VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

Šarūnas STANAITIS

RESEARCH OF SAFETY MESSAGE QUALITY CHARACTERISTICS IN INTER-VEHICLE COMMUNICATION

DOCTORAL DISSERTATION

TECHNOLOGICAL SCIENCES,
ELECTRICAL AND ELECTRONIC ENGINEERING (01T)

VGTU
LEIDYKLA
TECHNIKA
Vilnius 2012

Doctoral dissertation was prepared at Vilnius Gediminas Technical University in 2008–2012.

Scientific Supervisor

Prof Dr Habil Algimantas KAJACKAS (Vilnius Gediminas Technical University, Technological Sciences, Electrical and Electronic Engineering – 01T).

VGTU leidyklos TECHNIKA 2068-M mokslo literatūros knyga
http://leidykla.vgtu.lt

ISBN 978-609-457-360-6

© VGTU leidykla TECHNIKA, 2012
© Šarūnas Stanaitis, 2012
sarunas.stanaitis@vgtu.lt

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Šarūnas STANAITIS

TRANSPORTO PRIEMONIŲ RADIJO RYŠIO SAUGOS PRANEŠIMŲ KOKYBĖS CHARAKTERISTIKŲ TYRIMAS

DAKTARO DISERTACIJA

TECHNOLOGIJOS MOKSLAI,
ELEKTROS IR ELEKTRONIKOS INŽINERIJA (01T)

VGTU
LEIDYKLA
TECHNIKA
Vilnius 2012

Disertacija rengta 2008–2012 metais Vilniaus Gedimino technikos universitete.

Mokslinis vadovas

prof. habil. dr. Algimantas KAJACKAS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, elektros ir elektronikos inžinerija – 01T).

Abstract

The dissertation investigates communication quality issues in Vehicular Ad-hoc Network (VANET) using statistical analysis, experimental measurements, simulations and modelling. The Object of research is quality characteristics of Inter-Vehicle communication, which is based on IEEE 802.11p standard. The main objective of current research is to investigate Inter-Vehicle communication quality characteristics: packet loss and delay. Additionally propose a redundant safety message transmission method and create the confidence index concept and the calculation method. To reach these objectives following tasks have to be solved: define the boundary vehicular multi-hop transmission algorithms and investigate their performance for latency times defined in different use cases; analyze a packet loss caused by obstacles on the road and define approximation equations, for use in modelling tools; create the redundant packet transmission method for the lost safety message reduction; investigate the confidence index concept in a vehicular network and propose the confidence metrics calculation method; investigate the safe following distance dependency on road conditions and compare it to reliable communication distance.

The dissertation consists of introduction, 4 chapters, conclusions and references.

The introduction reveals the aim of the dissertation. The first chapter gives detailed overview of Inter-Vehicle communication environments and defines the main Inter-Vehicle communication parameters. The second chapter summarizes research of safety message transmission delays in vehicular multi-hop chains. Communications scenarios for the best performance and for the best reliability are modelled and delay values given. Experimental measurements were performed to investigate a packet loss due to obstacles on the road and results described in the third chapter. Given approximation equations, can be used in modelling tools and the redundant packet transmission method can be used to reduce a number of lost safety messages. The fourth chapter presents analysis of the driver information system. Flexible confidence index calculation algorithm is proposed and calculations of some safety metrics given. The results of the dissertation are summarized in the general conclusions.

Four scientific papers have been published in the reviewed scientific publications by the author within the topic of research: two in reviewed Thomson Reuters Web of Knowledge journals, one in reviewed Index Copernicus journals, and one in Conference Proceedings Citation Index. 8 presentations on the subject have been given in the conferences at the national and the international level.

Reziumė

Disertacijoje nagrinėjama VANET ryšio kokybės problematika, analizei naudojant statistikos metodus, eksperimentinius tyrimus, modeliavimą ir simuliacijas. Tyrimų objektas yra ryšio tarp automobilių, kurio pagrindas IEEE 802.11p standartas, kokybės charakteristikos. Pagrindinis darbo tikslas – ištirti ryšio tarp automobilių kokybės charakteristikas: vėlinimus ir paketų praradimus. Papildomai pasiūlyti metodus ir algoritmus, mažinančius prarandamų saugos pranešimų skaičių. Pasiūlyti vairuotojo pasitikėjimo indekso koncepciją ir skaičiavimo metodus. Norint pasiekti šiuos tikslus, buvo spręsti sekantys uždaviniai: apibrėžti ribinius perdavimo grandine algoritmus ir ištirti jų efektyvumą perduodant pranešimus grandine; išanalizuoti duomenų paketų praradimus dėl kliūčių ir pateikti atitinkamus aproksimavimo algoritmus, tinkamus modeliavimams; sukurti dubliuotų saugos pranešimų perdavimo metodą, kuris leistų sumažinti prarandamų saugos pranešimų skaičių; sukurti vairuotojo pasitikėjimo indekso koncepciją ryšio tarp automobilių tinkle ir pasiūlyti pasitikėjimo indekso dedamųjų skaičiavimo metodus; ištirti saugaus važiavimo atstumo priklausomybę nuo kelio sąlygų ir palyginti ją su patikimo ryšio nuotolio išraiška.

Disertaciją sudaro įvadas, 4 skyriai, rezultatų apibendrinimas, naudotos literatūros ir autoriaus publikacijų disertacijos tema sąrašai.

Įvade atskleidžiamas disertacijos tikslas. Pirmame skyriuje pateikiamas detalus ryšio tarp automobilių aplinkos savybių tyrimas. Yra aprašyti ryšio tarp automobilių komunikacijos scenarijai, išnagrinėti ir aprašyti avarinių pranešimų parametrai. Antras skyrius apibendrina saugos pranešimų, siunčiamų daugelio šuolių grandine, vėlinimo laikų tyrimą. Yra modeliuojami greičiausio perdavimo ir didžiausio patikimumo scenarijai ir pateikiami vėlinimo laikų skirstiniai. Atlikti eksperimentiniai tyrimai buvo aprašyti trečiame skyriuje, siekiant išanalizuoti paketų praradimus dėl kliūčių kelyje, kurios yra ryšio liniją kertantys automobiliai. Pateiktos aproksimavimo kreivės gali būti naudojamos modeliavimo įrankiuose, o aprašytas dubliuotų duomenų paketų siuntimo metodas efektyviai sumažina prarandamų pranešimų skaičių. Ketvirtame skyriuje analizuojama vairuotojų informavimo sistema. Sudarytas pasitikėjimo indekso skaičiavimo algoritmas ir pasiūlyti kelių saugos dedamųjų skaičiavimo metodai. Disertacijos rezultatai apibendrinami bendrosiomis išvadomis.

Disertacijos tema paskelbtos keturios mokslinės publikacijos: du straipsniai recenzuojamame moksliniame žurnale (Thomson Reuters Web of Knowledge), vienas (Index Copernicus) ir vienas IEEE konferencijos medžiagoje (Conference Proceedings Citation Index). Disertacijos tema perskaityti pranešimai aštuoniose Lietuvos ir tarptautinėse mokslinėse konferencijose.

Notations

Symbols

a_{d}	–	deceleration;
d	–	distance between centres of the cars;
d_s	–	car stopping distance;
D_{sf}	–	car safe following distance;
g	–	gravity of Earth;
g(t)	–	sum of Dirac delta functions;
$\mathrm{I}_0()$	–	Bessel function;
n	–	vehicle count;
p(r)	–	Rice probability density function;
PE_{GE}	–	error rate for Gilbert-Elliott model;
P_i	–	packet group rate;
p_{LOS}	–	packet loss ratio approximation for LOS case;
p_{NLOS}	–	packet loss ratio approximation for NLOS case;
q_i	–	lost packet trace approximation;
r	–	communication range;
$\mathrm{s}_1(\mathrm{t})$	–	transmitter signal;

$s_x(t)$ – sum of channel reactions;
t – continues time; time expenditures; risk indicator;
t_i – lost packet number;
ti – message counter;
T – one packet transmission period; derivative calculation cycle period;
T_x – lost packet ratio;
TI_{ID} – trust index;
v – velocity of the car;
v_0 – initial velocity of the car;
x_Σ – channel reaction;
α – truthful message coefficient;
β – malicious message coefficient;
$\Gamma(m)$ – complete gamma function of parameter m;
δ – safety margin;
Θ – confidence indicator;
κ – tire condition;
κ_i – i^{th} path transmission coefficient;
μ – static friction coefficient between tyres and road surface;
ξ – risk level;
σ^2 – dispersion describing signal level scatter;
τ_i – i^{th} path signal delay;
τ_{mean} – mean delay time;
Φ – risk function;
Ω – spread of the distribution.

Abbreviations

16QAM	–	16 points Quadrature Amplitude Modulation;
3G	–	Third Generation;
4G	–	Fourth Generation;
64QAM	–	64 points Quadrature Amplitude Modulation;
AASHTO	–	American Association of State Highway and Transportation Officials;
ADAS	–	Advanced DAS;
AU	–	Application Unit ;
BPSK	–	Binary Phase Shift Keying;
BSS	–	Basic Service Set;
CAM	–	Cooperative Awareness Message;
CCA	–	Clear Channel Assessment;
CCH	–	Control Channel;
CDF	–	Cumulative Distribution Function;
CI	–	Confidence Index;
CSMA	–	Carrier Sense Multiple Access;
CSMA/CA	–	CSMA/Collision Avoidance;
CW	–	Contention Window;
DAS	–	Driver Assistance System;
DSRC	–	Dedicated Short Range Communications;
EDCA	–	Enhanced Distributed Channel Access;
ESP	–	Electronic Stability Program;
ETSI	–	European Telecommunication Standard Institute;
GPRS	–	General Packet Radio Service;
GPS	–	Global Positioning System;
HS	–	Hot-Spot;
IEEE	–	Institute of Electrical and Electronics Engineers;
IP	–	Internet Protocol;
ITS	–	Intelligent Transportation System;
LLC	–	Logical Link Control;
LOS	–	Line of Sight;
MAC	–	Medium Access Control;

MSDU	–	MAC Serviced Data Unit;
NLOS	–	Non LOS;
OBU	–	On Board Unit;
OFDM	–	Orthogonal Frequency Division Multiplexing;
OS	–	Operating System;
OSI	–	Open Systems Interconnection;
PGP	–	Pretty Good Privacy;
PHY	–	Physical Layer;
PLCP	–	Physical Layer Convergence Protocol;
QoS	–	Quality of Service;
QPSK	–	Quadrature Phase Shift Keying;
RSSI	–	Received Signal Strength Indicator;
RSU	–	Road Side Units;
SCH	–	Service Channel;
STDMA	–	Self-organizing Time Division Multiple Access;
TTL	–	Time To Live;
UDP	–	User Datagram Protocol;
UTC	–	Universal Time Clock;
V2I	–	Vehicle to Infrastructure;
V2V	–	Vehicle to Vehicle;
VANET	–	Vehicular Ad-hoc Network;
WAVE	–	Wireless Access in Vehicular Environments;
WBSS	–	WAVE Basic Service Set;
WiMax	–	Worldwide Interoperability of Microwave Access;
WLAN	–	Wireless Local Area Network;
WSM	–	WAVE Short Message;
WSMP	–	WSM Protocol.

Contents

Introduction

The Investigated Problem

Road accidents and traffic jams are two the most important problems on the roads. Most road accidents happen because of human error and could be avoided if drivers would be informed about the existing accident ahead at least several seconds before. Traffic jams could be decreased if traffic management organizations could receive the detailed information about vehicle flows and their destinations and advise the driver to take alternative routes.

The answer for the mentioned problems above is Inter-Vehicle communication – Wireless Access in Vehicular Environments (WAVE). Recently WAVE has been attracting much attention from industry and academia. Many initiatives are going around the world concerning Inter-Vehicle communication (Zeadally *et al.* 2010, Liu *et al.* 2009, Veeraraghavan *et al.* 2011).

The base for WAVE is IEEE 802.11p standard, which together with IEEE 1609.1/2/3/4 describes Inter-Vehicle communication. As WAVE is based on the radio communication, it includes some drawbacks of it.

High frequency radio communication is sensible to obstacles between a transmitter and a receiver. As soon as the first WAVE equipped cars drive to public roads they will face many communication path crossing cars, which will be obstacles for the radio signal. This will cause a packet loss, which means that

safety messages will be lost and some accidents will not be avoided. The most popular modelling tools do not consider vehicles as obstacles, which is not realistic.

Another Inter-Vehicle communication problem will occur when a lot of vehicles are WAVE equipped. Here messages will be transported through several nodes – a multi-hop chain. Each communication node introduces delay time for a transmitted message to reach its destination and that can be crucial in the accident avoidance. Boundary multi-hop transmission algorithms should be created and investigated. Their performance should be tested for different use cases, which defines different allowed latency time.

Using Inter-Vehicle communication, drivers are alerted about the dangerous situations on the road. However, due to the mentioned delay and a packet loss, the communication can fail to deliver the emergency information. Therefore, the driver information methods, informing drivers about driving safety even when the communication is lost, should be created. The safety level should be presented for the driver with one unified confidence index expression, which shows a level of danger. The information disseminated in the Inter-Vehicle network should be reliable, because malicious messages from the driver with uncertain intentions can lead to the accidents and the trust on VANET can be broken.

This work presents Inter-Vehicle communication scenarios and characteristics, which are relevant for the safety applications. WAVE properties are analyzed and briefly described. Taking properties of described vehicular network into account, the safety message transmission delays using boundary multi-hop routing schemes are modelled and analyzed. Performed experiments on the road investigate the obstacle influence on a packet loss. The methods to reduce a packet loss rate are presented. The driver information method is proposed and equations for the confidence index calculation are given. A vehicle safe following distance is thoroughly analysed and it is aligned to opposing reliable communication range. The presented concept of social driver network pNET increases a trust and saves the privacy, which is important to avoid consequences of malicious messages and keep the driver's identity private.

Importance of the Dissertation

Inter-Vehicle communication is a quite new communication field, as a main standard IEEE 802.11p is released in 2010. There are still some unsolved quality issues regarding Inter-Vehicle communication.

VANET is a unique network, because the network topology is decentralised, nodes are very dynamic and build stochastic connections. Therefore analyzing VANET it is necessary to consider parameters, which are not characteris-

tic to stationary networks, i.e. node number in one hop, not known safety message destination, etc.

The information in VANET is transmitted using multi-hop communication. To route information in a multi-hop network, several routing scenarios are possible. Very important criterion for routing scheme is the message delay time, because an safety message should reach receivers on time. This sets twofold criterion: the message transmission should be fast and reliable. To implement this criterion boundary routing algorithms (the smallest delay and the biggest reliability) should be analyzed and the collected data compared to allowed latency time of different use cases.

Another quality issue in VANET is a packet loss. One of the reasons for packet loss are obstacles on the road. The packet loss means that safety messages can be lost due to the obstacles, which can cause the road accidents. There are some papers analyzing the radio signal attenuation due to obstacles (Meireles *et al.* 2010, Boban *et al.* 2011), but they do not build the packet loss models. The well-known modelling tools do not consider the communication path crossing vehicles as obstacles, causing non-realistic simulations.

A packet loss due to the obstacles on the road can cause the road accidents, because drivers will be not informed about the dangerous situation ahead. Therefore, the methods to reduce the lost safety message number should be created.

Using the Inter-Vehicle communication, the drivers are informed about dangerous situations on the road. A method to inform a driver is the driver information system, which should unite safety information from several sources and, in order not to confuse a driver, present it in one unified manner. This can be done using the confidence index expression, which should process data from many sources and present a level of danger for the driver. The confidence index should compare, for example, such values as a safe following distance and a reliable communication distance, as they can be opposing each other.

The vehicular environment consists of vehicles with human drivers creating the social environment as well. The malicious safety messages from the drivers with uncertain intentions can lead to the road accidents and so decrease a trust of VANET. Therefore the trust, risk and privacy issues should be analyzed and solutions proposed.

The Object of Research

The Object of research is quality characteristics of Inter-Vehicle communication, which is based on IEEE 802.11p standard.

Objective of the Work

The main objective of current research is to investigate Inter-Vehicle communication quality characteristics: packet loss and delay. Additionally propose a redundant safety message transmission method and create the confidence index concept and the calculation method.

Tasks

Following tasks should be accomplished to reach the objectives:

1. Define the boundary vehicular multi-hop transmission algorithms and investigate their performance for latency times defined in different use cases.
2. Analyze a packet loss caused by obstacles on the road and define approximation equations, for use in modelling tools.
3. Create the redundant packet transmission method for the lost safety message reduction.
4. Investigate the confidence index concept in a vehicular network and propose the confidence metrics calculation method.
5. Investigate the safe following distance dependency on road conditions and compare it to reliable communication distance.

Methodology of Research

To investigate the object of research statistical analysis, experimental measurements, simulations and modelling are performed.

Scientific Novelty

The theoretical and experimental research has brought the following new achievements for the science:

1. The experimental results of packet losses, which show lost packet trend due to obstacles and this trend describing mathematical models.
2. A proposed VANET message redundant transmission method, which increases reliability of safety message transmission.

3. The defined and analyzed boundary routing schemes for vehicular multi-hop chains and shown their suitability for different use cases using simulations.
4. A vehicle safe following distance is aligned to the reliable communication distance.

Practical Significance of the Results

The achieved results can be used for solving quality issues in VANET. The simulation results of multi-hop delay research can be used analysing VANET performance and implementing routing schemes for use cases with different allowed latency times. A redundant packet transmission method should be used in IEEE 802.11p protocols to increase the number of successfully transmitted safety messages. The packet loss approximations can be applied to existing modelling tools, to get the realistic obstructing vehicle influence on transmitted packets. The confidence index expression can be used creating the driver information systems.

Defended Propositions

1. A packet loss rate depends on the distance and obstacles and can be described using algebraic polynomials for use in modelling tools.
2. Sending very important messages redundantly with time shift 20 ms will reduce lost message 62% of the initial risk ratio and is getting lower with increased time shift.
3. The multi-hop routing algorithm selection is defined by allowed latency time of actual use case.
4. The VANET communication analysis should be related to a vehicle safe following distance because, in certain cases, keeping the safe following distance, the IEEE 802.11p communication can get unreliable.
5. The V2V information should be combined with onboard sensor information and presented for the driver with one unified Confidence index expression.

Approbation of the Results

Four scientific papers have been published in reviewed scientific publications by the author within the topic of research:

- 2 in reviewed Thomson Reuters Web of Knowledge journals;
- 1 in reviewed Index Copernicus journals;
- 1 in reviewed Conference Proceedings Citation Index editions.

The dissertation research results were announced in eight scientific conferences:

- International conference "ELECTRONICS" in 2009, 2011 and 2012;
- 2nd Baltic Conference on Future Internet Communications, joint session with COST IC0905, IC0906, Nets4Cars & Nets4Trains, 2012, April 25, Vilnius, Lithuania;
- Conference "Science – Future of Lithuania" in 2009, 2010, 2011.
- The third International Conference on Advances in Mesh Networks MESH'2010, July 18–25, Venice, Italy.

Structure of the Dissertation

Dissertation consists of introduction, four chapters and general conclusions.

Dissertation includes 93 pages of text, 48 equations, 9 tables, 44 figures and 64 references.

Acknowledgments

Firs of all, I would like to thank professor Algimantas Kajackas for his support and advice during all doctorate studies. His help was essential to finish the dissertation. I would like to thank my family and friends for their understanding and apologize for all these lost weekends working on my research.

1

Research of Inter-Vehicle Communication Environment

Road accidents and traffic jams are the most important problems on the roads. These problems can be reduced with means of communication between vehicles, and between vehicles and infrastructure. Communication conditions on the road are quite challenging, as there communicating nodes are moving quite fast and communication LOS path is often blocked with obstacles. On the other hand, a communication distance should be quite big in order to answer to emergency tasks.

This chapter presents the vehicular environment research and gives the main parameters of the Inter-Vehicle communication. Before investigating Inter-Vehicle communication questions, it is very important to understand communication scenarios on the road. The scenarios are described in the first part of this chapter. In different scenarios there are different communication conditions, therefore, different requirements are set for the nodes. The conditions for communication nodes are described in the second part of this chapter. The Inter-Vehicle communication node conditions set special requirements for the communication system. The base for the Inter-Vehicle communication is IEEE 802.11p standard together with IEEE 1609.1-4 standard group.

The analysis presented in this chapter is partially covered with author's publications (Kajackas *et al.* 2009; Stanaitis 2010).

1.1. Inter-Vehicle Communication Scenarios

The communication between vehicles offers many different communication scenarios. The safety and traffic management areas are the most important. As additional possibility of the Inter-Vehicle communication, can be separated infotainment and other communication scenarios.

Communication scenarios are depicted in Fig. 1.1.

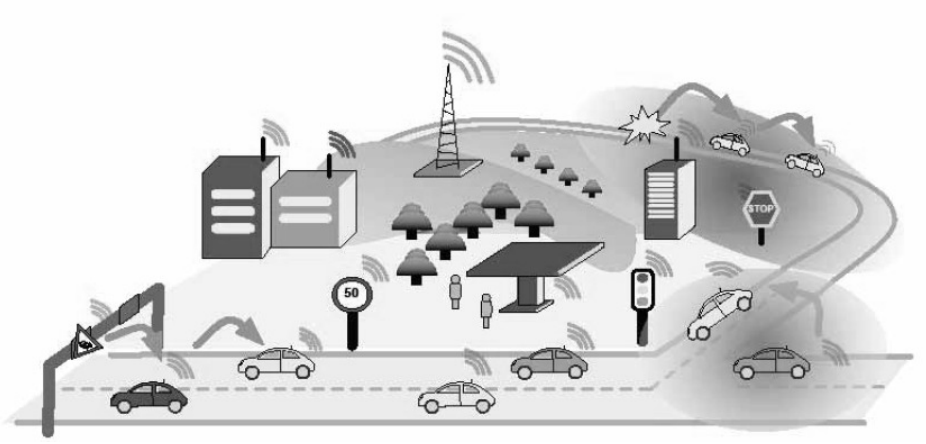

Fig. 1.1. Communication scenarios (Car-to-Car Communication Consortium 2007)

1.1.1. Safety

Safety use cases are those, where the safety of the cars is increased entering a safety zone. There are three safety use cases defined (Car-to-Car Communication Consortium 2007):

1. A cooperative forward collision warning – provides the assistance to the driver primarily to avoid rear-end collisions with other vehicles. On the road equipped vehicles share the information about the speed, position and heading with neighbour vehicles. To predict the collision each vehicle monitors its own data and compares it with neighbour vehicle's data. If the critical proximity is detected, a driver is warned. The warning should be triggered enough time before the accident happens, for a driver to be able to react to the emergency situation. In addition to the communication equipment, the object detection can be used to detect non-equipped vehicles. The cooperative forward collision warning use case requires:

a) the communication range from 20 to 200 m to share the information with other vehicles;

b) accurate positioning;

c) to trust information from other vehicles (as some information can be false);

d) minimal critical number of equipped vehicles to enable the safety system to function.

2. Pre-crash sensing/warning – here, the assumption is that a crash is unavoidable and will take place and this information can be used to prepare the car for the impact. Similar to the cooperative collision warning case, here vehicles also periodically share the information with neighbour vehicles. When a collision cannot be avoided, involved vehicles exchange more detailed information, i.e. a position, a size of vehicle. This information is used to prepare vehicles for the crash optimizing usage of actuators, such as air bags, motorized seat belt pre-tensioners and extendable bumpers. The pre-crash use case requires:

a) the communication range from 20 to 100 m to predict an unavoidable crash;

b) an accurate positioning;

c) to trust information from other vehicles;

d) the minimal critical number of equipped vehicles to enable safety system to function;

e) the fast and reliable communication between involved vehicles in case a crash is unavoidable.

3. The hazardous location Vehicle to Vehicle (V2V) notification – utilizes the network of vehicles to share information that relates to the dangerous locations on the roadway, as for example, slippery roadways or potholes. Here the main issue is detection and information generation of hazardous locations. One example can be the actuation of ESP (Electronic Stability Program) system. The involved vehicle generates an safety message about the situation type and the location, and distributes it for nearby vehicles. Vehicles, to which this information is relevant, prepare its safety systems and warn the driver about the situation ahead. Additionally, this information can be sent to the infrastructure network and then it can inform the road authorities about the situation and warn upcoming drives in advance. The hazardous location notification case requires:

a) to trust information from other vehicles;

b) to trust information from Road Side Units (RSU);

c) the minimal critical number of equipped vehicles to enable safety system to function;

d) an ability to share information about specific geographical location using multi-hop;

e) an ability to evaluate and track the validity of the information distributed over multi-hop.

1.1.2. Traffic Management

These uses cases are meant to increase the traffic performance by providing the information to the owners of the transportation network or to the drivers in the network. The traffic efficiency cases are following (Car-to-Car Communication Consortium 2007):

1. The enhanced route guidance and navigation – uses information collected by an infrastructure owner to deliver the route guidance information to a driver. An infrastructure owner constantly collects the information about the cars on the road and predicts the traffic congestion on the roads over the large area. When a vehicle moves towards its destination, a road operator provides the information about the current and expected situation ahead. According to this information, a vehicle can be guided to the alternative routes if the situation ahead is predicted to be jammed. The enhanced route guidance system requires:

a) the traffic management institution and a infrastructure network to collect road data;

b) to trust information from RSU;

c) RSU ability to offer the traffic management service.

2. The green light optimal speed advisory – provides information to the driver in an effort to make their driving smoother and avoid stopping. When a vehicle approaches the intersection it requests the information from a signalling unit about the traffic light timing and uses this time to calculate the optimal speed to arrive at the intersection at green light. It means that there is no need for a vehicle to stop at the intersection and less stopping means increased traffic flow and increased fuel economy. The green light optimal speed advisory requires:

a) a signalized intersection to transmit traffic light timing data for upcoming vehicles;

b) to trust information from signalling unit.

3. V2V merging assistance – allows merging vehicles to join the flowing traffic without disrupting the flow of the traffic. When a vehicle enters an on-ramp to a limited access roadway, it communicates with the vehicles on the traffic flow and requests a merging permission. With no objection the traffic will automatically adjust to a merging vehicle, to perform a smooth merging manoeuvre. The merging assistance use case requires:

a) an ability to share information between vehicles over the distances that all involved vehicles are able to communicate;
b) the trust information from other vehicles;
c) agree on actions to allow a merging vehicle to join the traffic flow.

1.1.3. Infotainment and Others

These use cases should include all other communication cases, which are not directly related to the traffic safety or the traffic efficiency. Infotainments can be (Car-to-Car Communication Consortium 2007):

1. The Internet access in the vehicle – allows a connection to the Internet. This use case enables all kind of IP based services in the vehicle. To enable the Internet access the multi-hop communication should be established to RSU, which is connected to the Internet. The multi-hop route is transparently masked to above layers of the protocol stack and therefore enables almost any IP based service. The Internet access in a vehicle case requires:

a) an ability to reach RSU which is connected to the Internet;
b) an ability for vehicles to address the Internet servers through RSU;
c) a multi-hop communication ability, when a vehicle cannot directly communicate RSU;
d) the dynamic route maintenance;
e) and an optional ability to connect to regular hotspots using regular 802.11 a/b/g/n Wireless Local Area Network's (WLAN's.)

2. The point of interest notification – allows the local businesses, tourist attractions, or other points of interest to advertise their availability to nearby vehicles. RSU broadcasts the point of interest information such as the location, hours of opening, prices, etc. The information is filtered in vehicles according to its relevance to the driver. For example, if the fuel tank is low, a vehicle can show the driver nearby fuel station and current prices. The benefit of this use case is that advertising can be targeted to geographically located vehicles and a driver gets up-to-date information from the current area. The point of interest notification use case requires:

a) the trust information from RSU;
b) a RSU ability to broadcast the information to surrounding vehicles.

3. Remote diagnostics – allow a service station to assess the state of a vehicle without making a physical connection to the vehicle. When a vehicle enters the area of the service garage, the service communication equipment queries vehicles diagnostic information and compares it with the information reported by the customer. Even if the vehicle approaches the service garage, its past history

and other necessary information can be retrieved from a vehicle and be ready for the technician to use. Software updates can also be installed remotely. This will result in lower costs for repair and reduce waiting time. Remote diagnostics use case requires:

a) the trusted and secure communication with service garages RSU;
b) a vehicle ability to identify itself by the request of authorized requester.

Mentioned use cases build the base for many applications. The detailed application list is given in AASHTO Connected Vehicle Infrastructure Deployment Analysis (Hill *et al.* 2011) and is shown in table 1.1.

Table 1.1. List of potential applications (Hill et al. 2011)

Local use cases	Network use cases
• Infrastructure-based Signalized Intersection Violation Warning • Infrastructure-based Signalized Intersection Turn Conflict Warning • Vehicle-based Signalized Intersection Violation Warning • Infrastructure-based Curve Warning • Highway Rail Intersection • Emergency Vehicle Pre-emption at Traffic Signal • Emergency Vehicle at Scene Warning • Transit Vehicle Priority at Traffic Signal • Stop Sign Violation Warning • Stop Sign Movement Assistance • Pedestrian Crossing Information at Designated Intersections • Approaching Emergency Vehicle Warning • Post Crash Warning • Low Parking Structure Warning • Wrong Way Driver Warning • Low Bridge Warning • Emergency Electronic Brake Lights • Visibility Enhancer • Cooperative Vehicle-Highway Automation System	• Vehicle as Probes: Traffic Information, Weather Data, Road Surface Conditions Data • Crash Date to Public Service Answering Point • Crash Data to Transportation Operations Centre • Advanced Warning Information to Vehicles • Electronic Payment: Toll Collection, Gas Payment, Drive-thru Payment, Parking Lot Payment • Public Sector Vehicle Fleet/Mobile Device Asset Management • Commercial Vehicle Electronic Clearance • Commercial Vehicle Safety Data • Commercial Vehicle Advisory • Unique Commercial Vehicle Fleet Management • Commercial Vehicle Truck Stop Data Transfer • Low Bridge Alternate Routing • Weigh Station Clearance • Cargo Tracking • Approaching Emergency Vehicle Warning • Emergency Vehicle Signal Pre-emption • SOS Services • Post Crash Warning • In-vehicle AMBER Alert

Table 1.1. continued

Local use cases	Network use cases
• Pre-Crash Sensing • Free-Flow Tolling • Cooperative Glare Reduction • Adaptive Headlight Aiming • Adaptive Drivetrain Management • GPS Correction • In-vehicle Signing: - Work Zone Warning - Highway/Rail Intersection Warning • Vehicle-to-Vehicle: - Cooperative Forward Collision Warning - Cooperative Adaptive Cruise Control - Blind Spot Warning - Blind Merge Warning - Highway Merge Assistant - Cooperative Collision Warning - Lane Change Warning - Road Condition Warning - Road Feature Notification • Rollover Warning • Instant Messaging • Driver's Daily Log • Safety Event Recorder • Icy Bridge Warning • Lane Departure-inadvertent • Emergency Vehicle Initiated Traffic Pattern Change • Parking Spot Locator • Speed Limit Assistant	• Safety Recall • Just-in-Time Repair Notification • Visibility Enhancer • Cooperative Vehicle-Highway Automation System • Cooperative Adaptive Cruise Control • Road Condition Warning • Intelligent On-Ramp Metering • Intelligent Traffic Flow • Adaptive Headlight Aiming • Adaptive Drivetrain Management • Enhanced Route Guidance and Navigation: - Point of Interest Notifications - Food Discovery and Payment - Map Downloads and Updates - Location-based Shopping/Advertising - In-Route Hotel Reservation • Traffic Information: Work Zone Warning, Incident, Travel Time • Off-Board Navigation • Mainline Screening • On-Board Safety Data Transfer • Vehicle Safety Inspection • Transit Vehicle Data Transfer (gate) • Transit Vehicle Signal Priority • Emergency Vehicle Video Relay • Transit Vehicle Data Transfer (yard) • Transit Vehicle Refuelling • Download Data to Support Public Transportation • Access Control • Data Transfer: - Diagnostic Data - Repair Service Record - Vehicle Computer Program Updates - Map Data Updates - Rental Car Processing - Video/Movie Downloads - Media Downloads - Internet Audio/Video • Locomotive Fuel Monitoring • Locomotive Data Transfer • Border Crossing Management • Stolen Vehicle Tracking

1.2. Communication Node Conditions

Communication nodes in vehicular applications are located in a dynamic environment and are moving themselves. Here several values, which are not relevant for stationary communication points, are important. These are the number of nodes (cars), the velocity of the nodes, the communication range of one hop, a transferred packet size, the data rate and other parameters, common to regular (stationary) access points.

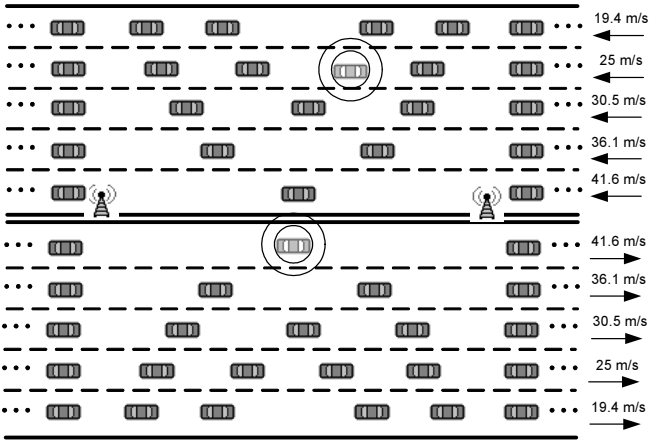

Fig. 1.2. Highway scenario – 5 lanes in each direction (Kajackas *et al.* 2009)

The communication scenario of 5 lanes in each direction is shown in Fig. 1.2. Mobility of the nodes is shown here describing the speed of the vehicle in each lane.

1.2.1. Communication Range

The communication range is one of the most important parameters in the Inter-Vehicle communication. On the one hand, it should be high enough to satisfy needs of all use cases, on the other hand, it should not be too high in order to avoid too many communication nodes in one hop range and less pollute the radio channel.

According to the requirements of (Car-to-Car Communication Consortium 2007), the communication range r should be between 300 m and 1000 m. (Bilstrup *et al.* 2008, 2009) are separating simulations into two parts for 500 m and for 1000 m communication range. For further investigation, presented in this work, both distances of 500 m and 1000 m are taken into account.

1.2.2. Distance Between Vehicles

The distance between vehicles is a necessary parameter, when calculating a number of the vehicle in the certain communication range, or when it is necessary to estimate in what time the impact with a front vehicle can happen at a sudden brake of the front vehicle.

An average distance between vehicles can be calculated using traffic flow measurements. Kononov *et al.* 2012 in their paper presents Flow rate of Denver urban area (Fig. 1.3).

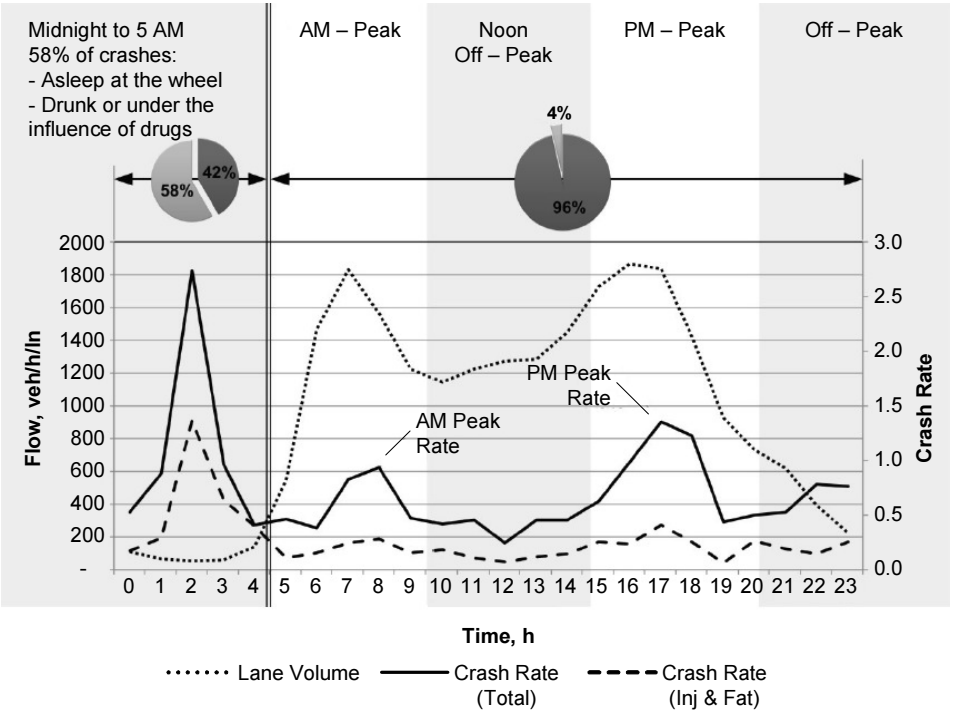

Fig. 1.3. Changes in Volume and Crash Rate over the 24 hr Period on Denver Area Urban Freeways (Kononov *et al.* 2012)

A traffic flow rate curve in Fig. 1.3 shows that the traffic flow is changing over daytime and is the smallest at night with less than 200 vehicles per hour per lane and has two peaks at 7 am and 4 pm reaching values of 1800 veh/h/ln.

The traffic flow is the number of vehicles passing the certain line of the road in a unit of time. The inverse of the traffic flow is a headway, which is the time that elapses between the i vehicle passing a reference point in the space and the i+1 vehicle. The headway for smallest traffic during the night is 6 s and on the peak hours is 2 s. This means that the average headway varies from 2 to 6 s

on the highway. These values will be taken into an account further analysing a distance between the vehicles.

Measured (Kononov *et al.* 2012) headway values are related to driver's ability to react to events on the road. Reaction times of drivers to the different road stimuli are different. The detailed research on the driver reaction time is done by (Triggs *et al.* 1982). This paper explains the different reaction types on the different obstacles on the road and in the different driving conditions. Experiments show, that the average reaction time to the different stimuli is from 2.5 to 3 s which fits to the measurement limits of (Kononov *et al.* 2012).

The results of (Triggs *et al.* 1982) can be found in the recommendations for the drivers. Different countries have slightly different recommendations, i.e. Swedish 3 – second rule, where drivers are advised to maintain a 3-second time space to the vehicle in front (Bilstrup *et al.* 2008, 2009). The research presented in this paper is based on the Lithuanian recommendations to the drivers, where the recommended distance from the front car is the same in meters as half of the cars speed in km/h:

$$d \approx \frac{v}{2}, \tag{1.1}$$

where d – a distance between the centres of vehicles in m (though the recommendation says, that the distance should be between the end and the front of two cars, but it is more reasonable to take the distance between the centres, because of different length of the cars); v – velocity of the car in km/h.

In (1.1) shown expression leads to 1.8 s headway.

1.2.3. Vehicle Velocity

The velocity of the vehicle is a very important parameter in Inter-Vehicle communication. It describes dynamics of the communication nodes and other traffic participants. The velocity of the vehicle influences the time before an accident can happen and the distance at which the accident can be avoided.

As shown in Fig. 1.2, the vehicle velocity v is different in different lanes. The vehicles in the middle lanes are usually moving faster than in the outer lanes. Different authors are proposing different velocities for the cars in the different lanes. For the two lanes in each direction highway scenario (Stibor *et al.* 2007) uses relative speeds from 60 km/h up to 180 km/h. (Bilstrup *et al.* 2008, 2009) for their simulations of three lanes in each direction highway use velocities: 23 m/s (~83 km/h), 30 m/s (~108 km/h) and 37m/s (~133 km/h) and a standard deviation of 1 m/s.

For the current research two highway scenarios are presented: a scenario of three lanes highway and five lanes highway (Fig. 1.2). In three lanes in each di-

rection highway scenario velocities are 19.4 m/s (70 km/h), 25 m/s (90 km/h) and 30.5 m/s (110 km/h). For 5 lanes highway following velocities are used: 19.4 m/s (70 km/h), 25 m/s (90 km/h), 30.5 m/s (110 km/h), 36.1 m/s (130 km/h) and 41.6 m/s (150 km/h).

1.2.4. Vehicle Count

The vehicle count is a very important parameter investigating the multi-hop communication, because it describes how many communication nodes can be in one communication range.

The vehicle count in one lane can be calculated using the following expression (Stanaitis 2010):

$$n = \frac{2 \cdot r}{d} \approx \frac{4 \cdot r}{v}, \tag{1.2}$$

where n – vehicle count; d – distance between vehicle centres; r – communication range.

The vehicle count, calculated using Formula (1.2), for 3 and 5 lanes highway, is given in Table 1.2.

Table 1.2. Vehicle count in 3 and 5 lane highway in each direction (Stanaitis 2010)

Range, m / Lanes	500	1000
3	68	138
5	98	194

A distribution of the vehicle count in different lanes with different velocities is shown in Table 1.3.

Note, that given vehicle count values are true for one hop, that means, that for the 500 m range this number is in lane length of 500 m, but for this communication range each vehicle can reach 500 m to both sides from itself, so the value of reachable vehicle will double.

The results in Table 1.3 are true for a highway with no cross sections (which would increase a number of vehicles in one hop) and can be easily adapted to highways with cross sections.

The results in Table 1.3 can be used for building up the suburban scenario. If the communication range is 500 m and the speed of the vehicle in all lanes is 50 km/h and there are 2 lanes in each direction, then there are 80 vehicles in one hop.

Table 1.3. Vehicle count distribution in different lanes with different velocities (Stanaitis 2010)

Range, m / Velocity, km/h	500	1000
10	100	200
20	50	100
50	20	40
70	14	29
90	11	22
110	9	18
130	8	15
150	7	13

Table 1.3 can be used also for the city scenario with the traffic jam, which means that the vehicle velocity is 10 km/h, and there are 3 lanes in each direction there will be 600 vehicles in one hop.

The presented highway, suburban and city scenarios are calculated for the perfect communication conditions, which means, that all cars are reachable in one hop. In the real world there will be no such case, especially in the city, there many obstacles for the communication exist. But this means, that there will be less communicating nodes in one hop and the communication load will be smaller. Therefore, given numbers represent maximal number of communicating nodes and build up the boundary task for communication system to support.

1.2.5. Delay Time and Critical Latency

The most important task for emergency warning system is to deliver warning messages on time. There can be several types of warning messages, but the messages of the sudden brake or crash in front have to be delivered as soon as possible. According to the Lithuanian rule to keep the distance from the front car same as half of the cars speed brings the time between vehicles positions 1.8 s. That means that after the crash in 1.8 s the following car should stop. Warning messages should be delivered to destinations faster than in 1.8 s. How much faster should be answered by doing the investigation on the driver's reaction time to emergency warnings in the car, as reaction times depend on many parameters and can vary from 0.5 s up to several seconds (Triggs *et al.* 1982).

The Inter-Vehicle communication has many emergency use cases. Each use case has a defined latency time when the safety message should reach the destination after the emergency situation is triggered.

Latency times for different use cases are given in Table 1.4.

Table 1.4. Permissible delay time for safety use cases (The CAMP project, 2005)

No	Latency time, ms	Description
1.	100	Traffic Signal Violation Warning
2.	100	Stop Sign Violation Warning
3.	100	Left Turn Assistant
4.	100	Stop Sign Movement Assistance
5.	100	Intersection Collision Warning
6.	100	Blind Merge Warning
7.	100	Pedestrian Crossing Information at Designated Intersections
8.	1000	Approaching Emergency Vehicle Warning
9.	1000	Emergency Vehicle Signal Pre-emption
10.	1000	SOS Services
11.	500	Post-Crash Warning
12.	1000	In-Vehicle Signage
13.	1000	Curve Speed Warning
14.	1000	Low Parking Structure Warning
15.	100	Wrong Way Driver Warning
16.	1000	Low Bridge Warning
17.	1000	Work Zone Warning
18.	1000	In-Vehicle Amber Alert
19.	5000	Safety Recall Notice
20.	na	Just-In-Time Repair Notification
21.	100	Cooperative Forward Collision Warning
22.	500	Vehicle-Based Road Condition Warning
23.	100	Emergency Electronic Brake Lights
24.	100	Lane Change Warning
25.	100	Blind Spot Warning
26.	100	Highway Merge Assistant
27.	100	Visibility Enhancer
28.	100	Cooperative Collision Warning
29.	20	Cooperative Vehicle-Highway Automation System (Platoon)
30.	100	Cooperative Adaptive Cruise Control
31.	1000	Road Condition Warning
32.	20	Pre-Crash Sensing
33.	1000	Highway/Rail Collision Warning
34.	500	Vehicle-To-Vehicle Road Feature Notification

Latency time, for use cases given in Table 1.4, can be grouped into several parts: 20, 100, 500, 1000 and more than 2000 ms. These delay times are used further analyzing the safety message redundant transmission.

1.3. Inter-Vehicle Communication WAVE Standards

Inter-Vehicle communication is based on IEEE organisation standards IEEE 802.11 p and IEEE 1609 family.

Table 1.5. WAVE IEEE standards

Standard	Description	Status
IEEE 802.11p-2010	IEEE Standard for Information technology – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments	Active Standard
IEEE P1609.0	Guide for Wireless Access in Vehicular Environments (WAVE) – Architecture (MP)	Active Project
IEEE P1609.1	Standard for Wireless Access in Vehicular Environments (WAVE) – Resource Manager (MR)	Active Project
IEEE P1609.2	IEEE Draft Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages (MR)	Active Project
IEEE 1609.3-2010	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services	Active Standard
IEEE 1609.4-2010	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Multi-channel Operation	Active Standard
IEEE P1609.5	Standard for Wireless Access in Vehicular Environments (WAVE) – Communication Manager (P)	Active Project
IEEE 1609.11-2010	IEEE Draft Standard for Wireless Access in Vehicular Environments (WAVE) – Identifier Allocations (MP)	Active Standard
IEEE P1609.12	Standard for Wireless Access in Vehicular Environments (WAVE) – Communication Manager (P)	Active Project

In Table 1.5 given standards describe communication means for vehicular applications. Several studies are written about WAVE communication (Bilstrup *et al.* 2008, Jang *et al.* 2008, Kosch *et al.* 2012, Muller 2009).

1.3.1. WAVE Architecture

WAVE architecture is described with IEEE 1609.0 standard (still under development). Main guidelines can also be found in C2CC Manifesto (Car-to-Car Communication Consortium 2007). WAVE reference architecture is shown in Fig. 1.4.

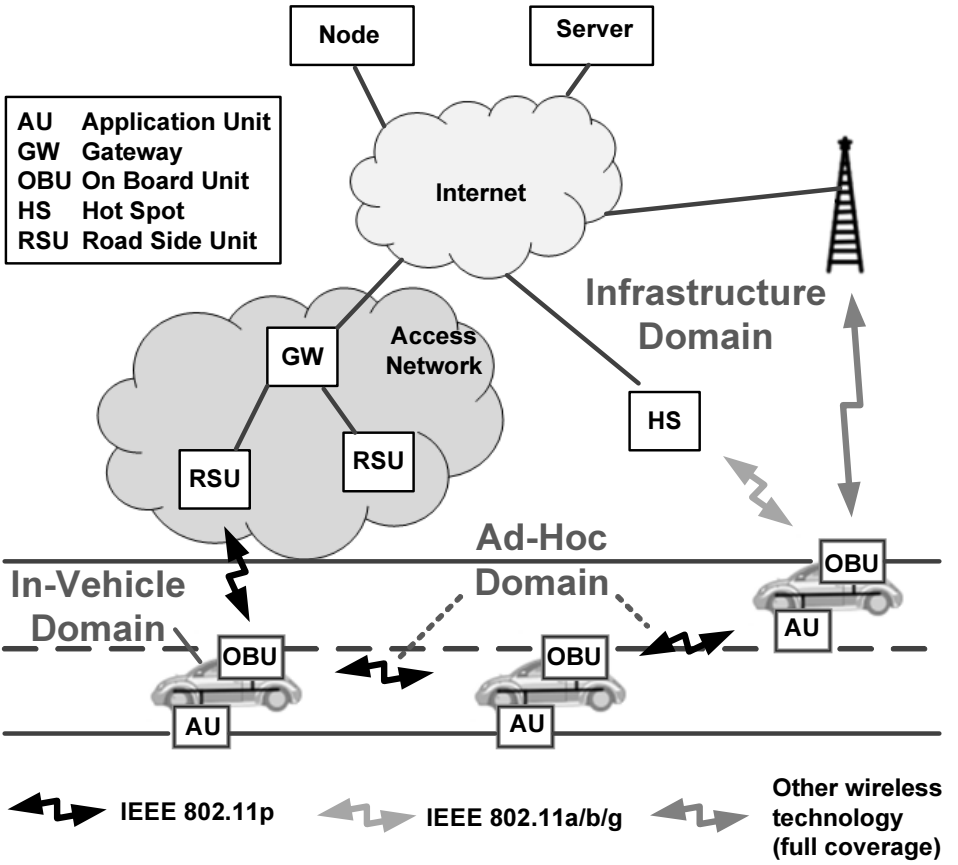

Fig. 1.4. WAVE reference architecture (Car-to-Car Communication Consortium 2007)

Reference architecture, presented on Fig. 1.4, consists of several main components:

a) OBU – On Board Unit, which is located on vehicles and is building communication with other OBU's and RSU's;

b) AU – Application Unit responsible for Application generation and execution. It is connected to RSU's;

c) RSU – Road Side Unit, which is located on the road infrastructure. In one side RSU's are connected to OBU's with 802.11 p and in other side they are connected to gateways, which are building connection to the Internet;

d) HS – Hot-Spot places, where OBU's can reach Internet via 802.11 a/b/g/n regular networks.

Described system components are depicted in Fig. 1.5.

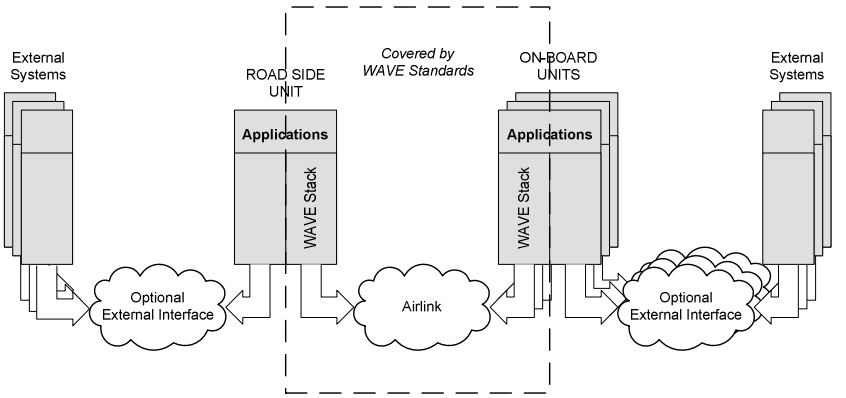

Fig. 1.5. WAVE system components (IEEE 1609.0)

Fig. 1.5 clearly defines boundaries of Inter-Vehicle communication. Inter-Vehicle communication is between OBUs and RSUs, where RSU can have external communication to the infrastructure (i.e. traffic management institutions, Internet, etc.). OBU can have additional radio technologies as well, which could be used as a redundant communication path and an additional connection to e.g. the Internet.

1.3.2. IEEE Standard

IEEE standard 802.11 and 1609 group describes WAVE communication. WAVE communication can be aligned to OSI model (Fig. 1.6).

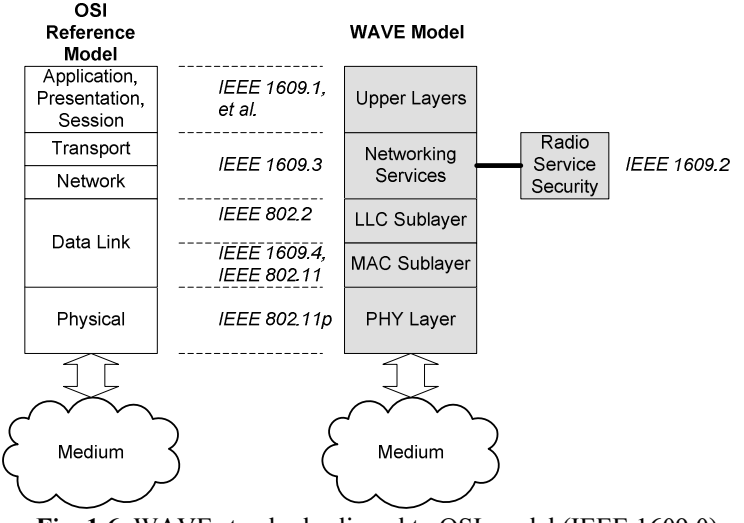

Fig. 1.6. WAVE standards aligned to OSI model (IEEE 1609.0)

IEEE 802.11p standard is an amendment to legacy IEEE 802.11 standard. It describes differences of legacy standard, which are necessary for WAVE communication. IEEE 802.11 standard specifies Medium Access Control (MAC) and Physical (PHY) layers. IEEE 802.11p will make use of the PHY supplement IEEE 802.11a and the MAC layer Quality of Service (QoS) amendment from IEEE 802.11e. (Bilstrup *et al.* 2009) WAVE PHY uses Orthogonal Frequency Division Multiplexing (OFDM). Radio frequency is similar to IEEE 802.11a and is allocated from 5.85 to 5.925 GHz into several 10 and 5 MHz channels.

WAVE frequency allocation is shown in Fig. 1.7.

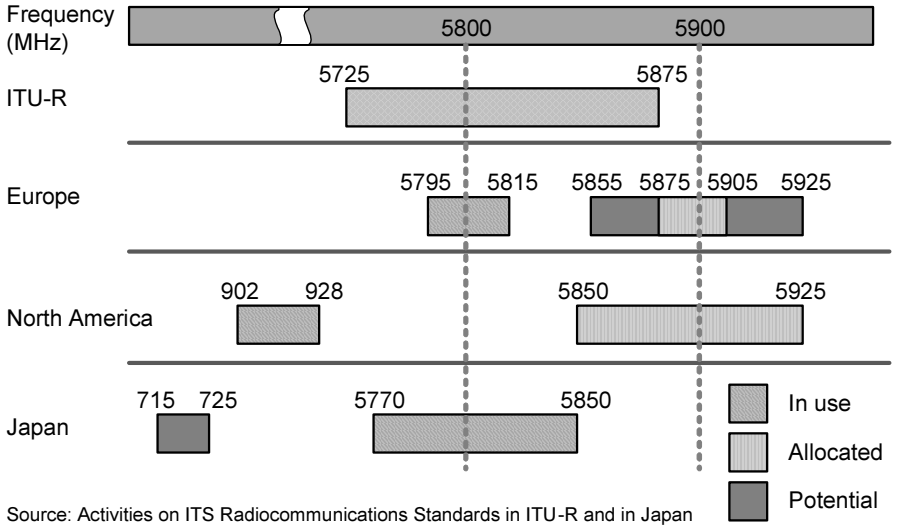

Fig. 1.7. WAVE frequency allocation (Muller 2009)

As it is shown in Fig. 1.7, frequency allocation is slightly different in Europe and other regions.

The data rate for IEEE 802.11 p is defined from 3 to 27 Mbit/s using Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK), 16 points Quadrature Amplitude Modulation (16QAM) and 64QAM modulations.

WAVE MAC is also specific and is described in IEEE 1609.4 standard. There is a timing allocation of channels. The Control Channel (CCH) is defined for safety message transmission and for service advertisement and Service Channel (SCH) is responsible for all other information transmission. In the CCH time frame all stations should stop transmission and listen to this channel and receive/transmit safety messages. During SCH channel time frame stations can use all other radio channels to transmit all types of information. Channels are divided into 50 ms frames.

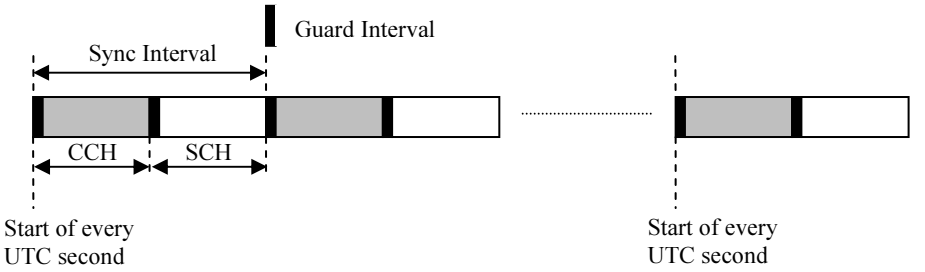

Fig. 1.8. Channel timing allocation (IEEE 1609.4)

Time synchronization of channels is done using Global Positioning Systems (GPS) Universal Time Clock (UTC) signal. The safety messages are sent by using WAVE Short Message Protocol (WSMP) described in IEEE 1609.3 standard.

The communicating nodes in the Vehicular Ad-hoc Network (VANET) are moving fast and they should be ready for transmission as soon as possible. The WAVE Basic Service Set (WBSS) provider first transmits WAVE Announcement action frames, for which the WBSS users listen. That frame contains all information necessary to join a WBSS. Unlike infrastructure and ad-hoc 802.11 BSS types, the WAVE users do not perform authentication and association procedures before participating in the WBSS. To join the WBSS, only configuring according to the WAVE Announcement action frame is required. In addition, a node in WAVE mode shall generate a Clear Channel Assessment (CCA) report in response to a CCA request to know the time-varying channel state precisely.

1.3.3. Communication Channel Switching

Two different communication channel switching types can be distinguished in Inter-Vehicle communication. One is hopping – switching between IEEE 802.11p nodes (horizontal handover). Another is inter-technological channel switching, where not only intermediate nodes change but the radio transmitting technology (vertical handover), as well.

The communication channel in hopping scenario is build between OBU's and RSU's with IEEE 802.11p communication devices. The master vehicle can have several paths, to connect to other OBU or to the Internet trough RSU (which is the Internet gateway in IEEE 802.11p). The example of multipath communication is given in (Fig. 1.9). Here a path A consists of three hops and a path B consists of two hops.

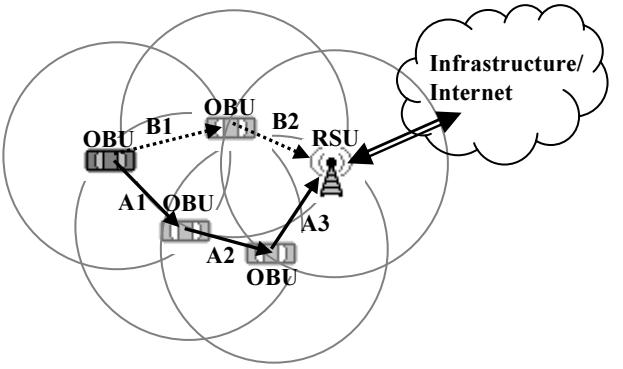

Fig. 1.9. Multipath hopping scheme

The vertical handover presents the communication case, where vehicle communication with master OBU is lost or poor and should decide whether to try use IEEE 802.11p to connect to other devices or to change radio transmission technology (Fig. 1.10). To retrieve the safety information or just to get the Internet access OBU can connect to the regular IEEE 802.11a/b/g equipment at the hotspot infrastructure places. For the wide range communication the Internet service can be provided by the mobile telecommunication companies, offering General Packet Radio Service (GPRS), Third Generation (3G), Fourth Generation (4G) or other connections to the Internet. Services of mobile telecommunication companies are typically paid and here a driver with help of OBU should decide whether to use paid connection or not. Some other radio technologies can be used as well. For example, Worldwide Interoperability of Microwave Access (WiMax) radio technology typically has the coverage of the entire city.

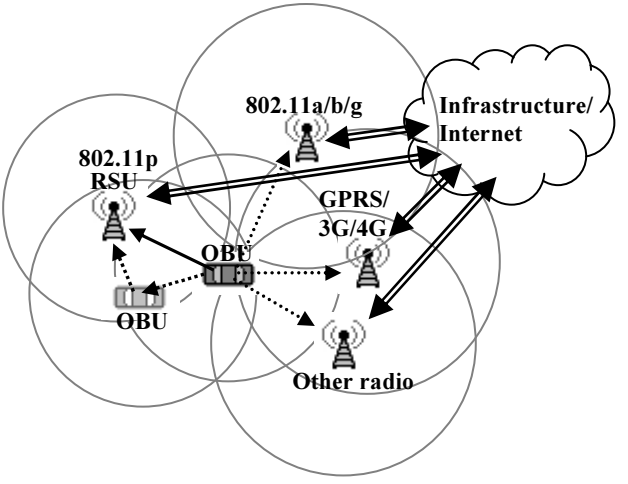

Fig. 1.10. Vertical handover scheme

1.4. "Trust" in Inter-Vehicle Communication

Safety messages, which include the crucial information about the safety situation on the road, have the highest priorities in VANET. Safety message can help to safe lives, therefore it is very important, that transmitted information is true and it can be trusted. The truthful message content is very important for traffic control system as well, because the false information can completely disrupt the traffic in the city.

A social network is required to implement a trust in vehicular communication and in the same time not to compromise the privacy of the driver. This section describes the idea of the social vehicular network and describes the main tasks of this network. Short and long term trust index calculation algorithms are given.

1.4.1. Trust and Risk Concepts

The trust concept is used in several fields of science and has various descriptions. Swami *et al.* 2009 in their paper give several trust definitions. The concept of trust is important to communication and network protocol designers where establishing trust relationships among participating nodes is critical to enabling collaborative optimization of system metrics. The trust is defined as a set of relations among entities that participate in a protocol. These relations are based on the evidence generated by the previous interactions of entities within a protocol. In general, if the interactions have been faithful to the protocol, then trust will accumulate between these entities. The trust has also been defined as the degree of belief about the behaviour of other entities (or agents), often with an emphasis on the context.

The short trust description is given in paper of Avizienis *et al.* 2004: the trust is accepted dependence.

The trust is close related to trustworthiness definition (Swami et al. 2009). They give several trustworthiness definitions: trustworthiness is a measure of the actual probability that the trustees will behave as expected; trustworthiness is the objective probability that the trustee performs a particular action on which the interests of the trustor depend.

Swami et al. 2009 in their paper give a definition of risk value, as well. The risk value is low for all trust values when the stake is close to zero. If the stake is too high, the risk is regarded as high regardless of the estimated trust value. The risk is generally low when the trust value is high. However, the risk value should be determined based on the value at stake as well as the risk probability.

Swami et al. 2009 distinguish three main trust properties: transitivity, asymmetry, and personalization. First, trust is not perfectly transitive in a

mathematical sense. That is, if *A* trusts *B*, and *B* trusts *C*, it does not guarantee that *A* trusts *C*. Second, trust is not necessarily symmetric, meaning not identical in both directions. A typical example of asymmetry of trust can be found in the relationships between supervisors and employees. Third, trust is inherently a personal opinion. Two people often evaluate trustworthiness about the same entity differently.

In vehicular case, trust is between the vehicle (e.g. *V1* and *V2*) information processing equipment (drivers just take the final decision on processed and assessed information, which is given by equipment). When *V1* sends a message to *V2*, then depending on the message contents *V2* trust this information and accordingly acts. *V2* trusts *V1* – it means *V2* is confident to trust *V1* – to be dependent on *V1*. *V2* is dependent on *V1* because if *V1* information is malicious, *V2* will perform wrong action.

Trust decision is made analyzing (Swami et al. 2009):

- particular data which is received from particular sender in particular situation;
- information about trustee;
- and tha situation when this data was transmitted.

The similar trust description gives Gerlach 2007 where he analyses the confidence definition. He defines what is truster and what is trustee. The truster is an application and the trustee would be any entities providing context information. As entities could be nearby vehicles, on-board sensors, road side units and the like. Four major attributes that could form a trust relation in vehicular networks are distinguished by Gerlach 2007:

1. Raw sensor information, which could either be provided by on-board sensors or by means of a communication service from another nearby vehicles.
2. Higher level sensor information, i.e. information that is aggregates of several pieces of raw sensor information.
3. Services, such as a communication service.
4. Attributes, such as being a vehicle, being a police car, treating information confidential, and the like. Attributes are often modelled using certificates.

There can be several ways to express a trust. Gerlach 2007 gives several methods. One of them is taken from Pretty Good Privacy (PGP) coding, where a public key can be tagged with the discrete values: unknown, untrusted, marginally trusted, or completely trusted. Such definition is not suited for vehicular applications, because here the decision about a received message should be clear and not doubtful, i.e. a message should be either trustworthy and can be proc-

essed, or should be dropped. Another method by Gerlach 2007 proposes to use values in the interval [−1, 1) where −1 expresses complete distrust and 1 represents "blind trust". This example gives more specific expression of trust, but here still is not clear the meaning of 1, which is not included. Following example of Gerlach 2007 formalizes the trust as the conditional expectation of the reputation of the trustee given his prior encounters with the trustee. The reputation is modelled as a value in the interval [0, 1], the expected value, and hence trust, will be in the same range. Such expression well suits for vehicular applications as is compatible with the confidence index expression discussed in the first section of this chapter.

1.4.2. Privacy Concept

Dok et al. 2010 gives a definition of privacy: privacy is the expectation that confidential personal information disclosed in a private place will not be disclosed to third parties, when that disclosure would cause either embarrassment or emotional distress to a person of reasonable sensitivities. And it is added, that personal information that can be used as identification should be kept private as well.

Privacy topic is close related to a trust, because if information disseminator reveals more private information, it can be trusted more as well. In the vehicular case vehicle *V1* sends a message to vehicle *V2* and so identifies itself. *V1* together with its message data reveals private information to *V2*, i.e. for *V1* is acceptable it will be identified by *V2*. Here should be noted, that WSMP message can contain a lot of private information: coordinates, a travel direction and a goal, data for road fee or parking fee collection, etc. In such case car owner's information can be used for his spying, for targeted advertising or for criminals, when they exactly know where the certain person is located. It can be misused for financial crime as well, when electronic payment data is intercepted and copied.

To safe the privacy, identification number of the car should always be changing and transmitted messages should be encrypted. Dotzer 2005 gives a requirement list necessary to ensure privacy:

1. Use of pseudonyms as identifiers instead of real-world identities.
2. Change these pseudonyms.
3. Number of pseudonym changes depends on the application and its privacy threat model.
4. Pseudonyms used during communication can be mapped to real-world identities in special situations.

5. A set of properties and/or privileges can be cryptographically bound to one or more pseudonyms.

Privacy implementation models can be of two types: with support of infrastructure and auto regulating. Infrastructure type models can be centralized and distributed and can have a connection to the higher level infrastructure or not.

1.4.3. pNET Vehicle Social Network

The trust appears just then, when the information disseminator is known and his reputation is positive, i.e. in the past his information was truthful. In VANET the sender of information is always unknown, because its pseudonym should always change. To connect the particular sender with the receiver with always changing IDs it is necessary to have the database, where private data is stored, i.e. social network – pNET is required.

An information sender should transmit the message with its pNET key, which lets to identify the driver decoding its key in pNET database. pNET key is unique for each user and is constantly changing. The user shares its key just with his friends on the network. Drivers should always update car databases with the keys of their friends, so in this case system can work without the connection to infrastructure. The key comparison is a fast process and depends just on the car equipment processing capabilities. In this case, the information transmitted by the friends on the network can be verified very fast, for the situations when the decision should be made as soon as possible, i.e. the information about front end collision, when reaction time is less than 2 s.

It can happen, that there are no friends in the surrounding area, therefore a trustee list can be expanded by the friends of the friends. In such case the key of the received message should be checked on line with pNET database, which will require a period of time for the recipient to get an answer from pNET database. The idea to include friends of the friends in mathematical view is transitive and symmetrical, which is not the case Swami et al. 2009 defines in their paper. Here should be noted, that friends of the friends are not completely strangers and in social networks it is more likely they can be trusted in certain cases, like seeking help, etc.

The recipient should be able to check not just friend of the friends, but also the reputation index of every pNET user. The reputation index can be increased or decreased by every pNET user who sends a positive or negative feedback about the transmitted message (if message is true index is increased, if false – decreased). In such case each user can check its reputation index and in some cases even find malfunctioning sensors, which are generating false messages and negative index is growing.

pNET is useful not just to safety use, but as a social sphere as well:

- after accident happens where will be possible to check which friends are closest and to ask for help;
- people from suburbs can share their daily routes and can combine to use less cars to go to work; friends can plan their weekend activities and share it on pNET asking for other friends to join for the trip;
- friends can mark POI's or mark attractive proposals in some places, i.e. a new restaurant;
- or just to share information like in other social networks: photos, videos, messages etc.

1.4.4. pNET User Trust Index

Minhas *et al.* 2009 present user trust index calculation algorithms. The trust index value is in the range from -1 to 1, where -1 is complete distrust and 1 complete trust. Such range is not comfortable to use in vehicular application if it is necessary to align its confidence index expression. The use range from 0 to 1 is more comfortable, where 0 complete distrust and 1 complete trust. Gerlach 2007 agrees to such trust range definition.

Trust index in pNET can be expressed:

$$TI_{\mathrm{ID}} = \frac{ti_{\mathrm{poz}}}{ti_{\mathrm{sum}}}, \tag{1.3}$$

where TI_{ID} – trust index (ID – key of certain pNET user); ti_{poz} – truthful message counter; ti_{sum} – total message counter.

Counters are calculated using following expressions:

$$ti_{\mathrm{poz}} = ti_{\mathrm{poz}} + 1, \tag{1.4}$$

$$ti_{\mathrm{neg}} = ti_{\mathrm{neg}} + 1, \tag{1.5}$$

$$ti_{\mathrm{sum}} = ti_{\mathrm{poz}} + ti_{\mathrm{neg}}, \tag{1.6}$$

where ti_{neg} – malicious message counter.

TI_{ID} shown in expression (1.3) presents long term tendency, where information is stored long time, because positive and negative indexes are always summed up.

Trust index value can be changed just then, when pNET receives information from other users about correct or malicious messages. Message data should include information about event (i.e. which sensors detected event), coordinates, time and date, was the message true or false and the message originator ID at

current moment. As user ID is changing all the time, just pNET can associate ID with particular user using time stamp.

It is not always possible to get trust index value, because in Inter-Vehicle communication the connection to infrastructure is not always available. Therefore each vehicle should have database where IDs of current geographical area should be stored and database should be updated every time the connection is made with infrastructure. Each ID in the internal database should have time stamp, so it will be known when ID is obsolete and should be renewed. Renewing can be done connecting other cars as well if the connection with infrastructure is not available.

TI_{ID} trust index shows long term trend and can be used for other tasks as well, i.e. if after long time suddenly the negative index number starts growing it means, that some onboard sensors can be damaged. In such case the trust index for a long time will be positive because to change it to negative side will take a long time until number of negative indexes will be more than positive. Therefore, one more index – short time trust index is necessary. It can be calculated:

$$TI_{\mathrm{ID\_ST}} = \begin{cases} TI_{\mathrm{ID\_ST}} = 0, & TI_{\mathrm{ID\_ST}} < 0, \\ TI_{\mathrm{ID\_ST}} + \alpha - \beta, & 0 \le TI_{\mathrm{ID\_ST}} < 1, \\ TI_{\mathrm{ID\_ST}} = 1, & TI_{\mathrm{ID\_ST}} \ge 1, \end{cases} \tag{1.7}$$

where $TI_{\mathrm{ID\_ST}}$ – short time trust index; α – truthful message coefficient; β – malicious message coefficient.

$TI_{\mathrm{ID\_ST}}$ should be stored in pNET database as well and it should constantly renew when cars communicate with infrastructure. Coefficients α and β are constant and their value is defined by pNET operator. Index $TI_{\mathrm{ID\_ST}}$ changes dynamically and change rate can be limited choosing α and β values. In some cases it is more useful to have β value bigger than α which means, that to lose trust is easier than to gain it back. To set exact values of α and β additional measurements of $TI_{\mathrm{ID\_ST}}$ in certain region are necessary, because depending on communicating vehicle number, vehicle dynamic and other factors, depends how fast trust coefficient can grow or fall.

pNET concept in general works when communication is reliable. If communication is poor connection to Internet is not possible, therefore trust index can not be checked. Short term trust index will not work as well, because information about truthful and malicious messages will be kept in few cars only. This all means that having bigger traffic, velocity of the cars should be kept under certain limits in current road conditions, to have reliable communication.

1.5. Conclusions of Chapter 1 and Formulation of the Dissertation Tasks

Inter-Vehicle communication is a new radio communication field with specific – very dynamic and decentralized network topology with stochastic node connections and strict latency requirements for transmitted safety messages of different use cases. To satisfy dynamic environment and strict communication requirements, new communication standard for vehicular applications (IEEE 802.11p with IEEE 1609.x) is released in 2010. As this is a new communication field, where still exists a lack of summarized communication parameters important for vehicular communication research: one node communication range, distance between vehicles, vehicle velocity, vehicle count in one hop, permissible delay time, and use case classification.

Safety messages transmitted in VANET are facing two unsolved quality problems: delay time and lost packets. Delay time arises due to multi-hop transmission and lost packets due to radio obstacles on the road. There are few papers analyzing multi-hop delay problem, but there is no research on boundary routing schemes and their suitability to certain use cases. There are some papers analyzing vehicular obstacle influence on radio signal, but given data can not be used to create packet loss models, suitable for modelling tools.

Another issue in vehicular communication is information about safety situation representation for the driver. Driver should receive information from several sources with one unified manner in order not to get confused. Existing driver information systems concentrates on one danger parameter representation, but does not provide one confidence index calculation algorithm, which is able to combine several safety parameters.

To reach objectives following task should be solved:

1. Description of main vehicular communication parameters and use cases.
2. Definition of boundary vehicular multi-hop transmission schemes and their suitability for different use cases.
3. Analysis of packet losses, caused by obstacles. Creation of packet loss models (suitable for modelling tools) and methods to reduce lost packet number.
4. Creation of Confidence index calculation algorithm and algorithms for other confidence metrics calculation.

2

Research of Safety Message Delay

The most important task of Inter-Vehicle communication is an increased safety by means of communication. Safety objectives are implemented by sending safety messages using WSMP. Safety messages should reach destinations on time to help avoid accidents on the road. Messages can reach their destination through several communications nodes – multi-hop communication, which leads to the increased delay time.

This chapter presents the research on the safety message delay. The first part analyses safety message delay problematic and defines the main parameters for delayed messages. In the second section of this chapter, the safety message delay investigation scenario and simulation parameters are defined. Here modelling tools are used for the delay simulation. In the third and fourth sections of this chapter, the boundary delay scenarios are described and the simulation data are analyzed. The fifth section shows which routing scheme can be used for the certain safety use case. A summary is given in the last part of this chapter – conclusions.

The analysis and part of the results presented in this chapter are published by author in (Kajackas *et al.* 2009).

2.1. Safety Message Delay – Overview

The safety message transmission is the most important Inter-Vehicle communication task. These messages should reach destinations on time – they have delay limitations. As the Inter-Vehicle communication offers multi-hop capability, safety message delays can increase because of hopping influence. Several studies are performed analyzing multi-hop chains in the vehicular environment.

The multi-hop chain research is presented in (Jerbi *et al.* 2008) and is based on experiments with real cars using IEEE 802.11b technology. Different scenarios have been tested and results analyzed. The influence of hop count is shown using 3 and 6 cars in the multi-hop chain. Authors conclude, that multi-hop chain suites the needs of VANET. Though optimistic results, there are no hints to IEEE 802.11p, which differs from IEEE 802.11b. There was no background traffic generated, which influence the performance of the network.

The packet delay in legacy IEEE 802.11 is analyzed in (Khalaf *et al.* 2006). Two transmission scenarios are presented: a single-hop and a multi-hop. Theoretical curves are compared with simulated. Therefore, there are some differences from the Inter-Vehicle communication. The received packets are acknowledged, which is not the case in WAVE, where the information is broadcasted.

Information dissemination in the network should be considered by building up the WAVE communication scenarios. A unified approach for disseminating data about different types of events in a vehicle network is presented in (Cenerario *et al.* 2008). This approach is not concentrating on a specific type of information, but it is unified approach based on encounter probability calculation, which gives a reason for simulated network described in this paper.

Two MAC methods have been evaluated according to their ability to meet real-time deadlines in (Bilstrup *et al.* 2009). IEEE 802.11p carrier sense multiple access (CSMA) was examined through the simulation and the conclusion was made, that CSMA is unsuitable for the real-time data traffic. The second evaluated algorithm self-organizing time division multiple access (STDMA) will always grant a channel access regardless the number of competing nodes. Despite the results of (Bilstrup *et al.* 2009), we show that standard CSMA suits the needs of WAVE.

GeoMAC protocol, presented in (Kaul *et al.* 2008), exploits spatial diversity, inherent in a vehicular channel. Forwarder selection for transmission over the next hop is enabled in a distributed manner via geobackoff, which selects forwarders in decreasing order of spatial progress. The simulated network consists just of one hop chain, which does not answer to the real life situation, but gives a clear overview of the possibilities of GeoMAC.

2.2. Investigation Scenario and Simulation Parameters

A scenario of 5 lanes highway (Fig. 1.2) is used in this research, as it describes the maximal node number in one hop range. Following the idea described in chapter 1, the vehicle velocity is different in different lanes. Velocities are: 19.4 m/s (70 km/h), 25 m/s (90 km/h), 30.5 m/s (110 km/h), 36.1 m/s (130 km/h) and 41.6 m/s (150 km/h).

According to described conditions there are ~100 vehicles in one communication range and this number is reflected in the simulation.

Simulations were performed in NCTUns 5.0 network simulation tool (Wang *et al.* 2008) under Linux Fedora Core 9 OS. NCTUns was chosen for its advanced IEEE 802.11 model library and the ability to integrate with any Linux networking tools.

With the simulations it is intended to investigate the delays experienced by the multi-hop link in vehicle ad-hoc scenarios. All simulations are based on IEEE 802.11a PHY and MAC, however the inferences about 11p performance can be drawn as well, since the contention mechanism after the transmission collision is the same. Only one type (priority) safety message transmission is simulated, no other non-critical data transmissions are used; therefore the behaviour of IEEE 802.11a and IEEE 802.11p/IEEE 1609 is very similar, because WSM transmission method is broadcasting, which does not require acknowledgements. WSMs in IEEE 802.11p/IEEE 1609 case may be transmitted in both CCH and SCH using legacy CSMA/CA. Thus, considering contention only between safety messages, the results are valid both for legacy IEEE 802.11a and IEEE 802.11p/IEEE 1609.

The delays, introduced by CSMA/Collision Avoidance (CSMA/CA), theoretically can be evaluated by time expenditures calculation (Kajackas *et al.* 2007).The Enhanced Distributed Channel Access (EDCA) mechanism is used for uncoordinated transmission (Kajackas *et al.* 2009b). In this case, the time required to send the packet consists of the actual packet transmission duration, inter-frame times and the medium access delay:

$$t_{exp} = t_{AIFS} + \text{rand}(CW) \cdot t_{slot} + t_{packet}, \quad (2.1)$$

where t_{exp} represents total time expenditures for one packet transmission; t_{AIFS} – time required for Distributed Inter Frame Space ($t_{AIFS} = 9 \cdot t_{slot}$ for IEEE 802.11e AC0); rand() – a random number function from uniform distributions; *CW* – Contention Window; t_{slot} – slot time ($t_{slot} = 9$ μs for OFDM, IEEE 802.11a); t_{packet} – time required for data and overhead transmission consisting of physical layer preamble and header time – t_{PLCP}, 30-byte MAC header

transmission time – $t_{MAC,}$ MAC service data unit time – t_{MSDU} and 4-byte Frame Check Sequence – t_{FCS} (2.2).

$$t_{packet} = t_{PLCP} + t_{MAC} + t_{MSDU} + t_{FCS}. \quad (2.2)$$

Since no acknowledgement is required for broadcasting, no other expenditures take place.

The contention window defines the set of possible delays for back-off algorithm. Every collision in the wireless channel results congestion window to double, shifting from minimum value of $CW_{min} = 15$ to maximum of $CW_{max} = 1023$ slots for AC0 access category.

IEEE 802.11a PHY was modified to support IEEE 802.11p PHY rates. In simulations the lowest possible – 3 Mbps PHY rate was used. The lowest modulation gives the best reliability and transmission range. Considering always changing radio environment on the roads due to unexpected obstacles (large vehicles, blocking the signal, rapid fading due to movement, etc.), the ability to use higher modulations is unpredictable and may lead to failure of transmission, thus the simulations are designed for the worst-case radio transmission scenario. However, the presented results can be theoretically recalculated for any other PHY rate.

The safety messages are simulated as 500 byte User Datagram Protocol (UDP) packets. Following the idea of (Bilstrup *et al.* 2009), a packet length of 100 bytes is just long enough to distribute the position, direction and speed, but due to the security overhead, the packets are likely longer. Bilstrup *et al.* 2009 in their research use 100, 300 and 500 bytes. In this research the packet length of 500 bytes is chosen to have the biggest packet transmission time. Messages are routed through the network using the Internet Protocol v4 (IPv4). Since no movement is simulated whatsoever, static routes are used to make the controllable transmission through hops. As all simulations are generally done on IP network, the initial Time To Live (TTL) value is modified to make hopping through a large number (greater than 64) of hops possible.

All the transmissions in the simulated network use layer 2 broadcasting.

Theoretically, using PHY rate of 3 Mbps and 500 byte payload (plus 8 byte UDP header, 20 byte IPv4 header and 8 byte Logical Link Control (LLC) to form single MAC Service Data Unit (MSDU)), according to formulas 1 and 2, time expenditures for a single safety message delivery can vary from 1.621 ms to 1.756 ms if no collisions effect the contention window and wireless medium is always free to access. With more hops, the variation is higher.

2.3. Single Safety Message Transmission

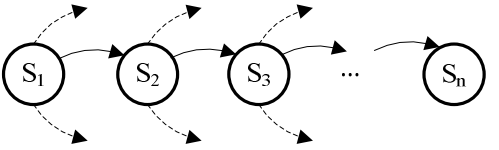

Fig. 2.1. Single safety message transmission through a multi-hop chain

The first scenario (Fig. 2.1) simulates single safety message transmission through a multi-hop chain. All nodes are located within radio transmission range and operating in the same radio channel, therefore they share the channel with equal rights. Since all the packets are transmitted as broadcasts, they are received by all stations and are not acknowledged. To control the "hopping" to one direction and to avoid broadcast storms, packets are filtered forwarding and routing them hop-by-hop, which means that packets are send in direction S_1 -> S_2 -> S_3, but not S_3 -> S_2 -> S_1.

The delay was measured at every node and delay distributions are presented in Fig. 2.2. The mean delay for 100 hops reaches 189.3 ms, minimum and maximum values respectively 184.4 ms and 194.0 ms. The delay and delay fluctuations are relatively small due to the low channel utilization. There is only one packet in the system at any given moment, therefore no contention takes place.

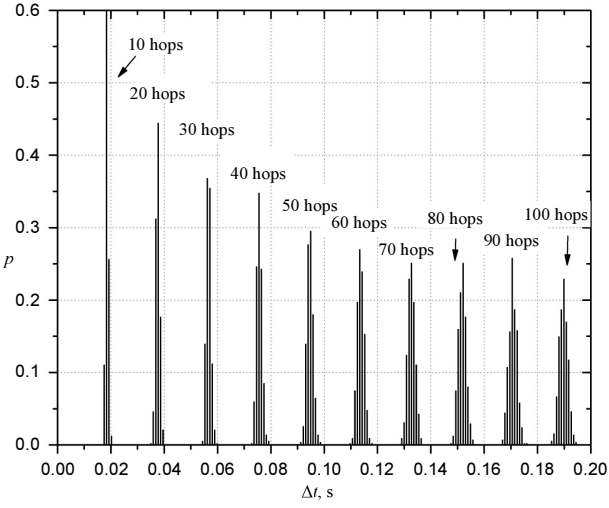

Fig. 2.2. Packet delay rate distributions for different hop number

It can be seen (Fig. 2.2) that a higher hop number introduces the higher delay time. With increasing node number, delay distributions are getting bigger as well. This happens because having a higher node number there are more possible delays caused by rand() function even if CW is constant.

However, this scenario is not realistic in VANET and is presented to give an understanding of transmission delays in perfectly controlled environment and to evaluate the minimal influence of MAC layer and physical transmission of signals. This scenario can be considered as the worst-case for reliability and the best-case for traffic load.

Another set of simulations demonstrates how channel utilization influences the delay spread.

There are several investigations on the efficient message broadcasting and for the simulations it is taken into an account, that the data dissemination with broadcasts can be controlled in the network (Wang *et al.* 2008, Kajackas *et al.* 2007, Kajackas *et al.* 2009b).

The presented simulations do not depend on the broadcasting solution and may be used to evaluate the influence of the solution on the transmission delay over different number of hops. The concept of "background traffic" has to be understood as an overhead, created by broadcasting method. A network topology remains the same, but more traffic is introduced into a network as the background traffic along with safety message stream. The background traffic is generated by neighbouring nodes on the same radio channel and has the same characteristics as measured (safety message) traffic.

One of the problems in the safety message transmission in VANET is reliable and at the same time efficient and robust broadcasting. Inevitably it has to have a significant overhead to ensure a guaranteed delivery. On the other hand, the overhead has to be reduced in order not to over utilize the radio channel, which will eventually lead to reception failures or extreme reception delays. The guaranteed reception can be achieved by acknowledging, however the messages have to spread fast, therefore, there is no time for seeking the best route in node mesh or confirm the reception. The broadcast messages cannot be acknowledged, thus the reliability has to be ensured by repeated broadcasts and neighbour retransmissions. This way the channel can be easily flooded with broadcasts degrading the network performance with excessive delays.

Fig. 2.3 shows delay distributions for different number of hops when light background traffic of 100 kbps has been applied. Delays are more spread and shifted, however the influence is relatively small due to the low channel utilization: for 100 hops the mean delay increases by 12 ms and maximum delay – by nearly 30 ms. By increasing the background traffic further, delay distributions shift and spread more (Fig 2.4-2.5).

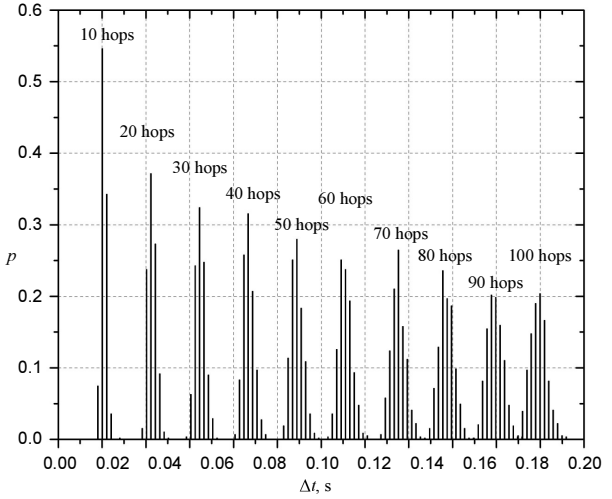

Fig. 2.3. Delay rate distributions for different hop number with 100 kbps background traffic

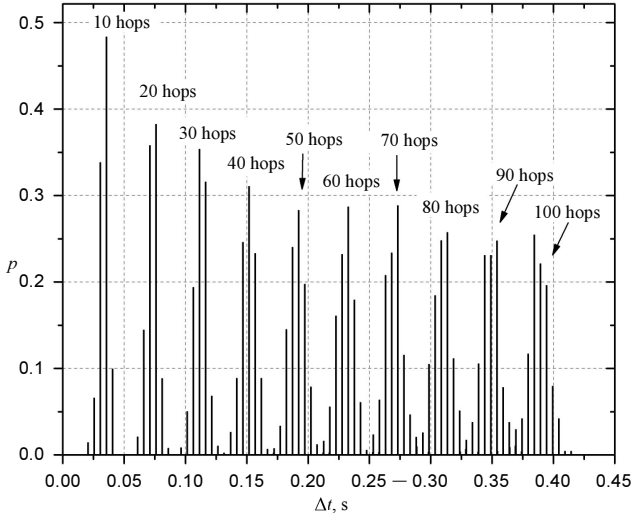

Fig. 2.4. Delay rate distributions with 1 Mbps background traffic

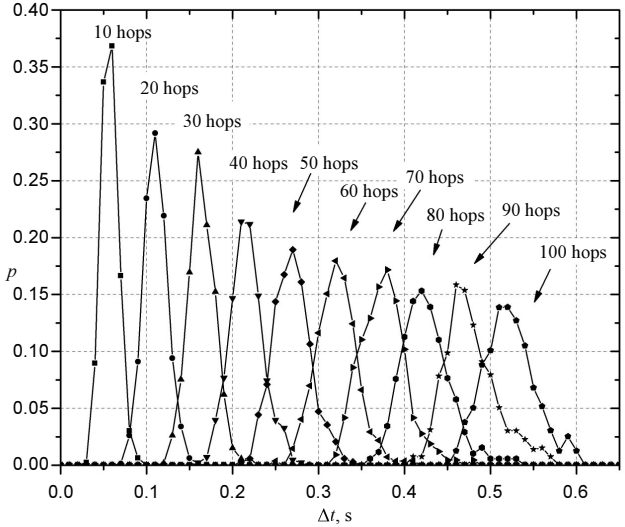

Fig. 2.5. Delay rate distributions with 2 Mbps background traffic

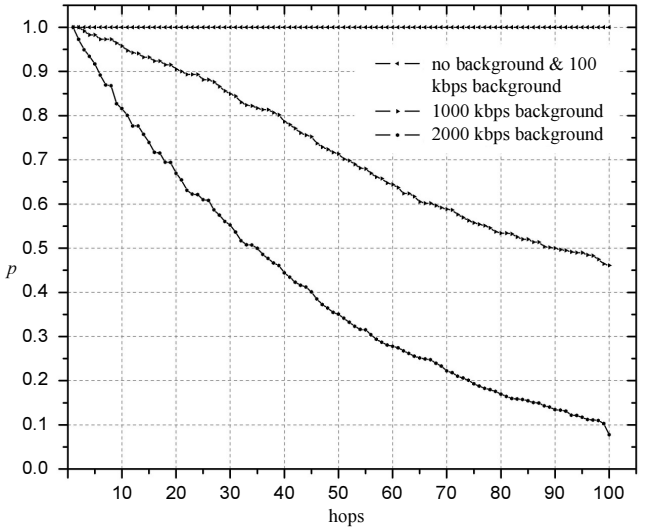

Fig. 2.6. Packet survive probability for different hop number

Fig. 2.4 shows delay distributions with 1 Mbps background traffic and Fig. 2.5 – with 2 Mbps background traffic. Those graphs do not include lost packets. With the significant background traffic, the contention for transmission becomes harsh and the probability of collision increases causing a packet loss. Since broadcast packets are never acknowledged, lost packets are not resent and

hopping through node chain brakes. Fig. 2.6 shows the probability for a packet to survive different number of hops.

Table 2.1. Results summary for 100 hops

Background traffic, kbps	Mean delay, s	Minimum delay, s	Maximum delay, s	Standard deviation
0	0.189	0.184	0.194	0.00173
100	0.218	0.209	0.230	0.00383
1000	0.386	0.355	0.411	0.00839
2000	0.523	0.458	0.603	0.03083

The result summary for 100 hops is presented in Table 2.1. It is shown, that by increasing background traffic the mean delay is growing proportionally and standard deviation is increasing. This means, that with growing background traffic the delay can vary in wider time range.

2.4. Controlled Flood Transmission Scenario

One of the ways to improve a reliability of multi-hop links is to make redundant paths to every node of the network. Flooding the network with broadcasts may seem the reliable way to ensure the message reception for every network node. Since the transmit range is not always known due to the ever-changing environment, every node in the network has to retransmit (rebroadcast) emergency message assuming that it may be at the transmission range edge of the message initiator. For this scenario an algorithm, controlling the floods must be employed, otherwise packet loops will cause broadcast storms (similarly as in looped Ethernet), which eventually will lead to the channel congestion. One way to avoid loops could be GPS coordinate tracking and making sure, that broadcasts are being forwarded only in one direction (similar as in Kaul *et al.* 2008). This can be tricky while considering a movement of vehicle. Another simple way – logging retransmitted node IDs: all nodes, retransmitting broadcast packets, put their ID into the frame body; before resending received packet, the node always searches this ID list; if own ID is found, the packet is dropped assuming it is in the transmission loop.

The controlled flood scenario is implemented in NCTUns 5.0 using same nodes and traffic characteristics as defined in previous section. The network topology is depicted in Fig. 2.7.

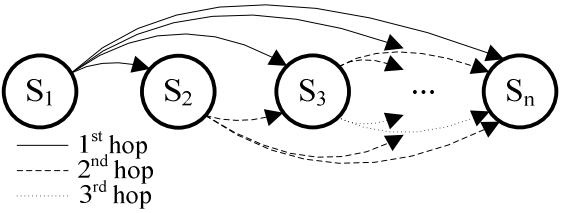

Fig. 2.7. Controlled Flood Scenario network topology

S_1 is the originator of safety message, which is broadcasted through the network. Every other node broadcasts the same message again following basic rule: if source ID is lower than own ID, then message should be broadcasted. Otherwise – received packets have to be dropped.

This way the network is flooded with the message copies, but no broadcast loops appear. This scenario can be considered as a worst-case for traffic load and a best-case for reliability.

Delay distributions for 10 and 20 hops scenario are presented in Fig. 2.8 and Fig. 2.9. The delays were measured at every node.

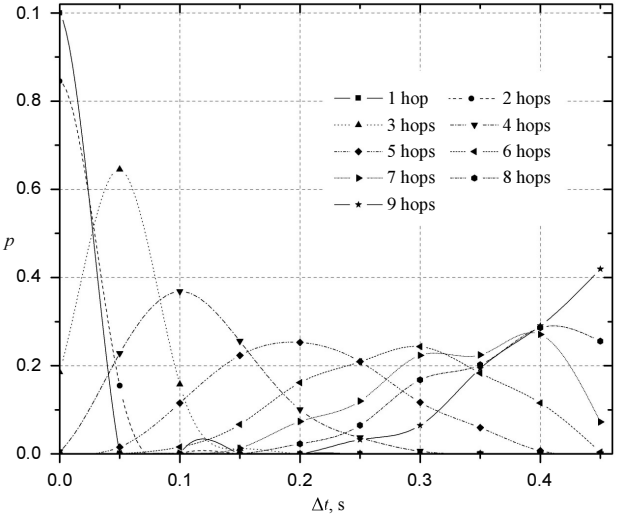

Fig. 2.8. Delay rate distributions in 10-node controlled flooded scenario

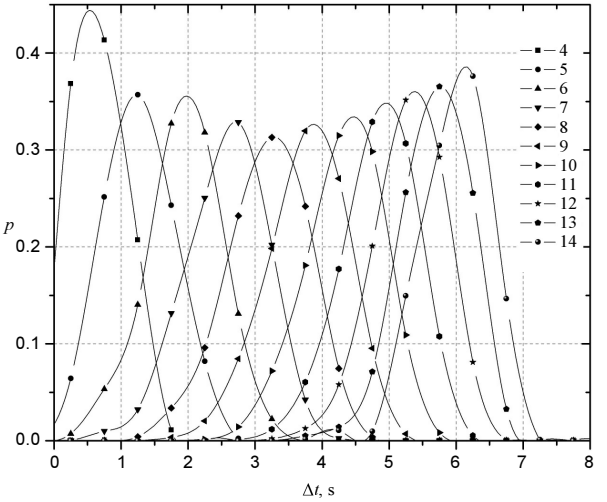

Fig. 2.9. Delay rate distributions in 20-node controlled flooded scenario

Since the broadcasts from any node are received by all other nodes and re-transmitted by all with the ID higher than source ID, increasing node (hop) number, the packet copies in the system grows exponentially. It can be seen (Fig. 2.8-2.9), that 10 node scenario shows quite reasonable delays, reaching 500 ms for all 9 hops, however doubling node number in the scenario it will result in excessive delay increase, mean value reaching almost 4 seconds for 9 hops and 7 seconds for 19 hops. The main cause is the higher collision probability.

2.5. Multi-Hop Delay Discussion

The main tasks of Inter-Vehicle communication are safety, traffic efficiency and infotainment. The delay time is most critical for emergency use case, where safety messages should reach their receivers on time. The delay time is also important for some infotainment applications, like a live video streaming, but safety messages should always have priority over infotainment packets and, therefore, this paper does not analyse infotainment use case.

Latency times, for emergency use cases, are given in Table 1.4. They can be grouped into several parts: 20, 100, 500, 1000 and more than 2000 ms. Most of allowed latency times are less than 2 s headway time. This means, that boundary hopping scenarios should be assessed for these use cases. Table 2.2 presents analysis of the node number, which can be used for certain use case.

Table 2.2. Allowed hop number for different routing schemes

Routing scheme / Latency time, ms	Single 0 Mbps	Single 1 Mbps	Single 2 Mbps	Controlled flood, 10 nodes	Controlled flood, 20 nodes
20	10	(No data <10)	(No data <10)	<1	(No data <4)
100	60	20	10	2	(No data <4)
500	>100	>100	70	7	(No data <4)
1000	>100	>100	>100	>10	(No data <4)
2000	>100	>100	>100	>10	4

Data given in Table 2.2 can be used creating safety message routing algorithms. It is shown, that a hop number should not be more than 10 nodes to keep 20 ms delay. Safety messages of current use case should be routed using the least reliable routing schemes, as more reliable routing will introduce a longer delay. The most reliable routing scheme – controlled flood scenario (20 nodes), can be used only for routing messages from use case with 2 s allowed latency. This scenario can be used for 100 ms latency only, if complete chain consists of 10 nodes and routed node number drops to 2 nodes.

2.6. Conclusions of Chapter 2

1. VANET is a decentralized network with many stochastic nodes, where information is sent using multi-hop communication. The main task of VANET is to deliver safety messages in time, therefore, boundary routing schemes in multi-hop are investigated.
2. It is shown that the delay in IEEE 802.11 multi-hop transmission depends on the following major components: the physical signal transmission, which depends on PHY rate and a distance; and the contention, which depends on the channel utilization.
3. The problem of safety message transmission is two-fold: the transmission has to be reliable and transmission delays have to stay in strict limits and this requirement defines two boundary routing sce-

narios: a single message (the smallest delay) and the controlled flood (the highest reliability).

4. Simulations show, that routing scheme should be changed depending on use case: for 20 ms latency only single message routing without background traffic can be used; for 2 s latency control flood scenario of 20 nodes can be used.
5. The number of nodes depends on maximal allowed latency time of current use case. The number of nodes is given in Table 2.2.

3

Research of Safety Message Loss

Inter-Vehicle communication equipment deployment is a long term process. Hill *et al.* 2011 says that it will take around 13 years from a day zero to reach 90% equipped vehicles on the road in the US. This means that in this time period there will be a great deal of non-equipped vehicles, which will result in many obstacles for Inter-Vehicle communication blocking LOS path.

This chapter presents an experimental study on the impact of vehicles as obstacles for the radio signal on the road and gives detailed analysis of lost packet trend. The lost packet trend can be approximated and approximation polynomials for Non LOS (NLOS) and LOS cases are calculated.

Lost packets have a tendency to build groups, i.e. 1 lost packet, 2 lost packets, *n* lost packets in a row. The most simple approximation algorithm describing lost packet grouping is geometric distribution. Lost packet groups can also be expressed with Gilbert-Elliott and *N*-State Markov models, which properties are discussed and given in this chapter as well.

Means to reduce the number of lost messages are analysed in this chapter as well. A proposed method is based on the redundant safety message transmission, which is proven to increase the safety message reception at receiver.

The analysis and part of the results presented in this chapter are published by author in (Kajackas *et al.* 2012).

3.1. Obstructed Vehicular Communication Overview

A rapidly changing network topology and highly mobile nodes have impact on throughput (Ipatovs *et al.* 2011, Petersons *et al.* 2011), packet loss and other communication parameters. Therefore, it is necessary to investigate communication conditions very accurately before engineering V2V and Vehicle to Infrastructure (V2I) communication systems.

The V2V propagation channel has a strong impact on the coverage, reliability, and real-time capabilities of V2V networks. Wrong assumptions about the fading lead to erroneous conclusions on the effectiveness of Inter-Vehicle warning systems at intersections. (A.F. Molish *et al.* 2009) provide an overview of existing V2V channel measurement campaigns, describing the most important environments.

Realistic models of propagation channel for V2V scenarios are different for LOS conditions and in obstructed case, when neighbouring cars are obstacles for radio propagation path and so compose NLOS conditions. A set of experiments, investigating an impact of vehicular obstructions in VANET's, is done in (Boban *et al.* 2011). Here authors identify the problem of wireless signal obstructions in VANET.

A set of experiments, investigating impact of vehicular obstructions in VANET, is done in (Meireles *et al.* 2010). Two types of experiments are performed: parking lot experiments and on the road experiments. In parking lot experiments Received Signal Strength Indicator (RSSI) value, which depends on distance and obstructing vehicle, is shown. RSSI attenuation can come up to 20 dB, which means, that it will reduce radio coverage. In LOS condition packet delivery ratio does not depend on the area (highway, suburban and urban), but on vehicles blocking the LOS. For the same distance between a sender and a receiver in NLOS condition packet delivery ratio in suburban and urban areas is smaller than in highway, as in highway cars are moving faster and distances between cars are bigger – less obstacles.

The results presented in the paper (Boban *et al.* 2011) inform on the impact of obstructing vehicles on V2V communication, particular on the mean packet delivery ratio. However, there is no information about a packet loss, about the loss correlation and grouping as this is important for developing ensured safety message transmission systems.

3.2. Experimental Conditions

3.2.1. Setup

We designed a set of experiments using two vehicles equipped with WLAN devices to characterize the impact of vehicles as obstacles. As WLAN equipment Acer Aspire One D250 notebooks, with integrated IEEE 802.11b/g network cards Atheros AR8132, working on 2.4 GHz frequency band. IEEE 802.11g mode channel 11, were used. Used 2.4 GHz frequency will have some differences from defined 5.9 GHz in IEEE 802.11p. Higher frequency more clear line of sight conditions, wherefore were will be a little bit more lost packets due to obstacles, but trend will remain the same.
Notebooks with network cards were installed on the roofs (approx. 1.4 m height) of the cars to eliminate the influence of car structure and to make it more close to IEEE 802.11p equipment, which will use external antennas on the roofs of the cars.

A web camera was installed at receiver PC, to be able to relate the lost packet trend to passing cars.

For signal generation LanTraffic v2 software (*http://www.zti-telecom.com /EN/LanTrafficV2.html*) was used. 500 bytes long, UDP packets were generated. Packets were marked to make it possible to find the lost ones. Wireshark v1.6.1 (*http://www.wireshark.org/*) was used for packet transmission at the transmitter side and for packet receiving at the receiver side. Received packet time, data and other parameters were registered.

3.2.2. Scenario

The objective of this experiment is to measure the influence on the packet loss of passing cars between a transmitter and a receiver. For this reason, an experiment is split into two parts: the LOS measurement and the obstructed measurement. The LOS measurement gives the distance limit, up to which is possible to estimate the influence of only those cars which cross the communication path.

Primary measurements are performed each 25 m up to 350 m in LOS. In this LOS case 200 m was the limit, at which packet loss starts happen. For obstructed measurement it is done up to 225 m.

Experiment was performed at a long and straight road, far away from obstructing 2.4 GHz devices (Fig 3.1).

Fig. 3.1. Satellite view of experiment area (source Google Maps)

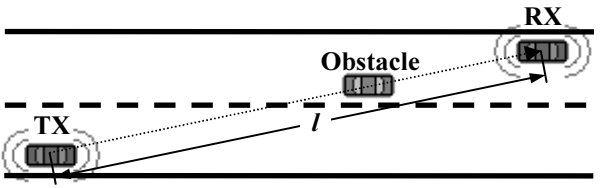

Fig. 3.2. Vehicle arrangement (here l – distance between cars)

The sending vehicle was positioned on one side of the road and the receiving vehicle on another side of the road as shown in Fig. 3.2. Each passing vehicle crosses LOS of a transmitter and a receiver. Such transmitter and receiver arrangement presents dangerous situation, e.g., one of communicating cars takes over a non-equipped vehicle; communicating cars are driving on different sides of the road. The similar conditions appear, when one of communicating cars is driving near a cross section.

3.2.3. Results

To investigate the vehicle obstruction problem we performed packet delivery measurements for different distances *l* between the cars without obstacles – LOS measurements, and on the same road for the same distances with obstacles between cars – passing cars and trucks. An experiment was performed from 25 to 350 m for LOS and from 25 to 250 m NLOS cases. Measurements for each distance were performed three times sending up to 20000 UDP packets.

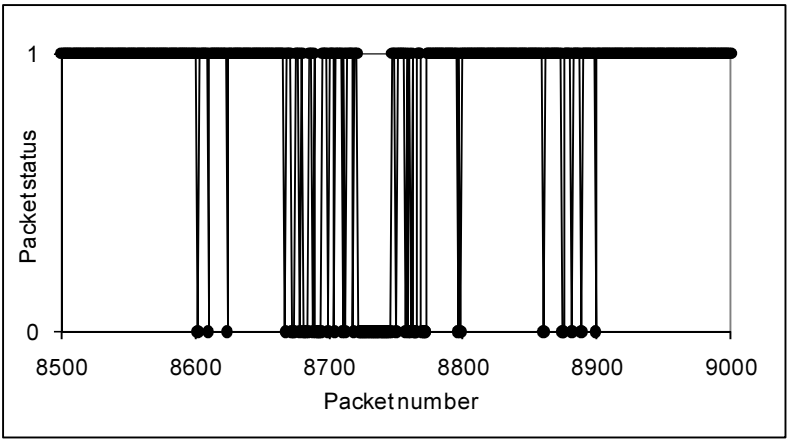

Fig. 3.3. Example of packet loss trace in obstructed measurement ("0" – corresponds to received packet, "1" – to lost)

Fig. 3.4. Passing cars snapshot – 150 m 1st obstructed measurement

A video camera was used during experiments, as video records were necessary for data analysis. An example of influence of approaching and passing cars on packet loss is shown in Fig. 3.3. Here "0" represents arrived packets, and "1" shows lost packets. Observing video records we clearly distinguish, when LOS is blocked, packets are being lost. When LOS is clear, all packets reach a receiver. A snapshot from Video record reflecting the lost packet trend shown in Fig 3.3 is presented in Fig 3.4.

LOS and NLOS packet loss ratio measurement results are shown in Fig. 3.5 and Fig. 3.6. Here should be noted, that in LOS case, a packet loss happens quite often, when the distance between cars is more than 200 m. And for LOS case no

packet loss was detected up to 200 m. In NLOS case lost packets occurs when distance is 25 m, which means, that this loss is dependent on obstacles, when LOS is blocked by the other vehicles on the road.

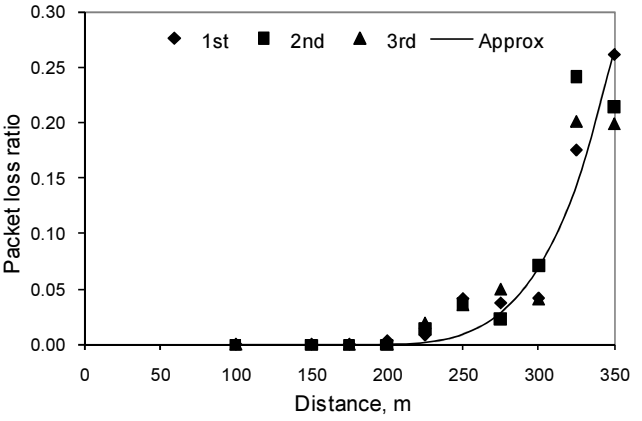

Fig. 3.5. Packet loss ratio respect to distance between cars – LOS conditions

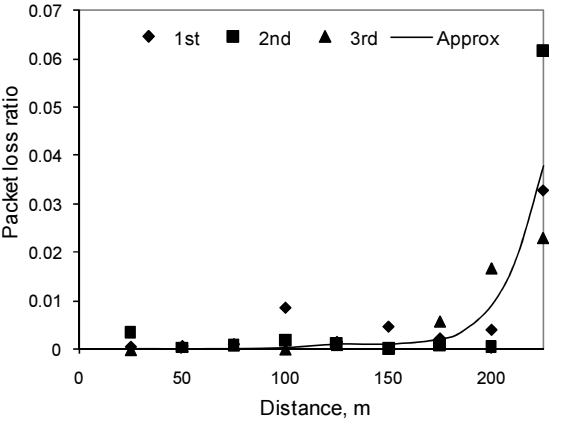

Fig. 3.6. Packet loss ratio respect to distance between cars – NLOS conditions

Packet loss result data cannot be directly used for simulation tasks. For this purpose, approximation curves should be found. Results of experiment show that the packet loss ratio is dependent on the distance and can be approximated using polynomials given in following equations.

For LOS approximation equation is:

$$p_{\mathrm{LOS}}(l) = A(l-175)^2 + B(l-175)^4, \tag{3.1}$$

where $A = 1 \cdot 10^{-7}$; $B = 2.8 \cdot 10^{-10}$; l – distance.

For NLOS approximation equation is:

$$p_{\mathrm{NLOS}}(l) = \begin{cases} A(l-50)^2, & \text{when } l < 110, \\ A(l-50)^2 + C(l-150)^4, & \text{when } l \geq 110, \end{cases} \tag{3.2}$$

where $A = 1 \cdot 10^{-7}$; $C = 1.1 \cdot 10^{-9}$; l – distance.

Parameters A, B and C are found using the root mean square error criterion. The fourth order polynomials are taken, to reach the closest approximation to measured values.

The given results show that packets are lost more frequently when a distance between communicating cars is increasing. It means that weaker signals are reaching the receiver. In NLOS case a packet loss happens in the smaller distance than in LOS case. The difference of this distance is 100 m and corresponds to 10% packet loss. It shows that the reception of emergency signals in NLOS case is worse.

Here should be noted, that in emergency situations, when cars are braking, distances between cars are getting smaller and the communication conditions are getting better. The packet loss, caused by obstacles, is getting smaller.

3.3. Lost Packet Group Research

Lost packets are forming groups[1] (as presented in Fig. 3.3), which depend on the shielding strength and the speed of the obstacle. The distribution of lost packet group occurrence rate for NLOS is shown in Fig. 3.7. Here it can be seen that lost packet groups up to 5 lost packets appear the most often. Longer lost packet groups appear less often and a group of 25 or more lost packets is very rear.

Lost packet group distribution, shown in Fig. 3.7, can be approximated using different approximation methods. Following sections shows approximation using geometric distribution, Gilbert-Elliott and *N*-State Markov models.

[1] Lost packet group is the number of lost packets in a row, i.e., 1 lost packet, 2 lost packets in a row, 3 lost packets in a row, *n* lost packets in a row.

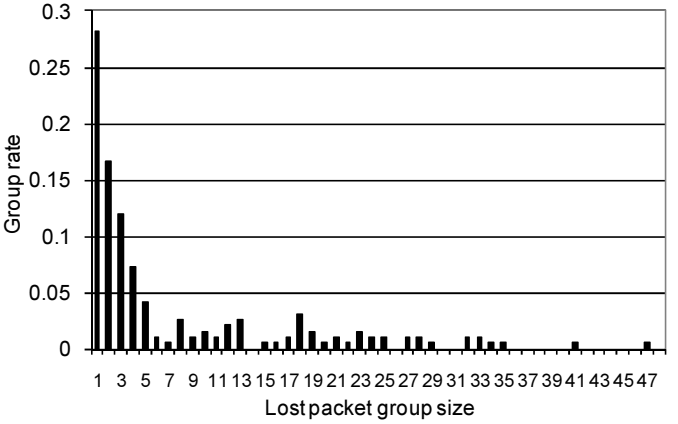

Fig. 3.7. Lost packet group rate distribution

3.3.1. Geometric Distribution Model

The most simple lost packet trace approximation is a model of geometric distribution. It is expressed:

$$q_i = (1-\alpha)\cdot\alpha^i, \tag{3.3}$$

where i – packet group size; i = 0,1,2,... . Coefficient α is also found using the root mean squared error criterion. For current case (Fig. 3.8) α is 0.62.

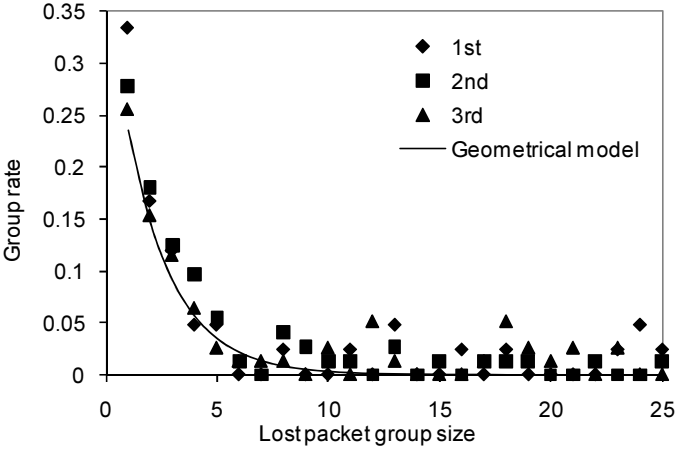

Fig. 3.8. Lost packet group rate compared with geometrical distribution approximation

The model of geometrical distribution is very simple and easy to implement. There is only one variable α, which influences a shape of the curve. Therefore, it suites Inter-Vehicle communication modelling tools, as it does not require many calculation parameters, which can be hard to gather for every situation on the road. The drawback of this model – it is not very precise, because it gives just a trend of all groups with one curve.

3.3.2. Gilbert-Elliott Model

Gilbert-Elliott model is two state Markov chain with states "1" – lost packet and "0" – arrived packet (Fig. 3.9).

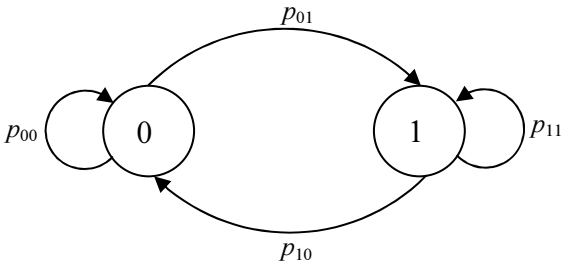

Fig. 3.9. Gilbert-Elliott model

Gilbert-Elliott model generates the chain of "1" and "0". In current research "1" represents lost packet and "0" – received packet.

Chain state probabilities are expressed as following:

$$PE_{GE} = \begin{pmatrix} p_{00} & p_{01} \\ p_{10} & p_{11} \end{pmatrix}, \tag{3.4}$$

where PE_{GE} – error rate for Gilbert-Elliott model.

In this case probabilities p_{00} and p_{11} are independent from each other. Probabilities p_{01} and p_{10} are expressed:

$$p_{01} = 1 - p_{00}, \tag{3.5}$$

$$p_{10} = 1 - p_{11}. \tag{3.6}$$

Following formulas (3.5) and (3.6) probability that one packet will be lost is p_{01}. Probability, that two packets in a row will be lost is $p_{01} \cdot p_{11}$, for three packets $p_{01} \cdot p_{11} \cdot p_{11}$ and so on.

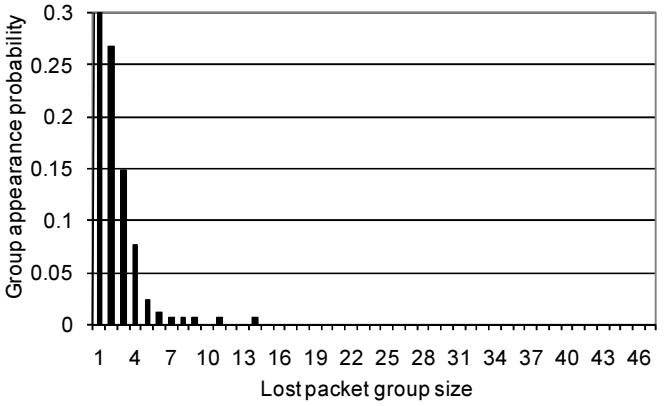

Fig. 3.10. Lost packet group in Gilbert-Elliott model

Data given in Fig. 3.10 show how lost packet groups are distributed using Gilbert-Elliott model. For current modelling probabilities are p_{01} = 0.58 and p_{11} = 0.07.

Gilbert-Elliott model suits very well for situations, where small groups are dominant, because it is very small probability to get the group longer than 15 lost packets. Another advantage is that this model does not require many parameters to add and chain implementations logic is simple.

3.3.3. *N*-State Markov Model

N-state Markov model gives the opportunity to generated very accurate packet loss trend, because here the probability of each lost packet group can be defined independently. Markov model is showed in Fig. 3.11.

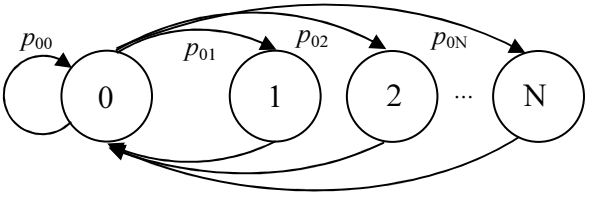

Fig. 3.11. *N*-state Markov model

N-state Markov chain (Fig. 3.12) generates lost packet rows separately. Here state "0" means received packet and states "1", "2" … "*N*" are lost packet chains with 1, 2 ... *N* lost packet in a row.

Lost packet group appearance probabilities generated using this model are shown in Fig 3.12.

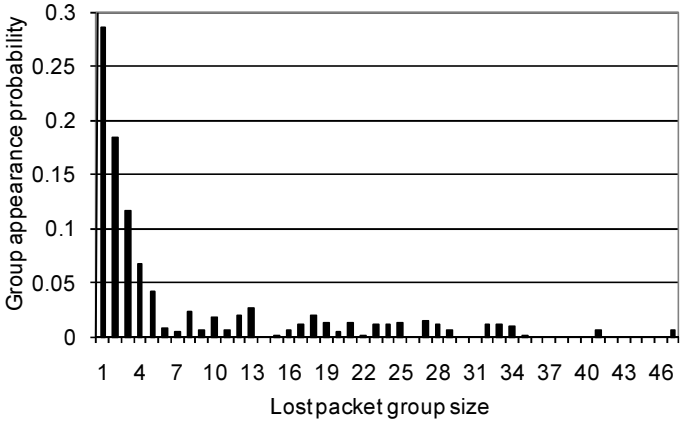

Fig. 3.12. Lost packet group rate in *N*-State Markov model

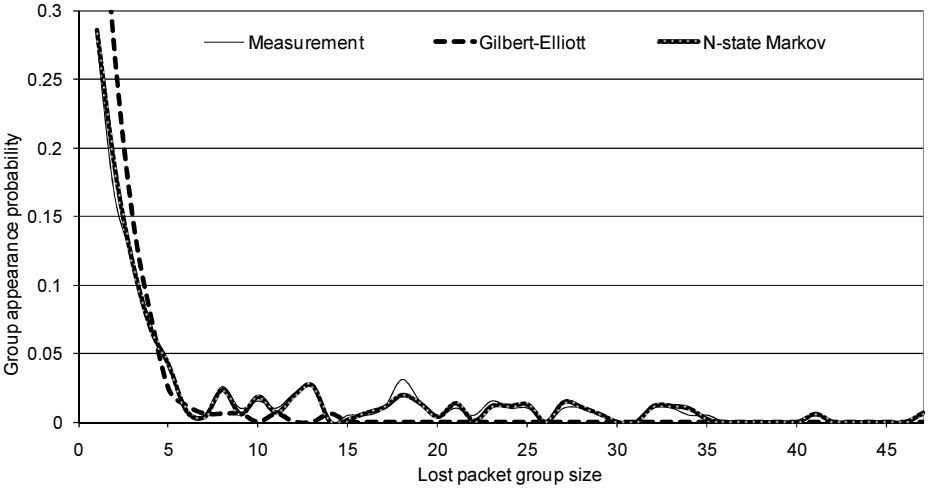

Fig. 3.13. Comparison of lost packet group rate model

Probability parameters of each group from 1 to 47 equals to probability of each group from measurement (Fig. 3.7). Therefore *N*-state Markov model is very accurate and using it generated data (Fig. 3.12) is very close to measurement results.

N-state Markov model is more accurate than Gilbert-Elliott model, but needs more data, because each state probability should be defined separately.

Comparison of Gilbert-Elliott model, *N*-state Markov model and measurement is shown in Fig. 3.13. There can be seen, that *N*-State Markov model is very accurate, and is following the measured curve very closely. Gilber-Elliott model is less accurate and has some difference from measured values.

3.4. Communication Loss Time

In NLOS condition some packets are lost and they are building lost packet groups. These packet losses are very important in emergency situations. When a vehicle is transmitting an safety message, triggered by the accident on the road, the communication may fail, because of obstacles on the road and safety messages may not arrive to destinations.

Mean delay time is calculated using following equation:

$$\tau_{\text{mean}} = \text{T}\sum_{i=1}^{47} i \cdot P_i \,, \tag{3.7}$$

where τ_{mean} – mean delay time; T – one packet transmission period (T = 1.2 ms); i – packet group size; P_i – packet group rate.

In current experiment τ_{mean} = 9.5 ms, this is relatively short, but can vary. Delay time varying characteristic is presented by the Cumulative Distribution Function (CDF) (Fig. 3.14).

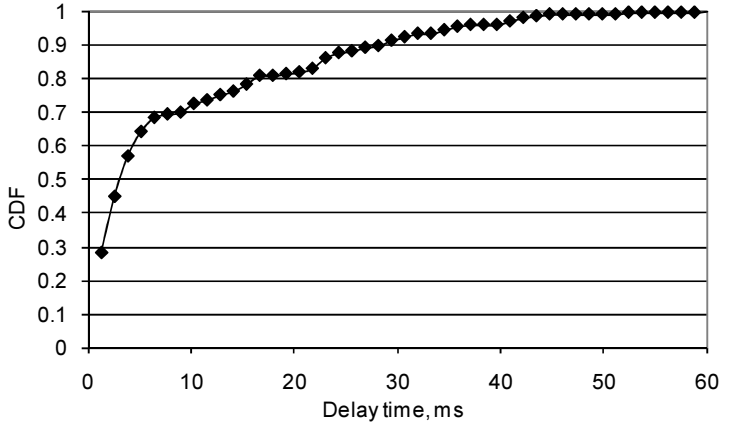

Fig. 3.14. Delay time cumulative distribution function

In (3.7) calculated mean delay time is relatively small, and fits to requirements of Inter-Vehicle communication, but calculated CDF shows, that the delay time can come up to 60 ms, which can be the problem for some communication tasks (NHTSA 2005): platooning (latency time 20 ms), pre-crash sensing (latency time 20 ms), free-flow tolling (latency time 50 ms).

Experiment data gives opportunity to investigate the duration of packet loss. When packet group i is lost, then the duration of communication channel loss is:

$$\tau_i = (i+1)\cdot \mathrm{T}\,, \tag{3.8}$$

where T – packet transmission period.

The cumulative probability distribution function, for packet loss smaller than kT, using lost packet group geometrical distribution, is expressed as following:

$$P(\tau \le k\mathrm{T}) = (1-\alpha)\cdot \sum_{i=0}^{k} \alpha^i = (1-\alpha^k)\,. \tag{3.9}$$

The parameters of lost packet group rate geometrical distribution depend on the distance between communicating cars. The results are shown in table 3.1.

Table 3.1. Parameter α dependency on distance for LOS and NLOS cases

NLOS		LOS	
Distance, m	α	Distance, m	α
225	0.78	325	0.85
200	0.51	300	0.77
175	0.5	275	0.77

IEEE 802.11g equipment was used in the experiment, which has made the influence on the packet transmission time. With changing communication condition, the data rate has slightly changed.

3.5. Communication Channel Model

The Inter-Vehicle communication has significant differences from other radio communication types – communicating nodes are dynamic, changing their locations rapidly with high speeds. An Inter-Vehicle network is full of changing nodes with changing communication channel parameters. In order to understand

the behaviour of Inter-Vehicle communication the channel radio wave propagation models should be analyzed.

The behaviour of link layer of Dedicated Short Range Communications (DSRC) is analyzed by Bai *et al.* 2006 from "General Motors". V2V communication is analyzed in a wide variety of traffic environment based on the experimental data. Here the authors point out that the reliability of communication channel is quite high, when single packets are lost, but gets worse if series of packets are lost. The measurements in this paper are done periodically (every 100 ms) sending packets. It is shown, that series of packet can be lost in on road experiments.

In order to explain series of lost packets, the models of radio wave propagation are created and analyzed. A propagation model tries to approximate the strength of the received signal, using parameters like the transmission power, distance a sender and a receiver.

It is well known propagation influencing factors: LOS loss, shadowing and multipath fading. There are many papers describing propagation models starting from simple free space models up to complex deterministic and probabilistic models (Eenennaam 2008). A deterministic model allows computing the received signal strength, based on particular properties of the environment.

If a transmitter sends a signal $s_1(t)$ in time period $0 \le t < T$, then, taken into account that the signal will travel several paths, the channel reaction can be described:

$$x_{\Sigma}(t) = \sum_i \kappa_i \cdot s_{li}^{*}(t - \tau_i), \tag{3.10}$$

where κ_i – i-th path transmission coefficient; s_{li} – signal at receiver; τ_i – i-th path signal delay.

In vehicular case the simplest is a two-variable model, which includes one LOS wave and another wave reflected from the road.

Stochastic several path radio channel models are created taking into an account radio wave propagation aspects and assuming that: signals are arriving from different paths, their number n is random, an independent signal component travels each path, amplitude and a delay of each component is random and changing. This channel's impulse response is expressed as a sum of Dirac delta functions:

$$g(t) = \sum_{i=1}^{n} \kappa_i \delta(t - \tau_i), \tag{3.11}$$

where κ_i and τ_i are the same as in (3.10). In this model all variables κ_i, τ_i and n are random.

Models described in (3.10) and (3.11) are referred to a small-scale model group. But there are also large-scale models, which are focusing not to instantaneous values, but on the mean values calculated for some period of time. Large-scale models are applied, when the task is to estimate a pattern of signal power change. The initial assumption for these models is – harmonic signal $s(t)=A_0\cos(\omega t+\varphi_0)$ is send to the channel. This signal will reach a channel exit – the receiver antenna in n different paths, there will be n reactions, and on the output pins will be sum of these reactions:

$$s_x(t) = A_0 \sum_{i=1}^{n} \kappa_i \cos[\omega(t-\tau_i)+\varphi_0]. \tag{3.12}$$

(3.12) equation can be easily transformed to:

$$s_x(t) = a_x \cos\omega t + b_x \sin\omega t = A_x \cos(\omega t - \varphi_x), \tag{3.13}$$

where

$$\begin{aligned} a_x &= A_0 \sum_{i=1}^{n} \kappa_i \cos(\omega\tau_i + \varphi_0), \\ b_x &= A_0 \sum_{i=1}^{n} \kappa_i \sin(\omega\tau_i + \varphi_0), \\ A_x &= \sqrt{a_x^2 + b_x^2}, \\ \varphi_x &= \arctan(b_x / a_x). \end{aligned} \tag{3.14}$$

When one of the stations is moving, or communication conditions are changing, parameters κ_i and τ_i are changing randomly; therefore randomly changes transferred signal amplitudes a_x and b_x (they can get negative as well). Theoretical boundary – random variables a_x and b_x become normal, when a channel has many paths ($n \to \infty$).

When narrowband signals are transmitted over such channel, all signal component amplitudes and phases are changing together, selective frequency dependent fading do not exist. General signal level changes are characterized as the multiplicative disturbance, which probability features are well expressed with Rice probability density function:

$$p(r) = \frac{r}{\sigma^2} \exp\left(-\frac{r^2 + A^2}{2\sigma^2}\right) I_0\left(\frac{Ar}{\sigma^2}\right), \quad r \geq 0, \tag{3.15}$$

where σ^2 – dispersion describing signal level scatter; A – LOS path wave amplitude; $I_0()$ – Bessel function.

A given model describing conditions is called Rice channel. The rice channel model is applied, when LOS wave reaches a receiver. It means no reflections are happening and a path from the transmitter antenna up to the receiver antenna is not blocked.

When there is no LOS between a transmitter and a receiver (A = 0) and many reflected waves are getting to the receiver antenna, Rice probability density function (3.15) gets simpler:

$$p(r) = \frac{r}{\sigma^2} \exp\left(-\frac{r^2}{2\sigma^2} \right). \tag{3.16}$$

Function (3.16) is called Rayleigh law. This model is called Rayleigh channel. The model is applied when there is no LOS (Zajic *et al.* 2006, Borries *et al.* 2007). Rice and Rayleigh models are quite accurate describing communication conditions, when the wave path number is high (Xiao *et al.* 2003). Feasibility of these models in urban, rural or motorway environments using empirical measurements and a simple channel model is performed in papers (Cheng *et al.* 2007, Taliwal *et al.* 2004).

The analysis performed in (Yin *et al.* 2006) reveals that fading can be approximated by Rice distribution within 100 m, while it seems to follow Rayleigh distribution beyond 100 m.

For vehicular environment Rice and Rayleigh models are not always accurate enough. Better results are achieved using Nakagami model (Yin *et al.* 2006). The Nakagami distribution has been shown to fit the amplitude envelope of empirical data well, and is, therefore, widely used as a generic fading model for wireless channels (Yin *et al.* 2006). The probability density function of Nakagami fading can be expressed as:

$$f(x) = \frac{2m^m x^{2m-1}}{\Gamma(m)\Omega^m} \exp\left[\frac{mx^2}{\Omega} \right], \quad x \geq 0, \quad \Omega > 0, \quad m \geq \frac{1}{2}, \tag{3.17}$$

where m – shape parameter; Ω – spread of the distribution.

If the signal amplitude follows the Nakagami distribution, the power of the signal follows the Gamma distributions, given by:

$$p(x) = \left(\frac{m}{\Omega} \right)^m \frac{x^{m-1}}{\Gamma(m)} \exp\left[-\frac{mx}{\Omega} \right], \tag{3.18}$$

where $\Gamma(m)$ – complete gamma function of parameter m.

When m = 1, the Nakagami distribution becomes the Rayleigh distribution, which models a harsh NLOS scenario. When m > 1, it approximates the Ricean distribution, r closely models begin of LOS scenario. When m < 1, fading repre-

sented by the Nakagami distribution is even more severe than by Rayleigh distribution. For different distance estimated m values could be very different due to the different fading statistics for a particular operating environment.
A successful wireless packet reception is determined by a number of influencing factors, such as radio wave propagation and interferences issuing from simultaneous transmissions. However, if only a single sender is considered, the effects reduce to the specifics of the environment and thus to the radio propagation. Under this assumption, it was shown in (Killat *et al.* 2007) that the probability of message reception can be analytically derived from the Nakagami $m = 3$ model as follows:

$$P_R(x,\delta,\psi,f) = P_R^{\text{single}}(x,\psi) = e^{-3(x/\psi)^2}\left(1+3\left(\frac{x}{\psi}\right)^2+\frac{9}{2}\left(\frac{x}{\psi}\right)^4\right), \qquad (3.19)$$

where ψ – transmission power; f – rate, x – distance to the sender.

In order to verify how the existing models reflect inter-vehicle wave propagation shielding effect experiment data was compared to Nakagami model results. The results of performed measurements show, that a packet loss ratio is dependent on the distance and can be approximated using algebraic polynomials (3.1) and (3.2).

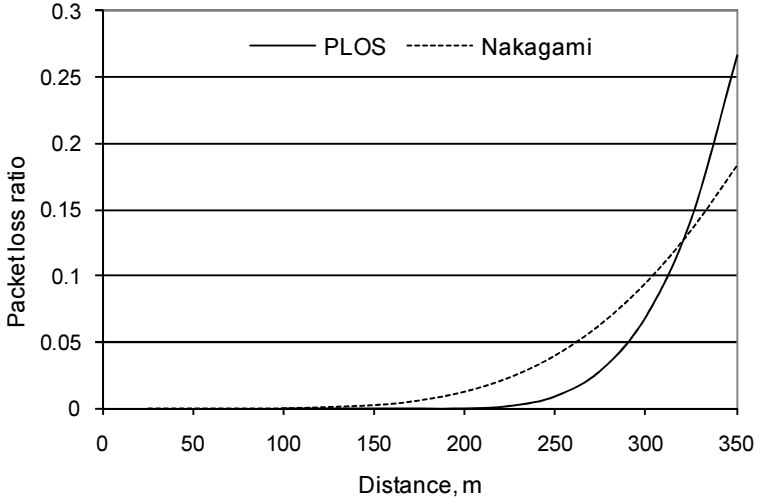

Fig. 3.15. LOS Lost packet ratio depending on distance using approximation model (3.1) and Nakagami model

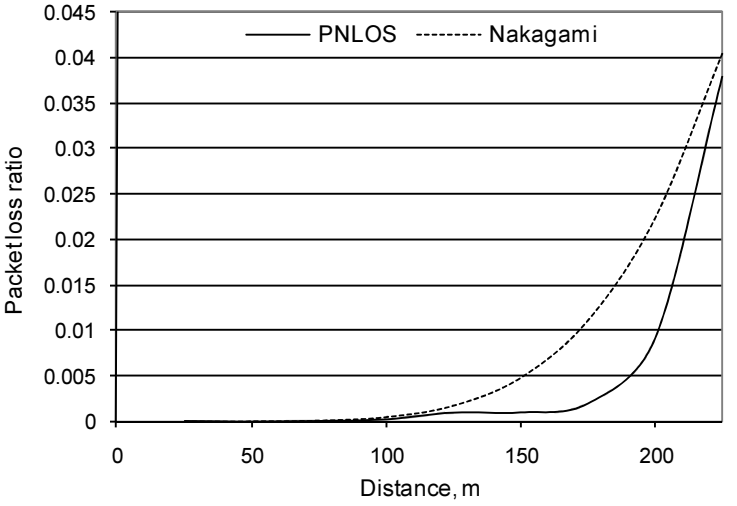

Fig. 3.16. NLOS Lost packet ratio depending on distance using approximation model (3.2) and Nakagami model

There is no model suitable for all road conditions. Classical models are poor suitable for big vehicles shadowing effects. Therefore, creating inter-vehicle communication modelling tools additional artificial screening obstacles should be applied. Such obstacles can be modelled using a stochastic signal disrupting model.

3.6. Safety Message Transmission Ensurance

As it is shown in this chapter previously safety messages can be lost, therefore, means should be taken to reduce a lost message number. This section presents an safety message transmission mechanism, which is robust ant cost effective. The proposed method is based on redundant message transmission when each safety message is repeated after some time. The efficiency of this redundancy method is proven by analyzing the experimental results.

Although, the redundant transmission method efficiently reduces a packet loss it does not guarantee zero packet loss. Therefore, an safety message signalling mechanism is presented and the main concepts drawn.

3.6.1. Safety Message Redundancy

An safety message transmission is not always ensured. Therefore, a redundant message transmission mechanism is necessary to increase a message delivery to destinations on time. The simplest mechanism is to repeat the message transmission after some time.

A packet loss correlation for x time shift can be calculated using following formula:

$$T_x = \frac{\sum_{i=0}^{N}(t_i \cdot t_{i+x})}{N}, \tag{3.20}$$

where T_x – lost packet ratio; x – time shift; t_i – lost packet; N – generated packet number, in current experiment $N = 20000$.

In current research packets were transmitted every ~1.2 ms, so the smallest time shift step is x=1.2 ms and all longer steps are the multiplication of x.

Results for different time shifts are shown in Fig. 3.16.

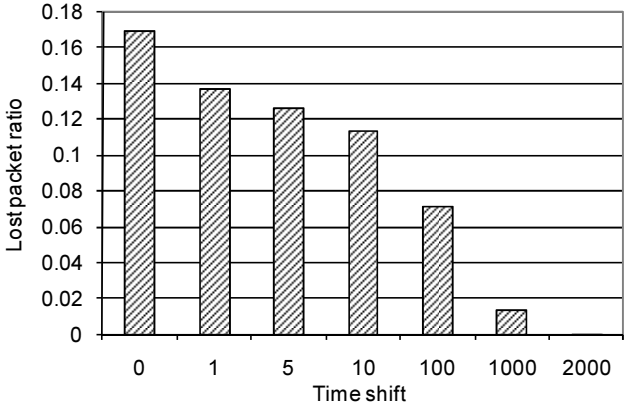

Fig. 3.17. Lost packet ratio with different time shifts

As it is shown in Fig. 3.17, repeating of message after some time reduces lost packet number. When time shift increases, a lost packet ratio gradually decreases. When time shift x equals 2000, then a lost packet number is close to zero, but this time shift is not allowed, because latency will grow up to 2.4 s. Time shift x should fit to requirements of critical latency (Table 1.4). Here should be noted, that as the lost packet ratio is decreasing when time shift increases, repeated packet should be delayed as long as possible, i.e. the first safety message should be send immediately after the emergency situation occurs

and the redundant message should follow after maximal allowed latency time for current emergency situation.

Use case latency time (The CAMP project, 2005) is grouped into five groups: 20, 100, 500, 1000 and more than 2000 ms. It is necessary to calculate maximal shift for each latency time. One shift equals 1.2 ms, so maximal latency time for each latency time is 16, 83, 416, 833 and more than 2000.

Lost packet ratio of use cases for different distances is shown in Fig. 3.18.

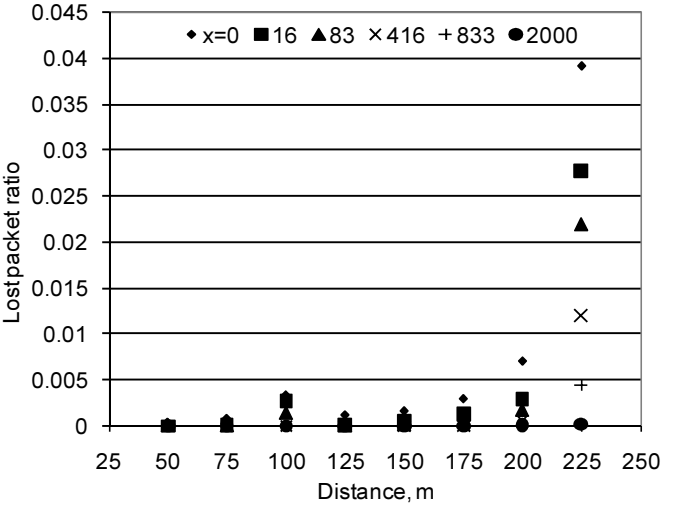

Fig. 3.18. Lost packet ratio for different distances

Fig. 3.18 shows how lost packet ratio depends on different time shifts for different distances. Time shift influence can be calculated and is shown in Table 3.2.

Table 3.2. Risk reduction for different time shifts

x	Risk ratio
0	1
16	0.6236
83	0.4566
416	0.2200
833	0.0787
2000	0.0038

Risk ratio calculations, given in Table 3.2 shows how redundant message transmission reduces risk to loose packet. Here can be seen, that for time shift x=16, risk to lose packet is reduced to 62% and gradually decreases with increasing time shift.

3.6.2. Safety Message Signalling Mechanism

The redundant message transmission significantly decreases the number of lost packet, but still some packets are lost. Therefore, more complex mechanism for lost packet reduction should be used.

Here is proposed a signalling mechanism, which will help to deliver safety messages to destinations. The main idea is that the safety message originator – sender sends messages to receivers, and then waits for response. If there is no response, or not on time, repetitive messages are sent, according to the situation: message life time or importance to receiver.

Emergency situation on the road is presented in Fig. 3.19.

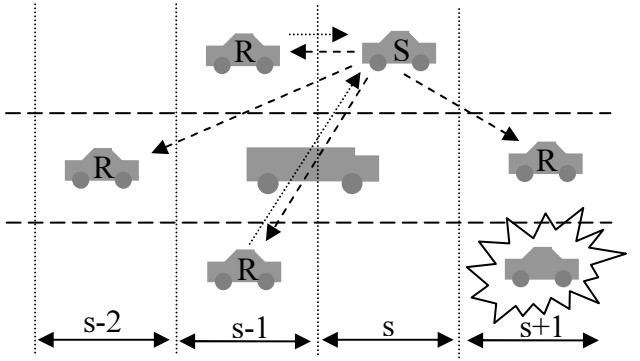

Fig. 3.19. Emergency scenario with one obstructed receiver

The emergency scenario, presented in Fig. 3.19, gives an overview on a situation on the road, when one receiver is obstructed. Here sender S detects emergency situation on the first lane, and transmits that situation to the receivers. There are two receivers on the first row s-1 after the sender, and one in the second row s-2. The sender will arrive at the emergency place in 1.8 s (Kajackas *et al.* 2009a), receivers s-1 in 3.6 s and receiver s-2 in 5.4 s.

According to the described scenario, the signalling mechanism works as following:

1. Beaconing – each equipped vehicle on the road periodically broadcasts beacons with its position and direction. The period of beacons depends on the car speed, and should be enough precise, for

equipped cars to recognize its neighbours. Beacons should be transmitted in SCH.

2. Emergency situation – the car, which detects an emergency situation, broadcasts safety message (transmitted in CCH), and waits response from all neighbour receivers, for whom this information is relevant. From example, given in figure 10, a sender waits for the response just from equipped receivers in zone s-1, because the current emergency situation is important for the cars in s-x zone, and cars in s-1 zone do have the shortest time to arrive to the emergency place. The sender does not wait for the response from the receiver in s+1 zone, as this car has already passed the emergency place.
3. The response to an safety message – if a sender gets the response from receivers in s-1, then it stops transmitting the safety message. But if the response does not come from a receiver, e.g. the receiver in the first lane is obstructed by the truck, sender tries regularly to resend an safety message, until it passes the emergency place and the information is no more relevant for the receiver.
4. A new sender – after 1.8 s passes, receivers in s-1 zone will move to s zone and one of them will be first to transmit the renewed safety message and will wait for the response.

The proposed scenario will work not only for the situation given in Fig. 3.19, but also on other situations. Zone s is an safety message generation zone and is close to the emergency situation, which can be a car crash, an oil leak, an obstacle on the road, the traffic jam on highway, etc. Zone s-1 is the closest area to the generation zone, where the cars, which will arrive to the emergency zone in few seconds, are.

3.7. Conclusions of Chapter 3

1. The problem of the vehicle as an obstacle is analyzed in a few papers, where the radio signal attenuation is measured. There are no papers giving the lost packet dependency on two major factors: the distance and obstacles. This chapter gives experimental results for LOS and NLOS cases.
2. The most popular modelling tools, like NCTUN's, do not consider vehicles as obstacles for the radio signal. Therefore, approximation equations of lost packets for LOS and NLOS cases can be used in modelling tools for realistic simulations.

3. While analysing the results it was observed, that lost packets are building groups and this grouping can be expressed using the geometric distribution, Gilbert-Elliott model or *N*-State Markov model. Given expressions should be used in modelling tools, to simulate not just the number of lost packets, but also the lost packet grouping.
4. The novel robust and the low channel consuming redundant safety message transmission mechanism is proposed. The efficiency of this method is proven by analyzing the experimental results.

4

Driver Information System

A great deal of car and electronic equipment manufacturers create and test different safety increasing devices. These can be high frequency radio radars, video observing systems, laser scanners, etc. All these devices should warn the driver when the emergency situation occurs. A driver cannot be informed by each device separately, because a high number of different emergency signals will be too disturbing. Therefore, the unified information system should be used, where the information is collected from many devices.

This chapter presents the research on the driver information system. The first section analyses the driver trust monitoring systems and proposes the confidence index calculation method. In the second section of this chapter the research on one of confidence index variable – safe following distance is presented. It is shown, that the safe following distance can be too high for reliable communication in certain cases. The summary of this chapter is given in conclusions.

The analysis and part of the results presented in this chapter are published by author in (Kajackas *et al.* 2012).

4.1. Inter-Vehicle Safety Monitoring System

Much of the existing literature on Inter-Vehicle communications is the navigation safety related (Gerlach *et al.* 2011). Collective safety applications are based on the frequent exchange of short status messages also known as beacons by the vehicles. Beacons carry the information about the vehicle, such as its position, velocity and acceleration (Vinel 2012). In VANETs, which are based on 802.11p, beacons are broadcast periodically by each vehicle. CSMA distributed MAC scheme is adopted in 802.11p. Therefore, beacons are a subject to collisions in the wireless channel.

One of the increased traffic safety tools is Driver Assistance System (DAS), which, using various methods gathers information about the road situation processes this information and forms notifications for the driver. For example, "Traffic View" (Nadeem *et al.* 2004) is a device that can be embedded in vehicles to provide the drivers with a real-time view of the road traffic far beyond what they can physically see. Vehicles equipped with TrafficView form an ad hoc vehicle-to-vehicle network to exchange the traffic information. The newest projects are oriented to create Advanced DAS (ADAS). Several ADAS systems are currently analyzed (Gieteling *et al.* 2006):

- driver information systems increase the awareness of the driver's situation, e.g. advanced route navigation systems (Venhovens *et al.* 1999);
- driver warning systems actively warn the driver of a potential danger, e.g. a lane departure warning, a blind spot warning, and forward collision warning systems (National Highway Traffic Safety Administration 2005);
- intervening systems provide an active support to the driver, e.g. an adaptive cruise control system (Winner *et al.* 1996, Venhovens *et al.* 2000);
- integrated passive and active safety systems that are activated during the crash, a pre-crash system can mitigate the crash severity by deploying active and passive safety measures before a collision occurs (Moritz 2000, Tokoro *et al.* 2004).

Fully automated systems are the next step beyond the driver assistance, and operate without a human driver in the control loop (Schladhover 2005).

The task of all ADAS systems (except fully automated systems) is to give more information for the driver about road conditions, to help the driver to orient better in the environment. The core most important problem in all ADAS and their services for the driver is the reliability of performed functions and to it related the driver trust level. Obstacles which are hard to detect and recognize can

occur on the road. The drivers of nearby cars can be errant and with uncertain intentions. Using radio communication between cars some of the messages can be distorted or lost because of bad communication conditions. False messages can be transmitted.

On the other hand, too much information can be presented to a driver, which can disturb attention and prevent from necessary actions.

This section presents specific view to ADAS, where information about situation on the road is given by one indicator – a vehicle safety index in the current road situation. This unique approach use Confidence Index (CI) expression to connect different safety parameters and display a danger value with possibility to distinguish between the danger and the emergency situation.

CI always assesses the environment and informs the confidence index to the driver. CI is Human – Machine interface, which is very important metrics to assess road conditions. There are many papers on information representation to the driver (summary given in Adell *et al.* 2008). One of conclusions – a driver can not be disturbed.

Driver can be informed, for example, using some pictogram near speedometer, which is changing when a safety parameter changes.

Implementing ADAS systems very important is to extend function list with specific function, which monitors trustworthiness of made decisions.

4.1.1. Confidence Index Description

The risk situation on the road ahead is constantly changing the value and depends on several probability factors. One of initial confidence metrics can be expressed trough trustworthiness and directly linked with probability metrics:

$$\Theta = \Phi\left\{v, v_x; l, l_x; s...\right\}, \tag{4.1}$$

where Θ – confidence indicator; $\Phi\{\}$ – risk functional, which depends on risk influencing values, i.e. v – current velocity and v_x – safe velocity for current case, l – current distance from the car in front and l_x – safe distance from car in front, s – visibility factor, and other, like vehicle type, mass, tyre condition, etc.

The trustworthiness indicator should be related to communication between cars condition for the use cases, when vehicles form communicating groups.

CI should have the highest score when situation on the road is in good condition and a car gets beacon messages from nearby vehicles constantly. When situation on the road changes to risky, or communication with nearby cars is lost, the confidence indicator should be reduced.

4.1.2. Inter-Vehicle Confidence Index Model

Communication between vehicles is implemented using IEEE 802.11p standard system, which sends safety messages periodically. Periodically sent beacons are called Cooperative Awareness Messages (CAMs) and are defined in ETSI ITS (Stanica *et al.* 2012) architecture. These beacons are transmitted with the purpose of sharing information gathered by the on-board sensors (e.g., geographical location, speed, acceleration etc.) with the neighbouring vehicles. The role of the CAMs is, therefore, not to announce a danger, but to extend the driver's knowledge about the surrounding environment, with the hope that this extra-information will help enhancing road safety.

Beacons are sent periodically all the time whether there is risk situation, or not. Each successfully received beacon proves the reliable communication channel. When a car regularly receives such messages, it proves it is connected to V2V network.

Using periodically sent beacons confidence recurrent index calculation in a receiving car can be expressed:

$$\Theta_n = \alpha\Theta_{n-1} + (1-\alpha)\Delta\Theta_n, \tag{4.2}$$

where n = 1,2,3,…; Θ – confidence index for the n-th moment after receiving n-th beacon; $\Delta\Theta_n$ – confidence index difference for the current n, which is calculated using situation describing index $\alpha < 1$.

If at some moment n_x renewed information gathering is stopped, the difference of the confidence index cannot be calculated. Then $\Delta\Theta_{nx} = 0$. If such situation continues for k steps, trust index reduces by formula:

$$\Theta_n = \alpha^k \Theta_{nx}, \quad n > n_x. \tag{4.3}$$

Constant reduction of confidence index is a signal for the driver that the vehicle emergency prevention tools can not be trusted and a driver should take complete control of vehicle.

When the emergency situation occurs a special message is transmitted. After decoding this message a receiver sets $\Delta\Theta_n < 0$ – to negative high number. Θ_n value drops down fast. In such case, other additional driver information tools can be turned on, i.e. horn.

The proposed system is effective even for such cases when the communication to other vehicles is lost, because CI will have a decreasing trend. The decreasing rate can be adjusted by changing α value. For highways α can have bigger values and for cities it can have smaller values, because in highways there are less cars around, and Θ should go down slower to detect communication loss, as in the city a communication loss can be detected very fast, because there are always many cars around.

4.1.3. Confidence Index Calculation

CI consists of several danger representing variables. These variables should each be able to influence CI level to necessary value, therefore, the multiplication procedure between variables suits best to connect different danger parameters.

$$\Theta_n = t_{\text{dist}} \cdot t_{\text{com}} \cdot t_{\text{v}} \cdot t_{\text{em}} \cdot t_{\text{beacon}} \cdot \ldots \cdot t_n, \quad (4.4)$$

where t – danger level of certain situation: t_{dist} – danger level of following distance; t_{com} – danger level of communication distance; t_{v} – danger level of actual velocity in current road; t_{em} – danger level of received VANET safety message; t_{beacon} – danger level of lost communication (no beacon messages received); t_n – n^{th} danger representing variable.

Θ_n value dynamically changes taking values in the interval [0, 1], where "1" means complete confidence – no danger and "0" means no confidence – complete danger. t values are changing in the interval [0, 1] as well, showing the level of confidence/danger in certain situation. Not all variables t have the same influence on general danger (i.e. low tyre pressure and safety message from the network about front end collision danger) therefore variables presenting lower danger should not have values equal to 0 but higher, i.e. emergency situation can be defined as Θ_n value in the interval [0, 0.5] and warning situation, when Θ_n takes values in the interval (0.5, 1).

In (4.4) shown CI calculation method is flexible and it is easy to add or remove additional danger variables (i.e. driver health/tiredness condition, tyre pressure, etc.).

The calculation of safe following distance, which influences the level of danger t_{dist}, is thoroughly analyzed in the following section. A safe distance from the car in front is opposing the reliable communication distance (level of danger – t_{com}) because a bigger distance is safer but the communication gets less reliable.

Safety messages received from network present some level of danger t_{com}. Received messages should not be blindly applied to CI calculation, but should be evaluated in the sense of trustworthiness. The research on risk, trust and privacy issues, which are unavoidable analyzing information disseminated in the network, are described in the first chapter.

The reliable communication can be analyzed tracking a constant reduction of confidence index as shown in (4.3). The lost communication level of danger is expressed using t_{beacon} variable. A beacon loss calculation function should continuously collect information about neighbouring vehicles and if no beacon is received from the estimated neighbouring vehicle t_{beacon} variable should be reduced using a following expression:

$$t_{\text{beacon}} = \begin{cases} 1, \text{ if all beacons received,} \\ t_{\text{beacon-1}} \cdot \alpha, \text{ if any beacon lost.} \end{cases} \quad (4.5)$$

In this expression t_{beacon} variable gradually decreases with every cycle until it goes down close to zero representing high danger.

4.1.4. Dynamic Danger Representation

Chen *et al.* 2008 present the idea of dynamic danger representation. Described study on the vehicle safety distance warning system uses a derivative d*D*/d*t* (here *D* – distance between cars) to represent if dangerous situation is getting better or more dangerous.

The dynamic danger calculation can be implemented using a following algorithm:

$$\frac{\Delta\Theta}{\Delta T} = \frac{\Theta_2 - \Theta_1}{\Delta T}. \quad (4.6)$$

where Θ_1 and Θ_2 are Θ values at current and previous calculation cycle; ΔT – calculation cycle time, which should be adapted to show fluent and fast change of danger.

If $\Delta\Theta/\Delta T$ is < 0 situation is getting more dangerous, and i.e. red arrow can be shown pointing down. If $\Delta\Theta/\Delta T$ is > 0 situation is getting better and i.e. yellow arrow can be shown pointing up, and if $\Delta\Theta/\Delta T$ is = 0, then no arrow is displayed, as situation is getting not worse nor better. Such danger representation can be very useful for people who are learning how to drive and for young drivers.

To know which value is changing, a dynamic danger of each parameter *t* can be calculated separately, e.g. $\Delta t_{\text{dist}} / \Delta T$, etc. These values can be used to know, which danger parameter is changing and the message can be displayed for the driver, i.e. "*Car following distance is getting safer*".

4.2. Communication Conditions for Safe Following Distance

Section 4.2 analyses the safe distance condition which is related to t_{dist} described in (4.4). The first part of this chapter presents an analysis of the car safe following distance dependency on velocity, technical parameters of the car and the road condition. In the second part, risk indicators and their dependency on real car following distance are analyzed. This part defines inter-vehicle communication boundaries, which are necessary for safe distance estimation on changing

road conditions (dry, icy, wet road on normal or foggy weather). Here two scenarios are analyzed. The first scenario describes the situation when cars have the same physical data and are travelling on the same speed before the emergency situation. In this case, the driver's reaction time and a distance are main factors influencing a risk parameter. In the second scenario, the first car crashes and its velocity goes to zero instantly. Here, one more parameter influencing a risk factor is added – a static friction coefficient which shows how fast car can stop in certain situation.

4.2.1. Vehicle Following Process and Safety Distance

The basic assumption in vehicle following is that each driver attempts to maintain a desired headway behind the vehicle in-front. Fig. 4.1 shows the n^{th} car C_n which is followed by n^{th}+1 car C_{n+1}. Car C_n position on the road at time t is $x_n(t)$ and velocity is $v_n(t)$.

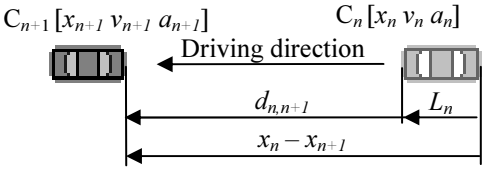

Fig. 4.1. Car in series model

At this moment spacing between cars is calculated in (4.7).

$$d_{n,n+1} = x_n - x_{n+1} - L_n\,, \tag{4.7}$$

where $d_{n,n+1}$ – distance between cars; L_n –length of car C_n.

For traffic safety acceleration values a_n and a_{n+1} are important, as well. When a car is accelerating $a > 0$ and when a car is breaking $a < 0$. Vehicles braking deceleration is an important indicator reflecting breaking performance of the vehicle. The maximum deceleration of the vehicle depends on the road type, weather condition and a type of the vehicle (Sokolovskij 2005). Depending on a car weight, size, and road conditions (dry, wet, icy, etc.) the braking deceleration can vary from 7.0 to 0.7 m/s^2 (Shiwen *et al.* 2009).

One of the most important parameters for car safety ensurance is d_s – stopping distance which car running at initial velocity v_0, travels after brakes are engaged until full stop. A theoretical stopping distance is calculated using following formula:

$$d_s(v) = \frac{v_0^2}{2\mu g}, \tag{4.8}$$

where μ – static friction coefficient between tyres and road surface (value is 0.8 for good tyres and good surface); g – gravity of Earth (9.81 m/s^2).

Some papers introduce additional parameters to the (4.8) formula: κ – tire condition [0, 1] and δ – safety margin in meters (Riener *et al.* 2012). With additional parameters formula (4.8) gets:

$$d_s(v) = \frac{v_0^2}{2\mu g\kappa} + \delta\,. \tag{4.9}$$

Safety margin δ covers the reaction time of the driver, mechanical latencies of the vehicle and other unpredictable delays.

Stopping distance is related to another important parameter – safe following distance – D_{sf}. It is a distance between moving cars, which is necessary to safely stop the car in an emergency situation. In (Arem *et al.* 2012) the safe following distance is computed on the basis of the current speed v of vehicles and the deceleration capabilities $a_{d(n+1)}$ and a_{dn}:

$$D_{sf} = \frac{v^2}{2\left(\frac{1}{a_{d(n+1)}} - \frac{1}{a_{dn}}\right)}. \tag{4.10}$$

Following the formula (4.10) safe following distance depends only on different deceleration capabilities of the cars.

Another safe following distance definition says: a safe following distance or a car following safe gap is defined as the proper distance between a leader and following vehicles in the same lane (Taleb *et al.* 2010):

$$D_{sf} = \alpha\left(v_{n+1}\cdot t_r + \frac{v_{n+1}^2}{2a_{dr(n+1)}} - \frac{v_n^2}{2a_{drn}}\right), \tag{4.11}$$

where α – tolerance factor; t_r – driver reaction time; a_e – emergency deceleration; a_r – regular deceleration. The tolerance factor α thereinafter in this paper is set
to 1.

In reality cars on the road are not the same, therefore, further analyzing this topic it is necessary to take into an account that stopping properties of C_n and C_{n+1} are different ($a_{dn} \neq a_{d(n+1)}$). To better estimate differences of different vehi-

cles in formula (4.12) stopping decelerations can be changed to static friction coefficient μ:

$$D_{\mathrm{sf}} = v_{n+1} \cdot t_{\mathrm{r}} + \frac{v_{n+1}^2}{2g\mu_{n+1}} - \frac{v_n^2}{2g\mu_n}. \tag{4.12}$$

Three components are important in a safe distance formula (4.12).The first component $v_{n+1} \cdot t_{\mathrm{r}}$ is a distance which the car C_{n+1} travels in driver's reaction time. The driver's reaction time here includes the braking system reaction time and the deceleration rising time. In general t_{r} means all the time which a vehicle travels without actual braking. The second component $v^2_{n+1}/2g\mu_{n+1}$ is the distance which a car C_{n+1} travels in normal deceleration conditions until a full stop. The third component $v^2_n/2g\mu_n$ is the distance which car C_n travels in normal or extreme braking time until a full stop.

In ideal conditions, when stopping performance of the cars C_n and C_{n+1} are equal, scilicet velocities are equal ($v_n = v_{n+1}$) and friction coefficients are equal ($\mu_n = \mu_{n+1}$), the second and third components in formula (4.12) are cancelling each other. In this case a possible safe distance is the smallest:

$$D_{\mathrm{sfmin}} = v_{n+1} \cdot t_{\mathrm{r}}. \tag{4.13}$$

The smallest safe distance depends only on the speed of the vehicle and on the driver's in car C_{n+1} reaction time t_{r}. According to (Yang *et al.* 2004) an average driver's reaction time is from 0.75 up to 1.5 s. In some other sources an average reaction time is from 0.8 up to 1.2 s. Drivers, who have a smaller reaction time, can safely keep a smaller distance between cars.

Popular 2...3 s safe distance rule can be easily applied setting an increased reaction time t_{r} into formula (4.13).

The stopping performance of different cars is different (Sokolovskij 2005), therefore, friction coefficients are not equal ($\mu_n \neq \mu_{n+1}$) and if $\mu_n > \mu_{n+1}$ vehicle safe following distances are bigger:

$$D_{\mathrm{sf}} = v_{n+1} \cdot t_{\mathrm{r}} + \frac{v_{n+1}^2}{2g} \cdot \frac{\mu_n - \mu_{n+1}}{\mu_n \cdot \mu_{n+1}}. \tag{4.14}$$

The safe distance gets the biggest following an assumption that at some moment a car C_n stops immediately (i.e. in darkness a car crashes into a standing truck). In this case $v_n = 0$ and formula (4.12) gets:

$$D_{\mathrm{sfmax}} = v_{n+1} \cdot t_{\mathrm{r}} + \frac{v_{n+1}^2}{2g\mu_{n+1}}. \tag{4.15}$$

Formulas (4.13), (4.14) and (4.15) are used for specific conditions calculating safe following distances. In reality drivers can choose distances from D_{sfmin} to D_{sfmax} (Fig. 4.2). A distance D_{sfmin} can be used for similar cars in highways where no obstacles are and it is sure, that a car in front can not stop instantly. D_{sfmax} should be used when driving conditions are bad (i.e. foggy) and obstacles can appear on the road.

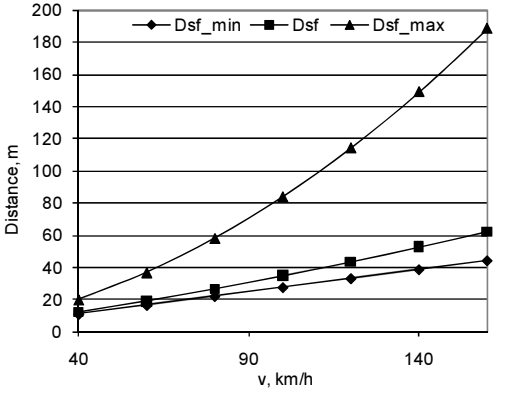

Fig. 4.2. Safe distance comparison: D_{sfmin}, D_{sf}, D_{sfmax}. Here t_r = 1s, μ_n = 0.8, μ_{n+1} = 0.7

In (Boban *et al.* 2011, Kajackas *et al.* 2012) given results show, that the Inter-Vehicle communication is reliable (packet delivery ratio >80%) when a distance is ≤200 m in LOS case. In good road conditions (Fig. 4.2) the reliable communication distance is not exceeded for all safe distance calculations (Shiwen *et al.* 2009, Riener *et al.* 2012, Arem *et al.* 2006) even driving 160 km/h. It may happen that cars without communication can enter the same lane between equipped cars. They are obstacles for the radio signal and the reliable communication distance will be smaller (Kajackas *et al.* 2012).

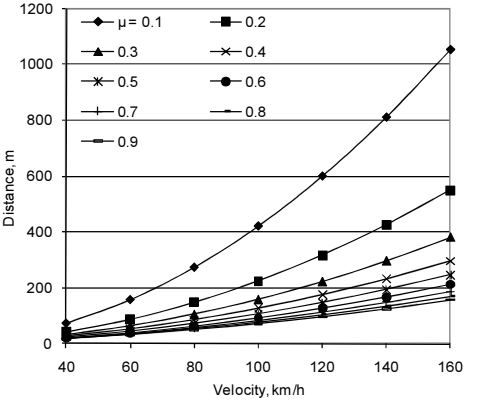

Fig. 4.3. Safe distance curves for different μ values. Here t_r = 1s

Fig. 4.3 shows safe distance D_{sfmax} curves for different μ values, which represents road conditions from an icy road (μ = 0.1) to a dry road (μ = 0.9). It can be seen, that the safe distance can be more than 200 m. in the higher velocity. This means, that keeping the safe distance can cause an unreliable communication.

4.2.2. Risk Indicators for the Car Following

Many risk factors can appear when driving the car on the road. A big part of these risk factors happens because of high speed and too short distances between the cars. Here, we will analyse the influence of these two factors (speed and distance) to a general risk.

When a distance $d_{n,n+1}$ is getting smaller between cars C_n and C_{n+1}, then a risk that collision will happen is getting higher. Also, when a velocity is getting bigger, the safe distance $D_{\text{sf}}(v)$ is getting bigger.

There are many risk indicator conceptions and formulas. In (Bevrani *et al.* 2011, Archer *et al.* 2005) summaries about different risk indicators are given.

A risk indicator, which relates a safe distance between cars (which depends on the speed of the vehicle, possible braking decelerations, the driver's reaction time) with the actual distance between cars, is given in (Guangquan *et al.* 2012). Following used symbols and marking a level of driver's risk is defined as follows:

$$\xi_{n+1}(\tau,t)=\frac{D_{\text{sf}}}{d_{n,n+1}(\tau,t)}, \tag{4.16}$$

where ξ – risk level which depends on distance; D_{sf} – safe following distance; $d_{n,n+1}(\tau,t)$ – actual distance between cars.

This risk indicator points out, that in a car following situation, the following car should maintain adequate space to ensure safety. When a driver of the lead car suddenly brakes, a driver of the following car should act accordingly to avoid a potential crash. The safety is ensured when $\xi_n(\tau,t) < 1.0$. When $\xi_n(\tau,t) \geq 1.0$, a driver of the following car risks to hit the front car in emergency situation.

Using (4.12) formula risk indicator can be expanded as follows:

$$\xi_{n+1}(t)=\left(v_{n+1}\cdot t_{\text{r}}+\frac{v_{n+1}^2}{2g\mu_{n+1}}-\frac{v_n^2}{2g\mu_n}\right)\frac{1}{d_{n,n+1}(t)}. \tag{4.17}$$

The formula (4.17) relates risk indicators value with vehicle parameters: a velocity, a static friction coefficient and the distance between cars. Using accepted risk value, safe distances can be calculated from (4.17) as well.

When ideal conditions are kept (velocities are equal $v_n = v_{n+1}$ and friction coefficients are equal $\mu_n = \mu_{n+1}$) a safe distance is calculated using (4.13). In this case risk factor is:

$$\xi_{n+1}(t) = \frac{v_{n+1} \cdot t_r}{d_{n,n+1}(t)}. \tag{4.18}$$

A risk factor in (4.13) depends on a velocity, a drive's reaction time and the distance between cars (Fig. 4.4).

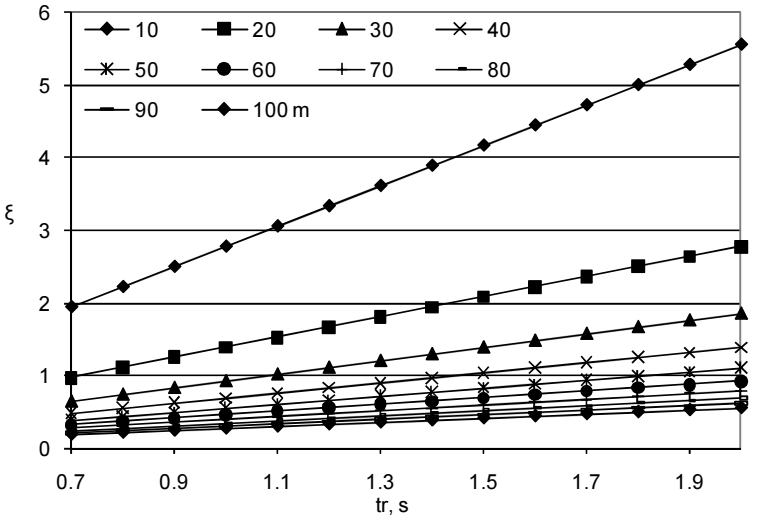

Fig. 4.4. $\xi_n(t)$ values for different distances with different t_r driving 100 km/h

Risk indicator using D_{sfmax} in formula (4.15) is expressed following:

$$\xi_{n+1}(t) = \left(v_{n+1} \cdot t_r + \frac{v_{n+1}^2}{2g\mu_{n+1}} \right) \frac{1}{d_{n,n+1}(t)}. \tag{4.19}$$

Risk indicator dependencies from different distances for different velocities using (4.19) are shown in Fig. 4.5. Here, a driver reaction time is set to 1 s, as this is almost in the middle of typical reaction times and $\mu_{n+1} = 0.9$. Similar curves are given in Fig. 4.6, but here a static friction coefficient is changing.

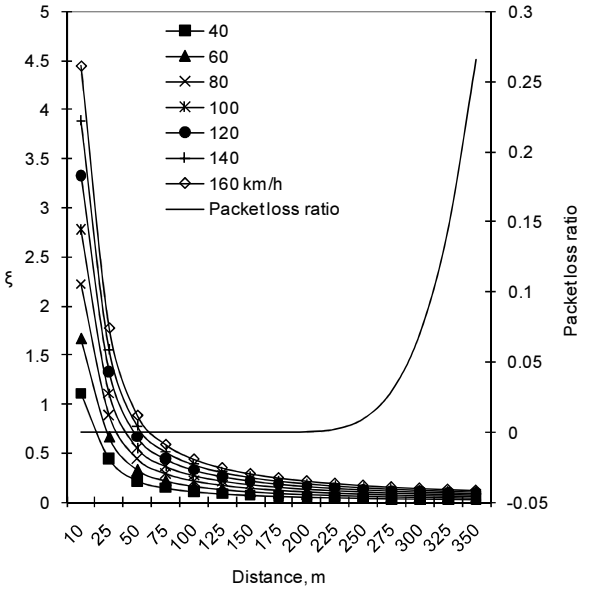

Fig. 4.5. Risk indicator as function of distance (t_r = 1 s, μ_{n+1}= 0.9, and variable velocities)

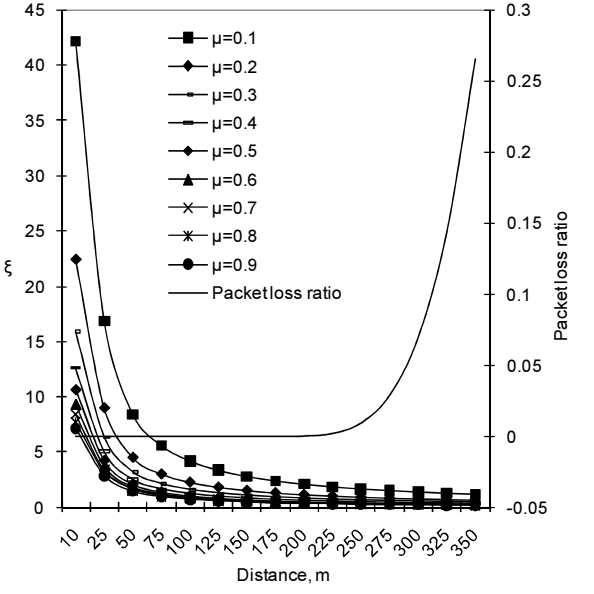

Fig. 4.6. Risk indicator as function of distance (t_r = 1 s, v = 100 km/h and variable μ values)

Fig. 4.5 shows that for the good road condition (μ_{n+1}= 0.9) a risk indicator is < 1 even for 160 km/h. However, when the road conditions are getting worse, a safe distance is increasing very fast. Risk indicator curves in Fig. 4.6 show that for smaller μ values driving 100 km/h a safe distance is more than 225 m. For icy road conditions (μ = 0.1 and 0.2) keeping $\xi \leq 1$ communication is not reliable. This means that keeping the safe distance on a wet or icy road will lead to unreliable communication and a driver might be warned too late to be able to stop the car safely. In this place a safe distance and the reliable communication oppose each other and additional means should be taken to ensure the reliable communication.

4.4. Conclusions of Chapter 4

1. Existing driver assistant systems inform the driver about a certain danger parameter separately. This chapter presents a novel view to a driver assistant system, presenting one confidence index expression.
2. Proposed the novel confidence index algorithm is flexible (additional safety parameters can be easily added) and shows a level of danger, where a driver can distinguish between emergency and warning situations. Additionally, a dynamic danger calculation method is proposed, which shows whether a dangerous situation is getting more dangerous or less dangerous. Existing danger representation parameters do not combine all these features together.
3. The safe following distance changes rapidly with changing static friction coefficient, therefore, it can happen, that for icy sections on the highway safe following distance is bigger than the reliable communication distance. These two opposing factors should be estimated in CI calculations. Fig. 4.6 shows from calculation and experiments derived data of a safe following distance and a reliable communication distance.

General Conclusions

1. Experimental results prove theoretical conclusions that a packet loss trend depends on the distance between vehicles – nodes and LOS obstructing other vehicles. Given approximation equations can be used for modelling tasks, which consider vehicles as obstacles.
2. Simulations show how the latency time of current use case influences multi-hop routing algorithm selection:
   a) when the allowed latency time is 20 ms, only a single message transmission scenario (worst reliability, lowest channel consumption) with 10 nodes chain can be used;
   b) when the allowed latency time is 2 s, a controlled flood scenario (reliable, most channel consuming) with 20 nodes can be used. In this scenario safety messages should be routed so, that a routing path will not be longer than 4 nodes.
3. Experimental results show that redundantly transmitting very important safety messages with time shift 20 ms will reduce lost message number by 62% and gradually decreases with increasing time shift. This redundant transmission method can be used developing WSM protocols.

4. It is proposed to relate a reliable communication distance with a safe following distance:
   a) in normal driving conditions, when a velocity is 90 km/h, a safe distance is ~60 m, therefore, the reliable communication in one hop is between three – four cars;
   b) with increasing velocity, a safe distance increases, therefore, the reliable communication is between a fewer vehicles;
   c) on the icy road, when a velocity is 90 km/h, a safe distance is ~340 m. Keeping this distance will lead to unreliable communication and part of transmitted packets will be lost.
5. Created the novel confidence index algorithm, where dynamic CI value can show a level of danger for the driver, who then can distinguish between warning and emergency situations. The proposed algorithm can be easily implemented in the driver assistant systems.

References

Adell, E.; Varhelyi, A.; Alonso, M.; Plaza, J. 2008. Developing human–machine interaction components for a driver assistance system for safe speed and safe distance, *Intelligent Transport Systems*, 1(2): 1–14.

Archer, J. 2005. Indicators for traffic safety assessment and prediction and their application in micro-simulation modelling: A study of urban and suburban intersections, *Doctoral Dissertation, Department Of Infrastructure, Stockholm, Royal Institute of Technology*, 254 p.

Arem, B.; Driel, C. J. G.; Visser, R. 2006. The impact of Co-operative Adaptive Cruise Control on traffic flow characteristics, *IEEE Transactions on Intelligent Transportation Systems*, 7(4): 429–436

Automotive Collision Avoidance System Field Operational Test (ACAS FOT), *Final Program Report* [Online]. 2005. [Cited: 06 05 2012.] http://www.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/Crash%20Avoidance/2005/ACAS%20FOT%20Final%20Program%20Report%20DOT%20HS%20809%20886.pdf

Avižienis, A.; Laprie, J.C.; Randell, B.; Landwehr, C. 2004. Basic Concepts and Taxonomy of Dependable and Secure Computing, *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*, 1 (1): 11–33.

Bai, F.; Krishnan, H. 2006. Reliability Analysis of DSRC Wireless Communication for Vehicle Safety Applications, *in Proceedings of Intelligent Transportation Systems Conference*, 355–362.

Bevrani, K.; Chung, E. 2011. An examination of the microscopic simulation models to identify traffic safety indicators, *in Proceedings of International Journal of Intelligent Transportation Systems Research*, 1–15.

Bilstrup, K.; Uhlemann, E.; Strom, E.G.; Bilstrup U. 2008. Evaluation of the IEEE 802.11p MAC Method for Vehicle-to-Vehicle Communication, *in Proceedings of IEEE Vehicular Technology Conference*, 1–5.

Bilstrup, K.; Uhlemann, E.; Strom, E.G.; Bilstrup, U. 2009. On the Ability of the 802.11p MAC Method and STDMA to Support Real-Time Vehicle-to-Vehicle Communication, *EURASIP Journal on Wireless Communications and Networking, Article ID 902414*, 13 p.

Boban, M.; Vinhoza, T.T.V.; Ferreira, M.; Barros, J.; Tonguz, O.K. 2011. Impact of Vehicles as Obstacles in Vehicular Ad Hoc Networks, *in IEEE journal on selected areas in communications*, 1(29): 15–28.

Borries, K.C.; Stancil, D.D. 2007. Efficient Simulation of Mobile-To-Mobile Rayleigh Fading using Gaussian Quadrature, *in Vehicular Technology Conference*, 534–538.

Car-to-Car Communication Consortium. 2007. C2C-CC Manifesto. Version 1.1 [Online]. 2007. [Cited: 04 03 2012.] http://car-to-car.org/fileadmin/ downloads/C2C-CC_manifesto_v1.1.pdf.

Cenerario N.; Delot T.; Ilarri S. 2008. Dissemination of information in Inter-Vehicle ad hoc networks, *in IEEE Intelligent Vehicles Symposium*, 736–768.

Chen, Y. L.; Wang, S. C.; Wang, C. A. 2008. Study on Vehicle Safety Distance Warning System, *in Proceedings of IEEE International Conference on Industrial Technology*, 1–6.

Cheng, L.; Henty, B.E.; Stancil, D.D.; Bai, F.; Mudalige, P. 2007. Mobile Vehicle-to-Vehicle Narrow-band Channel Measurement and Charachterization of the 5.9GHz DSRC Frequency Band, *IEEE Journal on Selected Areas in Communications*, 8(25): 1501–1516.

Dok, H.; Fu, H.; Echevarria, R.; Weerasinghe, H. 2010. Privacy issues in vehicular ad hoc networks, *International Journal of Future Generation Communication and Networking*, 3 (1): 17–32.

Dotzer, F. 2005. Privacy issues in vehicular ad hoc networks, *Workshop on Privacy Enhancing Technologies*, 15 p.

Eenennaam, E.M. 2008. A Survey of Propagation Models used in Vehicular Ad hoc Network (VANET) Research, [Online]. 2008. [Cited: 06 05 2012.] http://wwwhome.ewi.utwente.nl/~eenennaa/unpublished/vanEenennaam_MRC_paper.pdf

General motors. 2011. GM Develops Mobile Technology That Watches Road Ahead. [Online]. 2012. [Cited: 18 02 2012.] http://www.gm.com/article.content_pages_news_us_en_2011_oct_1017_v2v.html.

Gerlach, M. 2007. Trust for Vehicular applications, *in Proceedings of Eighth International Symposium on Autonomous Decentralized Systems*, 295–304.

Gerlach, M.; Kleinrock, L. 2011. Vehicular networks and the future of the mobile internet. Computer Networks, *The International Journal of Computer and Telecommunications Networking*, 2(55): 457–469.

Gietelink, O.; Ploeg, J.; De Schutter, B.; Verhaegen, M. 2006. Development of advanced driver assistance systems with vehicle hardware-in-the-loop simulations, *Vehicle System Dynamics International Journal of Vehicle Mechanics and Mobility*, 7(44): 569–590.

Hill C.J.; Garret J.K. 2011. AASHTO Connected Vehicle Infrastructure Deployment Analysis [Online]. 2011. [Cited: 04 03 2012.] http://ntl.bts.gov/lib/43000/43500/43514/FHWA-JPO-11-090_AASHTO_CV_Deploy_Analysis_final_report.pdf.

Ipatovs, A; Petersons, E; Jansons, J. 2011. Model for Wireless Base Station Goodput Evaluation in Vehicular Communication Systems, *Electronics and Electrical Engineering* 5(111): 19–22.

Yang, A.; Liu, J.; Zhao, F.; Vaidya, N.H. 2004. A vehicle-to-vehicle communication protocol for cooperative collision warning, *MOBIQUITOUS*, 114–123.

Yin, J.; Holland, G.; ElBatt, T. 2006. DSRC Channel Fading Analysis from Empirical Measurement, *in Proceedings of First International Conference on Communications and Networking in China*, 1–5.

Jerbi M.; Senouci S.M. 2008. Characterizing Multi-Hop Communication in Vehicular Networks, *in Proceedings of IEEE Wireless Communications and Networking Conference*, 3309–3313.

Jiang, D.; Delgrossi, L. 2008. IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments, *in Proceedings of IEEE Vehicular Technology Conference*, 2036–2040.

Kajackas A.; Pavilanskas L. 2007. Analysis of the Connection Level Technological Expenditures of Common WLAN Models, *Electronics and Electrical Engineering*, 2(74): 63–68.

Kajackas, A.; Vindašius, A. 2009b. Applying IEEE 802.11e for Real-Time Services, *Electronics and Electrical Engineering*, 1(89): 73–78.

Kaul S.; Gruteser M.; Onishi R.; Vuyyuru R. 2008. GeoMAC: Geo-backoff based cooperative MAC for V2V networks, *in Proceedings of IEEE International Conference – Vehicular Electronics and Safety*, 334–339.

Khalaf R.; Rubin I. 2006. Throughput and Delay Analysis in Single Hop and Multihop IEEE 802.11 Networks, *in Proceedings of Broadband Communications, Networks and Systems Conference,* 1–9.

Killat, M.; Rossel, C.; Schmidt-Eisenlohr, F.; Vortisch, P.; Assenmacher, S.; Hartenstein, H.; Busch, F. 2007. Enabling efficient and accurate large-scale simulations of VANETs for vehicular traffic management, *in Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks*, 29–38.

Kononov, J.; Durso, C.; Reeves, D.; Allery, B.K. 2012. Relationship between Traffic Density, Speed and Safety and its Implication on Setting Variable Speed Limits on Freeways, *TRB Annual Meeting*, 1–20.

Kosch, T.; Schroth, C.; Starssberger, M.; Bechler, M. 2012. Automotive Internetworking, Willey, 377 p.

Lu, G.; Cheng, B.; Lin, Q.; Wang, Y. 2012. Quantitative indicator of homeostatic risk perception in car following, *Safety Science*, 50 (9): 1898–1905.

Meireles R.; Boban M.; Steenkiste P.; Tonguz O.; Barros J. 2010. Experimental Study on the Impact of Vehicular Obstructions in VANETs, *in Proceedings of IEEE Vehicular networking conference*, 338–345.

Minhas, U.F.; Zhang, J.; Tran, T.; Cohen, R.; 2009. A Multi-faceted Approach to Modeling Agent Trust for Effective Communication in the Application of Mobile Ad Hoc Vehicular Networks, *IEEE Transactions on Systems, Man, and Cybernetics – Part C: Applications and Reviews*, 13 p.

Molisch, A.F; Tufvesson, F.; Karedal, J.; Mecklenbrauker, C. 2009. Propagation Aspects of Vehicle-to-Vehicle Communications – An Overview, *in Proceedings of IEEE Radio Wireless Symposium*, 18–22.

Moritz, R. 2000. Pre-crash sensing – functional evolution based on short range radar sensor platform [Online]. 2000. [Cited: 06 05 2012.] http://ametist.cs.utwente.nl /RESEARCH/BOSCH/Moritz_Precrash.pdf

Muller, M.; 2009. WLAN 802.11p Measurements for Vehicle to Vehicle (V2V) DSRC, *Application Note, Rohde & Schwarz*, 25 p.

Nadeem, T.; Dashtinezhad, S.; Liao, C.; Iftode, L. 2004. TrafficView: A Scalable Traffic Monitoring System, *in Proceedings of International Conference on Mobile Data Management*, 1–14.

Petersons, E.; Bogdanovs, N. 2011. Performance Evaluation of Three Layer Vehicular Network, *Electronics and Electrical Engineering*, 6(112): 25–28.

Riener, A.; Zia, K.; Ferscha, A.; Beltran, C.R.; Minguez, J.J.R. 2012. Traffic flow harmonization in expressway merging, *Personal and Ubiquitous Computing*, 1–14.

Shiven, L.; Shiwen, Z. 2009. Research on Fuzzy Inference of Driver's Risk Perception of Rear-end Collision on Freeway, *Intelligent Computation Technology and Automation*, (2): 772–775.

Shladover, S.E. Automated vehicles for highway operations (automated highway systems), *Systems & Control Engineering*, 1(219): 53–75.

Sokolovskij, E. 2005. Experimental investigation of the braking process of automobiles, *Transport*, 20(3): 91–95.

Stanica, R.; Chaput, E.; Beylot, A.L. 2012. Properties of the MAC Layer in Safety Vehicular Ad Hoc Networks, *Communications Magazine*, 5(50): 192–200.

Stibor, L.; Zang, Y; Reumerman, H.J. 2007. Neighborhood evaluation of vehicular ad-hoc network using IEEE 802.11p, *in Proceedings of The 8th European Wireless Conference, 7* p.

Swami, A.; Cho, J.H. 2009. Towards Trust-based Cognitive Networks: A Survey of Trust Management for Mobile Ad Hoc Networks, *in Proceedings of 14th International Command and Control Research and Technology Symposium*, 16 p.

Taleb, T.; Benslimane, A.; Letaief, K. B. 2010. Toward an Effective Risk-Conscious and Collaborative Vehicular Collision Avoidance System, *IEEE Transactions on Vehicular Technology*, 59 (3): 1474–1486.

Taliwal, V.; Mangold, H.; Chen, C.; Jiang, D.; Sengupta, R. 2004. Empirical Determination of Channel Characteristics for DSRC Vehicle-to-Vehicle communication, *in Proceedings of Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, 88 p.

The CAMP Vehicle Safety Communications Consortium. 2005. Vehicle Safety Communications Project, Task 3 Final Report, Identify Intelligent Vehicle Safety Applications Enabled by DSRC. [Online]. 2012. [Cited: 04 03 2012.] http://www.its.dot.gov/research_docs/pdf/59vehicle-safety.pdf.

Tokoro, S.; Moriizumi, K.; Kawasaki, T.; Nagao, T.; Abe, K.; Fujita, K. 2004. Sensor fusion system for pre-crash safety system, *in Proceedings of Intelligent Vehicles Symposium*, 945–950.

Triggs, T.J.; Harris, W.G.; 1982. Reaction Time of Drivers to Road Stimuli, *Monash University Human Factors Group - Report HFR-12*, 68 p.

U.S. department of transportation, NHTSA. Vehicle Safety Communications Project. Task 3 Final Report. Report number DOT HS 809 859, 2005. http://www.its.dot.gov/research_docs/pdf/59vehicle-safety.pdf

Venhovens, P.; Naab, K.; Adiprasito, B. 2000. Stop and go cruise control, *International Journal of Automotive Technology*, 1(2): 61–69.

Venhovens, P.J.Th.; Bernasch, J.H.; Lowenau, J.P.; Rieker, H.G.; Schraut, M. 1999. The application of advanced vehicle navigation in BMW driver assistance systems, *Vehicle Navigation Systems and Advanced Controls*, 43–52.

Vindasius, A. 2010. Analysis of Quality of Service in Heterogeneous Wireless Networks, Doctoral Dissertation, *Technika*, 112 p.

Vinel, A. 2012. 3GPP LTE Versus IEEE 802.11p/WAVE: Which Technology is Able to Support Cooperative Vehicular Safety Applications?, *Wireless Communications Letters*, 1(2): 125–128.

Wang S.Y.; Lin C.C. 2008. NCTUns 5.0: A Network Simulator for IEEE 802.11(p) and 1609 Wireless Vehicular Network Researches, *in Proceedings of IEEE Vehicular Technology Conference*, 1–2.

Wex, P.; Breuer, J.; Held, A.; Leinmuller, T.; Delgrossi, L. 2008. Trust Issues for Vehicular Ad Hoc Networks, *in Proceedings of Vehicular Technology Conference*, 2800–2804.

Winner, H.; Witte, S.; Uhler, W.; Lichtenberg, B. 1996. Adaptive cruise control system aspects and development trends, *International Congress & Exposition*.

Xiao, C.; Zheng, Y.R.; Beaulieu, N. 2003. Statistical simulation models for Rayleigh and Ricean fading, *in Proceedings of International Conference on Communications*, 5: 3524–3529.

Zajic, A.G.; Stuber, G.L. 2006. A New Simulation Model for Mobile-to-Mobile Rayleigh Fading Channels, *in Proceedings of Wireless Communications and Networking Conference*, 1266–1270.

List of Publications by the Author on the Topic of the Dissertation

Papers in the Reviewed Scientific Journals

Kajackas, A.; Vindašius, A.; Stanaitis, Š. 2009a. Inter-Vehicle Communication: Emergency Message Delay Distributions, *Electronics and Electrical Engineering* 8(96): 33–38. ISSN 1392-1215 (Thomson Reuters Web of Knowledge)

Kajackas, A.; Mikėnas, K.; Stanaitis, Š. 2012. Investigation of Link Layer in Inter-Vehicle Wireless Communication, *Electronics and Electrical Engineering* 6(122): 71–74. ISSN 2029-5731 (Thomson Reuters Web of Knowledge)

Stanaitis, Š. 2010. Intervehicle Communication Research – Communication Scenarios, Science – Future of Lithuania 2(1): 77–80. ISSN 2029-2341 (Index Copernicus)

Other Papers

Vindašius, A; Stanaitis, Š. 2010. Analysis of Emergency Message Transmission Delays in Vehicular Wireless Mesh Network, *IEEE Third International Conference on Advances in Mesh Networks*. Venice, 35–40. ISBN 978-0-7695-4092-4 (Conference Proceedings Citation Index)

Šarūnas STANAITIS

RESEARCH OF SAFETY MESSAGE QUALITY CHARACTERISTICS IN INTER-VEHICLE COMMUNICATION

Doctoral Dissertation

Technological Sciences,
Electrical and Electronic Engineering (01T)

TRANSPORTO PRIEMONIŲ RADIJO RYŠIO SAUGOS PRANEŠIMŲ KOKYBĖS CHARAKTERISTIKŲ TYRIMAS

Daktaro disertacija

Technological Sciences,
Electrical and Electronic Engineering (01T)

Technologijos mokslai,
elektros ir elektronikos inžinerija (01T)

2012 12 14. 10,75 sp. l. Tiražas 20 egz.
Vilniaus Gedimino technikos universiteto
leidykla „Technika“,
Saulėtekio al. 11, 10223 Vilnius,
http://leidykla.vgtu.lt
Spausdino UAB „Ciklonas“
J. Jasinskio g. 15, 01111 Vilnius