryptography for the design of secure authentication protocols. Pairwise session key establishment does not scale well with the number of vehicles (even with a few vehicles) and soon exceeds digital signatures in terms of overhead. In addition, non-repudiation cannot be achieved with symmetric keys. Hence safety-critical applications cannot rely on symmetric session keys.

*Group key establishment may lead to significant savings in bandwidth consumption but at the expense of more transmissions and the complexity needed to implement group protocols.*

Group key establishment may lead to significant savings in bandwidth consumption but at the expense of more transmissions and the complexity needed to implement group protocols. TESLA protocols were found unsuitable for delay-intolerant VANETs.

Hence, digital signatures seem to be the most convenient and reliable solution for authentication, even though its efficiency leaves some room for improvement. In the case of secure communication protocols, the size of cryptographic credentials (the size of signature and public key) and the time taken for authentication (signature verification) has a significant impact on safety communication. Hence Elliptic Curve Cryptography is preferred over RSA [17].

A performance analysis of secure authentication protocols involves:

- **Message size vs. message delay:** Messages of different sizes are considered and the maximum message delay per message is calculated for both highway and city scenarios. For the protocol to meet the performance requirement, the maximum message delay per message for the protocol should to be below the maximum processing delay calculated for each message.
- **Message size vs. throughput:** Messages of different sizes are considered and the maximum message throughput is calculated for both highway and city scenarios.

For the protocol to meet the performance requirement, the calculated throughput should be less than the minimum bandwidth of the radio

channel.

• **Message rate vs. processing delay:** The maximum tolerable processing delay of the message for each message rate is calculated. For the protocol to meet the performance requirement, the maximum tolerable processing delay per message for the protocol should to be below the maximum processing delay calculated for each message.

## 2.5 SECURE MESSAGING PROTOCOLS

Every vehicle that becomes a part of a VANET (employing digital signatures) is bound to two identities: a long-term identity (LTI) and a short-term identity (STI).

Electronic Licence Plate (ELP) is an LTI issued by an authority (government organisation, or a vehicle manufacturer) to vehicles. Each ELP is associated with a pair of unique long-term private (kV) and public (KV) cryptographic keys.

A digital certificate provided by the authority binds KV to ELP and to other data attributes of ELP like vehicle features (colour, brand etc). kV is used to generate digital signatures to authenticate ELP to an authority, which also acts as the Certificate Authority (CA). After successful authentication, the CA provides the vehicle with its STI.

STI are anonymous key pairs used for secure vehicular communications. An anonymous key pair is a short-term public/private key pair that is signed by the CA but contains neither information about nor public relationship with the actual identity (ELP) of the vehicle (i.e., this relationship cannot be discovered by an observer without a special authorization). When vehicles communicate, they authenticate each other using digital signatures signed by anonymous private keys. This provides privacy to vehicular communication.

The CA retains a mapping of anonymous key vs. ELP and ELP vs. owner details for purposes of liability.

Secure messaging protocols based on Baseline Pseudonyms (BP) [3], Group Signatures (GS) [3, 9] and Hybrid Scheme (HS) [12] are considered for the purpose of analysis. The

details of analysis is available in the original thesis [2].

## 3. CONTRIBUTIONS

Prior to security and performance analysis of safety-critical applications, a few basic assumptions have to be laid down.

• The North American 5.9 GHz DSRC messaging system will be assumed, since it forms the basis of safety messaging standards worldwide [8].

• **Two traffic scenarios are assumed:** highway and congestion. A highway scenario involves 6 lanes (3 in each direction) of 3 metres each. We assume a uniform presence of vehicles; with an inter-vehicle space of 30m. Each vehicle periodically sends messages over a single hop every 300m within a range of 10 seconds travel time (the minimum range is 110m and the maximum is 300m).

• In the congestion scenario, assuming the same lanes in highway scenario, vehicles are very slow or stopped and spaced by 5m (including the vehicle length). The inter-message interval drops to 100 ms and the range to 15 m (i.e., their speed is less than 10 miles/h or ffi 16 km/h).

The effect of message size on message delay by literature review and numerical analysis, and baselines for optimum performance were derived. Further, the cryptographic computation costs and overheads, which depend mainly on signature verification time and signature size, were noted for Baseline Pseudonyms, Group Signatures and Hybrid Scheme (based on Centrino 1.5 GHz platform). From the protocol analysis, the following observations were made.

• The optimum total message size (message size + cryptographic overhead) for safety-critical applications should be between 100 and 300 bytes in order to ensure maximum reception, minimum message delay and minimum throughput.

• For the ideal total message size of 100-300 bytes, the maximum tolerable message processing delay was found to be 5.5 ms for highway scenario and 8 ms for congestion scenario.

• The minimum average message delay for the messaging system was found to be 20 ms for the ideal total message size of 100-300 bytes. This makes it impossible for the messaging system to support applications like pre-crash sensing that require a message delay M20 ms. The message delay can be reduced either by reducing message size or by improved wireless media access schemes.

• Any authentication protocol that has a total message size between 100 and 300 bytes and does signature verification in 5.5 ms (highway scenario) and 8 ms (congestion scenario) is an ideal candidate for safety-critical applications.

• Baseline Pseudonyms and Hybrid Scheme (in both mobility scenarios) meet the maximum tolerable message processing delay constraints. Group Signature does not meet the processing delay constraints. Group Signature could meet the requirements if it works on a signature algorithm and/or platform that provides computation

capabilities at least 4 times faster than what is considered in this article. The preferred protocols for authentication seem to be Baseline Pseudonyms and Hybrid Scheme. Baseline Pseudonyms and Hybrid Scheme can work better on faster signature algorithms like NTRU .

### 3.1 CONCLUSIONS

The mobility patterns (highway and congestion) assumed in this article were very simple; vehicles moving in same direction, with the same speed, always separated by same distance, messaging at the same time. Practically vehicles move in same and opposite directions, at different speeds, maintain different spacing between them, change lanes and broadcast randomly.

In an ideal scenario, for the purpose of analysis and simulation, a practical mobility model has to be considered along with a suitable radio propagation model that can be validated. Further work based on these considerations will give more accurate results for the analysis compared to simple assumptions.

The results of analysis show that authentication protocols need to be designed that can support all safety-critical applications. Other considerations required for an effective implementation of VANET system include protection of cryptographic keys, verification of received data, vehicle privacy, and fast eviction of misbehaving vehicles from the network.

Perhaps the most important aspect would be how quickly improvements in technology can be integrated into VANET systems. Since VANETs are delay intolerant, quick adoption of faster operating cryptographic primitives can greatly improve VANET messaging and security. ■

**ABOUT THE AUTHORS**

*Abdul Kalam Aboobaker has worked in IT for companies in India and Dubai. Having completed his MSc at Royal Holloway, he is now applying to do a Doctorate in Mobile Ad Hoc Networks.*

*Dr. Stephen Wolthusen is a lecturer in information security at Royal Holloway with research interests in information assurance and the use of formal methods in security. He teaches courses in Network Security and Digital Forensics.*

## BIBLIOGRAPHY

[1] Vehicle Safety Communications Project Task 3 Final Report. Technical report, The CAMP Vehicle Safety Communications Consortium, Mar 2005. Sponsored by U.S. Department of Transportation (USDOT). Available through National Technical Information Service, Springfield, Virginia 22161.

[2] Abdul Kalam Aboobaker and Stephen Wolthusen. Performance Analysis of Authentication Protocols in Vehicular Ad Hoc Networks (VANET). MSc Thesis, Information Security Group, Royal Holloway, University of London, Sep 2009.

[3] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy. Efficient and Robust Pseudonymous Authentication in VANET. In Proceedings of the ACM International Workshop on Vehicular Ad hoc Networks (VANET), pages 19–28, September 2007.

[4] A. Festag, G. Noecker, M. Strassberger, A. Lübke, B. Bochow, M. Torrent-Moreno, S. Schnaufer, R. Eigner, C. Catrinescu, and J. Kunisch. NoW - Network on Wheels: Project Objectives, Technology and Achievements. In Proceedings of 6th International Workshop on Intelligent Transportation (WIT 2008), Hamburg, Germany, Mar 2008.

[5] Andreas Festag, Holger Füßler, Hannes Hartenstein, Amardeo Sarma, and Ralf Schmitz. FleetNet: Bringing Car-to-Car Communication into the Real World. In Proceedings of 11th World Congress on ITS, Nagoya, Japan, Oct 2004.

[6] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, and Piet Demeester. An Overview of Mobile Ad Hoc Networks: Applications and Challenges. The Communications Network, 3(3), 2004.

[7] Rainer Kroh, Antonio Kung, and Frank Kargl. VANETS Security Requirements Final Version. Technical report, Secure Vehicle Communication (Sevecom), Sep 2006. Available at http://www.sevecom.org/Pages/ProjectDocuments.html.

[8] Tim Leinmüller, Robert K. Schmidt, Bert Böddeker, Roger W. Berg, and Tadao Suzuki. A Global Trend for Car 2 X Communication, 2007.

[9] X. Lin, X. Sun, P.-H. Ho, and X. Shen. GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications. Towards a Security Architecture for Vehicular Ad Hoc Networks.

[10] Xiaomin Ma, Xianbo Chen, and Hazem H. Refai. Performance and Reliability of DSRC Vehicular Safety Communication: A Formal Analysis. EURASIP J. Wirel.

Commun. Netw., 2009:1–13, 2009.

[11] K. Matheus, R. Morich, I. Paulus, C. Menig, A. Lübke, B. Rech, and W. Specks. Car-to-Car Communication- Market Introduction and Success Factors. In ITS 2005: 5th European Congress and Exhibition on Intelligent Transport Systems and Services, Jun 2005.

[12] Panagiotis (Panos) Papadimitratos, Giorgio Calandriello, Jean-Pierre Hubaux, and Antonio Lioy. Impact of Vehicular Communications Security on Transportation Safety. In IEEE INFOCOM MOVE 2008.

[13] Panos Papadimitratos and Jean-Pierre Hubaux. Report on the "Secure Vehicular Communications: Results and Challenges Ahead" Workshop. ACM SIGMOBILE Mobile Computing and Communications Review (MC2R), 12(2):53–64, 2008.

[14] Bryan Parno and Adrian Perrig. Challenges in Securing Vehicular Networks. In Proceedings of Workshop on Hot Topics in Networks (HotNets-IV), November 2005.

[15] A. Perrig, R. Canetti, D. Tygar, and D. Song. The TESLA broadcast authentication protocol. Cryptobytes, 5(2), 2002.

[16] Maxim Raya and Jean-Pierre Hubaux. The Security of Vehicular Ad Hoc Networks. In SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, pages 11–21, New York, NY, USA, 2005. ACM.

[17] Maxim Raya and Jean-Pierre Hubaux. Securing Vehicular Ad Hoc Networks. Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, 15(1):39 – 68, 2007.

[18] P. Samuel. Of Sticker Tags and 5.9 GHz. In ITS International, 2004.

[19] Elmar Schoch, Frank Kargl, Michael Weber, and Tim Leinmuller. Communication Patterns in VANETs. *IEEE Communications Magazine*, 46:119–125, Nov 2008.

[20] A. Stampoulis and Z. Chai. Survey of Security in Vehicular Networks. Technical report, 2007. Project CPSC 534.