

Wireless and Wired Ethernet for Intelligent Transportation Systems

Ramez Daoud

▶ **To cite this version:**

Ramez Daoud. Wireless and Wired Ethernet for Intelligent Transportation Systems. Automatic Control Engineering. Université de Valenciennes et du Hainaut-Cambrésis, 2008. English. NNT : 2008VALE0033 . tel-03012174

HAL Id: tel-03012174
https://uphf.hal.science/tel-03012174

Submitted on 18 Nov 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

2008 VALE 0033

UMR CNRS 8530

Numéro d'ordre : 08/32

THESE

Présentée pour l'obtention du titre de
Docteur de l'Université de Valenciennes et du Hainaut Cambrésis

Préparée au LAMIH : Laboratoire d'Automatique, de Mécanique et d'Informatique industrielles et Humaines, UMR CNRS 8530

Dans la spécialité Automatique, Génie Informatique

Par

Ramez DAOUD

Ingénieur en Electronique et Communication
Master en Automatique Industriel et Communication

Wireless and Wired Ethernet for Intelligent Transportation Systems

Soutenue le 11 Décembre 2008 devant la commission d'examen composée de :

E. Rondeau	Rapporteur	Professeur à l'Université Henri Poncaré, Nancy I
J.-M. Thiriet	Rapporteur	Professeur à l'Université Joseph Fourier de Grenoble
T. Ernst	Examinateur	Docteur- Directeur à l'INRIA de Recquencourt
M. Bayart	Examinateur	Professeur à l'Université de Lille
H. Amer	Co-Directeur de thèse	Professeur à l'Université Américaine du Caire
C. Tahon	Directeur de thèse	Professeur à l'UVHC
Y. Sallez	Co-Encadreur	Maître de conférence à l'UVHC

UNIVERSITE DE VALENCIENNES ET DU HAINAUT CAMBRESIS
Le Mont-Houy F59313 Valenciennes CEDEX 9-tel: +33 3 27 51 14 63 - fax: +33 3 27 51 13 10

UMR CNRS 8530

Numéro d'ordre : 08/32

THESE

Présentée pour l'obtention du titre de

Docteur de l'Université de Valenciennes et du Hainaut Cambrésis

Préparée au LAMIH : Laboratoire d'Automatique, de Mécanique et d'Informatique industrielles et Humaines, UMR CNRS 8530

Dans la spécialité Automatique, Génie Informatique

Par

Ramez DAOUD

Ingénieur en Electronique et Communication
Master en Automatique Industriel et Communication

Wireless and Wired Ethernet for Intelligent Transportation Systems

Soutenue le 11 Décembre 2008 devant la commission d'examen composée de :

E. Rondeau	Rapporteur	Professeur à l'Université Henri Poncaré, Nancy I
J.-M. Thiriet	Rapporteur	Professeur à l'Université Joseph Fourier de Grenoble
T. Ernst	Examinateur	Docteur- Directeur à l'INRIA de Recquencourt
M. Bayart	Examinateur	Professeur à l'Université de Lille
H. Amer	Co-Directeur de thèse	Professeur à l'Université Américaine du Caire
C. Tahon	Directeur de thèse	Professeur à l'UVHC
Y. Sallez	Co-Encadreur	Maître de conférence à l'UVHC

TABLE OF CONTENTS

Content	Page
Acknowledgments	i
Abstract	ii
List of Figures	ix
Abbreviations & Symbols	xiii
Introduction	1
Chapter I: Survey	5
1.0. Introduction	5
1.1. Future Vehicle Model	7
1.2. On-Board Systems	9
1.2.1. By-Wire	12
1.2.2. Multimedia	13
1.2.3. Control	13
1.3. Vehicles Interaction with External Environment	14
1.3.1. Guidance	15
1.3.2. Present Guidance Systems and Projects	17
1.3.2.1. Car Navigation Systems using Generic Algorithm	18

Content	Page
1.3.2.2. Floating Car Data Project	19
1.3.2.3. Trafficopter	21
1.3.3. Modes of Communications	22
1.3.3.1. Vehicle-to-Vehicle Communications (V2V)	22
1.3.3.2. Vehicle-to-Infrastructure/Infrastructure-to-Vehicle (V2I/I2V) Communications	23
1.3.3.3. Hybrid Communication Model	25
1.3.4. Relevant Projects and Protocols	27
1.3.4.1. Dedicated Short Range Communication (DSRC)	27
1.3.4.2. RUNES	28
1.3.4.3. CALM	29
1.3.4.4. The Application-Based Clustering Concept and Requirements for Intervehicle Networks	31
1.3.5. Stigmergic Routing	32
1.4. Synthesis	35
1.5. Conclusion	37
Chapter II: Wired Systems	40
2.0. Introduction	40
2.1. Ethernet in Control	41
2.2. Fault-Tolerant Architecture	45
2.2.1. Fault-Tolerance at the Controller level	45
2.2.1.1. In-Line scheme	46

Content	Page
2.2.1.2. Hierarchical architecture	47
2.2.1.2.1. Passive Supervisor	47
2.2.1.2.2. Active Supervisor	48
2.2.2. Fault-Tolerance at the sensor level	48
2.3. Performance Metric	49
2.4. Industrial Networks	52
2.4.1. In-Line industrial NCS model	52
2.4.2. Reliability Modeling for Linear industrial NCS model	53
2.4.3. Hierarchical Industrial NCS model: Pyramid Model	55
2.4.3.1. Passive supervisor	57
2.4.3.2. Active Supervisor	58
2.4.3.3. Supervisor Computational Power	58
2.4.4. Reliability Modeling for Hierarchical Industrial NCS model	60
2.4.5. TMR at the sensor level of Industrial NCS	63
2.4.6. Reliability Modeling for TMR Industrial NCS	64
2.5. Vehicle On-Board Network	67
2.5.1. Fault-Tolerance at the controller level	70
2.5.2. Fault-Tolerance at the sensor level	71
2.6. Conclusion	72
Chapter III: Wireless Model	73
3.0. Introduction	73

Content	Page
3.1. Wireless Technologies and WiFi	73
3.1.1. WiFi Standards	75
3.1.2. WiMAX	79
3.2. Wireless Technology for This Research & Protocol Advantages	80
3.3. Basics of WiFi Mobility	82
3.3.1. MIPv4 (RFC3344)	85
3.3.2. MIPv6 (RFC 3775, RFC4068, RFC4260)	88
3.4. System Architecture	93
3.5. Model Variables	95
3.5.1. Communication load	95
3.5.2. Communication Internet Protocol (IP)	96
3.5.3. Network Parameter Boosting for IPv6	97
3.5.4. Burst Communication	97
3.5.5. Fault-Tolerant Architecture	98
3.6. Performance Metrics	99
3.6.1. Amount of Packet Loss	99
3.6.2. Confidence Level Calculations	100
3.6.3. Fault-Tolerant Architecture Analysis Technique	101
3.7. Conclusion	103
Chapter IV: Results	105
4.0. Introduction	105
4.1. Simulation Platform: OPNET	105

Content	Page
4.2. Context	106
4.3. Ethernet Cars Simulation Results	108
4.3.1. Ethernet Cars	109
4.3.2. Fault-Tolerant Networks	110
4.3.2.1. Fault-Tolerant Controllers	110
4.3.2.2. Triple Modular Redundancy	111
4.3.3. Fast Ethernet as NCS backbone for Cars	112
4.3.4. Discussion	113
4.4. Wireless System Parameters	114
4.4.1. Communication load	115
4.4.2. Effect of Router Advertisement Interval	117
4.4.3. Effect of Mobility Detection Factor	117
4.4.4. Fault-Tolerance Analysis	118
4.5. Wireless Simulation Results	118
4.5.1. MIPv4 Simulations Results	119
4.5.1.1. Single Vehicle Model	119
4.5.1.2. Congested Model	121
4.5.2. MIPv6 Simulations Results	124
4.5.3. Burst Communication	126
4.5.3.1. Two Packet Burst (2PB)	126
4.5.3.2. Three Packet Burst (3PB)	127
4.5.3.3. Effect of Router Advertisement Interval	130
4.5.3.4. Effect of Mobility Detection Factor	131

Content	Page
4.5.4. Fault-Tolerance	131
4.5.5. Protocol Comparison Study	133
4.5.5.1. Results for 802.11b	133
4.4.5.2. Results for 802.11g	134
4.5.5.2.1. Same-Power Architecture	134
4.5.5.2.2. Same-coverage-area architecture	134
4.5.5.2.3. Results Analysis	135
4.5.5.3. Effect of Changing the Packet Reception Power Threshold on network performance	136
4.5.5.3.1. Results	136
4.5.5.3.2. Comments	138
4.6. Hardware Tests Results	139
4.7. Conclusion	141
Conclusion	142
References	146
Appendix A	a
Appendix B	n
Appendix C	q
Appendix D	v

ACKNOWLEDGMENTS

I would like to express my deep thanks and sincere gratitude to Prof. Christian Tahon, and Dr. Yves Sallez, for their valuable guidance, deep interest, continuous encouragement, their supervision and their valuable advice through the whole course of this work.

I am greatly indebted to Dr. Hassanein Amer, Chair and Associate Professor, Electronics Engineering Department, American University in Cairo, for his help, support, and continuous back-up allover this study.

I would like also to thank Prof. Eric Rondeau and Prof. Jean-Marc Thiriet to report on this work. Also, I have to thank Prof. Mireille Bayart and Dr. Thierry Ernest to accept being part of the jury.

I am also grateful to Prof. Magdi El-Soudani deputy chairman, National Telecommunication Institute (NTI) and Dr. Hany Elsayed, Electronics and Communications Department, Faculty of Engineering, Cairo University, for their guidance allover this work.

I am also thankful to all SEAD team as well as OPNET technical support for the help and assistance they offered during the last years.

I can never forget Eng. Mohamed El-Dakroury, Vodafone Egypt, for his precious technical assistance.

I have also to acknowledge the help and support of Eng. Mohamed Mostafa, Electronics Engineering Department, AUC, and Eng. Sinout Shenouda, Computer Science Department, AUC, they offered to facilitate using departments' laboratories, tools and OPNET.

Last but not least, thanks go to all AUC and LAMIH technical team who facilitated the periodic Video Conferences between Egypt and France. These Conferences made the mutual cooperation come true.

ABSTRACT

This study focuses on the wireless as well as the wired aspect of Intelligent Transportation Systems (ITS).

The On-Board network of a future smart vehicle is designed using Switched Ethernet as a backbone. This architecture aims at minimizing the amount of wiring present in today's cars. With the increasing demand of entertainment and connectivity, the proposed model provides the vehicle passengers with internet connection, video on-demand, voice over IP (VoIP) and video conference capabilities. Also, to help the driver, a smart real-time interactive communication scheme is developed to supply traffic information.

A wireless communication model is built to support the moving entities in a light urban traffic area; the model is based on stigmergic algorithms running at the core of the system infrastructure. A WiFi model is used to supply wireless connectivity to mobile nodes in a given region. The Mobile IPv4 as well as Mobile IPv6 are tested. The mobile nodes always communicate with the central intelligence of the system to update the traffic information. The stigmergic algorithm processes this data and sends to all moving vehicles messages regarding the actual traffic map. This research focuses on the wireless aspect of the problem and optimizes the architecture to satisfy minimum packet loss in the path from the central correspondent node (CN) to the mobile nodes (MN).

It is found that based on MIPv6 technique and using redundant packet transmission (burst communication) one can statistically reach satisfactory packet reception at the MN.

RESUME

Cette étude se focalise sur les aspects de communications filaires et sans fil des systèmes de transports intelligents. Dans une première partie, le réseau embarqué d'un véhicule est constitué à l'aide du réseau Ethernet. Cette approche vise à diminuer la quantité de câbles présents dans les véhicules actuels. Le modèle proposé apporte une aide pour satisfaire les demandes de communications des passagers des véhicules futurs en ce qui concerne les connections Internet, les vidéos en demande, les communications Voice over IP (VoIP) et les vidéos conférences. Un système de communication, interactif et temps réel, est également proposé pour assister le conducteur en fournissant des informations sur le trafic. Une seconde partie est consacrée à la communication sans fil pour la gestion des informations échangées entre entités mobiles dans une zone de trafic urbain. Un modèle de système de communication, s'appuyant sur la technologie WiFi, est utilisé pour les échanges d'informations entre les entités mobiles et entre un point central de communication (noeud de correspondance). Des algorithmes stigmergiques sont utilisés pour le pilotage des entités mobiles. Les entités mobiles communiquent continuellement avec le système de pilotage pour mettre à jour les informations du trafic. Le système de pilotage analyse ces informations et diffuse à tous les véhicules, sous forme de messages, la cartographie du trafic. Le modèle de communication "burst communication" et les techniques de communications mobiles MIPv6 ont été exploités. L'optimisation de l'architecture du modèle de communication permet d'obtenir un nombre minimum de messages perdus lors de la communication entre le point central et les mobiles. Les résultats obtenus montrent que l'on peut parvenir à une réception satisfaisante des messages au niveau des entités mobiles.

LIST OF FIGURES

Figure	Caption	Page
Fig.: 1.1	Vehicle On-Board Network and Interaction with Surrounding Environment	7
Fig.: 1.2	Different Car On-Board Networks	11
Fig.: 1.3	Vehicles' Interaction with Surrounding Environment	15
Fig.: 1.4	Basemap Unit Screen Shot	16
Fig.: 1.5	Mapping Unit Screen Shot	16
Fig.: 1.6	Route by Shortest Distance	19
Fig.: 1.7	Route by Minimum Turning	19
Fig.: 1.8	Route Through Mountains	19
Fig.: 1.9	Route by the Side of the River	19
Fig.: 1.10	Active FCD Model	20
Fig.: 1.11	Multihop V2V Communication	23
Fig.: 1.12	Full Coverage V2I/I2V Communication	25
Fig.: 1.13	Hybrid Communication Model Scenario	26
Fig.: 1.14	Virtual pheromones modeling	34
Fig.: 2.1	Modeling Philosophy	40
Fig.: 2.2	NCS Block Diagram	42
Fig.: 2.3	A general network hierarchy model	44

Figure	Caption	Page
Fig.: 2.4	Linear Fault-Tolerant Controllers	46
Fig.: 2.5	Hierarchical Fault-Tolerant Controllers	47
Fig.: 2.6	Reliability Model	54
Fig.: 2.7	Availability Model	54
Fig.: 2.8	Markov Model	55
Fig.: 2.9	The Increase in Supervisor Computational Power	60
Fig.: 2.10	Markov Model	62
Fig.: 2.11	RBD for 2-Cont Configuration	65
Fig.: 2.12	RBD for TMR Configuration	65
Fig.: 2.13	Vehicle On-Board Network Block Diagram	67
Fig.: 2.14	Fault-Tolerant Vehicle On-Board Network Controllers	71
Fig.: 2.15	TMR Vehicle On-Board Network Sensors	71
Fig.: 3.1	Comparison of Different Technologies with Respect to Range, Bit Rate and Mobility	74
Fig.: 3.2	Network Layers and Their Relation with WiFi	76
Fig.: 3.3	Infrastructure of the 802.11 WLAN	76
Fig.: 3.4	Different Operations of WiFi	77
Fig.: 3.5	Wireless Technologies Mobility Curve	81
Fig.: 3.6	IPv4 MN at HA	86
Fig.: 3.7	IPv4 MN Moves to FA	87
Fig.: 3.8	IPv4 MN Establishes Tunnel at FA	87
Fig.: 3.9	IPv6 MN at Home Network	90

Figure	Caption	Page
Fig.: 3.10	IPv6 MN Moves to Foreign Network	90
Fig.: 3.11	IPv6 MN Performs Tunnel with CN via HA	91
Fig.: 3.12	IPv6 MN Performs Route Optimization with CN	92
Fig.: 3.13	IPv6 MN Moves to New Foreign Network	92
Fig.: 3.14	Basic Seven Cell Layout	93
Fig.: 3.15	Hexagon (Honey-Cell) Layout	94
Fig.: 3.16	System Star Backbone	94
Fig.: 4.1	End-to-end Delay with Added Video Terminal	110
Fig.: 4.2	Model Diagram of 2 Controllers	111
Fig.: 4.3	End-to-end Delay for Class C Control Load Only	111
Fig.: 4.4	End-to-end Delay for Class A and B with FTP and Video Loads	111
Fig.: 4.5	End-to-end Delay for TMR Sensors Network	112
Fig.: 4.6	Fast Ethernet End-to-end Delay for Pure Control Load	113
Fig.: 4.7	Fast Ethernet End-to-end Delay for with added Video Load	113
Fig.: 4.8	Snap Shot of OPNET environment for 1MN	120
Fig.: 4.9	1MN, V=33Km/hr; IPT=30sec;MIPv4	120
Fig.: 4.10	1MN, V=60Km/hr; IPT=30sec;MIPv4	120
Fig.: 4.11	1MN, V=33Km/hr; IPT 90sec; MIPv4	121
Fig.: 4.12	Snap Shot of OPNET Environment for Congested Model	121
Fig.: 4.13	MN V=6Km/hr; IPT 30sec; MIPv4, Congested Model	122
Fig.: 4.14	MN V=60Km/hr; IPT 120sec; MIPv4, Congested Model	123
Fig.: 4.15	MN V=60Km/hr; IPT30; MIPv6, Congested Model	124

Figure	Caption	Page
Fig.: 4.16	MN V=6Km/hr; IPT30; MIPv6, Congested Model	124
Fig.: 4.17	MN V= 33Km/hr, MIPv4, 2PB	127
Fig.: 4.18	Transmit Power Increase of Adjacent APs	131
Fig.: 4.19	φ Variations	132
Fig.: 4.20	Traffic Received in Packets/Second and AP Connectivity for A Mobile Node Moving at 60Km/Hr in 802.11g Architecture, Transmit Power 80mW	135
Fig.: 4.21	Traffic received in packets/second and AP connectivity for a mobile node moving at 33Km/hr in 802.11b architecture, transmit power 4mW	137
Fig.: 4.22	Signal Strength of AP	140
Fig.: 4.23	Interference caused by surrounding APs	140

ABBREVIATIONS & SYMBOLS

μs	Micro Seconds
2G	2nd Generation Mobile Communication
2PB	Two Packet Burst
3G	3rd Generation Mobile Communication
3PB	Three Packet Burst
ABS	Antilock Braking System
ADASE2	Advanced Driver Assistance System in Europe
AHSRA	Advanced Cruise-Assist Highway System Research Association
AP	Access Point
AP_D	Inter-AP distance
AP-P_t	AP Transmit Power
AR	Access Router
AUC	American University in Cairo
BA	Binding Acknowledge
BC	Binding Cache
Bps	Bytes per seconds
BR	Broadcast Rate

BSS	Basic Service Set
BU	Binding Update
BW	Band Width
CALM	Communications Architecture for Local Mobile environment
CAMP	Crash Avoidance Metrics Partnership
CAN	Control Area Network
CD	Compact Disc
CN	Central (Correspondent) Node
CoA	Care of Address
CRC	Cyclic Redundant Check
CSMA	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear To Send
DAB	Digital Audio Broadcast
DCF	Distributed Coordination Function
DDB	Digital Data Broadcasting
DHCPv6	Dynamic Host Configuration Protocol version 6
DRE	Distributed Real-time and Embedded systems
DS	Distribution System
DSRC	Dedicated Short Range Communications
DSSS	Direct Sequence Spread Spectrum
DVB	Digital Video Broadcasting
DVD	Digital Versatile Disc

ECU	Electronic Control Units
EMI	Electro-Magnetic Interference
EPS	Electric Power Steering
ESP	Electronic Stability Program
ESS	Extended Service Set
EUI	Extended Unique Identifier
FA	Foreign Agent
FCD	Floating Car Data
FHSS	Frequency Hopping Spread Spectrum
FLAC	Falaki Academic Center
FTP	File Transport Protocol
GA	Generic Algorithm
Gbps	Giga bits per seconds
GHz	Giga Hertz
GPS	Global Positioning System
GUI	Graphical User Interface
HA	Home Agent
HMI	Human Machine Interface
hr	Hour
HR-DSSS	High Rate Direct Sequence Spread Spectrum
HTTP	HyperText Transfer Protocol
I2V	Infrastructure to Vehicle
IP	Internet Protocol
IPT	Inter-Packet transmission Time

IPTV	Internet Protocol Television
ISM	Industrial Scientific and Medical
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITS	Intelligent Transportation Systems
IVC	Inter-Vehicle Communication
JARI/ITSC	Japan Automobile Reseach Institute/Intelligent Transportation Systems Center
Kbps	Kilo bits per seconds
KBps	Kilo Bytes per seconds
Km	Kilometer
L	The total number of packets lost in the overlapping region
LAN	Local Area Network
LoS	Line of Sight
MAC	Media Access Controller
MAN	Metropolitan Area Network
Mbits/s	Mega bits per seconds
Mbps	Mega bits per seconds
MDF	Mobility Detection Factor
MIP	Mobile Internet Protocol
MIPv4	Mobile Internet Protocol version 4
MIPv6	Mobile Internet Protocol version 6
MN	Mobile Node
MRB	Message Relay Box

ms	Milliseconds
MT	Mission Time
MTTF	Mean Time To Failure
mW	Milli Watts
NCS	Networked Control Systems
NES	Networked Embedded Systems
OFDM	Orthogonal Frequency Division Multiplexing
PDA	Personal Digital Assistant
PLC	Programmable Logic Controller
POF	Plastic Optical Fiber
QoS	Quality of Service
R	Cell Radius
RAI	Router Advertisement Interval
RBD	Reliability Block Diagram
RTS	Request To Send
S	The car speed
S_D	Shadow Distance (the overlapped distance between the cells)
sec	Seconds
SMS	Short Message Service
SSID	Service Set Identifier
Std	Standard
t_{burst}	the time between the first packets of two successive bursts
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access

t_{F2L}	the time between the first and the last packet in the same burst
TMR	Triple Modular Redundancy
t_{packet}	the time between two successive packets within the same burst
TV	Television
UDP	User Datagram Protocol
USAID	United States Agency for International Development
USDoD	United States Department of Defense
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V_H	High Speed
V_L	Low Speed
V_M	Medium Speed
VoIP	Voice over Internet Protocol
VSC	Vehicle Safety Communications
VSCC	Vehicle Safety Communications Consortium
WAN	Wide Area Network
WAVE	Wireless Access in Vehicle Environment
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WN	Wireless Node
WSN	Wireless Sensor Networks
z	Standardized normal random variable with mean=0 and variance =1
X	Random Variable

μ	Average of Random Variable X
σ^2	Variance of Random Variable X
i	Running Sum Counter
n	Number of Simulations
x	Sample Mean
s^2	Sample Variance
n_i	Number of Burst Loss

INTRODUCTION

WHILE the twentieth century was the century of connectivity and internetworking, the twenty first century will with no doubt be the century of wireless connectivity and mobility.

In the twentieth century Internet was firstly introduced, Ethernet was standardized, Decentralized control and distributed systems were studied. Several network standards and control strategies based on networks replacing centralized control were proposed and analyzed. The Famous CAN was strongly deployed as the standard deterministic control network for different application specially in automotive industries. The basic networks for railway industry automation are TCN and LonWorks. Personal Mobile Communication was strongly introduced and wireless phones became essential for our daily routine.

The twenty first century needs more throughput and mobility.

In 2000, the new Ethernet (IEEE 802.3z) standard allows Gigabit speed up to 10Gbps. The last ten years more studies to introduce the Ether-channel in control are developed. It is enough to have a look on [DEC 05] to find that Ethernet in control is a big issue. Ethernet is also important for home and building automation. It is deployed everywhere on the globe and getting cheaper. It is flexible, and scalable. It solves many problems, but it suffers non-determinism.

In 1999, the IEEE introduced to the world the new wireless internetworking standard (802.11). Now, Ethernet can go wireless. WiFi is the new protocol to be connected without wires. Over the last five years, one can see WiFi growth exponentially. Every

laptop computer is equipped with WiFi. Many hand-held phones are WiFi enabled. When there is a need for high throughput over wireless connection, you find WiFi.

Although WiFi is a big step in the world of wireless internetworking and communication, it suffers two main points: high data rate and mobility. While WiFi offers better data rates than the 2.5G and 3G of the personal mobile communication systems, it lacks the wired Ethernet speed. Hand-off is an issue for wireless data networks, but it is already resolved in personal mobile communication networks.

Hand-off (or handover) mechanism is an issue for wireless networks. In WiFi, each wireless node is identified by a unique address, its Internet Protocol (IP). It is then difficult to maintain connectivity when the mobile node (MN) changes its point of attachment to the network, because it changes its IP address. Changing IP means breaking an open session between two communicating nodes because the MN is no longer reachable by its old address. Lots of efforts are put in this topic to find the optimum and seamless hand-off techniques.

The large growth in network use generally demands a new address protocol to accommodate this large number. After IPv4, IPv6 is introduced and in its way for deployment. A big share of the network cards manufacturers are now making these cards IPv6 compatible, both for wired as well as for wireless.

With the presence of both IPv4 and IPv6, hand-off task forces worked first on MIPv4 (Mobile IPv4), and then migrated to MIPv6 (Mobile IPv6) to support mobility in IPv4 and IPv6 respectively. RFC (MIPv4) defines a hand-off mechanism for IPv4, while RFC (MIPv6) defines a hand-over mechanism for IPv6. Hand-off and hand-over are used interchangeably in this document.

A clear example of control can be a moving vehicle where two types of networks exist. The wired control network and the wireless communication network that can also be used for control. The wired network is for on-board control of the different vehicle systems. The wireless network is used to control traffic conditions in a given urban, sub-urban area

or on a highway. These are two different types of control applications using two different types of communication networks.

On-board the moving vehicle, different control applications are working together in harmony to satisfy a safe trip for the passengers. Power-train, chassis, safety and entertainment networks are always present and they suffer their implementation using incompatible protocols. Although each network has its own demands of bandwidth and critical deadlines to be met, sometimes the need to exchange information between different Electronic Control Units (ECU) of different networks exists. A simple example would be the need for friction index of wheels with the road surface (measured by the chassis network) to be used for the airbags expansion (actuated by the safety network) in case of accident. Also, the By-Wire systems are more deployed in cars specially the steering-by-wire systems. These are more electronics that need more communication to accomplish highest safety measures.

The use of a single network that interconnects all of these systems and unifies the communication protocol of the on-board system is required. The network must satisfy control systems' deadlines and at the same time guarantee the entertainment systems' Quality of Service (QoS). Ethernet implementation of Networked Control Systems can be the single protocol to accommodate all cars' services and requirements.

DVD and entertainment screens are more frequently included for rear-passengers. Also, navigation and guidance systems are often mounted in cars. These systems may need to have an interaction with the outside of the car. The guidance systems becoming smart, they may collect information from the surrounding environment for navigation use. This information can be centralized or de-centralized. In case of centralized traffic information, a central node collects information, processes it and then diffuses correct status for moving cars. In case of de-centralized, adjacent moving entities can share information based on knowledge collected from other surrounding cars for example. A video conference can also be done including the car's passengers. This demands wireless data communication and large bandwidth.

All of these wireless requirements may be implemented using WiFi.

Ethernet and WiFi are then becoming essential for tomorrow's cars. One can say that today's cars is an electronic systems that happened to have an internal combustion engine, while tomorrow's cars will also include an electric motor to become fully electric and electronic systems running on 4 wheels.

The rest of this research is organized as follows: Chapter I is a survey of the comely used guidance systems, wireless communication models, together with an introduction to the stigmergic approach and some relevant projects similar to the one presented in this research. Chapter II introduces and explains the proposed wired model of the on-board control and communication network of the vehicle based on Ethernet Networked Control System techniques early introduced by the research team in the context of Industrial control and informatics. The wireless proposed model of communication is presented in chapter III. This chapter introduces the different wireless protocols available nowadays. It as well presents the advantages and disadvantages of the proposed WiFi as communication protocol. Results of the wired model in cars and industrial applications are given together with the wireless model simulations and hardware implementation is presented in Chapter IV. Final conclusions are then given with some future works.

CHAPTER I

SURVEY

1.0. INTRODUCTION

SIGNIFICANT activities are underway worldwide to develop Vehicle Safety Communications (VSC) technologies. These include, for example, in the United States, the ITS America VII (Vehicle-Infrastructure Integration) effort on 5.9GHz, Wireless Access in Vehicle Environment (WAVE) communication for all vehicles, the U.S. Department of Transportation Intelligent Vehicle Initiative (IVI) program to accelerate R&D of crash avoidance technologies and initiatives such as the Crash Avoidance Metrics Partnership (CAMP), VSC Consortium (VSCC). Similar examples include, in the European Union, the e-Safety and ADASE2 (Advanced Driver Assistance Systems in Europe) efforts, and in Japan efforts in the ITS Infocommunications Forum, Japan Automobile Research Institute/ITS Center (JARI/ITSC) and Advanced Cruise-Assist Highway System Research Association (AHSRA) [NAV 05].

VSC may be broadly categorized into vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. In V2V communications, vehicles communicate with each other without support from the infrastructure. Vehicles communicate with each other when they are covered within the same radio range, or when multiple-hop [VEC 03] relay via other vehicles is possible. In the V2I communication case, vehicles communicate with each other with the support of infrastructure such as roadside wireless

access points (AP). In this case, vehicles may also communicate with the infrastructure only.

Examples of V2V safety communication may include collision warning, road obstacle warning, cooperative driving, intersection collision warning, and lane change assistance [NAV 05, BER 01, ZEN 05, WIL 05]. Examples of V2I safety communication may include hidden driveway warning, electronic road signs, intersection collision warning, railroad crossing warning, work zone warning, highway merge assistance, and automated driving [NAV 05].

Today luxury cars are equipped with many electronic components. These are control components as well as entertainment components. The control components include the new generation of Electronic Stability Programs, brake by-wire, steer by-wire, etc... The on-board entertainment especially for rear passengers is becoming more popular the last years. These systems include video screens, sound systems, etc... The future cars will include more navigation and sophisticated guidance systems. Also, internet connectivity will be a must. Voice over IP (VoIP) applications demanding internet connections will be an important component of tomorrow's cars. This requires internet wireless connection for the moving cars. It also demands more complex networks on-board of the moving vehicles. These networks will share resources and will work side by side to accomplish one aim: satisfaction and safety of the vehicles' occupants. A Proposed model for the future vehicle on-board networks is presented and studied in this research.

Next, some vehicle networks are introduced. These are control and entertainment networks. Some guidance systems are mentioned. Communication models as tool to communicate information between moving cars and system intelligence are then summarized. A discussion covering the stigmergic approach follows. The stigmergic approach within the context of this research is an algorithm to solve the vehicles traffic control in light urban areas or tourist resorts. Some relevant projects and protocols are also introduced. Finally the problem statement is presented.

1.1. FUTURE VEHICLE MODEL

Today's luxury cars are equipped with lots of sophisticated driving assistance as well as safety and entertainment features (Fig. 1.1). Among these features, one can list parking assistance, electronic stability program, brake assistance and brake-by-wire, cruise control, electric steering assistance, navigation assistance, run-on-flat tires, new airbags and seatbelts generations, climate comfort, premium acoustic systems, video entertainment, wireless phones connections, etc... These features and more will be standard configurations for tomorrow's cars.

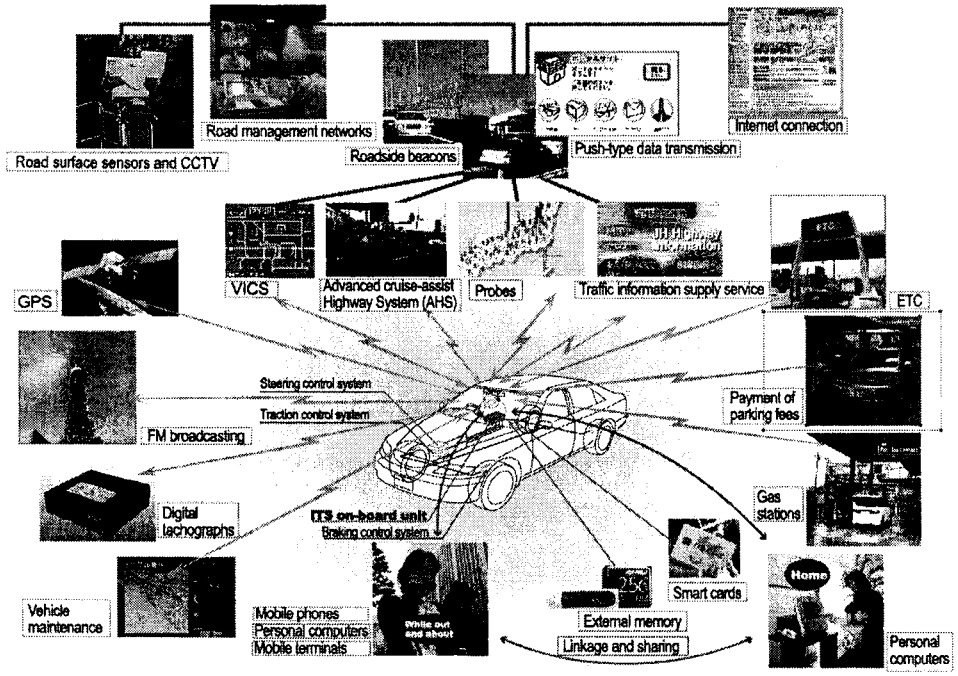


Fig. 1.1, Vehicle On-Board Network and Interaction with Surrounding Environment [ITS]

With the presence of traditional mechanical or hybrid engines, one can say that today's cars are electronic systems that happen to have an internal combustion engine. With future electric engines, cars will be full electronic systems moving on 4 wheels.

Tomorrow's car with its communication capabilities will be able to connect to the internet via the roadside infrastructure to facilitate data communication, internet surfing,

video on demand, video calls, and more entertainment features. Moreover, this roadside infrastructure will be useful to assist the on-board navigation systems for optimal guidance (Fig. 1.1).

With the help of two-way communication that will appear completely transparent to passengers, the moving cars will communicate with the surrounding environment to give information about actual traffic conditions, and to get data about the future traffic behavior. This will be with the help of central infrastructure intelligence that collects these data from allover the traffic map and after rendering, it broadcasts the present and forecasted traffic status.

Also, the moving cars will have their near space (in contrast to the far space presented in the previous paragraph) communication with surrounding moving entities. In this near space, the moving vehicles exchange data in a peer-to-peer fashion to prevent obstacles, increase driving safety by limiting driving speed or driving distance with respect to surrounding vehicles, etc... Here the word *entity* is used instead of "vehicle or car" to generalize the model applications.

All of these features demand: wireless communications and intelligence. There are three types of wireless communications in this model: satellite communications, infrastructure communications and peer-to-peer communications. Regarding the intelligence: vehicle on-board intelligence and infrastructure intelligence are needed.

Satellite communication is needed for the guidance systems to interact with current positioning systems for allocation of the starting point, current and final destinations of a moving entity on an electronic map.

Infrastructure communication is needed for system interaction and it is in two-way communication: moving entity-to-infrastructure and infrastructure-to-moving entity. This two way communication enriches the infrastructure intelligence with the current situation of the traffic map in one communication way. In the other way, it collects global information already processed on the central intelligence.

The on-board intelligence, processes the collected information from the infrastructure, together with the one received while it is connected with other moving nodes in the peer-to-peer communication mode. This process generates a final useful decision for the system user: either a simple pedestrian moving on foot using a handy navigation unit, or a driver in a moving car or finally in robotized cars (cyber cars) [CYB].

Table 1.1 summarizes some main vehicles functions and their requirements regarding communication networks.

Table: 1.1
Functions and Tools

Functions/Tools	On-Board Networks & Equipments	Ad-Hoc Communication	Infrastructure Communication
Navigation/Guidance Assistance	X	X	X
On-board Entertainment	X		X
Telematics	X		X
Parking Assistance	X		
Collision Avoidance	X	X	
Automatic Accident Detection	X	X	X
Passenger Safety	X		
Engine Diagnostics	X		
Steering Assistance	X		
On-Board Comfort	X		

1.2. ON-BOARD SYSTEMS

The use of networks for communications between the electronic control units (ECU) of a vehicle in cars dates from the beginning of the 1990s [NAV 05]. The specific requirements of the different car domains have led to the development of a large number of automotive networks such as Local Interconnect Networks, J1850, CAN, TTP/C, FlexRay, media oriented system transport, IDB1394, MOST and ByteFlight [NAV 05, VEC 03].

Antilock Braking System (ABS), Electronic Stability Program (ESP), Electric Power Steering (EPS), Active Suspensions, By-Wire systems and more functions are made

available nowadays due to the high reliability of hardware components integrated in car manufacturing [NAV 05, BRE 01]. Some parts can be partially mechanical and partially electronic like the steering model proposed in [ZEN 05]. More added functions for on-board entertainment also use networks. DVD, hands-free phones, navigation systems are clear examples of these. An important problem may however arise from this migration to electronic controlled cars, namely electromagnetic interference (EMI) [WIL 05].

As sharing of information is important for increased safety, the implementation of stand alone functions for every part like in the early days of automotive electronics, is inefficient. For example, the information from the braking system is important for seat-belts and air-bags activation. Another example is weather information for the adjustment of the on-board climate comfort.

From these two simple examples, it is clear that different functions have different quality of service (QoS) requirements and measures. Accordingly, these applications are divided into real-time and non-real-time functions.

Real-Time control and safety of the vehicle's behavior are the responsibility of the *powertrain* (control of engine and transmission) and the *chassis* (suspension, steering and braking control). The *body* mostly implements comfort functions (dashboard, wipers, lights, doors, etc). The *telematics*, *multimedia* and *human-machine interface* (HMI) take care of on-board entertainment (CD, DVD, car audio, navigation systems, rear seat entertainment, remote vehicle diagnostics, etc) with easy HMI to minimize driver distraction. *Active and Passive Safety* form an emerging domain that ensures the safety of the occupants (impact and rollover sensors, airbags deployment, etc) [NAV 05, BRE 01, UPE 96].

More explanations and detailed on-board popular networks for car control and entertainment (Fig. 1.2) can be found for example in [NAV 05, VEC 03, BRE 01, WIL 05].

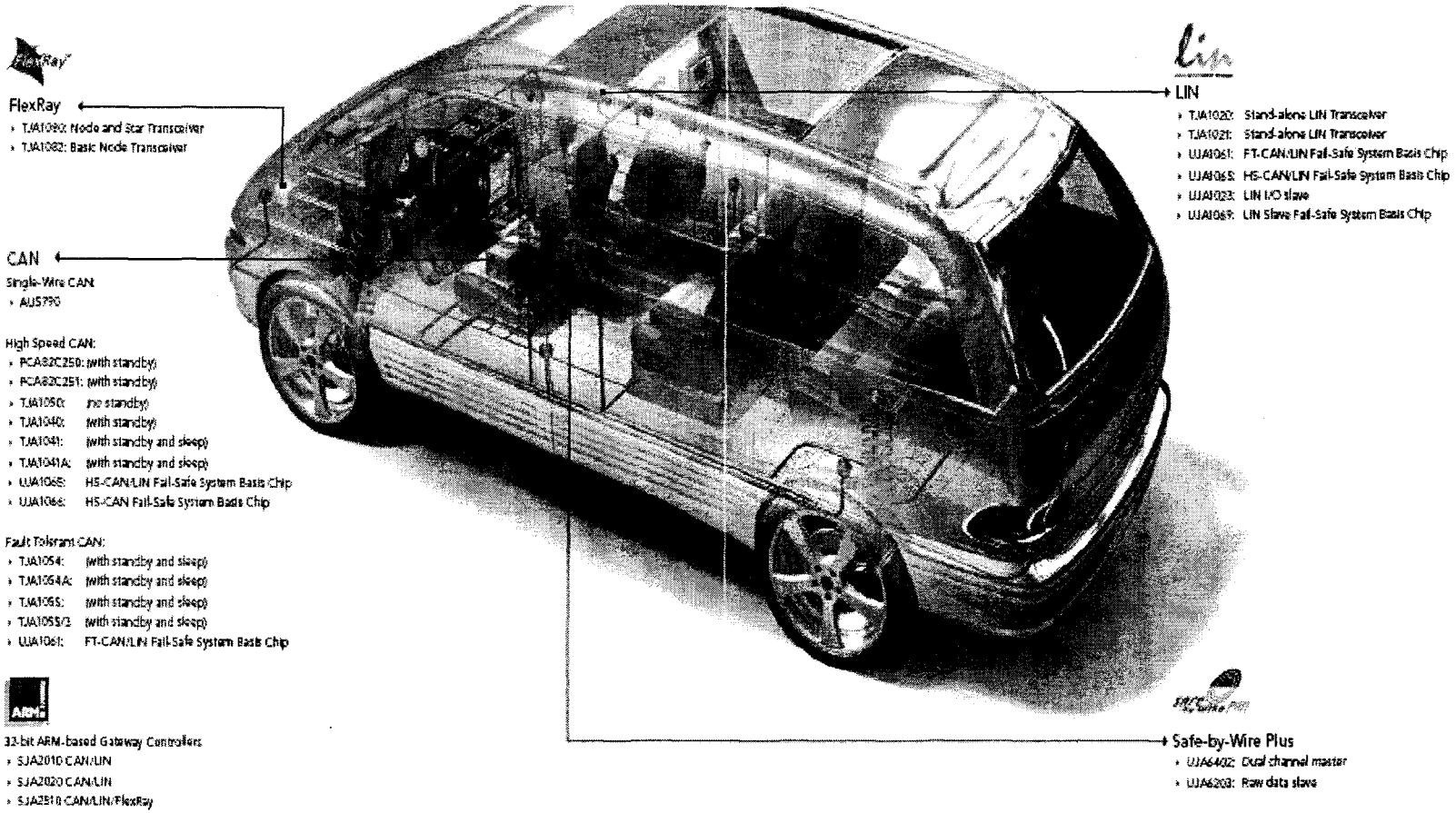


Fig. 1.2, Different Car On-Board Networks [NXP 06]

1.2.1. By-Wire

Someday, by-wire systems will automatically steer the car and reduce its speed from 80Km/hr to 40Km/hr to 0Km/hr without specific action on the driver's part. Instead, input will come from a built-in positioning system, road-condition sensors, and nearby cars to determine the safest path for vehicles likely to collide. The necessary calculations will be made by powerful on-board computers.

The transition from mechanical systems to the electronic systems of by-wire is being done step by step. Drive-by-wire has been used in diesel-fueled cars; it is implemented on some high performance gasoline-fueled cars now. Pressing the accelerator determines the position of the throttle plate within the air intake system for the engine cylinders. A mechanical linkage transmits the accelerator pedal position to the throttle plate. In throttle-by-wire, the throttle plate is controlled by a motor controlled by computer or microcontroller that is independent of the accelerator. Electronic control of this plate offers improved fuel economy and emissions by maintaining optimal throttle conditions at all times, something human drivers cannot do.

Front steer-by-wire eliminates the mechanical connection between a vehicle's front wheels and its driver, so turning the steering wheel does not directly turn them, it sends a signal to a motor at each of the front wheels. This signal instructs the motor to turn the wheels [ZEN 05, THO 06].

Brake-by-wire does everything: the antilock and traction-control functions of today's antilock braking systems plus brake power assist, vehicle stability enhancement control, parking brake control, and tunable pedal feel, all in a single modular system. With today's antilock brakes, the electronics do the brake-pedal pumping instead of the driver, but otherwise they are still mechanical systems.

Safety and stability are the heart of the push to develop automotive by-wire technology, especially for a breaking-and-steering combination. *"The goal is to make the average driver as skilled as a professional driver in stabilizing the car"* [BRE 01].

1.2.2. Multimedia

Many protocols have been adapted or specifically conceived for transmitting the large amount of data needed by emerging multimedia applications in automotive systems. Two main networks are currently of interest: MOST and IDB-1394.

MOST is a multimedia network developed by MOST Corporation. It provides point-to-point audio and video data transfer with a data rate of 24.8Mbps. This supports end-user applications like radios, global positioning system (GPS) navigation, video displays and entertainment systems. MOST's physical layer is plastic optical fiber (POF) which provides a much better resilience to Electromagnetic Interference (EMI) and higher transmission rates than classical copper wires [WIL 05].

IDB-1394 is an automotive version of IEEE 1394 for in-vehicle multimedia and telematic. It permits existing IEEE 1394 consumer electronics to interoperate with embedded automotive grade devices. IDB-1394 supports data rate of 100Mbps over twisted pair or POF, with a maximum number of 63 embedded devices.

1.2.3. Control

Commentaire [RD1] : Tell CAN, and others breifly

Controller Area Network (CAN) is a collision avoidance protocol. To access the shared media, all nodes wait for an idle channel before initiating a transmission. Each transmission begins with a unique identification number. Nodes transmitting simultaneously resolve contention by backing-off from the transmission when they detect a dominant bit while sending a passive bit based on the bit dominance algorithm (also known as binary countdown) [UPE 96].

Class C vehicle communications impose demanding requirements on an underlying communication protocol. The CAN protocol, developed for automotive applications, addresses these requirements through collision avoidance and global prioritization.

Class C communications incorporate three types of in- vehicle messages: low-speed body electronic information, medium-speed parametric sensor data, and real-time control signals. In particular, the high-speed control messages are driven by time-critical control systems such as the Powertrain Control Module, Anti-lock Brake System, and Passenger Safety System (air bags, etc...). These high performance systems require large network bandwidth, quick channel access time, reliable message delivery, and predictable response times to guarantee safe operation.

The actual model of vehicle on-board network suffers the presence of different incompatible networks. These networks sometimes need to communicate together to exchange or relay information. To switch from one network to the other, a need to use bridges appears. These bridges translate the data from one packet format to the other so that the information becomes accessible in the new network. Bridges are heavy components and their presence is a must in today's vehicle on-board network implementation.

1.3. VEHICLES INTERACTION WITH EXTERNAL ENVIRONMENT

As early explained, the moving vehicles need to interact with the surround environment in order to have access to enough information for smart guidance (Fig. 1.3). This interaction is based on the communication with satellite systems, infrastructure and neighboring vehicles. In the following, a brief introduction of the present systems that can assist for smart navigation is presented together with some undergoing projects.

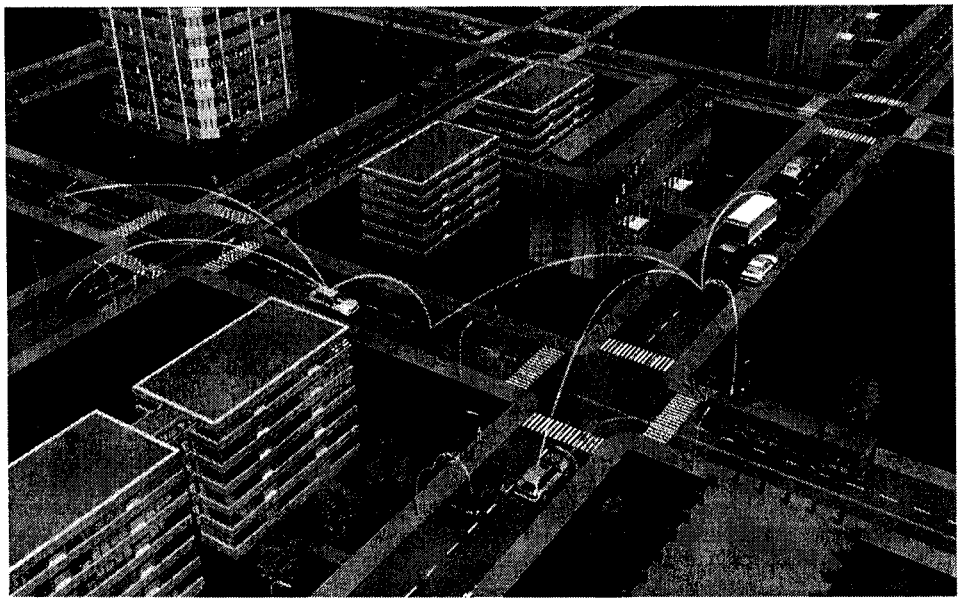


Fig. 1.3, Vehicles' Interaction with Surrounding Environment

1.3.1. Guidance

For a car to traverse from its starting point to its destination point, some navigation tools are present on the market to guide the driver in his journey. These navigation or guidance tools are using Global Position System technology (satellite communication).

There exist several types of GPS units: Nonmapping Units, Basemap Units and Mapping Units [GAR].

Nonmapping Units are GPS units with no map detail. They have a plotter screen that can show an overhead view of the location relative to any waypoints, routes or track logs created by the user. The plotter screen will help in determining the position in relation to these items.

Basemap Units (Fig. 1.4) show interstates, US and state highways, major thoroughfares in metro areas, lakes, rivers, railroads, coastlines, cities, airport locations, etc...

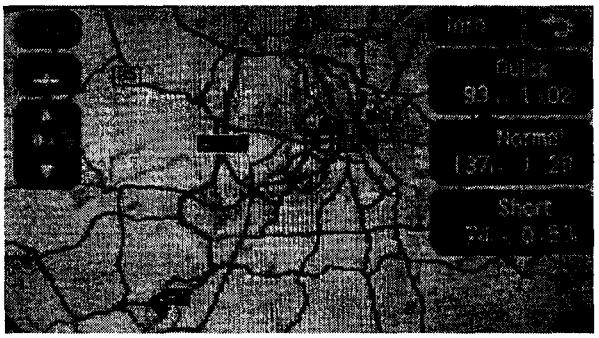


Fig. 1.4, Basemap Unit Screen Shot

Mapping Units (Fig. 1.5) can download detailed maps from CD. Map data include business and residential streets, restaurants, banks, gas stations, tourist attractions, marine navigational data, boast ramps, topographic detail, off-road trails and much more.

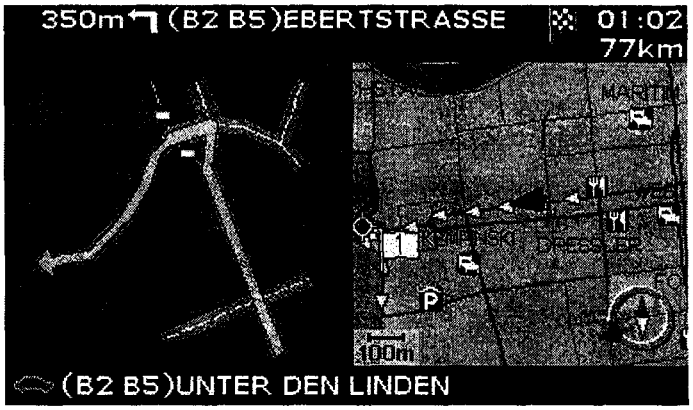


Fig.: 1.5, Mapping Unit Screen Shot

GPS is rapidly becoming commonplace in cars. Some basic systems are already in place, providing emergency roadside assistance at the push of a button (by transmitting the current location of the vehicle to an emergency center). Other systems can show the vehicle's position on an electronics map display, allowing drivers to keep track of where they are and look up street addresses, restaurants, hotels and other destinations. Some systems can also automatically create route and give turn-by-turn directions to a designated location.

Galileo is another satellite global positioning system that is under development. It will give more accurate localization based on correction feedback signals from complementary ground stations [GAL].

In General, positioning systems can be categorized into self positioning and remote positioning techniques. GPS and Galileo are perfect examples to help users to self position themselves, while cell identification and time delay methods are examples of remote positioning techniques [ZEI 02]. These two methods can be used independently, or can be combined [MOK 06].

1.3.2. Present Guidance Systems and Projects

Some navigation systems are available on the market. They rely on the use of OFF-line maps. Theses maps help to direct the user through the roads of a given city or the highways of a given country. Together with the help of the GPS, the handheld device mounted in a car, motorcycle or using a PDA, the navigation software directs the user to reach its destination point. These systems like TomTom [TOM] or ViaMichelin [VMN] are working without having an ON-line access of the traffic information. The knowledge of the traffic status is important for the guidance algorithm to help the drivers to take the most efficient trajectories to reach there destination. Stigmergic algorithm can be used to provide this assistance.

In the following, some examples for projects that try to integrate present navigation systems with traffic knowledge to increase the reliability of the offered service are discussed. For more projects, please consult the following references, [YAN 04, PRO 05, FAR 05, SCH 06, FRE 06, FRO 06] for cooperative and accident free driving, [BRI 06], introducing the safe tunnel project integrating wireless communication and intelligent infrastructure and [BAT 06, HOL 06] for accident free driving.

1.3.2.1. Car Navigation Systems using Generic Algorithm

One of the essential component of a car navigation system is route planning. Given a set of origin destination pair, there could be many possible routes for a driver. A useful routing system for car navigation should have the capability to support the driver effectively in deciding on an optimum route to his preference in a dynamic environment. Search for optimal route from one point to another on a weighted graph is a well known problem and has several solutions. There are several search algorithms for the shortest path problem: breadth first search, Dijkstra algorithm, Bellman-Ford algorithm to name a few. Although these algorithms can produce stable solutions, they exhibit high computational complexity specially in changing real time environment. Moreover, in case of car navigation, the shortest path may not be the best one from other considerations such as simplicity, traffic congestion environmental problem or simply user's satisfaction. The driver may need or like to visit specific sites on the way. So for an efficient practical car navigation device in dynamic environment, a need to specify multiple and separate good (near optimal) choices according to multiple different criteria which make the search space too large to find out the solution in real time by deterministic algorithms.

In the proposed method [CHA 05] a set of non-overlapping optimal routes are selected on the basis of different known criterion so that the driver can decide easily according to his choice. The proposed algorithm has been evaluated by simulation experiment with a piece of real road map.

Genetic algorithms (GA) are adaptive and robust computational models inspired by genetics and evolution in biology. These algorithms encode a potential solution to a specific problem on a simple chromosome like data structure and apply recombination operators to produce new solutions. GA are executed iteratively on a set of coded solutions called population initially randomly drawn from the set of possible solutions with three basic operators namely: selection, crossover and mutation in such a way that better solutions are evolved in each iteration. The goodness of a solution is measured by a problem dependent objective function called fitness function, the design of which is very

critical for the success of a GA based algorithm in finding out optimal solution. Genetic algorithms have been applied for shortest path routing, multicast routing or dynamic routing, band-width allocation and in several practical optimization problems.

Fig. 1.6 to 1.9 show sample choices for a user to choose from when starting his journey.

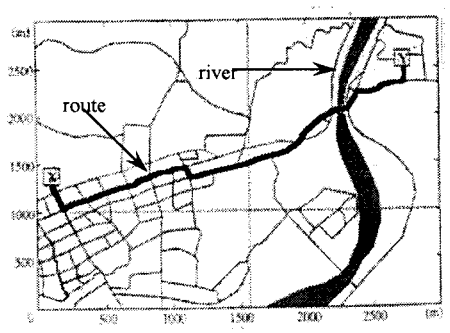


Fig. 1.6, Route by Shortest Distance

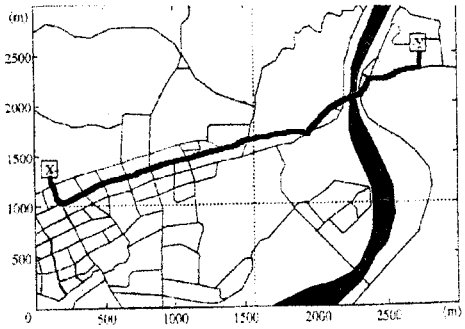


Fig. 1.7, Route by Minimum Turning

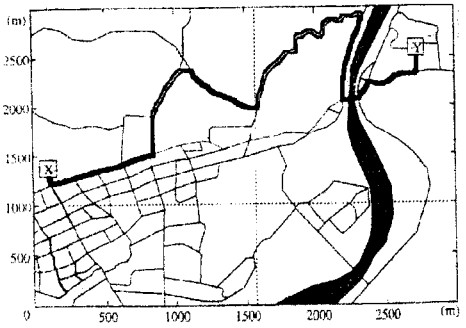


Fig. 1.8, Route Through Mountains

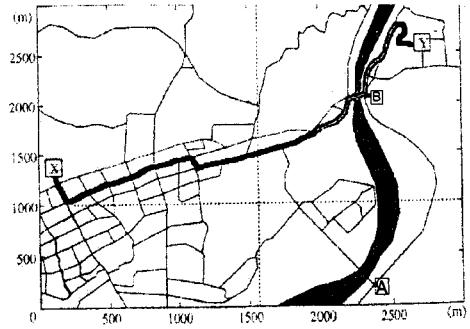


Fig. 1.9, Route by the Side of the River

1.3.2.2. Floating Car Data Project

The problem of estimating the current traffic situation on a road network in a metropolitan area is the interest of many researchers. The traffic situation can be described by different parameters; the current travel time on the roads between major intersections is one of them. The travel time is a main criterion for route choice in a road network, for private as well as for commercial users. However, travel times on metropolitan area roads are subject to strong fluctuations due to the variability of traffic demand and lots of interference like traffic lights.

Conventional stationary detectors observe traffic flow and local speed at certain locations of the road network and therefore are hardly able to provide reliable and area-wide travel time estimations.

An alternative approach is the use of floating car data (FCD) discussed in [LOR 03]. There are two approaches of how FCD can be collected: the *passive* and the *active* FCD approach.

Passive FCD extraction means "recognizing" a vehicle at one section of the road network and later on at another section, e.g. by automatic vehicle identification or passive onboard transponders responding on the signal of a stationary beacon. The time interval between the events allows an estimation of the average travel time between the two sections.

Active FCD extraction (Fig. 1.10) requires a positioning system (e.g. GPS) and a wireless communication unit onboard of the car. The position is transmitted at regular intervals or event driven to a data server. Here the positions are processed by applying a map matching and routing algorithm which assigns the positions to the segments given by a digital road map and calculates the travel time.

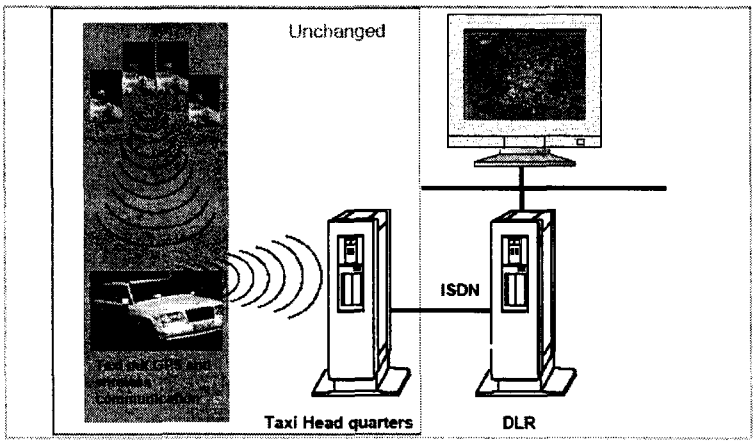


Fig. 1.10, Active FCD Model [LOR 03]

However, both FCD extraction approaches are very costly in terms of hardware requirements as well as communication effort, what was the main obstacle for `introducing this technique in a larger scale. This obstacle can be overcomed by using

position data from commercial vehicle fleets (Taxis). Figure shows the working concept of the project.

1.3.2.3. Trafficopter

Trafficopter [MOU 98] is a multiagent system that provides a fast and reliable way of assisting the driver of a vehicle in deciding the most convenient route to his/her destination without using any special road infrastructure. These suggestions change in regular time intervals according to real-time traffic conditions. The approach stems from the simple observation that the a reliable witness of the traffic conditions that lay ahead are the cars that are there now, or have been there recently.

An attempt to exploit this is by creating a virtual distributed network of intercommunicating agent nodes that pass along information (messages) that is enough for drawing conclusions on local traffic conditions. These traffic conditions are depicted on dashboard mounted map-viewing facilities. Extreme accuracy in the quantity of vehicles is not of paramount importance and the performance of the system gracefully degrades as the number of vehicles equipped with the system drops.

When driving, in order to find the fastest way to go somewhere one needs two things: a computer map with one's position on it (usually derived by a GPS) and the traffic conditions along the possible paths from the origin to the destination. The GPS map already exists in a set of high-end vehicles. In trfficopter proposal the vehicles themselves collect and distribute information about the traffic conditions they are experiencing to other interested vehicles.

The next step in navigation assistance or route guidance, is to make these systems more conscience of the surrounding environment. In other words, it is required that the navigation assistance systems get full information about the actual traffic conditions. This will help the system user to detect and allocate traffic bottlenecks. This will require, other

than the wireless satellite communication, a wireless communication with the surrounding: either with a centralized database or using ad-hoc data from other users. Next, some wireless communication models with the surrounding environment are presented.

1.3.3. Modes of Communications

Moving vehicles can communicate traffic as well as other useful information. Example of other communicated data would be for example VoIP, video on demand, internet access, etc... This information may be communicated in many different ways. Communication can be shared between vehicles using single or multi-hop in ad-hoc fashion. These different modes and more are introduced in the following sub-sections.

1.3.3.1. Vehicle-to-Vehicle Communications (V2V)

The basic approach to establish Inter-Vehicle Communication (IVC) is to have a V2V model. In this model, vehicles equipped with wireless interface modules can exchange information in a similar manner to ad-hoc networks (also known as VANET) [WIS 06].

To establish V2V communication model, Mobile Nodes (MN) need to be in each others RF range (Fig. 1.11). For data to be spread over a big population of Wireless Nodes (WN), multi-hop must be performed [BLU 04 ,BRU 05]. One of the known schemes for collective communication based on ad-hoc is the cluster concept [CHE 05, REU 05].

The cluster concept is used in IVC to minimize the amount of data communicated between cars and to create an ordered scheme for data exchange [CHE 05]. Although this technique optimizes data exchange between moving cars, it suffers the relative big amount of control data to maintain the cluster stability [CHE 05]. The range and types of physical interfaces for V2V are well discussed and presented in [HIR 99.; MOU 98; KAT 02.; MIC 96].

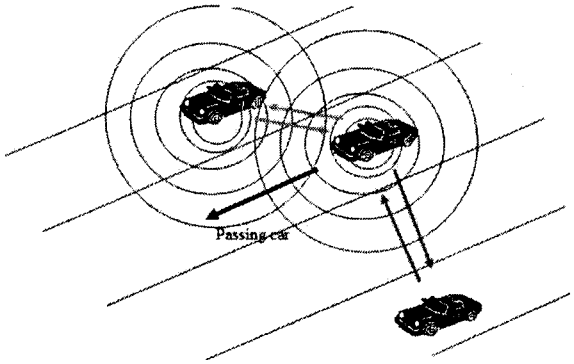


Fig. 1.11, Multihop V2V Communication

V2V is very well introduced in the literature for highway implementation [BIS 06; CHE 05]. Either based on cluster formation or not, the emergency messages are transmitted from the source backward on the road to all moving vehicles to minimize the probability to have a massive accident for example. Also, these messages can be transmitted in a proactive or reactive manner [YAN 04].

In the Proactive approach, all vehicles frequently broadcast their motion information all the time. It is the receiver's responsibility to determine the necessary information it is in need. It requires high-precession vehicle motion information, and high refresh rate (i.e. the frequency of sending information) to prevent false alerts.

In the Reactive approach, vehicle sends information only when it acts abnormally. This can be defined as a strong deceleration rate, a dramatic change in direction, or any other dangerous defined state. In this case the vehicle is named an *abnormal vehicle* (AV). Only AVs generate *Emergency Warning Messages* (EWMs) to warn other vehicles in the neighborhood.

1.3.3.2. Vehicle-to-Infrastructure/Infrastructure-to-Vehicle (V2I/I2V) Communications

In this model, mobile nodes (vehicles) do not communicate to each other in a single-hop or multi-hop scheme like the case of V2V which can be generalized as Ad-Hoc networks.

In contrast, the nodes communicate to a centralized access point (denoted MRB in Fig. 1.12) that covers a certain geographical area. Within the coverage of one Access Point (AP) a certain number of Wireless Nodes (WN) is in general present and can communicate data to and from this AP. Each AP has a given capacity, in other words, it can communicate only with a limited number of WN. Accordingly, it is important during design phase to determine the exact coverage footprint of an AP that is reflected into transmit power and number of WN that this AP can support (or communicate with).

In the V2I/I2V scheme, a hierarchical system is present. In other words, an infrastructure is present that links several AP to each other. This infrastructure can be wired or wireless (wired backbone or wireless backbone). In this infrastructure, intelligence is needed to gather data from the Mobile Nodes (MN) or even the WN present in the system. Also, information from traffic monitoring and platoon officers is useful, and takes part of the data collection. This information is useful to have a complete understanding of the current traffic situation in a given geographical area for example. Depending on this knowledge, messages are propagated into the network to reach the MN. These messages may be alerts messages for example, or they can be traffic information tags.

This information is collected by the WN and processed by the on-board intelligence of the cars. This intelligence can be integrated with other navigation systems like GPS. Now this can be useful in building an on-line judgment of the present situation of the traffic in a given sector of the city. Accordingly, the system calculates a new route and informs the driver to change its trajectory.

In this model, the routing intelligence and major computation is performed on-board of the vehicle. Part of the system intelligence is based on some processing done on the network side. This is mainly the information gathering.

Information gather is important because the system is aware of the complete status of the traffic in a given city. This helps for example when a new vehicle starts its journey, it has complete knowledge from the start that certain sectors of the city are blocked by high traffic jams. In other hands, if these sectors are not of interest for this vehicle (i.e. during

its traverse of the city form its source to its final destination it will not pass by these sectors), this information may not be relevant [CAL].

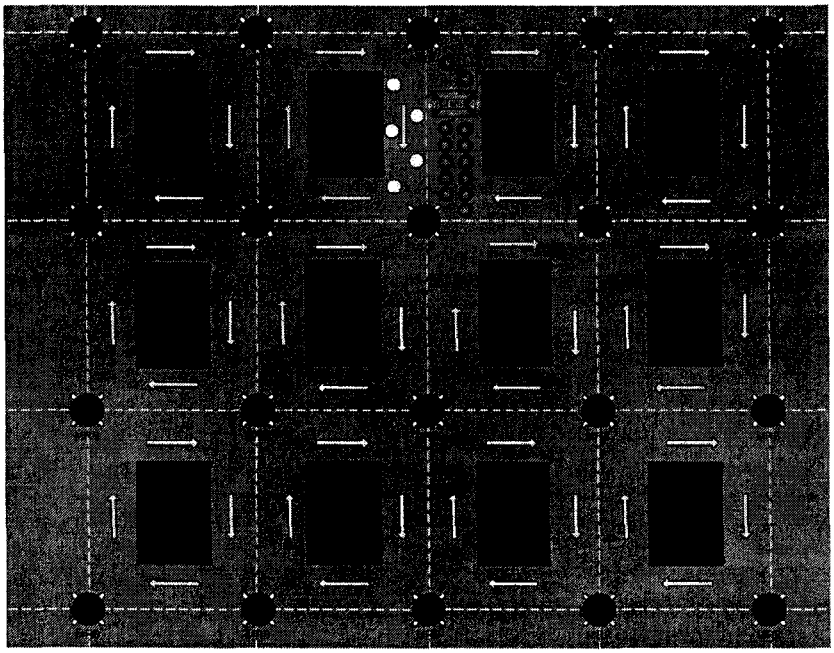


Fig. 1.12, Full Coverage V2I/I2V Communication

The model of Fig. 1.12 shows an infrastructure implementation in a Manhattan map. Roads are strait and intersect at constant intervals. Blue blocks are buildings and red circles are Message Relay Box (MRB) (the system APs). Yellow dots are vehicles free to roam in the map while blue dots are those cars that are trapped in a jam.

1.3.3.3. Hybrid Communication Model

In the hybrid model, V2V as well as V2I/I2V scenarios are integrated together (Fig. 1.13) [REU 05, CAL]. This model is very useful when complete coverage by AP is difficult. A typical example can be the highway case. Although the highway can be totally relaying on V2V (cooperative driving) mode of communication, information at certain important points must be transmitted to certain group of vehicles.

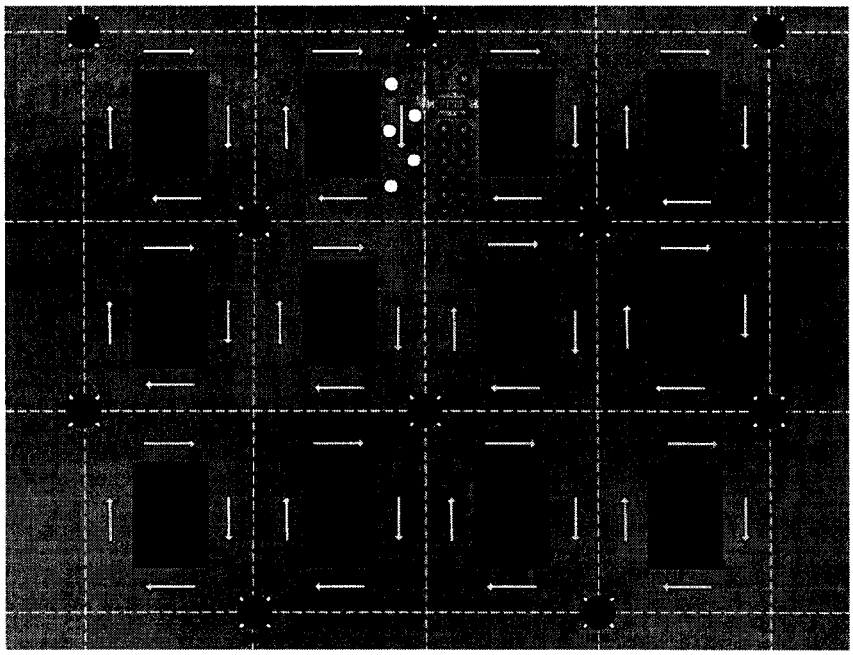


Fig. 1.13, Hybrid Communication Model Scenario

Also, on the other hand, vehicles getting out of the city to the highway, they can gather information from AP on the motorway entrance. this information describes the current situation: where are the bottlenecks, the estimated delay and queue length, etc.

In Fig. 1.13, the MRBs are distributed in a sparse form: one MRB is located every 2 roads' intersections. In this model, vehicles that are covered by the transmit range of an AP (MRB) use the V2I/I2V mode of communication, while those cars that are out of this communication range use the V2V mode. This is where the name hybrid came from.

In more details, vehicles that are using a highway for long trips are mainly interested in the traffic along the highway as far as possible. They need to have information about accidents, regions where ahead moving cars are decelerating, queue length if any is there, etc... On the other hand, MN reaching the end of their journey and preparing to exit the highway, need to get a-priory knowledge of the city traffic conditions. For this purpose, AP at the highway exits are of great importance. They are linked to the city infrastructure, and diffuse useful information for the on-board driving assistance program. Now, the

guiding system drives the vehicle into the city as optimally as possible to avoid traffic jams.

1.3.4. Relevant Projects and Protocols

This section briefly introduces two main projects: the CALM and the RUNES. Because of the confidential measures, only little data can be found to explain these projects. Also, the DSRC is introduced in some words as a future standard protocol of the IEEE (the IEEE 802.11p) for vehicle communication. Some other projects can be found in [CHE 05].

1.3.4.1. Dedicated Short Range Communication (DSRC)

DSRC (Dedicated Short Range Communications) is a short to medium range communications service that supports both Public Safety and Private operations in roadside to vehicle and vehicle to vehicle communication environments. DSRC is intended to be a complement to cellular communications by providing very high data transfer rates in circumstances where minimizing latency in the communication link and isolating relatively small communication zones are important.

The IEEE 802.11p is described as the Wireless Access in Vehicular Environments (WAVE). It is a wireless communication between fast moving vehicles or between a fast moving vehicle and a stationary object. It supports high speeds (~100km/h) and ranges of up to 1km. The frequency range is 5.850-5.925 GHz. This protocol is still under development [STD 11P]. This protocol expands on conventional 802.11 wireless networking.

It allows for provisions that are specifically useful to automobiles:

- a more advanced handoff scheme;
- mobile operation;

- enhanced security;
- identification;
- peer-to-peer (ad hoc) authentication;
- communications in the automotive-allocated 5.9 GHz spectrum.

This protocol will be used as the groundwork for the Dedicated Short Range Communications (DSRC), or automotive-targeted communications that can occur both between vehicles and from a vehicle to a network of roadside infrastructure.

1.3.4.2. RUNES

RUNES [RUN] is a Frame Work 6 project. Many industries are integrated within the project, mainly automotive and communications industries (SCANIA, ERICSSON, etc...). Its typical application is gathering information from many remote sensors, providing geographically dispersed operators with the ability to interact with the collected information, and controlling remote actuators. Those applications are part of the Distributed, Real-time and Embedded systems (DRE systems).

The RUNES indicates a focus first on the Wireless Sensor Networks (WSN), which are characterized by the radio communication and a set of micronodes, having limited resources and several sensing and/or actuating devices, second on the integration of the WSN with other types of networks. The project aims at developing a generic, reconfigurable middleware for that platform of heterogeneous networks to provide a framework for the development of data collection and control applications with more ease than current technologies and tools afford.

RUNES will provide the architecture and tools to facilitate the creation of large-scale Networked Embedded Systems (NES). Validating the approach, a combination of real deployment and simulation will be developed.

Within the framework of RUNES, different scenarios are introduced to validate the concept. These scenarios are:

- Integrated Cardiac Telemonitoring and the Smart Environment Scenario;
- Disaster/Emergency Scenario;
- Integrated Wine Production and Distribution Scenario;
- Automotive Scenario;
- Fire in a Road Tunnel Scenario.

What is interesting and related to our research is the automotive and fire in road tunnel scenario. In the automotive scenario, it is interesting to couple the on-board system of the vehicle to the outside world (the road-side communication system) to exchange information forming Intelligent Transportation Systems (ITS). For the fire in road tunnel scenario, it is an emergency scenario that explains how the on-board system of a vehicle reacts with the outside environment to inform about the accident and help in saving lives.

1.3.4.3. CALM

The scope of Communications Architecture for Land Mobile environment (CALM) [CAL] is to provide a standardized set of air interface protocols and parameters for medium and long range, high speed ITS communication using one or more of several media, with multipoint and networking protocols and upper layer protocols to enable an efficient communications service.

This service includes the following communication modes:

- Vehicle-to-Vehicle: A low latency peer-to-peer network with the capability to carry safety related data such as collision avoidance, and other vehicle-to-vehicle services such as ad-hoc networks linking multiple vehicles;
- Vehicle-to-Infrastructure: Multipoint communication parameters are automatically negotiated, and subsequent communication may be initiated by either roadside or vehicle;
- Infrastructure-to-Infrastructure: The communication system may also be used to link fixed points where traditional cabling is undesirable.

Media defined in the current phase of CALM are:

- Cellular systems, e.g. 2/2.5G GSM/HSDSC/GPRS and 3G UMTS;
- Infrared communication;
- 5GHz wireless LAN systems based on IEEE 802.11a/p;
- 60GHz systems;
- A common convergence layer to support media such as existing DSRC (802.11p) protocols, broadcast protocols and positioning receivers.

A Network layer is defined as follows:

- Kernel is IPv6;
- Mobile IPv6 elements are included for handover;
- Header compression;
- Internet connectivity;
- Mobile connectivity and routing in fast ad-hoc network situations;
- Common Service Access Points (SAP) towards the lower layers (LSAP) and for management services.

Management services are defined to provide:

- Quasi continuous, protracted and short term communication possibilities;
- Quasi simultaneous or simultaneous multi-terminal operation within vehicles via one or more communication protocol;
- Support for multipoint MAC layer handover between different communication points within any specific medium;
- Network layer handover between different protocols and different providers using IETF NEMO functionality;
- Application layer support for session transfer/resumption across different protocols or different service providers;
- Initialization and registration of protocols and clients;
- Management of multiple regional/regulatory spectrum restrictions;

- Management of QoS parameters required by user services and offered by the different available protocols;
- Interpretation of high-level instructions into media specific actions.

Some examples of applications include so called "infotainment", including the update of roadside telemetry and messaging, in car internet, video and image transfer, traffic management, monitoring and enforcement in mobile situations, collision avoidance, route guidance, car-to-car safety messaging, Radio LAN, co-operative driving, and in car entertainment.

Global Positioning Systems (GPS/GALILEO), Digital Audio Broadcasting (DAB), Digital Video Broadcasting (DVB), Digital Data Broadcasting (DDB), TETRA, Mobile Broadband Systems (MBS, W-ATM), Radio LANs/WLANs, Internet Protocols and DSRC are also of use in the CALM.

The CALM standards are currently being developed by ISO TC204 WG16. The first drafts have been released in ISO TC204.

1.3.4.4. The Application-Based Clustering Concept and Requirements for Intervehicle Networks

A new network clustering concept for foresighted driving applications is introduced [REU 05], taking into account the specific requirements for highly dynamic intervehicle networks. Considering initially low system penetration in the market, the concept includes so-called message relay boxes (MRB) without backbone network connection for temporary roadside storage of messages. MRBs are able to store, process and forward messages received from passing vehicles. One of the major issues for cooperative systems is consistent message delivery to all vehicles pertaining to a particular application, such as obstacle warning or lane merge warning.

The application cluster may be either moving or quasi-stationary. While moving clusters can reuse most of the existing concepts for cluster organization, taking into account the

increased node mobility and network dynamics, quasi-stationary clusters with fluctuating participants at a fixed geographic location pose more severe challenges, such as the repeated transfer of the cluster control function from one vehicle to another in a very short period of time. More issues like high level congestion control, application priority determined by external conditions rather than network-related conditions, and sophisticated message handling algorithms tied to the car navigation system were not studied.

Although the early introduced projects are perfect examples for interaction of navigation systems and surrounding environment, still these systems lacks intelligence. Here intelligence is in the sense that the navigation assistant or the guidance system, based on the collected data from the surrounding environment, can transparently re-route the user in the optimal trajectory. This is not as simple as it appears. How this works can be discussed in next section.

Next section introduces the stigmergic approach as platform to induce intelligence in the guidance system. This intelligence is based on environment marking: moving entities communicates with a centralized intelligence unit that collects general information on a traffic map. This information after being processed is diffused in the system in form of coefficients that are useful for the smart navigation assistance to use for re-routing. This part of the work is developed at the LAMIH.

1.3.5. Stigmergic Routing

The Team "Systèmes de production" of the LAMIH works in the field of the FMS (Flexible Manufacturing Systems) and ITS (Intelligent Transportation systems). In this last research area, the works focus more precisely on bio-inspired approaches for dynamic routing, as stigmergic paradigm [BER 06].

French entomologist Grassé (1959) introduced the term "stigmergy" to describe the mechanism by many individuals participate in a collective task, and the stimuli provided by the emerging structure are used to coordinate the individual actions [THE 99]. A similar mechanism is used by ants laying down pheromone trails between a food source and their nest.

A light urban area can be seen as a network of nodes that are interconnected by uni/bi-directional paths on which vehicles navigate (Fig. 1.14). These vehicles move from one node to another until they reach their destination node. Vehicles continuously and automatically send the travel time from node to node, to a central node. In this central node, information from all vehicles is compiled. Using the stigmergic approach, coefficients (virtual pheromones) are assigned to each node and updated using data sent by vehicles. At the beginning of a trip, the driver sends a message to the central node indicating the departure and destination nodes of the trip. The central node uses the coefficients mentioned above to calculate the best path from the departure node to the destination node then communicate it to the vehicle. In the approach adopted below notations $N = \{n_i\}$, n_i being any node in the light urban network.

Progression based on virtual pheromones: In analogy with biological systems, for each node *nk*, a P_{nk} matrix characterizes the pheromone rate on different paths. Based on the information stored on the current node *nk*, the value $P_{nk}(nn,nd)$, is assimilated to the preference, from the current node *nk* (destination node *nd*), for choosing the possible intermediate neighbor node *nn*.

$$P_{nk}(nn,nd) \in [0;1] \qquad 1.1$$

$$P_{nk}(n_j,nd) > P_{nk}(n_p,nd) \qquad 1.2$$

implies n_j allows the vehicle to reach *nd* more rapidly than n_p, where n_j and n_p are elements of *Vnk* (neighborhood of *nk*). After standardization:

$$\sum_i P_{nk}(n_i, nd) = 1; \quad i/n_i \in Vnk \tag{1.3}$$

For routing, the vehicle chooses the best neighbor *nc*, such that:

$$P_{nk}(nc, nd) = \max(P_{nk}(n_i, nd)); \quad i/n_i \in Vnk \tag{1.4}$$

Figure 1.14 below gives an example of P_{nk} matrix for a vehicle V1 on the current node n_3.

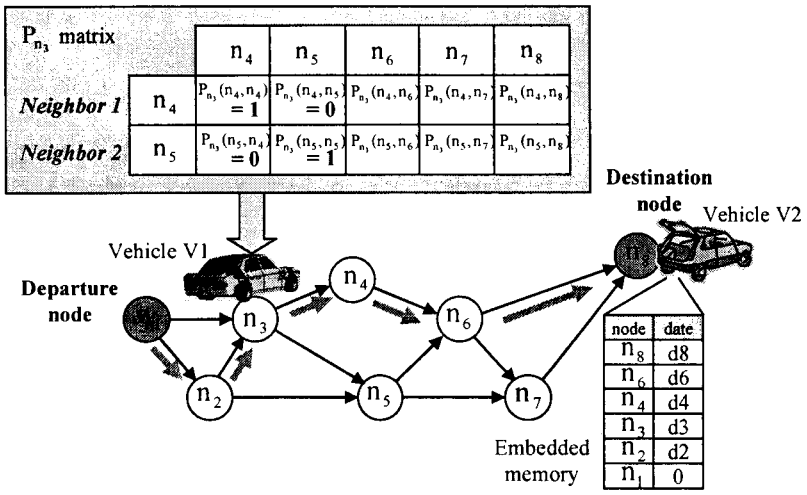


Fig. 1.14, Virtual pheromones modeling

Virtual pheromone updating: While moving, each vehicle stores data in an embedded memory. The memory records the vehicle's path through successive nodes *nk*, including crossing time. When the vehicle reaches the destination, the information contained in the embedded memory is used to update coefficients at each node *nk* that was crossed. On the node *nk*, the last measured time *T(nk,nd)* (time span needed to go from *nk* to *nd*) and the mean $\mu(nk,nd)$ of the previous *T(nk,nd)* are compared. The P_{nk} matrix is then updated by increasing the coefficient $P_{nk}(nc,nd)$ (the possibility of choosing neighbor *nc* when the destination is *nd*) and decreasing other coefficients $P_{nk}(no,nd)$. A reinforcement value r is used as follows:

$$P_{nk}(nc,nd) \Leftarrow P_{nk}(nc,nd) + r \times (1 - P_{nk}(nc,nd)) \tag{1.5}$$

Coefficients $P_{nk}(no,nd)$ for the destination nd of the other neighbors no are negatively reinforced through a process of normalization:

$$P_{nk}(no,nd) \Leftarrow P_{nk}(no,nd) - r \times P_{nk}(no,nd) \quad no \in Vnk \tag{1.6}$$

with $no \neq nc$.

Figure 1 exhibits the embedded memory for a vehicle V2 reaching destination node n_8, with

$$T(n_3,n_8) = d_8 - d_3 \tag{1.7}$$

1.4. SYNTHESIS

Table 1.2 presents a synthesis of the available networks and algorithms together with their pros and cons.

Table: 1.2
Summary of Network efficiency

	Pros	Cons
Single Ethernet On-Board Network	Less wiring Less weight Large BW Large number of nodes POF immune to EMI Easy to troubleshoot Large number of specialist Low cost implementation Large number of equipment manufacturer Well known and established communication protocol Industrial switches are now available on the market that are EMI and shock proof New Network adaptors are available to connect simple microcontrollers to Ethernet for industrial applications Showed success in implementation as industrial NCS backbone in mixed communication environment	Non-deterministic nature On-board electronics EMI sensitive like other N/W Not mature technology in control

	Pros	Cons
Stigmergic	Intelligent algorithm based on environment marking Showed success when implemented in industrial applications	Needs large computational power if implemented for large number of moving entities
V2V	Fast interaction based on instant data collection from the surrounding environment Most suitable for near space data collection Data can be relayed for large distances using multi-hops No infrastructure needed May be used in urban, light urban and highways Can be implemented to complement the Infrastructure model	May cause interference with surrounding nodes that want to communicate at the same time Not suitable to relay entertainment data Do not support mobile Internet Complex routing protocols
V2I/I2V	Most suitable to give a global view of the actual traffic condition based on data collection from different points Once the infrastructure is built, it can be used to communicate all kind of data else than traffic information (like entertainment and video calls) Low Cost implementation if built using standard protocols Used to cover large geographical areas Supports mobile Internet Easily deployed in highways and light urban areas Conventional routing protocols can be used Data can be centralized or distributed among different intelligent nodes of the infrastructure Can be implemented to complement the V2V model	Needs infrastructure investment Technology considerations must be very well studied to be able to cover large crowded geographical areas Mobility at high speeds may not be supported in some technologies

1.5. CONCLUSION

Vehicles designed for the future rely heavily on electronics. It is a very important aspect in today's vehicles. This thesis addresses improving the efficiency and the cost-effectiveness of vehicle electronics. Two main aspects will be focused on: On-board networks and Traffic control.

Current cars on-board network technology suffers the presence of different incompatible networks. This problem becomes more critical when dealing with more services for the future vehicles. The use of a single network is an attractive solution. This single network will help different Electronic Control Units (ECU) share information when needed. The choice of this network must satisfy the usual control requirements of bounded end-to-end delays. It also has to meet the large bandwidth that the current and future passenger entertainment applications demand. The use of Ethernet is attractive to solve this problem. But, Ethernet does not satisfy the essential constraint of bounded end-to-end delay due to its non-deterministic protocol. To solve this, high speed Ethernet and Switched Topology will be used. This is based on previous work done in industrial control [DAO 03, DAO 04a, DAO 04b] using Star Gigabit Ethernet to control heavy control traffic machines.

The proposed Ethernet on-board network model will be tested to accommodate the control traffic. The success or failure criteria will be subject to the end-to-end delay measurement of the control packets. This delay must be less than one sampling period for a given control application. Entertainment loads will be then added as an overhead to the control traffic. The network is again tested to verify that it meets the end-to-end delay requirements of the control messages in the new mixed traffic environment of control and entertainment applications. Ethernet will be tested at two speeds: 100Mbps (Fast Ethernet) and 1Gbps (Gigabit Ethernet).

This future luxury car will provide its passengers with all kinds of entertainment on-board while traveling from a starting point to a destination. It will also be important to choose the best paths to reach the destination. To do so, the on-board navigation system, either

for manned or unmanned vehicles, must interact with the outside environment to get traffic information. This requires wireless communication with a traffic information center.

The type of information the navigation system needs is not anymore what conventional GPS systems offer nowadays. The on-board system of the future vehicles will need information like the location of the bottlenecks in the traffic map. Of course, not all bottlenecks in the traffic maps are of relevant use for the system, but those that appear in the trajectory it will take to reach its final destination. These traffic problems may be not present at the start of the vehicle journey, that it why an on-line dynamic system is required.

This kind of routing assistance mechanism requires that the moving vehicles has two-way communication with the infrastructure. This two-way communication is from vehicle to infrastructure (V2I) and from infrastructure to vehicle (I2V). In V2I, the moving vehicles transfers the current traffic status to the central intelligence of the system, while in I2V, the central system intelligence sends the traffic map information to the moving nodes. It is at the moving nodes (vehicles) intelligence level that the decision is made to change its route to reach its final destination based on the I2V messages. This smart routing can be integrated with current navigation systems.

Large geographical areas need to be covered by wireless communication for this project implementation. Also, a robust wireless communication roaming mechanism is essential to maintain connectivity of the moving cars with the infrastructure. Once this wireless network is established it can also be used for additional applications different than relaying traffic information only.

In this research, the design of such wireless communication network is presented based on the wireless communication protocol of the IEEE 802.11 Std (WiFi). The roaming mechanism is also treated based on the use of the Mobile IPv4 and Mobile IPv6. The problem will be addressed within the context of a light urban area such as tourist resorts and will use the Stigmergic approach. Although WiMAX as well as 3G could have been used implement such project, WiFi was chosen because it has the advantage of a well

established and tested protocol for almost 6 years. WiFi silicon pricing continues to decrease, making it a very economical networking option. WiFi networks support roaming, in which a mobile client station can move from one access point to another as the user moves around a building or area. It is a global set of standards. Unlike cellular carriers, the same WiFi client works in different countries around the world.

The next chapter introduces and explains the vehicle on-board wired control model. It is based on previous studies conducted in industrial automation. The chapter shows a path from what is special case: Ethernet implementation in industrial control systems, to what is general: Generic approach. This Generic approach is then applied to automotive on-board control and entertainment networks.

CHAPTER II

WIRED SYSTEMS

2.0. INTRODUCTION

THE use of Ethernet as communication protocol for NCS is first tested in industrial control applications. Many models within the context of industrial NCS are developed and tested. What is presented here is in fact a path from what is special case: industrial NCS using Ethernet, to the development of a generic model for Ethernet implementation in automated workcells. An attempt to apply these generic models in another field which is terrestrial transportation systems is then conducted. Within the context of this research, cars on-board network is the application model for terrestrial transportation systems (Fig. 2.1).

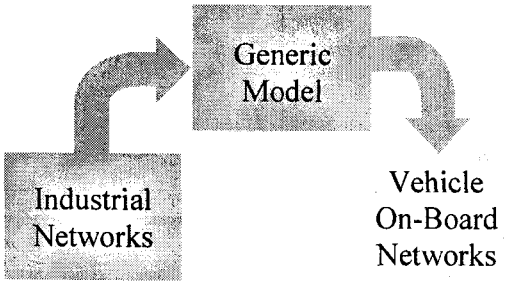


Fig. 2.1, Modeling Philosophy

The generic models are the general models that can be adapted for use in many fields. Not all these architectures will be used in all application fields. On the other hand, from

this set, one chooses the suitable models that can be implemented within the application context.

During the development of the vehicle (car) on-board network, it was very difficult to find sufficient information for actual on-board network implementation; this is due to the confidentiality of this information. The search led to some data from Ford that dates from late nineteen nineties [UPE 96]. This is one reason not all models are tested for vehicle on-board network implementation. Another reason is that not all control schemes will lead to an efficient increase in system reliability.

The rest of this chapter is organized as follows: The generic model of Ethernet use for NCS is presented in section 2.1. Section 2.2 introduces the Fault-Tolerant models that can be implemented for the proposed Ethernet NCS. The Performance evaluation metrics of the models are presented and justified in section 2.3. Two application fields of the generic models are then presented: the industrial application model is given in section 2.4 and the vehicle on-board network model is presented in section 2.5. The chapter is concluded in section 2.6.

2.1. ETHERNET IN CONTROL

The use of Ethernet as a communication network for Networked Control Systems (NCS) is an attractive subject. For interested readers, please refer to [KUM 01, LIA 01a, NIL 98, SKE 02, DEC 05, FEL 05, MAR 06, GEO 05, BRA 07]. It has even been studied for adoption in aerospace systems [GRI 04]. Automated workcells [MOR 05] always consists of sensors, controllers and actuators connected over the network. Sensor nodes, known as source nodes because the data flow originates at these nodes, are smart ones. Actuator nodes, also called sink nodes because the data flow ends at these nodes, are also smart. Smart sensors/actuators have network communication capabilities and sometimes they have self diagnostic and calibration features as well. The smart sensor collects physical data from the process under control and sends it in a packet format after encapsulation over the communication network to reach the controller. At the controller the data is de-

capsulated, analyzed and processed; control word is generated, encapsulated and sent over the network once again to reach the smart actuator node. The smart actuator collects the control word from the network and applies it to the physical process after de-capsulation.

In general, NCS reduce the amount of wiring in contrast to point-to-point communication and it does not demand redundancy in sensors. Introducing TMR to increase reliability of the system will increase the wiring in NCS as well as in point-to-point control system. The amount of wiring in the NCS scheme will no doubt be less than in the conventional control system.

The control packet flow on the Ethernet channel is based on publisher/subscriber mode of communication: once the packet is generated, it can be heard by any node on the network. This facilitates the data flow and eliminates the duplication of sensors. The packet will be consumed only by the relevant node (the controller node in the case of a packet sent by a sensor). A comparison between different methods of communication is given in [MAR 06]. The model of Fig. 2.2 [NIL 98] shows a schematic of NCS.

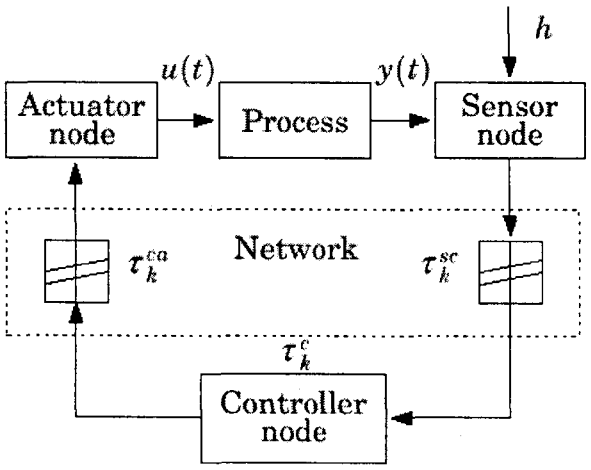


Fig. 2.2, NCS Block Diagram [NIL 98]

In this model, the physical data is sensed on a periodical basis (clock driven) every h seconds. It is transmitted from the sensor to the controller of the network facing a delay

τ_k^{sc}. It is consumed at the controller node and processed over τ_k^c delay. The controller sends the control action over the network to reach the actuator after a delay τ_k^{ca}.

The source of non-determinism in switched Ethernet is queuing delays. For example, the controller node may generate non-real-time traffic (also known as explicit messaging, in contrast with implicit messaging used to designate the real-time control) like FTP sessions or HTTP. This will perturb the queues and the processing loads at the controller node. Accordingly, the end-to-end delays (the delay measured from the sensor node to the actuator node taking into consideration all kind of encapsulation/de-capsulation, processing and propagation delays) will not be constant. This is what is called mixed traffic environment. It is important to test the Ethernet NCS behavior in simple control environment (only control packets are communicated) and mixed traffic environment.

Fig. 2.3 illustrates a general network hierarchy model [LIA 01b].

This model consists of five levels, each one having different goals and also different communication capabilities, protocols and complexity. In modern manufacturing systems, level one is the device or sensor-actuator level that is used to interconnect controllers, sensors or actuators. Level two is the cell control level and it is designed to be used with cell controllers such as at milling, lathe and control workstations in manufacturing plants. Generally, levels one and two are called *sensor* and *fieldbus*, respectively. Level three is the supervisory level and is used to interconnect machine cells that perform different manufacturing processes. Level four is the plant management level and is used to coordinate various tasks executed inside a plant such as manufacturing engineering, production management, and resource allocation. Level five is the corporate management level. It may interconnect workstations located in different cities or countries [LIA 01b].

Ethernet is now the dominant local area networking solution in the home and office environments. It is fast, low cost and easy to install. Most computerized equipments now come with built-in Ethernet Interfaces. These are some of the reasons why a number of

manufacturers of industrial control systems are now migrating to the use of Ethernet on the production floor and integrate it with the management floor [DEC 05].

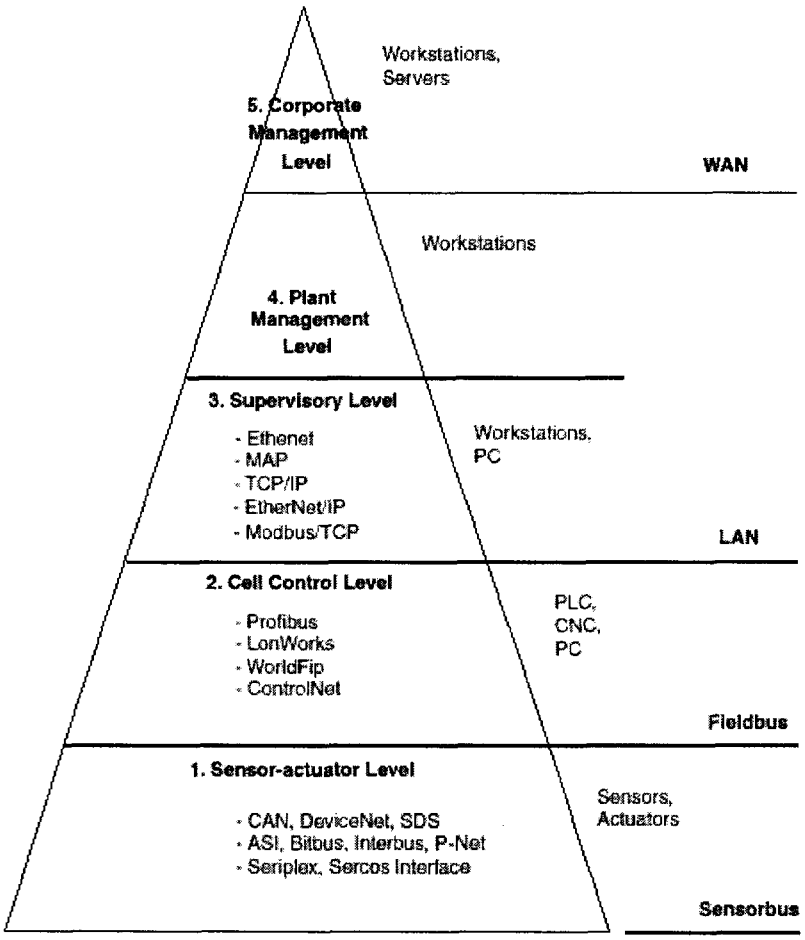


Fig. 2.3, A general network hierarchy model [LIA 01b]

An essential requirement in this implementation is for the office Ethernet communication capability to be fully retained when applying it for control, i.e., the best solution would be if no protocol change were introduced [FEL 05, DAO 03].

What is proposed in this study is really a merge of all these levels to use only Ethernet as a communication protocol. Security issues are out of the scope of this study. The main focus of this research is to test the network operation and performance in the presence of mixed traffic.

2.2. FAULT-TOLERANT ARCHITECTURE

Fault-tolerance is a crucial aspect in control. It can be implemented in different ways. Within the context of this research and using Ethernet to implement NCS, only two types of fault-tolerance are investigated. First, fault-tolerance at the controller level is interpreted. In this model, controllers on the same network share information that will be useful for future intervention by an active controller upon the failure of any other controller node. This type of fault-tolerance may be linear or hierarchical.

Second, fault-tolerance at the sensor nodes level is tested. This technique is not new, but it demands large network bandwidth. This large bandwidth is needed to absorb the excess in communicated data when the number of sensors responsible of a given physical information is increased.

In the models to follow, some simplifying assumptions were made:

- In most of the literature, the coverage parameter is assumed to be independent of time [TRI 02]. That is why the recovery time was not included in the models.
- The sensors are sampled using synchronous clocks. The problem of synchronization was the scope of many previous researches in the literature [SUN 05].
- The network wiring (cabling) is assumed to be reliable. The problem of building reliable network on the physical layer is the scope of other researches in the literature [CRO 06, JAS 04b].

Important research treating the Fault-Tolerant aspect of NCS are [BRA 07] and [NeSCT].

2.2.1. Fault-Tolerance at the Controller level

Fault-tolerance at the controller level can be introduced in automated workcells. This can be done by interconnecting the LAN of each workcell together. Having all nodes: sensors, controllers and actuators sharing the same communication medium, data can be sent and received by any node without the need for bridges (to translate from one packet

format to the other). Also, upon the failure of any controller on the network, another controller can take over the control system. This minimizes the system down time. This controller switchover is subject of synchronization between controllers of the same network. In other words, not every controller sharing the same network with another controller can switchover. It is subject of mutual communication that permits that upon the failure of a given controller another one that keeps the history of the failed controller and that can receive the packets from the relevant sensors can takeover the control smoothly.

2.2.1.1. In-Line scheme

Fault-tolerance at the controller level can be linear (Fig. 2.4). In this case all controllers of separate workcells are interconnected together to form one big linear or closed network. Any new controller can be added, and any controller, member of this linear architecture, can be disconnected without affecting the general operation of the overall system. Controllers can be operating independently, or they may be synchronized together in an in-line fashion so that the concatenated workcells are all collaborating to produce a final product. In both cases, life messages may be exchanged between controllers and a back-up scheme must be scheduled a-priory. Accordingly, if a controller goes OFF for maintenance or because of failure, another ON controller can take over its functions until it comes ON again. This shows that the in-line scheme can also be used to maintain the system operation during scheduled or preventive maintenance [DAO 04B, AME 04, DAO 05a, AME 06b, AME 05, DAO 07d].

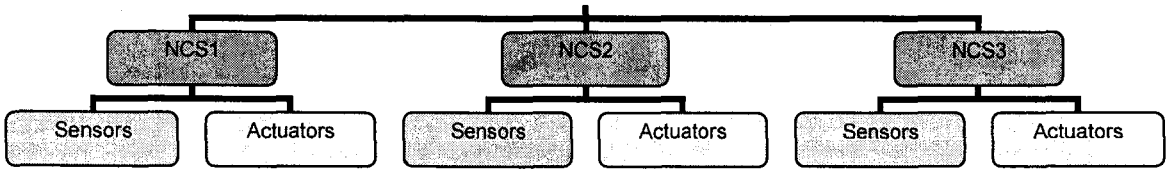


Fig. 2.4, Linear Fault-Tolerant Controllers

2.2.1.2. Hierarchical architecture

Distributed control systems are typically implemented in a hierarchy of functions comprising a supervisory control level. The role of this level is to monitor whether the control objectives are met, and to support the overall coordinated control in different phases of normal operation. In addition, this level should allow the diagnosis of all foreseeable faults, and should be able to take the necessary corrective actions, including the change of controller parameter or structure [BLA 01].

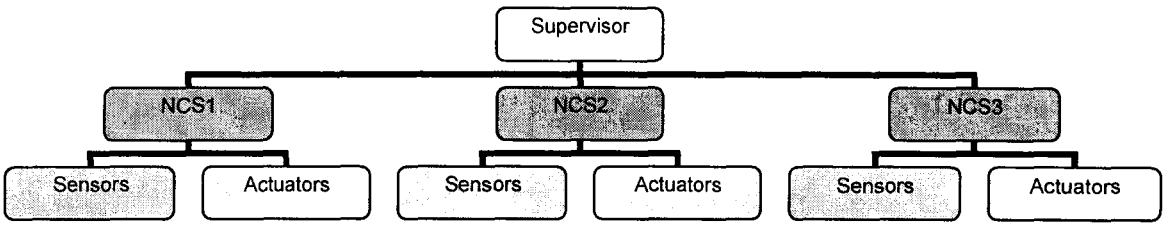


Fig. 2.5, Hierarchical Fault-Tolerant Controllers

In the hierarchical fault-tolerant model, another level of control can be added (Fig. 2.5). This control level is essentially used for supervision. It can be simply described as a linear fault-tolerant model with a supervisor controller node that collects information from several independent workcell controllers. It resembles very much a tree structure, with the supervisor being the root and the workcell controllers being the leaves. The leaves may be interconnected with each other or they may be loose. Two types of supervisor nodes can be treated: the passive supervisor model and the active supervisor model [DAO 05b, DAO 06e].

2.2.1.2.1. Passive Supervisor

When the supervisor is passive, it monitors the other controllers only and does not make control actions. The controller of each workcell reports from time to time to the supervisor node its status vector (all information concerning production rate, cam position, number of defected parts ...etc...). Also, for the purpose of synchronization, it

sends another file to the controller of the other workcell. Here synchronization is done by inter-controller communication; it can also be done through supervisor [DAO 05b].

2.2.1.2.2. Active Supervisor

The supervisor in this scheme does not only collect information from individual controllers, but it has a vital role in system synchronization. The inter-controller communication is virtually not present. This is because the synchronization information needed is transferred from one controller to the other through supervisor. Here, it can be said that the supervisor is an upper layer controller for the machine controllers. It is clear that supervisor node failure drives the system to complete failure for in-line production schemes [DAO 05b].

2.2.2. Fault-Tolerance at the sensor level

The Triple Modular Redundancy (TMR) technique, first introduced in the fifties, is a special case of N-Modular redundancy, which is a fault-masking technique. Fault masking is a static (or passive) form of redundancy because there is no reconfiguration involved. The disadvantage of TMR is obviously cost since three sensors are required to produce an output that could be generated by just one sensor. On the other hand, the advantage of TMR is an increase in reliability. If each sensor has a reliability R, the reliability of the three sensors will be:

$$R_{3-sensors} = \sum_{i=0}^{1} \binom{3}{i} (1-R)^i R^{(3-i)} \qquad 2.1$$

Where $R(t)$=Prob (sensor continues to function throughout (0,t) assuming that it is functioning at time zero) [TRI 02].

As long as two sensors function properly, the controller will be able to obtain the correct output. It is assumed here that failures of the three sensors are independent of each other. The outputs have to go through a voter. When implemented in hardware, a TMR voter for

three digital signals is a majority function or the Carry output of a three-bit full adder. Voting can also be done in software. This is the approach that will be used here. The controller, after reading the outputs of the three sensors, executes a routine that compares these three outputs. A major problem here is that the three outputs may not completely agree because the sensors, while identical, may not produce the same exact output. Analog-to-digital conversion, for example, can produce digital data that disagrees in the least significant bits. Two approaches have been reported in the literature to solve this problem [JOH 89]. The first solution is the "mid-value select" technique. The software routine compares the three readings and chooses the value that lies between the other two. The second technique is to ignore the least significant bits of the data. The number of significant bits that have to agree depends on the application.

If one of the three sensors fails in such a way as it stops sending packets, the software routine will use the data from the other two functional sensors. This will prolong the Mean Time To Failure (MTTF) of the system because as long as one of the 3 *copies* of the sensor is operational, the system can still function. Second, if the sensor fails such that it sends a packet with wrong information but with correct CRC, the controller will not be able to detect this problem and the system fails. With TMR, the data from the three copies of the sensor is compared and voted upon. As long as there is only one failed sensor, the controller will know which of the three packets to discard and the system will remain operational. When the second sensor fails, the entire system will fail [DAO 07d, AME 08].

2.3. PERFORMANCE METRIC

The performance metrics of network systems that impact control system requirements include: access delay, transmission time, response time, message delay, message collisions (percentage of collision), message throughput (percentage of packets discarded), packet size, network utilization, and determinism boundaries. For control systems, candidate control networks generally must meet two main criteria: bounded time

delay and guaranteed transmission; i.e., a message should be transmitted successfully within a bounded time delay [LIA 01b]. Unsuccessfully transmitted or large time-delay messages from a sensor to an actuator may deteriorate system performance or make a system unstable. Several protocols have been proposed to meet these requirements for control systems [NIL 98]. The performance metrics mentioned above are used to determine the capability of the network medium and to provide design specifications to control parameters such as sampling rates as well as network parameters such as communication rates [DAO 04a].

As in [GEO 05] the focus of this research is to use Ethernet IEEE802.3 Std without modifications. A previous study was made to use Ethernet in control by changing the frame structure for real time packets [TOL 97]. Another study was made to design a real-time controller to control traffic of the communication medium in case of real-time constraint [LEE 01]. More research can be found in [EKE 99, LIA 01a, WAN 99, WIT 98, ZHA 01, JAS 04a, VAT 06, GEO 06, BRA 06].

In [MAR 06a] analysis to define the source of delay in an Ethernet NCS is made and showed that the overall response time is the sum of three delays: processing time, waiting time for synchronization of asynchronous processes and waiting time for availability of shared resources. A comparison between two methods to evaluate this response time (simulation and colored Petri nets) can be found in [MAR 06b]. Our work includes the synchronization delays as well as the time for availability of shared resources in the processing delays of the nodes. Also, these two major time delays analysis are the focus of other research works like in [SUN 05]."

Gregory et al. in [WAL 01] have proposed a new dynamic scheduling technique for NCS. The network here is not only dedicated for control purposes, but it can also accommodate communication frames. This makes rise to network induced delays due to unpredictable loads. In [WAL 01], the control algorithm was made off-line ignoring network delays. This simplified the analysis tremendously. Including time delays is a new approach to validate their work. Also, the simplicity of this approach makes it attractive to be used in

general studies for any NCS. Simplicity of [WAL 01] approach comes from the fact that they are using a simple state space representation of the overall NCS (Appendix A).

$$\begin{aligned} \dot{x} &= Ax + Bu \\ y &= Cx + Du \end{aligned} \qquad 2.2$$

In this research, the system success or fail is evaluated based on measuring the delay faced by the sensor data traveling over the network to reach the controller, the processing delay at the controller node, the propagation delay from the controller to the actuator node faced by the control packet, and finally the processing delay at the actuator node before applying the control word to the physical process. This end-to-end delay takes into consideration all kind of data encapsulation, propagation, de-capsulation and processing in all nodes on the network. End-to-end delay for Ethernet NCS can also be analyzed with network calculus like what in [GEO 05, GRI 04]

$$D_T = D_T\big|_{\text{controller}} + D_T\big|_{\text{actuator}} \qquad 2.3$$

where D_T is the total end-to-end delay.

$$D_T\big|_{\text{controler}} = T_{ps}\big|_{\text{sensor}} + T_{encap}\big|_{\text{sensor}} + T_p\big|_{\text{sensor}\rightarrow\text{controller}} + T_q\big|_{\text{controller}} + T_{decap}\big|_{\text{controller}} \qquad 2.4$$

$$D_T\big|_{\text{actuator}} = T_{ps}\big|_{\text{controller}} + T_{encap}\big|_{\text{controller}} + T_p\big|_{\text{controller}\rightarrow\text{actuator}} + T_q\big|_{\text{actuator}} + T_{decap}\big|_{\text{actuator}} \qquad 2.5$$

Where T_{ps} is the processing delay

T_{encap} is the encapsulation delay

T_p is the propagation delay

T_q is the queuing delay

T_{decap} is the de-capsulation delay

Also, the system must guarantee zero packet loss.

2.4. INDUSTRIAL NETWORKS

In Networked Control Systems (NCS), machines can be transformed into automated workcells as described in [DAO 03] and [TOL 97]. In such machines, sensors and actuators have "smart" capabilities. This is because such nodes have features that would include self diagnostics, calibration, and network communication. Data originating at smart sensors nodes (source nodes) are encapsulated into network format and transmitted over the physical medium to reach the controller. At the controller node, which is an Industrial Personal Computer (IPC) in this study, the control action is taken and transmitted in packet format over the network to reach the dedicated smart actuator. Finally, to close the control loop, data is received by the smart actuator (sink node). It is de-capsulated and applied to the system either in analog or digital format, depending on the application and the type of system [LIA 01a], [DAO 03].

A basic model that includes 16 sensors, 1 controller and 4 actuators is the building block of the industrial NCS study. It is named *light traffic model* in [DAO 03]. The sampling period at the sensor nodes is 1,440 Hz. The use of 1,440 Hz as the sampling frequency follows from the fact that a machine running at a speed of 1 revolution per second is encoded into 1,440 electric pulses for electrical synchronization and control over traditional PLCs [SKE 02]. Consequently, the system will have a deadline of 694μs, i.e. a control action must be taken within a frame of 694μs as round-trip delay originating from the sensor, passing through the controller, and transmitted once more over the network to reach the actuator. The *heavy traffic model* [DAO 03] is in fact a TMR model at the sensor level of the light traffic model as it will be explained in the following sections.

2.4.1. In-Line industrial NCS model

Fault-tolerance on the controller level can be either linear [AME 04, AME 05, AME 06b, DAO 04b, DAO 05a] or hierarchical [AME 06a, DAO 05b, DAO 06e, DAO 07b]. In the linear scheme, each controller is controlling the group of sensors/actuator nodes of its machine. The controllers are interconnected over the same communication network with

the sensors and the actuator (the Ethernet). These controllers form what is called in-line production scheme [DAO 04b, DAO 05a]. Upon the failure of any controller, another controller detects this failure and takes care of the control loads of this failed node. Analysis for load switching and network performance was performed as well as for network reliability and availability [AME 04, AME 05, AME 06b].

2.4.2. Reliability Modeling for Linear industrial NCS model

This section presents a Markov model that is used to calculate the reliability of the system consisting of two machines, as described in [PRA 86, BIL 83, TRI 02, JOH 89]. From a reliability point of view, this system will remain operational if one of the two controllers fails. If any of the sensors and/or actuators fails, the entire system fails. In summary, the following events lead to system failure [AME 04]:

- Failure of any of the 32 sensors (16 sensors on each of the 2 machines).
- Failure of any of the 8 actuators (4 actuators on each of the 2 machines).
- Both controllers fail.

When one controller fails the entire system does not fail because the other controller can take over and perform its tasks (along with its own tasks). However, if the remaining controller fails, the entire system fails.

Fig. 2.6 shows the Markov model that is used to calculate system reliability. It consists of 3 states: State 0, state 1 and state 2. State 0 represents the starting state; all components are operational. State 1 describes the situation where one controller has failed but all other components are still operational. State 2 represents the situation where the entire system has failed. The transition rates are explained together with equations governing the model in appendix A.

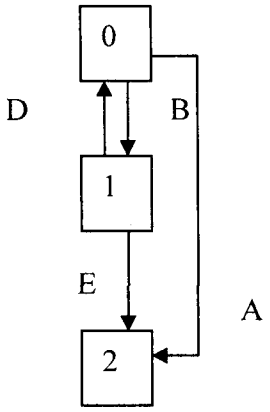


Fig. 2.6, Reliability Model

The Markov model in Fig. 2.6 can be modified by adding transitions from state 2 to states 0 and 1. Fig. 2.7 shows the modified model. If the system is in state 2 due to the failure of the second controller before the first controller is repaired, both controllers have to be repaired.

Also, if the system is in state 2 due to the failure of any of the 32 sensors or 8 actuators, the repair of the failed sensor or actuator will take the system back to state 0. Furthermore, if the presence in state 2 is due to the unsuccessful switchover to the second controller upon the failure of the first one, the repair of the failed controller will also be represented by a transition from state 2 back to state 0.

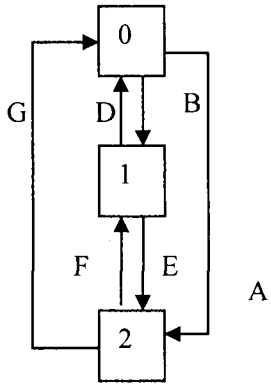


Fig. 2.7, Availability Model

Next, analysis considers the behaviour of the controller failure without taking into account the sensor/actuator failure, for simplicity. Moreover, the sensor/actuator failure term may be regarded as constant with respect to the deep study given for the controller failure causes [AME 06b].

Consider the system of Fig 2.8 with different transitions as shown in figure. The system will move from state 0 to state 1 when one of the two controllers fails, assuming that the controller failure is detected and that the recovery software successfully transfers control of both machines to the remaining operational controller. Otherwise, the system moves directly from state 0 to state 2. This explains the transition from state 0 to state 2.

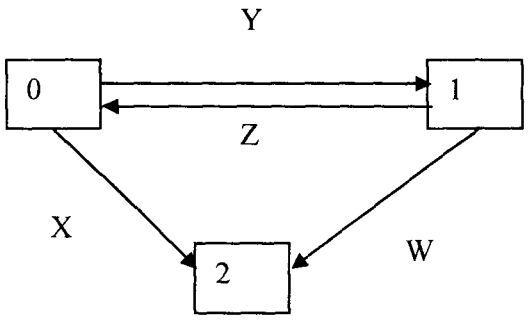


Fig. 2.8, Markov Model

Equations as well as parameters of Fig. 2.6 to 2.8 are detailed in appendix A.

2.4.3. Hierarchical Industrial NCS model: Pyramid Model

In this research, a Pyramid Architecture for general NCS is presented. This model is built in the sense of having running machines for in-line production, and these are monitored by a supervisor controller. This supervisor is either passive or active. This means that, in normal operation, when all controllers are running and no production difficulties exist, the supervisor simply collects information from the controllers it is mastering. It is more like a tree structure with the supervisor as the root and the controllers as the leaves. Inter-leaves communication is present when these controllers are part of an in-line production

scheme. So, the root collects information to be displayed on the main control room screen, in the passive mode.

In case of any controller failure, the supervisor node turns on to be active depending on the proposed switching technique. That is, the supervisor can take over control of the machine with failed controller, or it can switch the control of this machine to another operating controller on the same network. The last scenario can usually be done in the case of in-line production schemes and it resembles what was introduced in [DAO 04b] and [DAO 03]. The main difference here is that a new redundant node in the new scenario exists (the supervisor), i.e., if the only remaining controller is now out of service for any reason, still the system is not down because the supervisor node can take over the control.

This research presents two Pyramid models: two machines with a supervisor, and three machines with a supervisor. Simulations are run to test all possible points of failure and the capability of the proposed system to absorb these failures [DAO 05b].

The supervisor-controller communication in normal conditions is mainly of FTP sessions for gathering information about the machine operation. This kind of explicit messaging is jamming real-time operation of machine controllers. Another FTP is present for inter-controller communication. This is for system synchronization and data back-up [DAO 03, DAO 04b DAO 05b]. Every FTP session must be accompanied by a telnet session for authentication and security measures. Another added non-real-time traffic of e-mail check and HTTP is introduced in the simulations. These are the four non-real-time traffic flavors always present in all previous researches [DAO 03, DAO 04b, DAO 05b, AME 04].

The maximum permissible round-trip delay is of 694usec. This is equivalent to a sampling frequency of 1,440Hz. Under such conditions, the machines are running at a speed of 1 revolution per second producing 60 strokes a minute. The network performance was tested [DAO 05b, DAO 06e, DAO 07b] as well as system reliability [AME 06a].

The Two-Machine Model consists of two machines running under a supervisor node. It simulates the case of having 2 machines for in-line production with inter-controller communication. In the proposed design the control is carried out by the supervisor in case one controller failed.

The Three-Machine model consists of three machines running under a supervisor node. It simulates the case of having 3 machines for in-line production with inter-controller communication.

Two cases can be analyzed. These are passive and active supervisor.

2.4.3.1. Passive supervisor

The failure of the supervisor will not harm the control scheme. This is because synchronization is conducted by inter-controller communication. Supervisor failure causes the system to be disconnected from the outside world communication. That is, the controller nodes are connected to the internet for HTTP and e-mail checks through the supervisor node. Its failure forces the system to work in a closed network over the industrial floor. Moreover, the failure of a machine controller will make the system work in a critical mode with only one controller taking control of the rest of the machines.

With an operational supervisor and upon the failure of one controller, two scenarios are suggested. First, the other controller can take over the control of the other machines with failed controller automatically (as described in [DAO 04b]). This is done through back-up software running on controller nodes platforms.

Second, the supervisor node comes into operation and takes control of the machine with failed controller. In this case, the operational controller nodes load is not changed: they still report to the supervisor node and collect synchronization information from the supervisor instead of the other controller.

In the previous case, where the supervisor is engaged and one of the controllers is active, supervisor failure engages one of the operating controllers to take control of the rest of the machines. This will again give a scenario similar to the one introduced in [DAO 04b].

For the Three-Machine Model, upon the failure of one controller node, the supervisor node is automatically engaged to take over control action of the machine with failed controller. Another controller failure must drive the supervisor node to take control of both machines. Also, FTP sessions between the remaining operating controller and the supervisor must be switched OFF. This is a result of the study conducted in [DAO 04b]: the supervisor node acts like a controller node having the charge of two machines control. The failure of the third controller drives the supervisor to take charge of complete control of the system [DAO 05b].

2.4.3.2. Active Supervisor

Upon the failure of one of the machines' controllers, the supervisor node must take over control of this machine. Complete system failure occurs when the supervisor node goes out of operation for any hardware or software failure [DAO 05b].

2.4.3.3. Supervisor Computational Power

In this study, estimation of the minimum required increase in computational power of the supervisory node is made by simulation.

Simulations were run to test worst case scenarios. Worst case scenario from previous discussion as well as previous studies, is the one having all leaves down and only the root functional. Simulations for 3, 4, and 5 machines and one supervisor were run.

In these simulations, all machines had their real-time control traffic handled by only the supervisor controller. The packets originating at the smart sensors (source of traffic) travel over the network to reach the supervisory controller. After computing the

necessary control action, the control data is once again sent over network to reach the smart actuators (sink of traffic). Data after being de-capsulated, is applied to the physical system under control.

Simulations took into consideration all kinds of delays, regarding data encapsulation/de-capsulation, queuing, processing, and propagation delays over the communication medium.

The supervisor controller node has to have a computational power that was greater than that of any of its leaves controller in the case of a 3-machine production line. This problem was solved in [DAO 05b] by having 100% increase in the computational power.

Increasing the computational power of a supervisor requires enhancing the control software performance. The model in [DAO 03] was processing 28,800 packets per second. This number has to be increased.

A 100% increase may be excessive and not cost effective. In this study, a gradual increase in the computational power is made to reach the minimum increase necessary to get satisfactory end-to-end performance of the system. The measure of system performance is the end-to-end delay of real-time control packets. It has to be less than one sampling period. The proposed system in [DOA 04b], that was also studied in [DAO 05a] and [DAO 05b], had a sampling period of 694μs (1,440Hz, 1 revolution per second).

Increasing the supervisor's processing capabilities [DAO 06a] (Fig. 2.9) is not a drawback of the proposed system. A conclusion from previous studies in [DAO 04b] and [DAO 05a] was that FTP sessions must be switched OFF in critical operating conditions. This is acceptable for normal machine controller implementation. The proposed machines' controllers processing capabilities are of 28,800 packets per second [DAO 03] and [DAO 04b]. The supervisor when running with such processing speed and supervising two machines showed success (previous section). In the case of monitoring 3 machines and requiring intervention when two or three machines' controllers fail, this switching speed will be very low and the supervisor node will fail to fulfil its duties. An

increase of its switching speed is not that expensive when a need to have a robust control scheme is there.

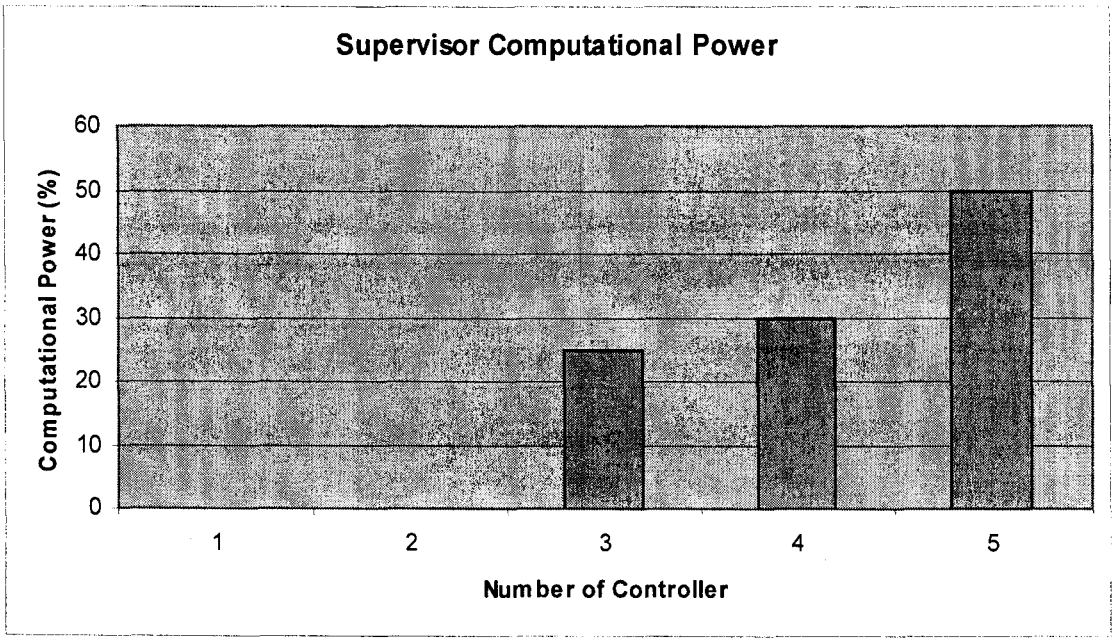


Fig. 2.9, The Increase in Supervisor Computational Power

2.4.4. Reliability Modeling for Hierarchical Industrial NCS model

Now, let us consider the hierarchical model (Pyramid). One of the main advantages of this pyramid architecture is its fault-tolerance aspect. Fault-tolerance increases system reliability/availability. In this research, Markov models [JOH 89, SIE 98] will be used to estimate the unavailability of both the passive and active pyramid architectures. System availability is defined as the probability that a repairable system is operational at any given time [JOH 89, SIE 98]. It is a function of time. System unavailability is defined as: (1- availability). Let UnAv(t) be system unavailability. UnAv(0) is obviously equal to 0. It increases with time due to failures and stabilizes at a steady-state value of $UnAv_{ss}$. Next, Markov models are developed for 2-machine production lines connected in a passive pyramid architecture.

Figure 2.10 shows the Markov model of a 2-machine production line. The system being modeled consists of three main modules: a supervisor S and two machines' controllers M1 and M2. To understand the states of the Markov model, it is important to note that there are **3!** possible sequences of failure: (S,M1,M2), (S,M2,M1), (M1,S,M2), (M1,M2,S), (M2,S,M1) and (M2,M1,S). Each branch of the model describes one of these sequences. The top branch, for example, describes the sequence (S,M1,M2), i.e., the supervisor fails first then M1 and finally M2. The starting state is SM1M2. As the name indicates, S, M1 and M2 are operational. Let the failure rate of S be Xs. Consequently, the model moves from state SM1M2 to state M1M2 at a rate of Xs. Obviously, in state M1M2, M1 and M2 are operational and S has failed. When M1 fails at a rate Xm1, the system moves to state M2 (only M2 is operational). Finally, when M2 fails at a rate Xm2, the system goes to the Failure state F. In this state all three controllers S, M1 and M2 will have failed. The other five branches of the Markov model follow the same logic. Note that states M1M2 and M2M1 both indicate that S has failed and that M1 and M2 are still operational. The names are intentionally different in the Markov model for clarity. The same argument applies for (SM2, M2S), (SM1, M1S), (M2, 2M), (M1, 1M) and (S, SS).

The repair process is modeled in an unconventional way as in [AME 05]. From any state with one or more failed controllers, a transition with a rate μ takes the system back to the initial failure-free state SM1M2. This technique describes situations where the repair time does not vary with the type or number of failures. In developing countries, for example, spare parts are not stocked on premises. In the event of a failure, the defective part is identified, the machine manufacturer is contacted and the appropriate spare part is imported. This process usually takes a long time because of shipping time, customs, etc. A realistic Mean Time To Repair (MTTR) is two weeks (on average). Whether one, two or three parts need to be imported and installed, it will still take an average of two weeks for the production line to become operational again.

To calculate system unavailability, the failure states must be defined. In the context of a passive architecture and since all three controllers S, M1 and M2 are connected by the same network; it was shown in [DAO 05b] that the system remains operational as long as at least one controller is functional. However, the system has to remain observable. If S

and M1 fail, for example, the production line has to be observable through M2. This implies that M2 is equipped with an access panel. In other words, for the production line to remain operational after the failure of two of the three controllers, the supervisor as well as both machines must be equipped with access panels. This argument leads to the following three different modes of operation in the context of the passive pyramid architecture: MAX, PARTIAL and MIN modes [AME 06a].

In the MAX mode, it is assumed that both M1 and M2 are equipped with panels. The supervisor, of course, has a panel. In certain 2-machine production lines, it is possible to have only one of the machines equipped with a panel. This is the PARTIAL mode. In the MIN mode, only the supervisor has a panel.

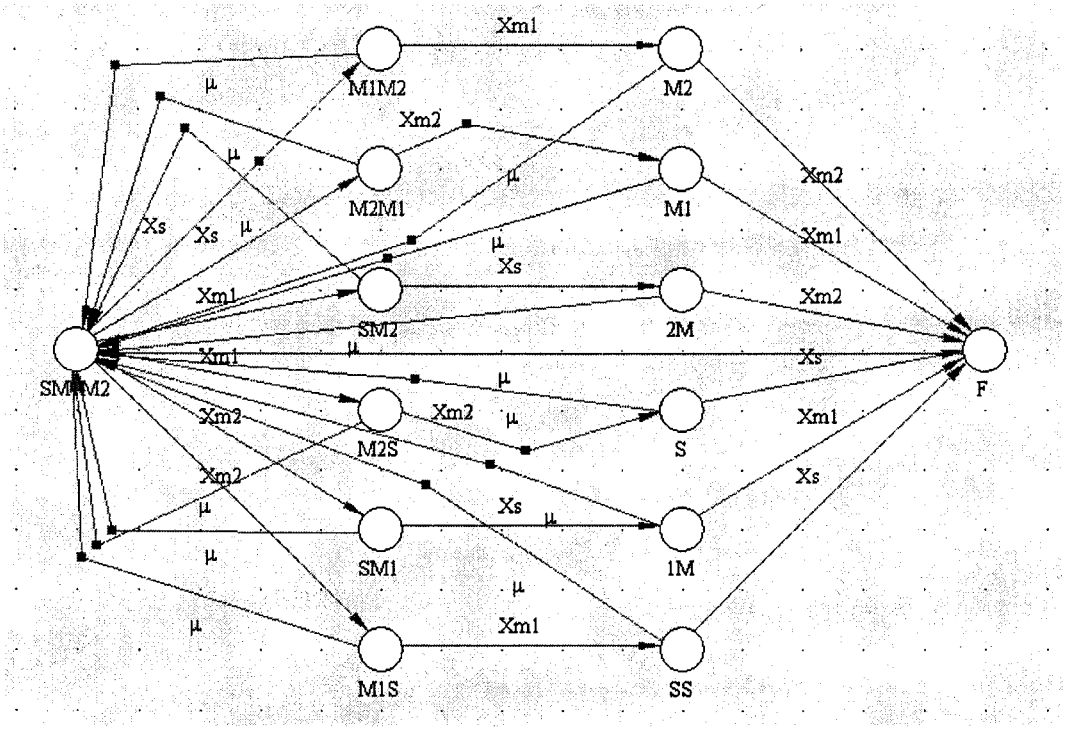


Fig. 2.10, Markov Model for Hierarchical NCS

As mentioned above, an active supervisor takes control actions. From a reliability point of view, this makes the supervisor a single point of failure. Comparing an active supervisor with a passive supervisor in MIN mode, it is clear that they are the same.

Consequently, $UnAv_{ss}$ for the active architecture is identical to that of the MIN mode in the passive architecture.

The two models of Fig. 2.6 and Fig. 2.8 (repeated as Fig. A and Fig C of appendix A pages e and g) are similar in the sense that they both represent a two machine production line. Here is a comparison of both models:

- The model on Fig. 2.6 takes into account failures in the sensors and the actuators. This is why $A = \sum_{i=1}^{32} \lambda_i + \sum_{j=1}^{8} \lambda_j + (1-c)(2\lambda_{com})$ (the equation of page c of the appendix A). The model in Fig 2.8 only studies the controllers in the two-machine production line
- Both models assume that the cabling is failure-free (for simplicity).

The model of Fig. 2.10 discusses a hierarchical pyramid architecture. This is different from the system modeled in figures 2.6 and 2.8 above.

The model in Fig. 2.7 is an availability model and not a reliability model; both F and G transitions represent repair actions AFTER the system goes into the failure state.

2.4.5. TMR at the sensor level of Industrial NCS

Triple Modular Redundancy (TMR) is a well-known fault tolerance technique [JOH 89, SIE 98]. Each sensor is triplicated. The three identical sensors send the same data to the controller. The controller compares the data; if the three messages are within the permissible tolerance range, the message is processed. If one of the three messages is different than the other two, it is concluded that the sensor responsible for sending this message has failed and its data is discarded. One of the other two identical messages is processed. This is known as masking redundancy [JOH 89, SIE 98]. The system does not fail even though one of its components is no longer operational. Triplicating each sensor in a light-traffic machine means that the machine will have 48 (=16×3) sensors, one controller and 4 actuators. The first important consequence of this extra hardware is the

increased traffic on the network. The number of packets produced by sensors will be tripled. A machine with 48 sensors, one controller and 4 actuators was simulated and studied [DAO 03]; this is the *heavy-traffic* machine mentioned in the previous section. The OPNET simulations in [DAO 03] indicated that Gigabit Ethernet was able to accommodate both control and communication loads. Another important issue regarding the triplication of the sensors is cost-effectiveness. From a reliability point of view, triplicating sensors is expected to increase the system Mean Time Between Failures (MTBF) and consequently, decrease the down time. However, the cost of adding fault tolerance has to be taken into account. This cost includes the extra sensors, the wiring, bigger switches and software modifications. The software is now required to handle the "voting" process; the messages from each three identical sensors have to be compared. If the three messages are within permissible tolerance ranges, one message is processed. If one of the messages is different from the other two, one of the two valid messages is used. The sensor that sent the corrupted message is disregarded till being repaired. If a second sensor from this group fails, the software will not be able to detect which of the sensors has failed and the production line has to be stopped. It is the software's responsibility to alert the operator using Human Machine Interface (HMI) about the location of the first malfunctioning sensor and to stop the production line upon the failure of the second sensor [AME 08].

2.4.6. Reliability Modeling for TMR Industrial NCS

Reliability Block Diagrams (RBDs) can be used to calculate system reliability [SIE 98]. The SHARPE [SHA] package is used to build the RBD of the system under study. Three configurations will be studied in this Section. In the first configuration, there is no fault tolerance. Any sensor, controller, switch or actuator on either machine is a single point of failure. For exponentially-distributed failure times, the system failure rate is the sum of the failure rates of all its components. Let this configuration be the *Simplex* configuration [AME 08]. If fault tolerance is introduced at the controller level only (as in [DAO 04b]), this configuration will be called *Two-Cont* [AME 08]. Fig. 2.11 shows the RBD of the

Two-Cont production line with two light-traffic machines. It is clear that fault tolerance only exists at the controller level. Fig. 2.12 describes the RBD of the same production line but with two heavy-traffic machines. Now, every sensor is a TMR system and will fail when two of its sensors fail (2-out-of-3 system).

Let this configuration be called the *TMR* configuration. Only the actuators and the switches constitute single points of failure. Instead of calculating system reliability, another approach is taken in this research, namely the Mission Time (**MT**). $MT(r_{min})$ is the time at which system reliability falls below r_{min} [JOH 89, SIE 98]. r_{min} is determined by production management and represents the minimum acceptable reliability for the production line. SHARPE will calculate the MT for the three configurations mentioned above (Simplex, Two-Cont and TMR). The production line will run continuously for a period of MT. Maintenance will then be performed; if one of the controllers has failed, it is repaired as well as any failed sensor. r_{min} is chosen such that the probability of having a system failure during MT is minimal.

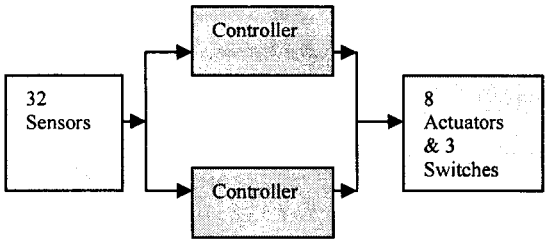


Fig. 2.11, RBD for 2-Cont Configuration

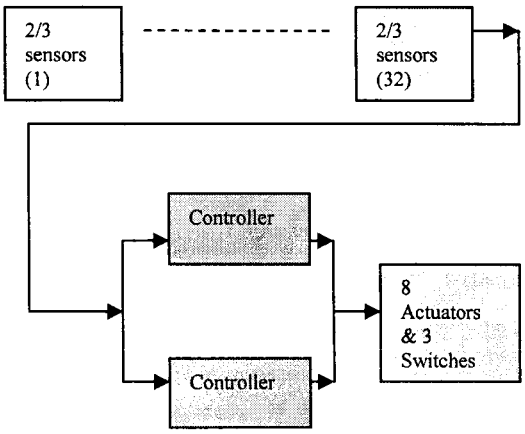


Fig. 2.12, RBD for TMR Configuration

It is assumed in this research that the production line is totally fault-free after maintenance. If r_{min} is high enough, there will be no unscheduled down time and no loss of production. Of course, if r_{min} is very high, MT will decrease and the down time will increase. Production can of course be directly related to cost. Let R_{sys} be the reliability of the production line. R_{sens}, R_{switch}, R_{cont} and R_{act} will be the reliabilities of the sensor, switch, controller and actuator, respectively. For exponentially-distributed failure times:

$$R = e^{-\lambda t} \tag{2.6}$$

R is the component reliability (sensor, controller, ...) and λ is its failure rate (which is constant [JOH 89, SIE 98]). Assume for simplicity that the switches are very reliable when compared to the sensors, actuators or controllers and that their probability of failure can be neglected. Furthermore, assume that all sensors on both machines have an identical reliability. The same applies for the controllers and the actuators. Next, the reliabilities of the production line will be calculated for the three configurations: Simplex, Two-Cont and TMR.

In the Simplex mode, there is no fault tolerance at all and any sensor, controller or actuator failure causes a system failure [SIE 98]. Hence:

$$R_{sys} = (R_{sens}^{32})(R_{cont}^{2})(R_{act}^{8}) \tag{2.7}$$

Remember that each machine has 16 sensors, one controller and 4 actuators and the system (production line) consists of two machines. If fault tolerance is introduced at the controller level (as in [DAO 04b])

$$R_{sys} = (R_{sens}^{32})(1-(1-R_{cont})^{2})(R_{act}^{8}) \tag{2.8}$$

The next level of fault tolerance is the introduction of Triple Modular Redundancy at the sensor level. Each of the 32 sensors will now be a sensor assembly that consists of three identical sensors

$$R_{sys} = (3R_{sens}^{2}-2R_{sens}^{3})^{32}(1-(1-R_{cont})^{2})(R_{act}^{8}) \tag{2.9}$$

It was assumed that a failed sensor will send incorrect data in a correct packet. The controller will decapsulate the three packets coming from the three identical sensors, compare the three readings, disregard the reading that is different from the other two and use one of the two similar readings. Another potential failure mode is that where a failed sensor stops sending packets; but, as long as the sensor is operational, the data it sends is correct. From a reliability point of view, the three sensors are no longer a two-of-three system but a one-of-three system. As long as one of the three identical sensors is operational, the machine (and hence the production line) does not fail. The RBD will be identical to the one in Fig. 2.12 except that each sensor block will be a 1/3 block instead of 2/3. Let this fourth configuration be called *1-of-3*.

2.5. VEHICLE ON-BOARD NETWORK

The study presented here is relying on what is presented in [UPE 96]. The network is first implemented using 90 nodes (sensors and actuators) and a controller. The model built in OPNET for simulation is based on the Networked Control System scheme of Fig. 2.13.

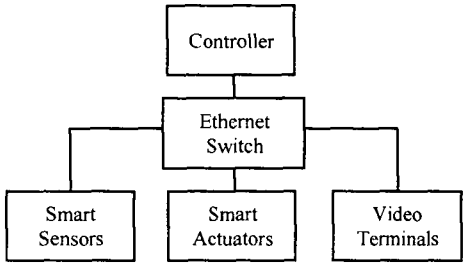


Fig. 2.13, Vehicle On-Board Network Block Diagram

In the model of Fig. 2.13, sources and sinks of real-time loads are smart sensors and actuators respectively. These nodes are smart because they are capable of performing several functions else than sensing the physical phenomena of the process. They are capable of self diagnostic as well as calibration. They also have communication functionality: they encapsulate data in network packet format, send it over the network

based on the type of protocol the network support, receive data and de-capsulate it...etc...

Table 2.1
Sample of Vehicle On-Board Network Signals

Msg ID	Name	Frequency	Class	Type
0	Crash_Sensor1	200	C	S
8	Wheel_Speed_Sensor4	200	C	S
9	Stearing_Rotation_Rate_Sensor	200	C	S
10	Hydraulic_Stearing_Assist	200	C	C
11	Speed_Control_Signal	200	C	C
12	Clutch_Position_sensor	200	C	S
17	Rear_Wheel_Spin_Sensor1	100	C	S
22	Accelerator_Position_Rate_Sensor	100	C	S
23	Trans_Clutch_Line_Press	100	C	S
24	Ignition_Diagnostic_Monitor	50	B	C
25	Cylinder_Id_Sensor	50	B	S
26	Manual_Lever_Position	50	B	S
30	Throttle_Postion_Sensor	50	B	S
31	Engine_RPM	50	B	S
32	Handbrale_Position_Sensor	10	B	S
39	Engine_Coolant_Temperature	10	B	S
40	Transmission_Lube_Pressure	10	B	S
41	Intake_Air_temperature	5	B	S
42	Suspension_Status	1	A	C
43	Outside_Temperature	1	A	S
49	Heat/Cool_Control	1	A	C
51	Cruise_Control_Indicator	1	A	C
52	Auto_Headlamp_Sensor	1	A	S
53	Ignition_Switch_Position	1	A	S
54	Horn_Sensor	1	A	S
59	Fuel_Level_Sensor	1	A	S
60	Alternator_Warning_Indicator	1	A	C
61	Octane_Adjust_Plug	1	A	S
83	ABS_Status_Lamp	1	A	C
84	ABS_Brake_Lamp	1	A	C
85	Airbag_Indicator_Lamp	1	A	C
86	Seatbelt_Lamp	1	A	C
87	Door_Lamps_ON/OFF	1	A	C
88	Airbag_Status	1	A	C
89	Washer_Fluid_Sensor	0.1	A	S

The video terminal nodes are sources of non-real-time loads. Although video streaming is considered as real-time communication load, in the context of vehicle automation, one can consider it as source of undesirable communication load that jams the communication of useful control data. These nodes are added to test the functionality of the system when integrating control and communication networks over the same communication media.

A study is conducted by transforming the network studied in [UPE 96] to use Ethernet instead of CAN. Only control loads are considered [DAO 06b]. Then, non-real-time traffic in added to the system to test the performance of the network in the mixed communication load environment [DAO 06b]. Fault-tolerance study is then conducted [DAO 06c] to test the availability of bandwidth in the network to support redundancy in sensor nodes. This is because increasing the number of sensor nodes will automatically reflect in an increase in the number of packets sent over the network.

Based on the conclusions of [DAO 03] showing the possibility of using Ethernet as backbone for industrial control systems, cars on-board control networks using Gigabit Ethernet were implemented in [DAO 06b]. Gigabit Ethernet mandates high speed microcontrollers for sensors/actuators implementation. This is achievable by microcontrollers available from [FUJ]. Since the results of [DAO 06b] showed that the deadlines of control actions were met and that there was still enough network bandwidth, two options are possible: testing the network with more added functions to find the upper bound of the network operation before the Networked Control System (NCS) gets out of control [DAO 06b], [DAO 06c], or testing a lower network speed and evaluating its performance. In this research, the last approach is investigated. A comparison between Fast and Gigabit Ethernet for backbone implementation is also performed [DAO07e].

Gigabit Ethernet is first tested as NCS backbone for cars. This is based on the conclusions of [DAO 03]. In [DAO 03], studies on using Ethernet as communication network for industrial NCS were conducted. It was concluded that Ethernet can absorb mixed communication traffic of control and communication packets and meet the desired deadlines for the control system. The control system's deadlines in [mw] were tighter than in the case of the vehicle control as it is explain in Table 2.1. Moreover, Gigabit

Ethernet in its switched version with optical links is more attractive for more load addition to the network. The 90 nodes model of [UPE 96] is used. Table 2.1 shows a sample of the communication instances of the network indicating sources and sinks of loads. The complete table can be found in appendix B.

While in CAN the system is divided into three main network categories: A, B and C, where C is the most critical network, followed by class B and finally, Class A. In the proposed model all sensors and actuators are grouped in one big network. The type column indicates whether the signal is originating at a sensor node (S) or sinking at an actuator node (C). Also, it has to be noted that the study in [UPE 96] only analyzed network delay while, in this research, all kinds of delay faced by the data from the moment it originates at the sensor node till it is consumed by the actuator node are taken into consideration.

In this research, fault-tolerance is proposed at the controller level by using 2 different controllers: one controller for Class C applications, and another one for Class A and Class B applications. Data messages are communicated between both controllers for back-up. Upon the failure of either controllers, the load is transferred to the active controller. Simulation runs using OPNET are done to test the possibility to build this system. This architecture is based on what was early proposed in industrial control [DAO 04b, DAO 05a].

2.5.1. Fault-Tolerance at the controller level

Automotive on-board Class C CAN networks treats the most critical applications. In this research, a fault-tolerance is proposed at the controller level by using 2 different controllers (Fig. 2.14): one controller for Class C applications, and another one for Class A and Class B applications. Data messages are communicated between both controllers for back-up. Upon the failure of either controllers, the load is transferred to the active controller. This architecture is based on what was early proposed in industrial control [DAO 04b, DAO 05a].

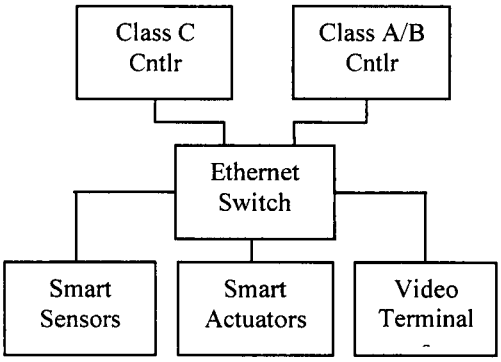


Fig. 2.14, Fault-Tolerant Vehicle On-Board Network Controllers

2.5.2. Fault-Tolerance at the sensor level

Triple Modular Redundancy (TMR) is a way to introduce fault-tolerance in the control network of the vehicle. It is based on a triplication of each sensor node in the system. The physical phenomena is sensed 3 times, and sent to the controller. At the controller node, a majority voting is implemented. The 3 different packets of the three sensors module must fall within a given tolerant range. If one of these 3 information is far beyond this range, the sensor responsible of this packet is declared faulty. The system operation is still maintained and the controller looks to the information of the two other sensors. If the two results happen to be different, this time, the system fails.

In this research, TMR sensors of vehicle on-board system (Fig. 2.15) are analyzed from the communication point of view.

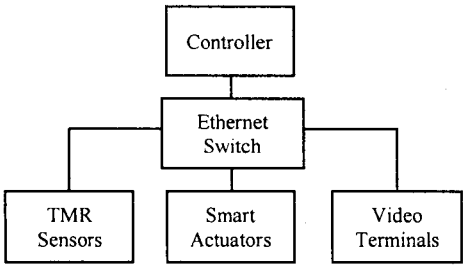


Fig. 2.15, TMR Vehicle On-Board Network Sensors

No pyramid (hierarchical) model is tested for vehicle on-board networks. This is because it is hard from the technical point of view to have a second control level for cars' on-

board network. This level will in first place increase the total electronics weight, while the study is in first place conducted to take off electronic components to lower this weight burden.

Reliability models were very difficult to elaborate because of the extreme conditionality of the subject: it was very difficult to have access to on-board network communication loads and data, it was then much more difficult to have a dialog with car manufacturer to tell their thought and maintenance as well as reliability plans.

2.6. CONCLUSION

An attempt to deduce a generic model for previous studies in the field of wired NCS is proposed. This helps in generating a general model from what was early studied as a special case in industrial automation. Application is new field of wired control system is then presented. This new field is the Automotive on-board control networks.

General model of vehicles on-board networks is first presented. Fault-Tolerance at the controller as well as on the sensor level is then treated. Fault-tolerance aspect of control networks in general is very important and attractive field of research. This is because in case of having a system control relaying on network behavior and intelligent nodes availability, it is crucial to understand and study different system nodes' reliability. Studies in this line were conducted and introduced briefly in this chapter, while more equations can be found in appendix A.

The next chapter presents a survey of some wireless technologies. The wireless model of Chapter 3 is used to establish wireless communication between moving cars (the on-board vehicle model introduced in this chapter) and the central intelligence of an infrastructure. These moving cars need to exchange traffic information for optimal path calculation during their journey from a start point to a destination location.

CHAPTER III

WIRELESS MODEL

3.0. INTRODUCTION

Wireless communication plays a major part of our daily routine. Wireless connectivity to exchange information in data or voice format is widely used nowadays. In this chapter, a model to design a fully WiFi covered light urban area is proposed. This coverage enables the exchange of traffic data to minimize circulation bottle necks for example. It can also be used for video conferencing and video streaming as well as VoIP to complement the future vehicle on-board entertainment.

Section 3.1 summarizes the available wireless technologies while section 3.2 proposes the suitable wireless technology for this project's implementation and a fast discussion regarding the benefits of using standard protocols. Basics of WiFi mobility are introduced in section 3.3. System architecture is the focus of section 3.4. Proposed system parameters are introduced in section 3.5. Performance metrics are given in section 3.6. This chapter is summarized and concluded by section 3.7.

3.1. WIRELESS TECHNOLOGIES AND WIFI

Different Wireless Technologies are available on the market. In the following, a survey of the relevant technologies are briefly introduced and summarized. Fig. 3.1 illustrates

the different technologies with respect to bandwidth, speed and coverage of the mobile node [WTG].

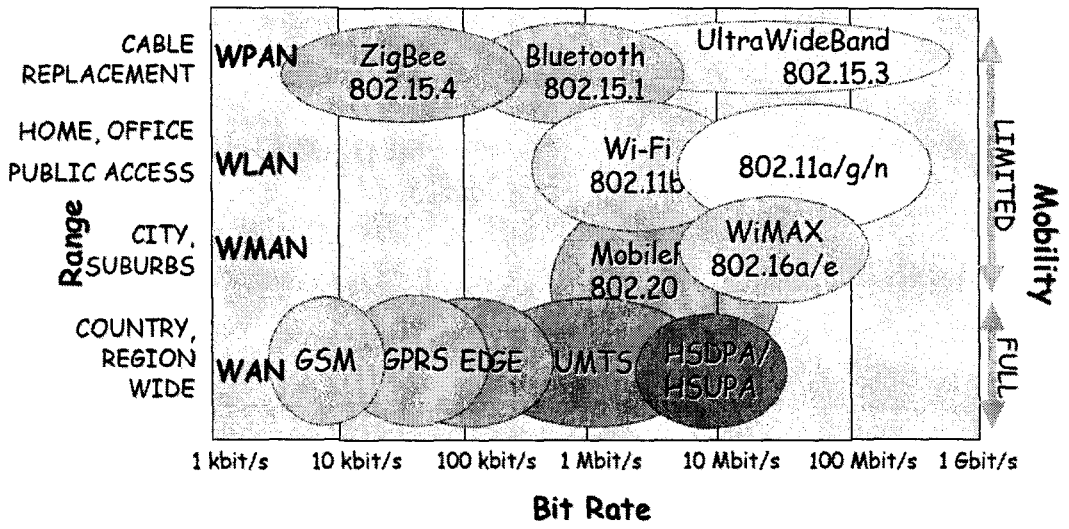


Fig. 3.1, Comparison of Different Technologies with Respect to Range, Bit Rate and Mobility [WTG]

Table 3.1: Generations of Data Standards

	Actual	Circuit switching	Packet switching (IP)
GSM (2G)	14.4 Kbps	√	
GPRS (2.5G)	56 Kbps		√
EDGE or EGPRS (2.75G)	180 Kbps		√
UMTS (3G)	≈1 Mbps		√
HSDPA (3.5G)	3.6 Mbps		√

In the last 3 decades, wireless technologies have evolved dramatically in the field of Internet communication. Beginning with the Global System for Mobile Communications (GSM), the 2nd Generation (2G), which is widely used nowadays in the world, communication has grown up from circuit switching to packet switching and reached a data transfer of 3.6Mbps in High-Speed Downlink Packet Access (HSDPA) (the 3rd Generation, 3G). Previous cellular telephone systems were mainly circuit-switched, i.e. connections are always dependent on circuit availability. A packet-switched connection

uses the Internet Protocol (IP), i.e. a virtual connection is always available to any other end point in the network. The Packet switching opened the possibility of Internet communication and thus connecting mobile nodes to the Internet. Table 3.1 illustrates the evolution in the different generations.

In the following only WiFi and WiMAX are introduced as examples of potential wireless data networks candidates for this research.

3.1.1. WiFi Standards

A WiFi LAN is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure. It is based on the IEEE 802.11 protocol [STD 11]. It was developed by Kyle Brown to be used for mobile computing devices, such as laptops, in LANs, but is now increasingly used for more services, including Internet and Voice over IP (VoIP) phone access, gaming, and basic connectivity of consumer electronics such as televisions and DVD players, or digital cameras. Like all IEEE 802 standards, the 802.11 standards focus on the bottom two levels of the ISO model; the physical layer and link layer (Fig. 3.2). Any LAN application, network operating system, protocol, including TCP/IP and Novell NetWare, will run on an 802.11-compliant WLAN as easily as they run over Ethernet [TAN 03, WLT].

WiFi is based on the IEEE 802.11 protocol, thus the terms 802.11 and WiFi will be used interchangeably. Each computer (node) in 802.11 is referred to as a station. When two or more stations communicate with each other, they form a Basic Service Set (BSS). The minimum BSS consists of two stations. 802.11 LANs use the BSS as the standard's building block. Two or more BSSs are interconnected using a Distribution System (DS). Thus, each BSS becomes a component of an extended, larger network. Entry to the DS is accomplished with the use of access points (AP). An access point is a station, thus addressable. So, data moves between the BSS and the DS with the help of these access

points (More details in appendix C). This leads to the higher level in the hierarchy, the Extended Service Set or ESS. The architecture described above is illustrated in Fig. 3.3.

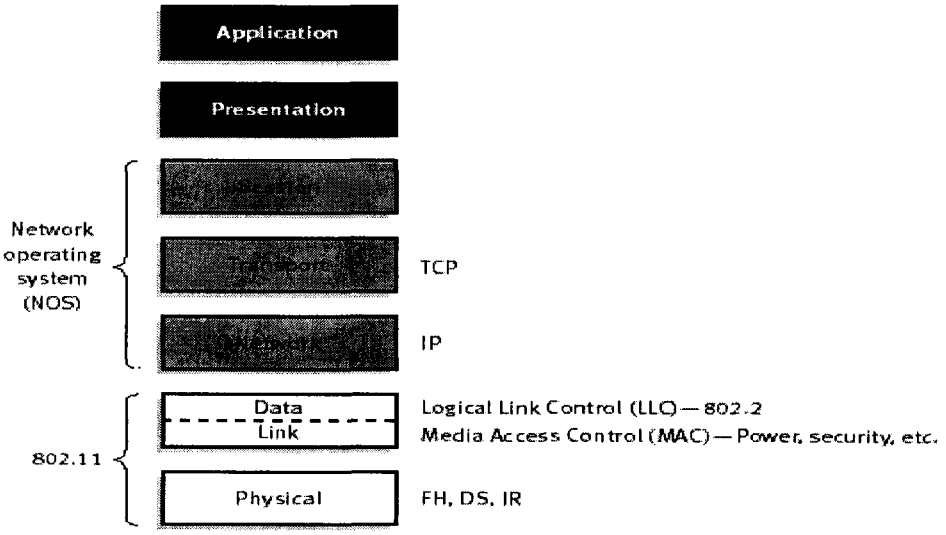


Fig. 3.2, Network Layers and Their Relation with WiFi

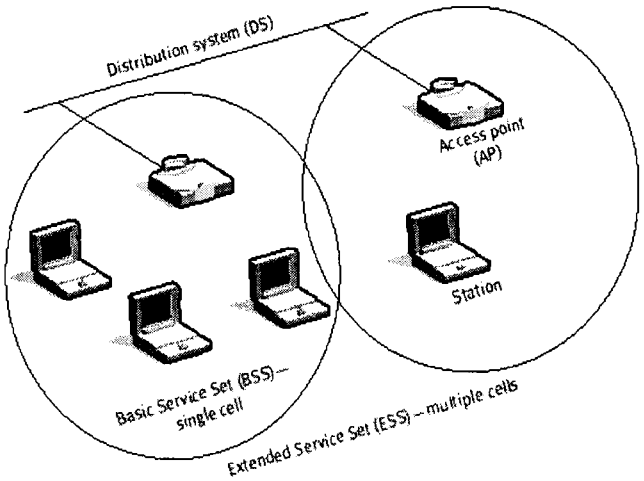


Fig. 3.3, Infrastructure of the 802.11 WLAN

The 802.11 standard operates in two modes:

- In the presence of a base station;
- In the absence of a base station.

In the first case, a typical WiFi setup contains one or more access points and one or more clients. An AP broadcasts its SSID (Service Set Identifier, "Network name") via packets that are called beacons, which are usually broadcasted every 100ms. The beacons are transmitted at 1Mbit/s, and are of relatively short duration and therefore do not have a significant effect on performance. Since 1Mbps is the lowest rate of WiFi it assures that the client who receives the beacon can communicate at a rate of at least 1Mbps. If two APs of the same SSID are in range of the client, the client firmware might use signal strength to decide which of the two APs to make a connection to. Thus, a person with a WiFi enabled device such as a cell phone, PDA or a laptop can connect to the Internet when in proximity of an access point. The region covered by one or several access points is called a hotspot. Hotspots can range from a single room to many square miles of overlapping hotspots.

In the second case, the computers would just send to one another directly. This mode is sometimes called ad-hoc networking or peer-to-peer. This connectivity mode is usually useful in certain applications such as gaming. Fig. 3.4 shows the different operations of WiFi in the presence and absence of base station.

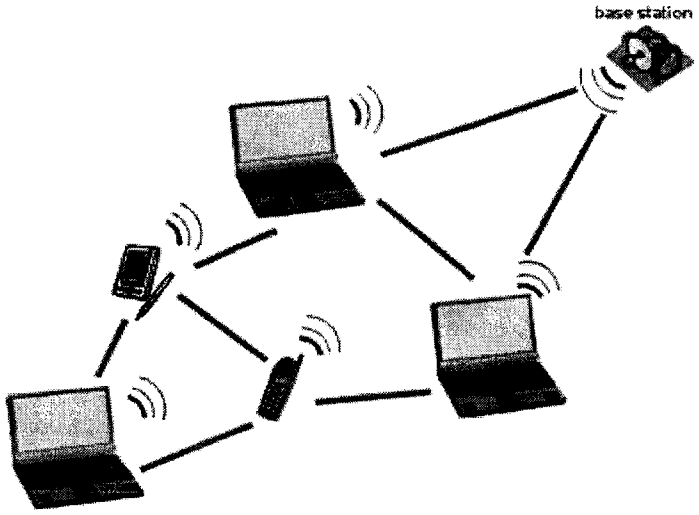


Fig. 3.4, Different Operations of WiFi [ERC]

There are five techniques used in the physical Layer to send a MAC frame. They differ in the technology used and the speed achievable. The technologies used are the Infrared (line of sight), the FHSS (Frequency Hopping Spread Spectrum), the DSSS (Direct

Sequence Spread Spectrum), the OFDM (Orthogonal Frequency Division Multiplexing), and the HR-DSSS (High Rate Direct Sequence Spread Spectrum).

The radio-based standards operate within the 2.4GHz ISM band. These frequency bands are recognized by international regulatory agencies radio operations. Thus, 802.11 based products do not require extra regulations or licenses. The original 802.11 wireless standard defines data rates of 1Mbps and 2Mbps via radio waves using frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS). The FHSS and DSSS are two totally different techniques that are not interoperable.

Advantages of WiFi Includes:

- WiFi allows LANs to be deployed without cabling, typically reducing the costs of network deployment and expansion. Spaces where cables cannot be run, such as outdoor areas and historical buildings, can host wireless LANs;
- WiFi silicon pricing continues to come down, making WiFi a very economical networking option;
- WiFi networks support roaming, in which a mobile client station such as a laptop computer can move from one access point to another as the user moves around a building or area;
- WiFi is a global set of standards. Unlike cellular carriers, the same WiFi client works in different countries around the world;
- WiFi is widely available in more than 250,000 public hot spots and millions of homes and corporate and university campuses worldwide [TAN 03].

Some of the disadvantages of WiFi are:

- WiFi can interfere with other devices, notably 2.4GHz cordless phones and microwave ovens;
- Spectrum assignments and operational limitations are not consistent worldwide; most of Europe allows for an additional 2 channels beyond those permitted in the US (1-13 vs. 1-11); Japan has one more on top of that (1-14). Some countries, like Spain, prohibit the use of lower-numbered channels;

- Power consumption is fairly high compared to some other standards, making battery life and heat a concern;
- Many 2.4GHz 802.11b and 802.11g access points default to the same channel, contributing to congestion on certain channels;
- WiFi networks can be monitored and used to read and copy data (including personal information) transmitted over the network when no encryption such as VPN is used;
- Interoperability issues between brands or deviations from the standard can disrupt connections or lower throughput speeds on other user's devices within range. WiFi Alliance programs test devices for interoperability and designate devices which pass testing as WiFi CERTIFIED [TAN 03].

3.1.2. WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) is a wireless technology that has the potential to replace a number of existing telecommunications infrastructures. In a fixed wireless configuration it can replace the telephone company's copper wire networks, the cable TV's coaxial cable infrastructure while offering Internet Service Provider (ISP) services. In its mobile version, WiMAX has the potential to replace cellular networks.

WiMAX is a term describing the IEEE 802.16 [STD 16] wireless networks. Its standards are 802.16-2004 (fixed wireless applications) and 802.16e-2005 (mobile wireless applications).

WiMAX provides fixed, portable or mobile non-line-of sight service from a base station to a subscriber station. Some goals for WiMAX include a radius of service coverage of 6miles from a WiMAX base station for point-to-multipoint, non-line-of-sight service. This service should deliver approximately 40Mbps for fixed and portable access applications. For line-of-sight, point to point its goal is to cover 30Miles with a data rate of 72Mbps.

Mobile WiMAX takes the fixed wireless application a step further and enables cell phone-like applications on a much larger scale. It offers superior building penetration and improved security measures over fixed WiMAX. It allows any telecommunication service to go mobile.

WiMAX is very different from WiFi in the way it works. In WiFi, the media access controller (MAC) uses contention access: all subscriber stations that wish to pass data through a wireless access point are competing for the AP's attention on a random interrupt basis. This can cause subscriber stations distant from the AP to be repeatedly interrupted by closer stations, greatly reducing their throughput. This makes services such as Voice over IP or IPTV, which depend on a predetermined type of Quality of Service (QoS), difficult to maintain for large numbers of users.

In contrast, the 802.16 MAC uses a scheduling algorithm, where the subscriber station only has to compete once (for initial entry into the network). After that it is allocated a time slot by the base station. The time slot can enlarge and contract, but it remains assigned to the subscriber station, meaning that other subscribers cannot use it. This scheduling algorithm is stable under overload and over-subscription (unlike 802.11). It can also be more bandwidth efficient. The scheduling algorithm also allows the base station to control QoS parameters by balancing the time-slot assignments among the application needs of the subscriber stations.

3.2. WIRELESS TECHNOLOGY FOR THIS RESEARCH & PROTOCOL ADVANTAGES

The Wireless technology used allover this research is the IEEE802.11Std (WiFi) [STD 11]. Although WiFi is not the best wireless protocol to use for such implementation, it offers lots of advantages that make it feasible. For the application introduced in this study, WiFi is competing with WiMAX and 3G personal mobile communication.

WiFi is advantageous in the sense that it is a well established and tested protocol for almost 6 years. WiFi silicon pricing continues to come down, making it a very economical networking option. WiFi networks support roaming, in which a mobile client station such as a laptop computer can move from one access point to another as the user moves around a building or area. It is a global set of standards. Unlike cellular carriers, the same WiFi client works in different countries around the world.

Although WiMax offers more advantages over WiFi, it is not commercialized to the moment of preparation of this document for personal use to implement its mobile wireless application based on the IEEE802.16e-2005 Std. The third generation mobile communication (3G) is an easy solution to broadcast information through cell broadcast for example, or by SMS. But in comparison to WiFi, 3G is an emerging technology to the local market, which makes it expensive. Also the price of building a 3G infrastructure is higher than the one required to build a WiFi one. 3G is built for commercial use, as any other personal mobile communication network, while WiFi is offered for free almost everywhere. Fig. 3.5 shows the advantage of WiFi over both technologies regarding bandwidth availability.

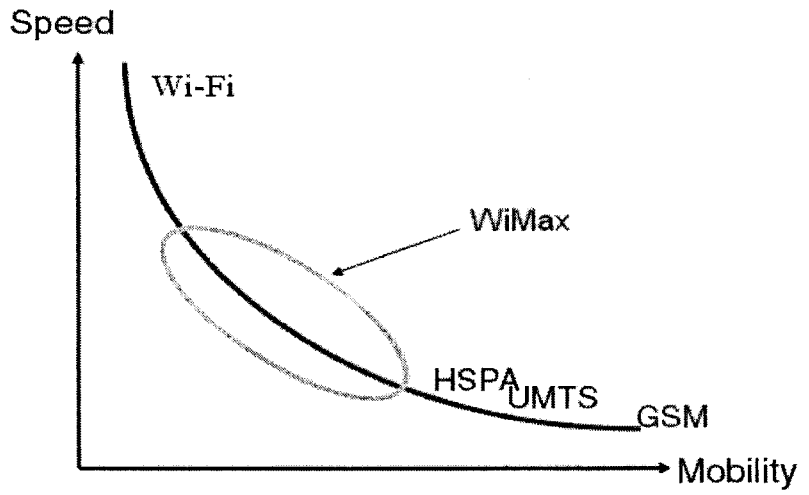


Fig. 3.5, Wireless Technologies Mobility Curve

First, the main advantage behind the use of a protocol is to give the design flexibility in its implementation. Due to the protocol standardization the system could be easily built

using protocol compatible devices. Cost, as well, is minimized by using off-the-shelf equipments rather than designing a specific transceiver.

Second advantage resides in resolving the problem of setting up the wireless channel in terms of modulation techniques, error check and channel allocation. In fact the payload, which consists of a given number of data bits, is transmitted transparently using one of the available standards.

Third advantage is that the 802.11 and the 802.15.4 [STD 15] use a Carrier Sense Multiple Access (CSMA) scheme to control access to the transmission medium. However, rather than the Collision Detection (CSMA/CD) employed by Ethernet, 802.11 uses Collision Avoidance (CSMA/CA) which is a distributed access scheme with no centralized controller.

The access to the wireless medium is controlled by the Distributed Coordination Function (DCF) which is the basis of the CSMA/CA access mechanism. It first checks if the radio link is clear before transmitting. To avoid collisions, stations use a random backoff after each frame, with the first transmitter seizing the channel. In some circumstances, the DCF may use the Request To Send (RTS) and Clear To Send (CTS) clearing technique to further reduce the possibility of collisions.

3.3. BASICS OF WIFI MOBILITY

Mobility is the ability to move readily from place to place. Roaming describes the act of moving between access points. In general terms, there are two types of roaming:

Seamless Roaming: As in cellular phones the user roams from the coverage range of a Time Division Multiplexing Access (TDMA) cell to another while using the services of the cellular phone, i.e. supposedly if the user is having a phone call while roaming between cells no degradation of sound quality will occur.

Nomadic Roaming: As in laptops when the user undocks his laptop and roams between access points, then after sitting again he reopens his laptop and uses it. This type of roaming is deemed *nomadic* because the user is not using network services when he roams, but only when he reaches his destination.

802.11 roaming is known as "break before make" referring to the requirement that a station serves its association with one AP before creating an association with a new one. This process might seem unintuitive because it introduces the possibility for data loss during roaming, but it facilitates a simpler MAC protocol and radio. The difficulty of having the protocol reversed i.e. "make before break", is that safeguards will be needed in the MAC to ensure loop free topology, i.e., it would require an algorithm that resolves any potential loops, adding overhead to the MAC protocol. In addition, the client radio would have to be capable of listening and communicating on more than one channel at a time, increasing the complexity of the radio specially that 802.11 mobility is defined for low speeds (walking speeds).

The operation of the running application and its behavior during roaming depends on the high level protocol this application uses. For example, Transmission Control Protocol (TCP) based applications tolerate packet loss during roaming. This is because TCP requests acknowledgment of receipt just as the MAC does. This makes it a reliable protocol that requests any data that has been lost to be resent. However, other applications may be running over User Datagram Protocol (UDP) as the layer 4 transport protocol. UDP is a low-overhead, connectionless protocol. Applications such as Voice over IP (VoIP) and video conferencing/streaming use UDP packets. The retransmission capability that TCP offers does little to enhance packet loss for VoIP applications. Retransmitting VoIP packets proves more annoying to the user than useful. As a result, the data-loss roaming might cause a noticeable impact to UDP-based applications [LEA 04].

A mobile node must be able to communicate with other nodes after changing its link-layer point of attachment to the Internet, yet without changing its IP address. A mobile node must be able to communicate with other nodes that do not implement these mobility

functions. No protocol enhancements are required in hosts or routers. All messages used to update another node as to the location of a mobile node must be authenticated in order to protect against remote redirection attacks.

The link by which a mobile node is directly attached to the Internet may often be a wireless link. This link may thus have a substantially lower bandwidth and higher error rate than traditional wired networks. Moreover, mobile nodes are likely to be battery powered, and minimizing power consumption is important. Therefore, the number of administrative messages sent over the link by which a mobile node is directly attached to the Internet should be minimized, and the size of these messages should be kept as small as possible.

Mobile IP (MIP) enables a Mobile Node to maintain its connectivity to the Internet when moving from one Access Router to another, a process referred to as *handover* (or hand-off). During handover, there is a period during which the Mobile Node (MN) is unable to send or receive packets because of link switching delay and IP protocol operations. This *handover latency* resulting from standard MIP procedures, namely movement detection, new Care of Address (CoA) configuration, and Binding Update, is often unacceptable to real-time traffic such as Voice over IP (VoIP). Reducing the handover latency could be beneficial to non-real-time, throughput-sensitive applications as well [RFC 05a].

In the following, some Mobile IP networks definitions can be listed.

The Home address is an address assigned to the mobile node when it is attached to the home link and through which the mobile node is always reachable.

The Home Agent (HA) is a router on the home link that maintains registrations of mobile nodes that are away from home and the different addresses that they are currently using. If the mobile node is away from home, it registers its current address with the home agent, which tunnels data sent to the mobile node's home address to the mobile node's current address

The Care of Address (CoA) is an address used by a mobile node while it is attached to a foreign link. A mobile node can be assigned multiple care-of addresses; however, only

one care-of address is registered as the primary care-of address with the mobile node's home agent. The association of a home address with a care-of address for a mobile node is known as a *binding*. Correspondent nodes and home agents keep information on bindings in a binding cache.

The Correspondent Node (CN) is a node that communicates with the Mobile Node in a Mobile IP network.

The Mobile Node (MN) is a node with wireless interface that moves from one point of attachment to another one in a Mobile IP network.

The Foreign Agent (FA) is a router on a different network than the home network of the Mobile Node.

Mobile IP protocols are tested since they represent a generic model to support mobility.

3.3.1. MIPv4 (RFC3344)

IP version 4 (IPv4) assumes that a node's IP address uniquely identifies the node's point of attachment to the Internet. Therefore, a node must be located on the network indicated by its IP address in order to receive datagrams destined to it; otherwise, datagrams destined to the node would be undeliverable. For a node to change its point of attachment without losing its ability to communicate, currently one of the two following mechanisms must typically be employed:

- the node must change its IP address whenever it changes its point of attachment, or
- host-specific routes must be propagated throughout much of the Internet routing fabric.

Both of these alternatives are often unacceptable. The first makes it impossible for a node to maintain transport and higher-layer connections when the node changes location. The

second has obvious and severe scaling problems, especially relevant considering the explosive growth in sales of notebook (mobile) computers.

A new, scalable, mechanism is required for accommodating node mobility within the Internet. RFC3344 defines such a mechanism for MIPv4, which enables nodes to change their point of attachment to the Internet without changing their IP address.

RFC3344 specifies protocol enhancements that allow transparent routing of IP datagrams to mobile nodes in the Internet. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a CoA, which provides information about its current point of attachment to the Internet. The protocol provides for registering the care-of address with a home agent. The home agent sends datagrams destined for the mobile node through a tunnel to the CoA. After arriving at the end of the tunnel, each datagram is then delivered to the mobile node.

Fig. 3.6-3.8 illustrate an example of MIPv4 triangular routing.

In Fig. 3.6, the Mobile Node (MN) is located at its Home network communicating to the Correspondent Node (CN) through its Home Agent (HA). Now the MN moves from Network A to reach Network B.

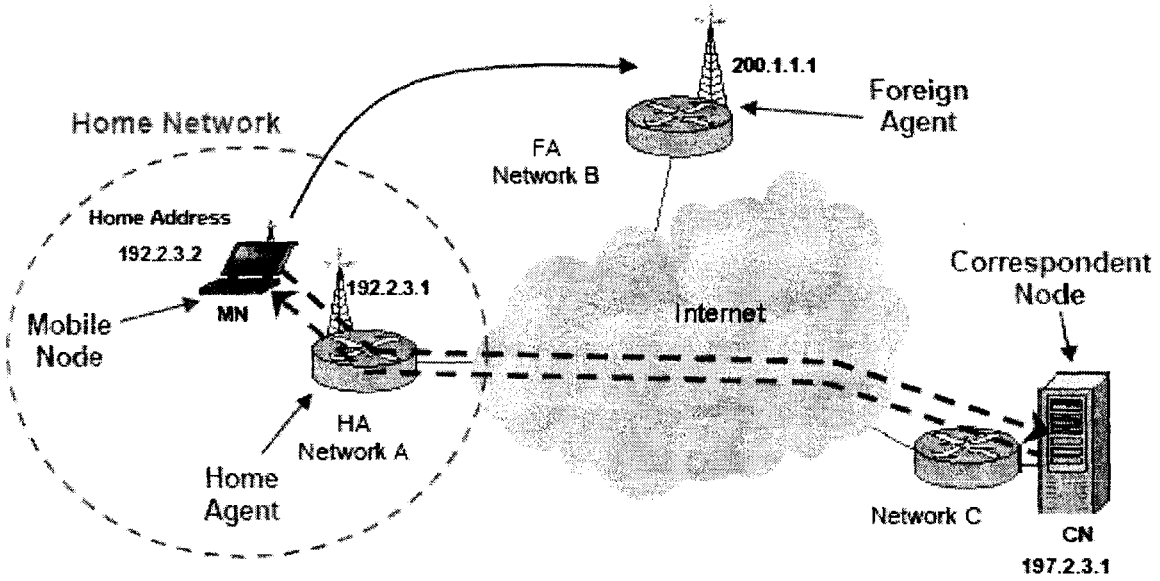


Fig. 3.6, IPv4 MN at HA [OPN]

The traffic sent from CN to MN is dropped because the MN had changed its point of attachment as illustrated in Fig. 3.7. The MN registers to the Foreign Agent (FA) of Network B and acquires a Care of Address (CoA). The FA performs registration with the HA on behalf of the MN.

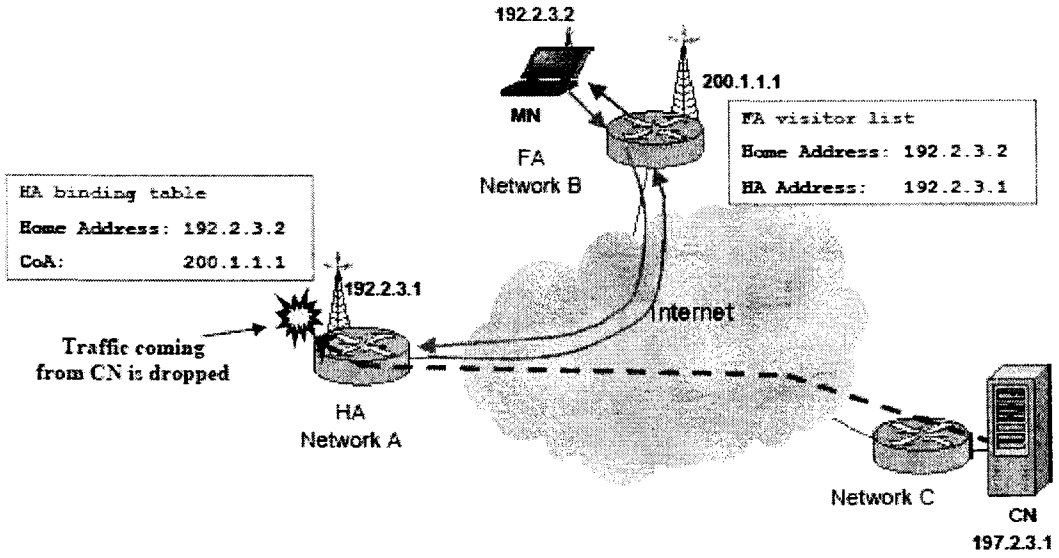


Fig. 3.7, IPv4 MN Moves to FA [OPN]

Now the HA tunnels the traffic from the CN to the FA to reach the MN at Network B. On the other hand MN sends its data directly to CN via the FA as it is shown in Fig. 3.8.

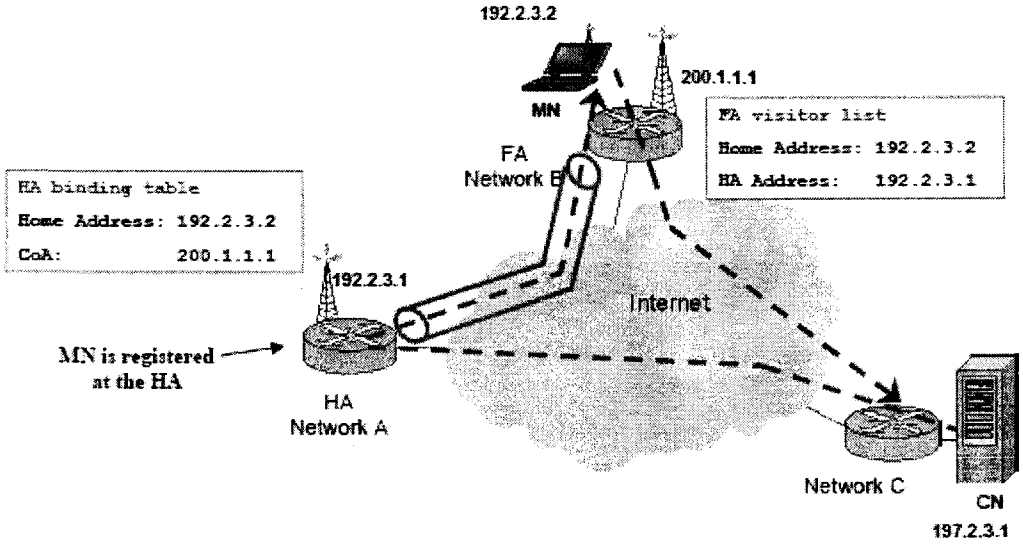


Fig. 3.8, IPv4 MN Establishes Tunnel at FA [OPN]

The RFC3344 protocol places no additional constraints on the assignment of IP addresses, i.e. a mobile node can be assigned an IP address by the organization that owns the machine. This protocol assumes that mobile nodes will generally not change their point of attachment to the Internet more frequently than once per second. It also assumes that IP unicast datagrams are routed based on the destination address in the datagram.

Mobile IPv4 (MIPv4) is intended to enable nodes to move from one IP subnet to another. It is just as suitable for mobility across homogeneous media as it is for mobility across heterogeneous media. Meaning that Mobile IP facilitates node movement from one Ethernet segment to another as well as it accommodates node movement from an Ethernet segment to a wireless LAN, as long as the mobile node's IP address remains the same after such a movement.

One can think of Mobile IP as solving the *macro mobility* management problem. It is less well suited for more *micro mobility* management applications, for example, handoff amongst wireless transceivers, each of which covers only a very small geographic area. As long as node movement does not occur between points of attachment on different IP subnets, link-layer mechanisms for mobility (i.e., link-layer handoff) may offer faster convergence and far less overhead than Mobile IP [RFC 02].

3.3.2. MIPv6 (RFC 3775, RFC4068, RFC4260)

While a mobile node is attached to some foreign link away from home, it is also addressable at one or more care-of addresses. A care-of address is an IP address associated with a mobile node that has the subnet prefix of a particular foreign link. The mobile node can acquire its care-of address through conventional IPv6 mechanisms, such as stateless or stateful auto-configuration. As long as the mobile node stays in this location, packets addressed to this care-of address will be routed to the mobile node. The mobile node may also accept packets from several care-of addresses, such as when it is moving but still reachable at the previous link.

Stateless address auto-configuration is based on the fact that nodes are allowed to learn all the necessary information about their links by using Neighbor Discovery. This allows the node to have an address that is globally unique when communicating with other foreign nodes in foreign networks. This is made useful by the RFC2462 that provides a method by which a node can use its 48 bit Ethernet address to generate an (Extended Unique Identifier) EUI-64bit interface identifier. For stateless address configuration, the care-of address is a combination of the foreign subnet prefix and an interface ID determined by the mobile node.

Stateful address configuration needs Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server in the network that allocates addresses to hosts. DHCPv6 is also being currently extended to allocate prefixes to routers [SOL 05].

The association between a mobile node's home address and care-of address is known as a *binding* for the mobile node. While away from home, a mobile node registers its primary care-of address with a router on its home link, requesting this router to function as the *Home Agent* for the mobile node. The mobile node performs this binding registration by sending a *Binding Update* message to the home agent. The home agent replies to the mobile node by returning a *Binding Acknowledgement* message [RFC 04].

The basic idea behind a Mobile IPv6 fast handover is to leverage information from the link-layer technology to either predict or rapidly respond to a handover event. This allows IP connectivity to be restored at the new point of attachment sooner than would otherwise be possible. By tunneling data between the old and new access routers, it is possible to provide IP connectivity in advance of actual Mobile IP registration with the home agent or correspondent node. This allows real-time services to be reestablished without waiting for such Mobile IP registration to complete. Because Mobile IP registration involves time-consuming Internet round-trips, the Mobile IPv6 fast handover can provide for a smaller interruption in real-time services than an ordinary Mobile IP handover.

The particular link-layer information available, as well as the timing of its availability (before, during, or after a handover has occurred), differs according to the particular link-layer technology in use [RFC 05b].

The Fig. 3.9-3.13 illustrate an example of MIPv6 Stateless hand-off.

In Fig. 3.9, the Mobile Node (MN) is located at its home network and it has established a communication with the Correspondent Node (CN). Now the MN is moving from Network A to Network B.

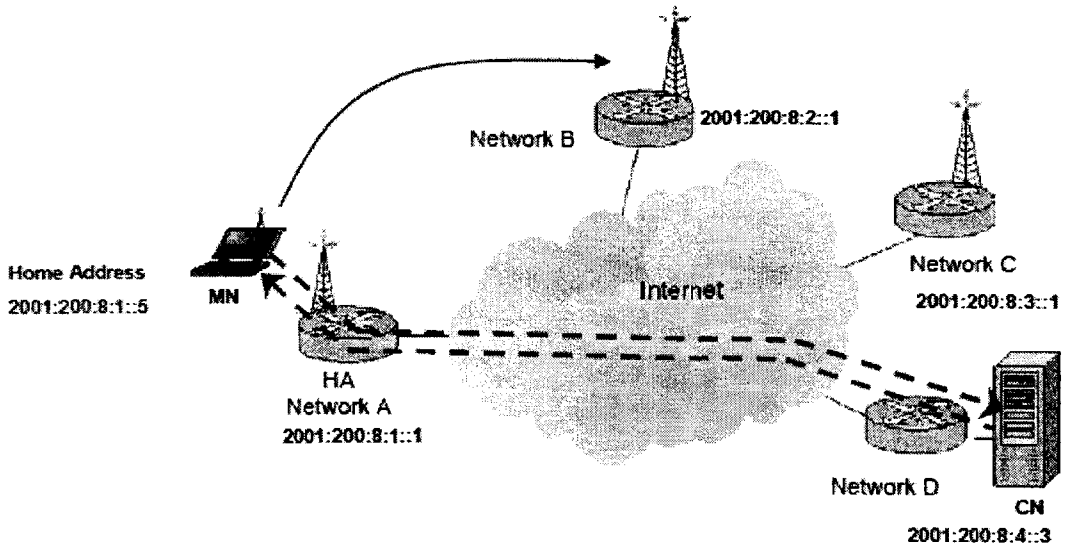


Fig.3.9, IPv6 MN at Home Network [OPN]

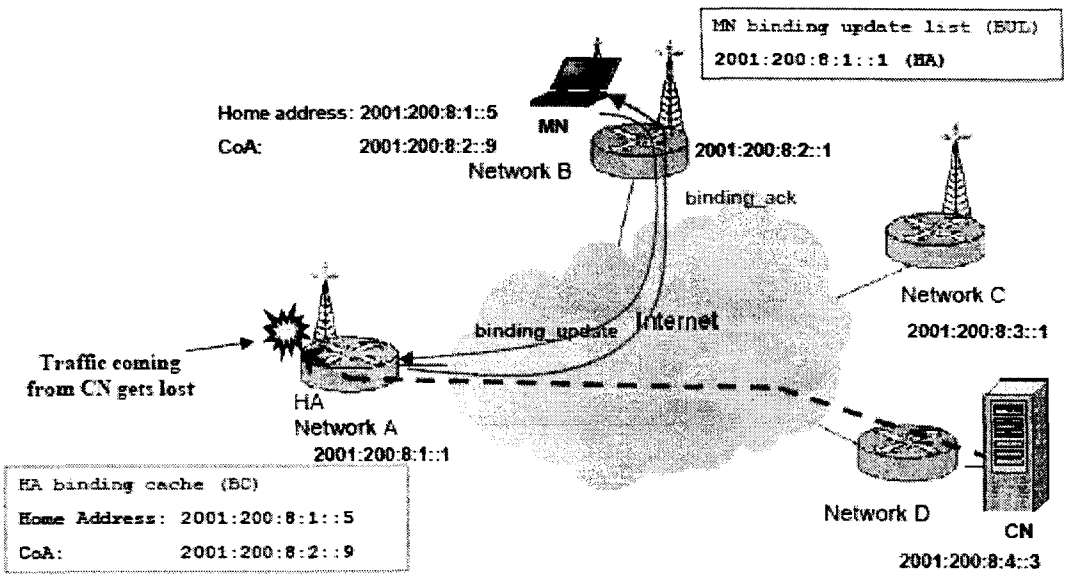


Fig.3.10, IPv6 MN Moves to Foreign Network [OPN]

The traffic from the CN cannot reach the MN because it had changed its point of attachment. MN performs Duplicate Address Detection (DAD) in network B, and sends its Care of Address (CoA) to its Home Agent (HA) in network A performing Binding Update (BU). The HA sends Binding Acknowledge (BA) to the MN and updates its list in the Binding Cache (BC) (Fig.3.10).

HA tunnels traffic to MN's current location. MN sends traffic to CN via reverse tunnel through HA. Also, MN performs routability test with the CN via tunnel for authentication. And finally, MN performs binding procedure with CN via tunnel same as with HA (Fig.3.11).

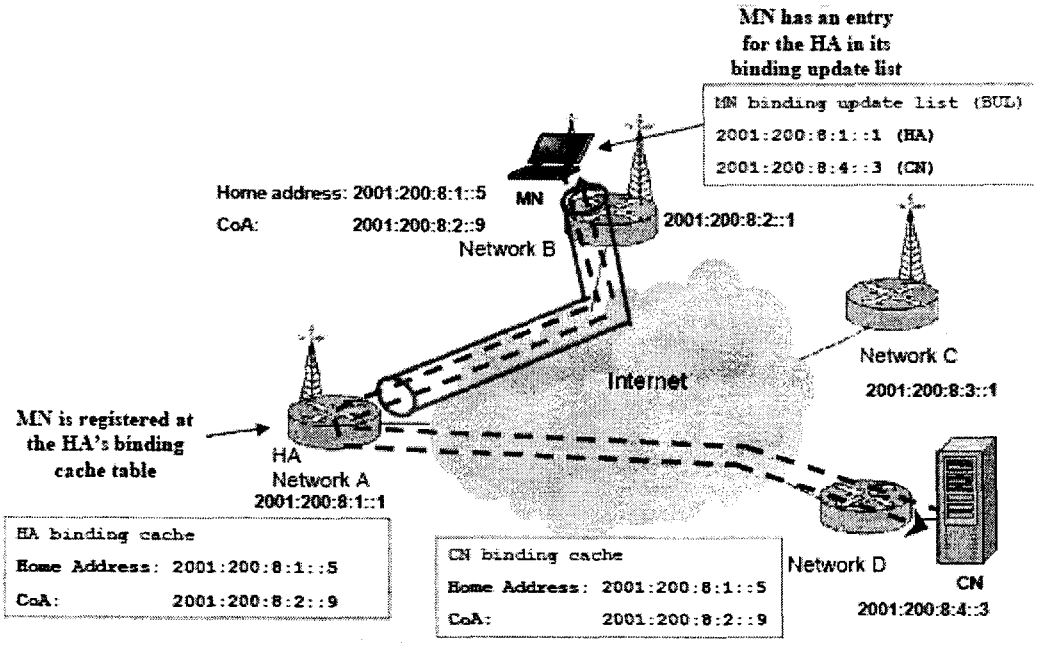


Fig.3.11, IPv6 MN Performs Tunnel with CN via HA [OPN]

Now MN and CN communicate directly. Destination option and routing IPv6 extension headers are used to perform route optimization (Fig. 3.12).

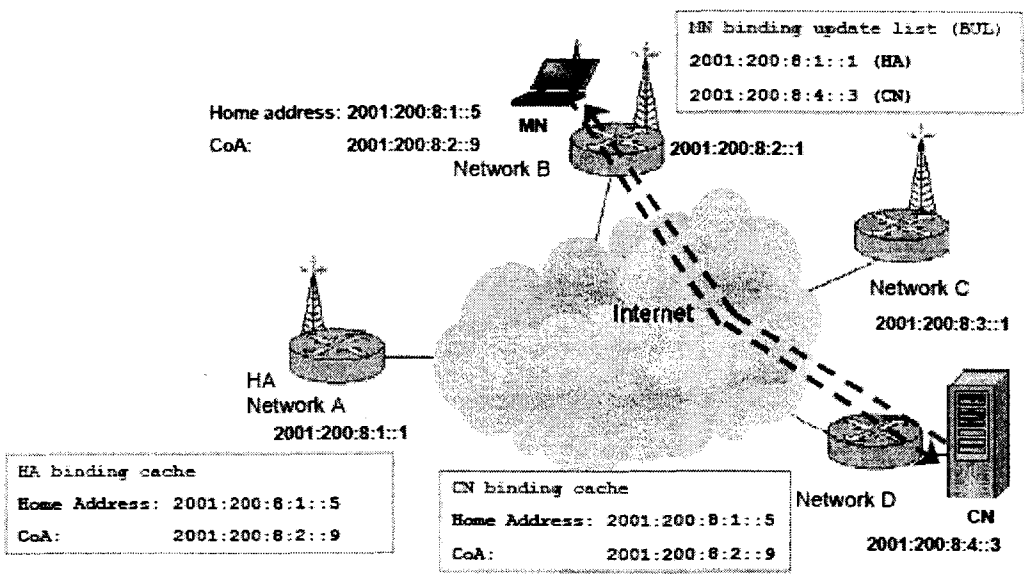


Fig. 3.12, IPv6 MN Performs Route Optimization with CN [OPN]

The same procedure is repeated again when MN moves from Network B to network C. Always keep in mind that HA of MN is network A (Fig. 3.13).

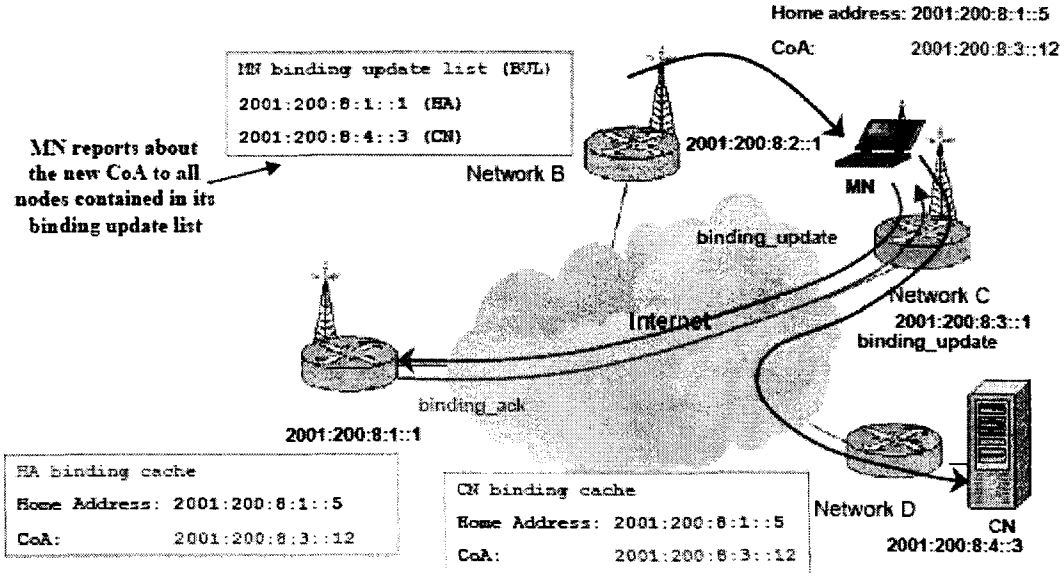


Fig. 3.13, IPv6 MN Moves to New Foreign Network [OPN]

3.4. SYSTEM ARCHITECTURE

The proposed model is based on a basic seven coverage cell layout as shown in Fig. 3.14.

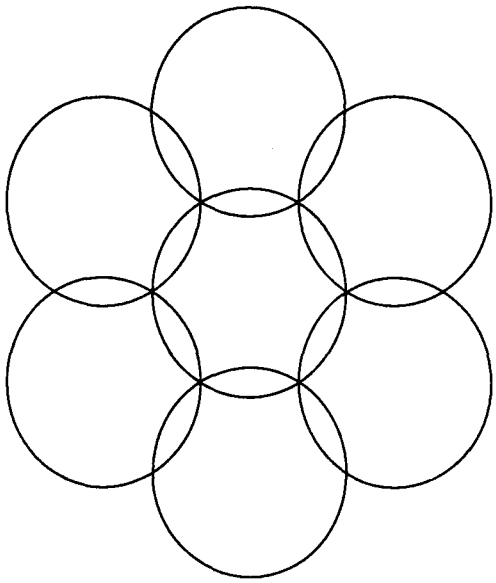


Fig. 3.14, Basic Seven Cell Layout

The coverage areas of these cells intersect to form the conventional hexagon (honey-cell) coverage known in Personal Mobile Communication Systems [RAP 02] (Fig. 3.15). This coverage model showed success as the best coverage layout for wireless communication systems. These hexagon shapes are as they appear in regular shapes in free space and for mathematical and analytical analysis. When deployed in real sites, these shapes deviate from there ideal forms. It is the duty of the Radio Network Engineering (RNE) engineers to make enough site surveys as well as best placement strategies to get the best positions for Access Points (AP) locations to approach the ideal case.

While the frontiers between a micro-cell and its neighbors are just a line as in Fig. 3.15, it appears to be a region as in Fig. 3.14. These overlapping regions are useful for hand-off (handover) mechanism, to take place. These overlaps are called *shadow areas.*

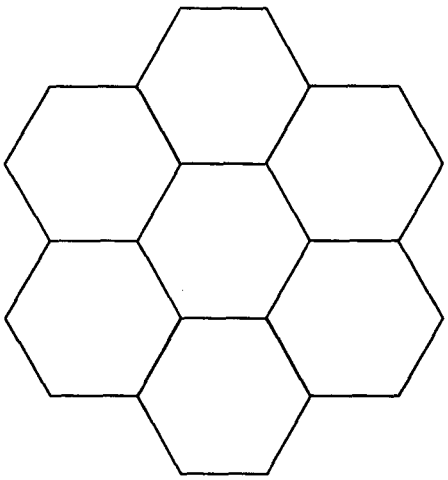


Fig. 3.15, Hexagon (Honey-Cell) Layout

Since these seven hexagons are the basic building block in the context of this research, a means to interconnect the AP of these micro-cells is needed. A Switched Star topology based on Ethernet 802.3 Gigabit links is proposed (Fig. 3.16). A Correspondent Node (CN) exists at the center of the system. The CN forms the intelligence of the system. Each Access Router (AR) that includes a wireless interface (or the Access Point) is linked to the main switch of the center of the system using Fiber links. At the end the CN is also connected to this center switch.

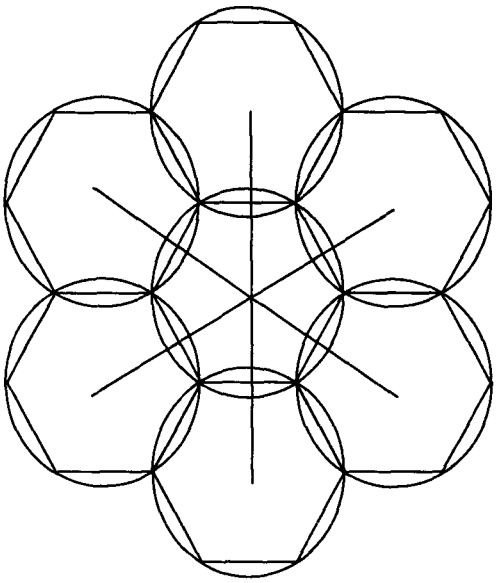


Fig. 3.16, System Star Backbone

This building block will be referred to as a *sector*. Any number of sectors can be repeated in two dimensions to cover as much area as needed.

3.5. MODEL VARIABLES

The proposed model of study is composed of seven symmetric hexagon-shape coverage layout. AP for each micro-cell is located at the center of this micro-cell. The AP is in fact composed of a wireless interface and an Access Router (AR). In the rest of this research AP and AR are used interchangeably (in fact what is studied is layer 3 handover). WiFi 802.11b protocol is used for wireless communication. Each AP transmit power is AP-P_t. For simplicity, free space analysis is studied. In free space, for a given AP-P_t, the coverage radius is R.

Access Points are interconnected in a Switched Star Ethernet topology with the AR of the center. At the center a Correspondent Node (CN) is located to establish communication with the Wireless Nodes (WN) in the system. The Correspondent Node is also referred to as the Central Node in the rest of the research (CN designate both).

Inter-AP distance is AP_D. In other words, coverage areas' centers are spaced by AP_D.

Wireless Nodes roaming within the system are tested at three speeds: V_L, V_M and V_H. V_L is simulating the pedestrian speed. V_H is simulating the maximum allowable speed for a vehicle moving on the periphery of the resort or in low density city centers. V_M is an average speed between the maximum and minimum ones explained earlier.

3.5.1. Communication load

For city centers, it is important to send messages based on collected information from all over the traffic map to guide drivers. The data being processed in a central node for example is sent either on demand or at periodic instances to the moving entities. In this

research, the architecture is tested for sending alert messages from the Correspondent Node (CN) to the Wireless Nodes (WN) within the coverage of 1 sector. This will be referred to as Infrastructure-to-Vehicle Communication (I2V). The messages are sent on-top of UDP. These messages are sent on a periodic basis. An Inter-Packet transmission Time (IPT) is defined [DAO 06d] to send packets from the CN to the WNs. Four IPTs were suggested and tested.

3.5.2. Communication Internet Protocol (IP)

The Two IP protocols (IPv4 and IPv6) are tested in this research along with their Mobile versions. The mature IPv4 and its MIPv4 are first introduced as Internet and Mobile Protocols respectively. They are tested for the proposed architecture. Optimized MIPv4 model is derived and simulated. This optimization tends to minimize (or cancel) packet loss at hand-off while keeping the standard MIPv4 (based on RFC).

The newly introduced, not yet widely deployed IPv6 and MIPv6 are then introduced in the research and tested. Although MIPv6 RFCs solved delay problems of MIPv4, optimized communication scheme had to be used to minimize to eliminate packet loss at handovers. Again, the philosophy of keeping the standards and the RFCs untouched is used, and the purpose of this research is to solve the problem by changing the communication parameters without modifying the standards.

For every simulation run, the number of dropped packets at hand-off is reported and compared with the expected analytical number of lost packets. The analytical number is derived from the equation introduced in [DAO 06d]. According to the honey-cell structure of the cell coverage, the car will cross the overlapped distance between the cells S_D in time T depending on the speed S of the car.

$$T = \left(\frac{S_D}{S} \right) \qquad 3.1$$

The total number of packets lost in the overlapping region (L) is given by:

$$L = \left(\frac{T}{IPT}\right) + 1 \qquad 3.2$$

The extra "1" added is to account for having a packet loss the time a MN signs in or out of an AP.

3.5.3. Network Parameter Boosting for IPv6

It is the MN duty to manage its connection when roaming between different AR in a MIPv6 network. To be able to do so, it relies on Router Advertisement (RA) messages sent from different ARs in the network. Also, it is important to adjust the Mobility Detection Factor (MDF) of the MN itself. The effect of changing these parameters on the overall network performance is then studied.

3.5.4. Burst Communication

Burst communication will be used to minimize information loss during transmission from the CN to the MN (I2V). In the context of this research, burst communication is defined as several identical packets sent in succession [DAO 07b, DAO 07c]. Several parameters are used to define a burst. These are namely t_{packet}, t_{burst}, t_{F2L} and the number of packets per burst.

Let t_{packet} be the time between two successive packets within the same burst. Also, let t_{F2L} be the time between the first and the last packet in the same burst. Finally, let t_{burst} be the time between the first packets of two successive bursts. t_{F2L} and t_{burst} must satisfy the following constraints:

- t_{F2L} must be greater than the longest time spent in the shadow area between two adjacent APs to guarantee that at least one packet per burst is sent when the MN is

outside the shadow area. This longest time corresponds to the lowest speed of an MN; it is also the longest time for the handover to take place. Note that, at V_L, the MN is already in a traffic jam in which case information sent from the CN has little importance. Consequently, let the slowest speed be V_M.

$$t_{F2L} > \left(\frac{S_D}{V_M}\right) \quad 3.3$$

- t_{burst} must be less than or equal the shortest time spent traveling from one AP in a Manhattan map to another one on the radial path , i.e., it is the minimum time a MN needs to update its traffic information to change routes if needed. The shortest time corresponds to the highest speed which is V_H.

$$t_{burst} \leq \left(\frac{AP_D}{V_H}\right) \quad 3.4$$

Based upon the previously calculated values for t_{F2L} and t_{burst}, a scenario with two packets per burst (optimum burst model for channel utilization) is introduced.

3.5.5. Fault-Tolerant Architecture

After analyzing the proposed model using MIPv4 and MIPv6, a fault-tolerant study is conducted. This study aims to solve the problem that may appear when an AP fails. This AP failure means a loss of coverage within a sector. Two main strategies to solve this problem can take place.

First strategy is the *hot standby*. In this strategy, a duplication of APs can take place. In this case, each AP has a *hot stand by* AP that is engaged once the main AP is out of service. This solution is not cost effective.

Second strategy is the *degraded performance*. In this strategy, the architecture itself resolves the problem by increasing the power of the six neighboring APs to recover the

Blind Area caused by the failure of the center AP. This solution is subject to federal power regulation constraints. Also, it needs to be optimized to know what is the optimal amount of power increase in the surrounding APs to minimize packet loss without facing major problems of interference (by increasing the shadow areas). It is worth noting that this power increase is not for long periods, it is only for the time needed to repair or replace the defected AP and then the system returns again to its normal operating conditions.

3.6. PERFORMANCE METRICS

In this study, the wireless network is developed to communicate information for Wireless Nodes (WN) while moving. This movement may drive the WN to roam from one Access Router (AR) to another one. During the hand-off mechanism explained earlier, data is lost.

3.6.1. Amount of Packet Loss

A measure of packet loss due to hand-off is the performance metric for the success or fail of the proposed model. It is the clever system design that guarantees minimal packet loss during hand-off. In other words, no protocol modification is suggested in this research. It is a design problem. This research studies different techniques to minimize the amount of packet loss during hand-off.

These techniques are:

- Defining the best wireless Access Point (AP) inter-distance placement;
- Defining Broadcast Rate (BR) or Inter-Packet transmission Time (IPT) for data communication;
- Using the best Mobile Internet Protocol;
- Using Burst Communication techniques.

3.6.2. Confidence Level Calculations

A statistical analysis is performed in order to obtain more accurate results regarding the total amount of burst loss. Let:

- X: random variable representing the number of complete burst losses during a trajectory;
- μ: Average of random variable X;
- σ^2: Variance of random variable X;
- X_i: Number of complete burst losses during i^{th} simulation;
- n: Number of simulations;
- x: Sample mean;
- s^2: Sample variance.

$$x = \frac{1}{n}\sum_{i=1}^{n} X_i \qquad 3.5$$

$$s^2 = \frac{1}{n-1}\sum_{i=1}^{n}(X_i - x)^2 \qquad 3.6$$

Let n simulations be performed with different seeds. Random seeds are generated to run multiple simulation scenarios. This is done by configuring the simulations' starting and ending seeds together with the step of seed change. Each simulation produces X_i. The average of the X_i's is x and their variance is s^2. x on its own can be considered as a random variable with its own distribution. The Central Limit Theorem indicates that, regardless of the original distribution of the random variable X, the distribution of x approaches the normal distribution. This approximation is better when n is large. Furthermore, the theorem states that the mean of x is μ (mean of X) and its variance is σ_x is equal to $\frac{\sigma^2}{n}$ (σ^2 is the variance of X) [OPN, TRI 02].

Since x is normally distributed with mean μ and variance $\frac{\sigma^2}{n}$, it is possible to calculate the probability that x is within a certain distance of μ. This probability is the confidence level. Let:

$$z = \frac{x - \mu}{\sigma_x} \tag{3.7}$$

z will be a standardized normal random variable with mean=0 and variance =1. Let:

$$P(-z_\alpha < z < z_\alpha) = \alpha \tag{3.8}$$

$$P\left[\frac{|x - \mu|}{\sigma_x} < z_\alpha\right] = \alpha \tag{3.9}$$

Finally, it is important to note that $\sigma_x = \frac{\sigma}{\sqrt{n}}$ is difficult to obtain since σ is unknown. However, if n>30, the sample standard deviation s can be used instead of σ. If the number of simulations were less than 30, the Student T distribution would have to be used instead of the normal distribution [TRI 02].

3.6.3. Fault-Tolerant Architecture Analysis Technique

In this section, a technique is described that will minimize the impact of burst losses in the case of AP failure. The honey cell architecture consists of a center AP and six adjacent APs. If the center AP fails, the transmit power of the 6 adjacent APs is increased in order to minimize the blind area created by the failure of the center AP. Because of the blind area, the MN will not be aware of the system parameters (traffic status, location of traffic jams,...) during the time it traverses this area. This may cause degradation in system performance. The disadvantage of increasing the transmit power is that it will increase the AP coverage area. Consequently, the shadow area between two adjacent APs will also increase. It has been shown in [DAO 06d] that there is a high probability of packet loss in the shadow area during handoff.

A metric is therefore required to quantify system performance in order to obtain the optimum transmit power after the failure of the center AP. This metric has to take into consideration not only the number of packets lost during the transmission from the infrastructure to the vehicle, but, the manner in which this information is lost.

A primary figure of this parameter φ can be [DAO 08]:

$$\varphi = \alpha f(\text{burst loss}) + \beta g(\text{severity of burst loss}) \qquad 3.10$$

where:

- α and β are constant coefficient;
- f(burst loss) indicates the amount of burst loss in the system;
- g(severity of burst loss) reflects the severity of these burst losses on the system.

The following simple example clarifies the difference between the functions f and g. Assume that 3 bursts are lost during a certain MN trajectory, one at the beginning, one at the middle and the third one at the end of the trajectory. After any of the first two burst losses, the MN will quickly receive information from the CN to rectify the trajectory if needed. However, if the three bursts are lost consecutively, the MN will not receive any information from the CN for a relatively long period. When the first burst is received after the long period of silence, the MN may already be in the middle of the traffic jam mentioned in the three lost bursts.

Let φ be the total number of bursts lost added to the weighted sum of the number of consecutive burst losses as follows:

$$\varphi = \sum \text{Number of Burst Losses} + \sum_i \left((n_i + 1)\sum \text{Number of consecutive } n_i \text{ Burst Loss}\right) \qquad 3.11$$

Where: n_i is the number of Burst Loss

i is the sum counter

It can be seen that $\alpha=\beta=1$, f is the number of burst losses and g is the weighted sum of the number of consecutive burst losses.

In this case, any consecutive burst loss is calculated twice: first in f and second in g. To take into account the effect of MN speed, φ is calculated at V_M and at V_H. The final metric will be:

$$\varphi = \varphi|_{V_H} + \left(\frac{V_M}{V_H}\right)\varphi|_{V_M} \quad 3.12$$

Again, the severity of burst loss at high and low speeds is taken into consideration [DAO 08].

More estimates for φ were also tested. The most important ones are the exponential and the running sum.

Let the exponential version of φ at a given speed be:

$$\varphi_v = \sum \text{Number of Burst Losses} + \sum_i \left(\left(2^{n_i}\right)\sum \text{Number of consecutive } n_i \text{ Burst Loss}\right) \quad 3.13$$

Let the running sum version of φ at a given speed be:

$$\varphi_v = \sum \text{Number of Burst Losses} + n\sum \text{Number of } n \text{ Bust Loss} \quad 3.14$$

3.7. CONCLUSION

WiFi as a wireless communication standard is chosen to be the implementation protocol of the proposed model. Working with a standard always has it benefits. The Mobility in WiFi can be implemented using either MIPv4 or MIPv6. Both mobile versions' implementation support handover (handoff). A general model of 7 hexagon shaped micro-cells is introduced with AR in the middle of each. These AR are interconnected in Star topology. Gigabit Ethernet optical links forms the backbone of the wireless model. The center cell includes the CN which forms the intelligence of the system. Fault-

Tolerant models for faulty AP recovery are also introduced: hot standby and degraded performance strategies. It is important to guarantee mobility with minimum packet loss during handoff. This is why the performance metric of the wireless networks within the context of this research is the amount of packet loss during handover. Analysis techniques for fault-tolerant wireless architecture are also introduced.

Chapter 4 presents simulation results of the models introduced in chapters 2 and 3. The simulation platform is first introduced. Simulations scenario as well as model parameters are then presented.

CONCLUSION

In this research a wireless model of communication is introduced and tested by OPNET Simulations based on WiFi technology (IEEE 802.11b Std). This model is useful for light urban traffic control and tourist resort implementation. WiFi is chosen as communication protocol after conducting a survey for different kinds of wireless communication protocols. Its implementation simplicity as well its low price and availability are the motive behind choosing this protocol.

Several communication schemes exist to perform a wireless communication model between wireless nodes (WN). Namely, there exists the ad-hoc as well as the infrastructure and hybrid topologies. In this research, the infrastructure model was chosen and simulated using OPNET. This forms what is called an Infrastructure-to-Vehicle (I2V) communication model.

A seven hexagon shaped micro-cell implementation is used to form what is called *sector* within the infrastructure. This sector is implemented using 7 Access Routers (AR) interconnected in a star topology using Switched Gigabit Ethernet backbone. Each AR is 2Km far from the nearest AR on a radial path. Each AR has a wireless (WiFi) interface as well as a wired (Ethernet) interface. A sector radius is 3.15Km; this is why 1 sector implementation is targeting tourist resorts in first place as well as light urban traffic model with low profile city center buildings (approximately 5 floors buildings with an average floor height of 3m).

Wireless Nodes (WN) with WiFi interface are roaming within a sector where the name Mobile Nodes (MN). These nodes are communicating with the sector intelligence located in the center node of the sector called Central or Correspondent Node (CN). At the correspondent node, a stigmergic algorithm is running to calculate, based on collected

data from the moving entities, coefficients at intersections. These coefficients are useful for the on-board intelligence of the vehicle to direct the driver in an optimum path to follow from a source node to a destination node.

The metric of success of the proposed wireless communication model is the amount of data drop during I2V communication. The data drop is the result of an MN roaming. During an MN roaming in the sector, it changes continuously its point of attachment with the Infrastructure (it changes the AR). Based on the MIPv4 protocol, as well as MIPv6, data must be dropped. It is the designer duty to build a communication scheme without changing the roaming standards (MIPv4 and MIPv6) as well as the wireless communication standards (IEEE 802.11 Std) that minimizes the data drop at handoff.

MIPv4 as well as MIPv6 are tested as mobile communication protocols. It is found that MIPv6 has better performance over MIPv4 as expected. But, still the amount of data drop during handover (or handoff) is not satisfactory. A burst communication model is introduced to enhance the communication model. Within the context of this research *Burst Communication* means sending the same information multiple times within a given period of time. It was shown that Burst Communication with a clever selection of *inter-packet* as well as *inter-burst* time and *number of packets* per burst achieves acceptable results. Namely, 3 packet burst (3PB) with inter-packet time of 36sec and inter-burst time of 120sec shows acceptable performance.

Fault-Tolerance on the Access Points (AP) level was also investigated. This study is important to find a repair strategy upon the failure of one of the infrastructure's wireless interfaces. Two strategies are mainly discussed: *hot standby* and *degraded performance* strategies. For hot standby strategy, a faulty AP is replaced by another one within a short period. For degraded performance, simulation studies helped to find the optimal increase in transmit power of neighboring APs to cover the disconnected region. Minimizing the amount of data loss due to the increase in the shadow area between adjacent APs and due to the uncovered area is the target of this study. The optimal operating transmit power is derived based on statistical analysis of the OPNET simulation results.

Boosting some parameters of the WN as well as the AR are also tested. Namely the Mobility Detection Factor (MDF) for the WN and the Router Advertisement Interval (RAI) of the AR are investigated. A relation between these two parameters is derived to help choosing the best values to enhance the system performance. These two parameters are accessible through the wireless driver of the nodes (WN or AR).

Some hardware tests are performed on a very small scale at the American University in Cairo premises and showed success. Also, it showed that the proposed model is not far from realistic.

Not only is the wireless aspect of the system investigated within the context of this research, but, the wired system of the on-board communication of the vehicle was also studied. The data after being communicated from the Infrastructure, is processed on board of the WNs which are the moving vehicles.

A new concept is introduced for on-board networks. It is based on previous studies in the industrial information systems. A single network to interconnect all sensors, actuators and controller nodes on-top-of Ethernet is introduced and tested using OPNET simulations. Based on a model of FORD CAN bus cars, the study was conducted to test the end-to-end packet delays of the system. The performance metric was to satisfy a packet end-to-end delay that is less than the minimum sampling period of 5ms.

Several models of the Ethernet Car were tested in the OPNET environment. First, a pure control network was tested. This network has only sensors, actuators and a controller connected using Switched Star Gigabit Ethernet. End-to-end delays are met based on the model of 90 nodes of FORD. Second, an overhead of video streaming simulating a video terminal on-board of the vehicle is tested originating from the same node of the control. The end-to-end delays were also met. Third, a TMR model of the sensor nodes is tested successfully. Fourth, a TMR control model with entertainment communication loads is tested and showed success.

Switched Star Fast Ethernet is also tested for Ethernet Car implementation. Results for both systems (using Fast and Gigabit Ethernet) were very close. An interpretation of this

finding is made based on the fact that control loads are very low compared with the added entertainment loads (video and voice streams).

Future work to this dissertation may cover several fields, mainly Vehicle Safety Communications (VSC) and transportation systems on-board control networks. Among the ongoing studies, Vehicle to Vehicle (V2V) [MAT 08] communication between moving cars for safety collective driving is part of VSC. Other wireless communication protocols can be tested for V2I/I2V communication. Co-existence of different wireless communication protocols within one communication system and problems due to many factors like interference and system migration must also be taken into consideration.

Dedicated Short-Range Communications (DSRC) use in Vehicular Ad Hoc Network (VANET) is another important subject of study, specially that the FCC in the USA has allocated 75MHz of spectrum at 5.9GHz [CHE 08]. WiMAX issues related to mobility and coverage as well as vertical handoff are of great importance [ALI 08, MAT 08].

Also, general Ethernet implementation in transportation systems is of great interest. Train on-board control and entertainment networks are currently under study [AZI 08]. EMI issues are also very important during implementation of such wired systems [WIL 05]. More research has to focus on faults due to EMI as well as other sources of errors when using Ethernet or other wired networks in noisy environment.

Although the proposed wired system did not treat the case of noisy environment, it is of great importance. With the evolution of on-board safety and high technology driving assistance using By-Wire and other technologies, more electronics are introduced in the decision making process. Furthermore, electronic circuits' failure may have a negative impact on the passengers' safety. This issue may drive the research in the direction of redundant methods of safety as well as the study of error immune systems.

Other fault-tolerant aspects of the wireless as well as the wired systems are of prime interest for today's and tomorrow's market. Research in these areas is very beneficial to give a complete understanding of system behavior.

REFERENCES

[ALI 08] N.A. Ali, A.M. Taha, H.S. Hassanein and H.T. Mouftah, "IEEE 802.16 Mesh Schedulers: Issues and Design Challenges," IEEE Network, Vol. 22, No. 1, JAN 2008, pp.: 58-65

[AME 04] H.H. Amer and R.M. Daoud, "Reliability and Availability of Fault-Tolerant Networked Controlled Systems," *1st International Computer Engineering Conference, ICENCO*, Cairo-Egypt, December 2004

[AME 05] H.H. Amer, M.S. Moustafa, and R.M. Daoud, "Optimum Machine Performance in Fault-Tolerant Networked Control Systems," *The IEEE International Conference on "Computer as a Tool", IEEE EUROCON*, Belgrade-Serbia and Montenegro, November 2005

[AME 06a] H.H. Amer, M.S. Moustafa and R.M. Daoud, "Availability of Pyramid Industrial Networks," *IEEE Canadian Conference on Electrical and Computer Engineering, IEEE CCECE*, Ottawa-Canada, May 2006

[AME 06b] H.H. Amer and R.M. Daoud, "Parameter Determination for the Markov Modeling of Two-Machine Production Lines," *4th International IEEE Conference on Industrial Informatics, IEEE INDIN*, Singapore, August 2006

[AME 08] H.H. Amer and R.M. Daoud, "*Increasing Network Reliability by Using Fault-Tolerant Sensors,*" To appear in the International Journal of Factory Automation, Robotics and Soft Computing, 2008

[AME 87] H.H. Amer and E.J. McCluskey, "Calculation of Coverage Parameter," *IEEE Transactions on Reliability*, June 1987, pp. 194-198

[ARN 73] T.F. Arnold, "The concept of coverage and its effect on the reliability model of a repairable system," *IEEE Trans. On Computers,* vol. C-22, No. 3, March 1973

[AZI 08] M. Aziz, B. Raouf, N. Riad, R.M. Daoud, and H.M. Elsayed, "The Use of Ethernet for Single On-board Train Network," *IEEE International Conference on Networking, Sensing and Control, ICNSC*, Sanya-China, April 2008

[BAT 06] T. ElBatt, S. Goel, G. Holland, H. Krishnan and J. Parikh "Cooperative Collision Warning Using Dedicated Short Range Wireless Communications," HRL Laboratories, LLC, ACM VANET, Los Angeles, California, USA, 2006

[BER 06] T. Berger, Y. Sallez, C. Tahon "Bio-inspired approach for autonomous routing in FMS," In Manufacturing the future, Ed. By Vedran KORDIC, Advanced Robotics Systems International, July 2006, ISBN N° 3-86611-198-3

[BIL 83] R. Billinton and R. Allan, *Reliability Evaluation of Engineering Systems: Concepts and Techniques*, Pitman, 1983

[BIS 06] S. Biswas, R. Tatchikou and F. Dion, "*Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety,*" IEEE Communications Magazine, Jan. 2006

[BLA 01] M. Blanke, M. Staroswiecki, and N. Wu, "Concepts and Methods in Fault-Tolerant Control," *Proceedings of the American Control Conference*, Arlington, VA, June 2001, pp. 2608-2620

[BLU 04] J.J. Blum, A. Eskandarian and L.J. Hoffman, "*Challenges of Intervehicle Ad Hoc Networks,*" IEEE Transactions on Intelligent Transportation Systems, Vol. 5, No. 4, Dec. 2004

[BRA 06] B. Brahimi, C. Aubrun, E. Rondeau, "Modelling and Simulation of Scheduling Policies Implemented in Ethernet Switch by Using Coloured Petri Nets," Proceedings of the 11th IEEE International Conference on Emerging Technologies and Factory Automation, Prague, Czech Republic Sept. 2006

[BRA 07] B. Brahimi, "Proposition d'une approche intégrée basée sur les réseaux de Petri de Haut Niveau pour simuler et évaluer les systèmes contrôlés en réseau," *PhD Thesis*, Université Henri Poincaré, Nancy I, Dec. 2007.

[BRE 01] E.A. Bretz, "*By-Wire Cars Turn the Corner,*" IEEE Spectrum, April 2001

[BRI 06] R. Brignolo, "Infrastructure/Vehicle Communication," Second International Symposium Safe & Reliable Tunnels. Innovative European Achievements, Lausanne 2006

[BRU 05] R. Bruno, M. Conti and E. Gregori, "*Mesh Networks: Commodity Multihop Ad Hoc Networks,*" IEEE Communications Magazine, March 2005

[CAL] Website of CALM: www.fischer-tech.de

[CHA 05] B. Chakraborty, T. Maeda and G. Chakraborty, "Multiobjective Route Selection for Car Navigation System using Genetic Algorithm," *IEEE Mid-Summer Workshop on Soft Computing in Industrial Applications, IEEE SMCia/05*, Espoo-Finland, June 2005

[CHE 05] W. Chen and S. Cai, "*Ad Hoc Peer-to-Peer Network Architecture for Vehicle Safety Communications,*" IEEE Communications Magazine, April 2005

[CHE 08] L. Cheng, B.E. Henty, R. Cooper and D. Stancil, "A Measurement Study of Time-Scaled 802.11a Waveforms over the Mobile-to-Mobile Vehicular Channel at 5.9GHz," IEEE Communication Magazine, Vol. 46, No. 5, May 2008, pp.: 84-91

[CRO 06] M. Crocker, J. Baranski, and G.Y. Lazarou, "*Fault-Tolerant Reconfigurable Ethernet-Based IP Network Proxy,*" International Journal of Computers and Applications, Issue 3, 2006

[CYB] Cyber Cars: www.cybercar.org

[DAO 03] R.M. Daoud, H.M. Elsayed, H. H. Amer, and S.Z. Eid, "Performance of Fast and Gigabit Ethernet in Networked Control Systems," *Proceedings of the IEEE International Mid-West Symposium on Circuits and Systems, MWSCAS*, Cairo, Egypt, December 2003

[DAO 04a] R.M. Daoud, *Performance of Gigabit Ethernet in Networked Control Systems*, MSc Thesis, Electronics and Communications Department, Faculty of Engineering, Cairo University, 2004

[DAO 04b] R.M. Daoud, H.M. Elsayed, and H.H. Amer, "Gigabit Ethernet for Redundant Networked Control Systems," in *Proceedings of the IEEE International Conference on Industrial Technology, ICIT*, Hammamet, Tunis, December 2004.

[DAO 05a] R.M. Daoud, H.H. Amer, and H.M. Elsayed, "Fault-Tolerant Networked Control Systems under Varying Load," *IEEE Mid-Summer Workshop on Soft Computing in Industrial Applications, IEEE SMCia/05*, Espoo-Finland, June 2005

[DAO 05b] R.M. Daoud, H.H. Amer, and H.M. Elsayed, "Fault-Tolerant Two-Level Pyramid Networked Control Systems," *10th IEEE International Conference on Emerging Technologies and Factory Automation, IEEE ETFA*, Catania-Italy, September 2005

[DAO 06a] R.M. Daoud and H.H. Amer, "Optimum Supervisor Computational Power for Small Scale In-Line Production Networked Control Machines," *IEEE Canadian Conference on Electrical and Computer Engineering, IEEE CCECE*, Ottawa-Canada, May 2006

[DAO 06b] R.M. Daoud, H.H. Amer, H.M. Elsayed and Y. Sallez, "Ethernet Based Car Control Network," *IEEE Canadian Conference on Electrical and Computer Engineering, IEEE CCECE*, Ottawa-Canada, May 2006

[DAO 06c] R.M. Daoud, H.H. Amer, H.M. Elsayed and Y. Sallez, "Fault-Tolerant On-Board Ethernet-Based Vehicle Networks," *32nd Annual Conference of the IEEE Industrial Electronics Society, IEEE IECON*, Paris-France, November 2006

[DAO 06d] R.M. Daoud, M.A. El-Dakroury, H.M. Elsayed, H.H. Amer, M. El-Soudani and Y. Sallez, "Wireless Vehicle Communication for Traffic Control in Urban Areas," *32nd Annual Conference of the IEEE Industrial Electronics Society, IEEE IECON*, Paris-France, November 2006

[DAO 06e] R.M. Daoud and H.H. Amer, "*Heavy-Traffic Model for Pyramid Networked Control Systems,*" International Journal of Factory Automation, Robotics and Soft Computing, June 2006

[DAO 07a] R.M. Daoud, M.A. El-Dakroury, H.H. Amer, H.M. Elsayed and M. El-Soudani, "WiFi Architecture for Traffic Control using MIPv6," *15th IEEE Mediterranean Conference on Control and Automation, IEEE MED*, Athens-Greece, June 2007

[DAO 07b] R.M. Daoud and H.H. Amer, "Analysis of Pyramid In-Line Production at Higher-than-Nominal Speeds," *15th IEEE Mediterranean Conference on Control and Automation, IEEE MED*, Athens-Greece, June 2007

[DAO 07c] R.M. Daoud, M.A. El-Dakroury, H.M. Elsayed, H.H. Amer, M. El-Soudani and Y. Sallez, "Burst Communication for Traffic Control in Light Urban Areas," *International Workshop on Logistics and Transportation 2007, IEEE LT*, Sousse-Tunis, November 2007

[DAO 07d] R.M. Daoud and H.H. Amer, "*Ethernet for Heavy Traffic Networked Control Systems*," International Journal of Factory Automation, Robotics and Soft Computing, January 2007

[DAO 07e] R.M. Daoud and H.H. Amer, "*Fast Ethernet Implementation of Cost Effective Vehicle On-Board Networks,*" (Refereed/Invited Contribution), Journal of Factory Automation, Robotics and Soft Computing, June 2007

[DAO 08] R.M. Daoud and H.H. Amer, "Fault-Tolerant Access Points in a Mobile IPv6 WiFi Light Urban Traffic Communication Model," *IEEE 21st Canadian Conference on Electrical and Computer Engineering, CCECE*, Niagara Falls-Ontario Canada, May 2008

[DEC 05] J.-D. Decotignie, "*Ethernet-Based Real-Time and Industrial Communications,*" Proceedings of the IEEE, vol. 93, No. 6, June 2005

[EKE 99] J. Eker and A. Cervin, "A Matlab Toolbox for Real-Time and Control Systems Co-Design," *Department of Automatic Control, Lund Institute of Technology, 6th International Conference on Real-Time Computing Systems and Applications*, Hong Kong, P.R. China, Dec. 1999.

[ELC] "Summary of some of the key standards regulating the use and design of WLAN products," Available: http://www.elcard.fi/standards.htm

[ELP] "Performance of Different Frequency Bands," ELPRO Technologies, Technical Article, Available: http://www.elprotech.com/UserFiles/File/PDFs/white_paper_-_frequencies_1.3.pdf

[ERC] Official website of ERCIM: www.ercim.org/

[FAR 05] P.B. Farradyne, "Vehicle Infrastructure Integration (VII) Architecture and Functional Requirements," ITS Joint Program Office, US Department of Transportation, 2005

[FCC] Official Site for FCC regulations: www.fcc.gov

[FEL 05] M. Felser, "*Real-Time Ethernet – Industry Prospective,*" Proceedings of the IEEE, vol. 93, No. 6, June 2005.

[FRE 06] G. Fremont, "Systemes Coopératifs pour la Sécurité Routière Le Projet européen SAFESPOT," Saint-Brieuc – Côtes d'Armor 3ème Congrès ITS, 2006

[FRO 06] A. Froetscher, M. Boehm, "coopers – Co-operative Systems for Intelligent Road Safety," ITS World Conference, London, 2006

[FUJ] Official Site for Fujitsu: www.fujitsu.com

[GAR] "GPS Guide for Beginners," GARMIN Official Website: www.garmin.com

[GEO 05] J.-P. Georges, "Systèmes contrôles en réseau: Evaluation de performances d'architectures Ethernet commutées," *PhD thesis*, Centre de Recherche en Automatique de Nancy CRAN, Nov. 2005

[GEO 06] J.-P. Georges, N. Vatanski, E. Rondeau and S.-L. Jämsä Jounela, "Use of Upper Bound Delay Estimate in Stability Analysis and Robust Control Compensation in Networked Control Systems," 12th IFAC Symposium on Information Control Problems in Manufacturing, INCOM 2006, St-Etienne, France, Mai 2006

[GRI 04] J. Grieu, "Analyse et évaluation de techniques de commutation Ethernet pour l'interconnexion des systèmes avioniques," PhD Thesis, Institut National Polytechnique de Toulouse, Ecole doctorale informatique et telecommunications, Sep. 2004

[HEN 07] K. Henain, M. Milad, R. Morgan, S. Ramzy, R.M. Daoud and H.H. Amer, "Optimization of 802.11b/g Networks for High Mobility and Dynamic Data Applications," *9th IEEE International Conference on Telecommunications, IEEE ConTel*, Zaghreb-Coratia, June 2007

[HIR 99] H. Hiraishi, H. Ohwada, F. Mizoguchi, "Intercommunicating CarNavigation System with Dynamic Route Finding," *Proceedings of the Intelligent Transportation Systems,* Tokyo-Japan, 1999

[HOL 06] W. Holfelder, "Wireless Communication The next logical step in Vehicle Safety," IEEE Communications Society Joint Meeting, Oakland-East Bay and Santa Clara Valley Chapter, May 2006

[ITS] "Towards Smart Mobility Society," SMARTWAY Project, ITS official website: http://www.its.go.jp/ITS/topindex/topindex_smartway.html

[JAS 04a] J. Jasperneite and E. Elsayed, "Investigations on a Distributed Time-triggered Ethernet Realtime Protocol used by PROFINET," *3rd International Workshop on Real-Time Networks (RTN 2004)*, Catania, Sicily, Italy , Jun 2004

[JAS 04b] J. Jasperneite, K. Shehab and K. Weber, "Enhancements to the time synchronization standard IEEE-1588 for a system of cascaded bridges," Proceedings of the IEEE International Workshop on Factory Communication Systems, WFCS.2004, Sept. 2004, pp.: 239- 244.

[JOH 89] B.W. Johnson, "*Design and Analysis of Fault-Tolerant Digital Systems*", Addison-Wesley, 1989.

[KAT 02] S. Kato, S. Tsugawa, K. Tokuda, T. Matsui, and H. Fujii, "*Vehicle Control Algorithms for Cooperative Driving With Automated Vehicles and Intervehicle Communications,*" IEEE Transactions on Intelligent Transportation Systems, Vol. 3, No. 3, Sep. 2002

[KUM01] P.R. Kumar, "New Technological Vistas for Systems and Control: The Example of Wireless Networks," IEEE Control Systems Magazine, vol. 21, no. 1, pp. 24-37, 2001.

[LEA 04] J. Leary, P. Roshan, "*Wireless LAN Fundamentals: Mobility,*" CISCO Press, 2004. Available: www.ciscopress.com/articles/article.asp?p=102282&rl=1

[LEE 01] S.H. Lee and K.H. Cho, "Congestion Control of High-Speed Gigabit-Ethernet Networks for Industrial Applications," *Proceedings of IEEE International Symposium on Industrial Electronics*, vol. 1, pp. 260-265, 12-16 June 2001.

[LIA 01a] F.L. Lian, J.R. Moyne, and D.M. Tilbury, "*Performance Evaluation of Control Networks: Ethernet, ControlNet, and DeviceNet,*" IEEE Control Systems Magazine, Vol. 21, No. 1, pp.66-83, Feb. 2001

[LIA 01b] Lian, F. L., Moyne, J. R., and Tilbury, D. M., "*Networked Control Systems Toolkit: A Simulation Package for Analysis and Design of Control Systems with Network Communication,*" Tech. Rep., UM-ME-01-04, July 2001.

Available: http://www.eecs.umich.edu/~impact

[LKS] Official Site of Linksys: www.linksys.com

[LOR 03] S. Lorkowski, P. Mieth and R.-P. Schäfer, "*New ITS applications for metropolitan areas based on Floating Car Data,*" German Aerospace Center, 2003

[LOU] Musee du Louvre, Available: www.louvre.fr

[LOU 01] B. Lounsbury and J. Westerman, "Ethernet: Surviving the Manufacturing and Industrial Environment," White Paper, May 2001.
Available: http://www.ab.com/networks/enetpaper.html

[MAR 06a] G. Marsal, "Evaluation of time performances of Ethernet-based Automation Systems by simulation of High-level Petri Nets," *PhD Thesis,* Ecole Normale Superieure De Cachan, Dec. 2006

[MAR 06b] G. Marsal, B. Denis, J.-M. Faur and G. Frey, "Evaluation of Response Time in Ethernet-based Automation Systems," Proceedings of the 11th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA'06, Prague (Czech Republic), pp. 380-387, Sep. 2006

[MAT 08] D.W. Matolak, "*Channel Modeling for Vehicle-to-Vehicle Communications,*" IEEE Communications Magazine, Vol. 46, No. 5, pp.:76-83, May 2008

[MIC 96] L.B. Michael and M. Nakagawa, "Multi-Hop for Inter-Vehicle Communication over Multiple Lanes," *Proceedings of the Intelligent Vehicles Symposium, Tokyo-Japan, 1996*

[MOK 06] E. Mok, G. Retscher and L. Xia,, "Investigation of Seamless Indoor and Outdoor Positioning Integrating WiFi and GNSS," *Proceedings, XXIII International FIG Congress*, Munich, Oct. 2006

[MOL 07] D. Molta, "802.11r Holds Promise Of Secure Wi-Fi Mobility," Apr 16, 2007 Available: http://i.cmpnet.com/nc/design07/0416/0416tt_file.pdf

[MOR 05] S. B. Morriss, *Automated Manufacturing Systems Actuators, Controls, Sensors, and Robotics*, McGraw-Hill, 1995

[MOU 98] A. Moukas, K. Chandrinos and P. Maes, "Trafficopter: A Distributed Collection System for Traffic Information," *Proceedings of Cooperative Information Agents*, volume 1435 of *Lecture Notes in Artificial Intelligence*. Springer-Verlag, 1998

[NAV 05] N. Navet, Y. Song, F. Simonot-Lion, and C. Wilwert, "*Trends in Automotive Communication Systems,*" Proceedings of the IEEE, vol. 93, no. 6, June 2005

[NeSCT] "Systèmes contrôlés en réseau tolérants aux fautes (NeCST : Networked Control Systems Tolerant to fault," Projet Européen STREP n° IST – 2004-004303, Available: http://www.strep-necst.org

[NIL 98] J. Nilsson, "Real-Time Control Systems with Delays," *PhD thesis*, Department of Automatic Control, Lund Institute of Technology, Lund, Sweden, 1998,

Available: http://home.case.edu/ncs

[NTC] Official Site of NetworkChemistry: www.networkchemistry.com/

[NXP 06] "*The Vital Link in the Interconnected Car,*" Founded by Philips, 2006, Official website: www.nxp.com

[OPN] Official Site of OPNET: www.opnet.com

[PRA 86] D.K. Pradhan, *Fault-Tolerant Computing: Theory and Techniques*, Prentice-Hall, 1986

[PRO 05] M. Provera, "Activities and Applications of the vehicle to vehicle and vehicle to infrastructure communication to enhance road safety," Centro Ricerche FIAT, 2005

[RAP 02] Th.S Rappaport, *Wireless communications : Principles and Practice*, Prentice Hall, 2nd Edition, 2002

[REU 05] H.-J. Reumerman, M. Roggero and M. Ruffini, "*The Application-Based Clustering Concept and Requirements for Intervehicle Networks,*" IEEE Communications Magazine, April 2005

[RFC 02] RFC3344, August 2002

[RFC 04] RFC3775, June 2004

[RFC 05a] RFC4068, July 2005

[RFC 05b] RFC4260, November 2005

[RFC 83] RFC 879, 1983

[RFP] Datasheet Available at: www.butlertech.ie/products

[RUN] Official website of RUNES: www.ist-runes.org

[SCH 06] A. P. Schalk, "CVIS-CORTECH Core Technologies and Architecture," CVIS-Forum, Brussels 2006.

[SHA] SHARPE. Available: http://www.qualitybooks.co.uk/software/reliability_modeling_software.htm

[SIE 98] D.P. Siewiorek and R.S. Swarz, *Reliable Computer Systems – Design and Evaluation.* A K Peters, Natick, Massachusetts, 1998.

[SKE 02] T. Skeie, S. Johannessen, and C. Brunner, "*Ethernet in Substation Automation,*" IEEE Control System Magazine, Vol. 22, No. 3, pp. 43-51, June 2002

[SOL 05] H. Soliman, *Mobile IPv6 Mobility in a Wireless Internet*, Pearson Education, 2005

[STD 11] IEEE Std 802.11

[STD 11P] IEEE Official 802 Standards website: http://ieee802.org

[STD 15] IEEE Std 802.15.4

[STD 16] IEEE Std 802.16

[STD 3] IEEE Std 802.3

[SUN 05] B. Sundararaman, U. Buy and A.D. Kshemkalyani, "Clock Synchronization for Wireless Sensor Networks: a survey," Ad Hoc Networks, vol. 3, 2005, pp: 281-323

[TAN 03] Tanenbaum, Andrew S., Computer Networks, 2003, 4th edition.

[THE 99] G. Theraulaz and E. Bonabeau, "*A brief history of stigmergy,*" Journal of Artificial Life, vol. 5, No 2, pp. 97-116, 1999

[THO 06] J.S. Thomsen and M. Blanke, "Fault-Tolerant Actuator System for Electrical Steering of Vehicles," *Proceedings of the the 32nd Annual Conference of the IEEE Industrial Electronics Society, IECON*, Paris, France, November 2006

[TOL 97] K. Tolly, "*The Great Networking Correction: Frames Reaffirmed,*" Industry Report, The Tolly Group, IEEE Internet computing, 1997

[TOM] Official website of TomTom: www.tomtom.com

[TRI 02] K. S. Trivedi, *Probability and Statistics with Reliability, Queuing and Computer Science Applications*, 2nd ed, John Wiley and Sons, 2002

[UPE 96] B.P. Upender, "*Analyzing the Real-Time Characteristics of Class C Communications in CAN through Discrete Event Simulations,*" Advanced Digital Systems, United Technologies Research Center, 1996.

[VAT 06] N. Vatanski, J.P. Georges, C. Aubrun, E. Rondeau. and S.-L. Jämsä-Jounela, "Control Compensation Based on Upper Bound Delay in Networked Control Systems," *17th International Symposium on Mathematical Theory of Networks and Systems, MTNS 2006*, Kyoto, Japan, July 2006.

[VEC 03] Vector CANtech Inc., "Overview of Current Automotive Protocols," 2003, Available: www.vector-cantech.com

[VMN] Official website of ViaMichelin: www.viamichelin.com

[WAL 01] G.C. Walsh, and H. Ye, "*Scheduling of Networked Control Systems,*" IEEE Control Systems Magazine, vol. 21, no. 1, pp. 57-65, Feb. 2001

[WAN 99] J. Wang and S. Keshav, "Efficient and Accurate Ethernet Simulation," Cornell Network Research Group (C/NRG), Department of Computer Science, Cornell University, May 1999.

[WEC] Official Site: www.connected-egypt.org

[WIL 05] C. Wilwert, F. Simonot-Lion, Y. Song and F. Simonot, "Quantitative Evaluation of the Safety of X-by-Wire Architecture subject to EMI Perturbations," *10th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA,* Catania-Italy, September 2005

[WIS 06] L. Wischhof, H. Rohling and A. Ebner, "Self-Generated Road Status Maps based on Vehicular Ad Hoc Communication," *Proceedings of the 3rd International Workshop on Intelligent Transportation, WIT*, Hamburg, Germany, Mar. 2006

[WIT 98] B. Wittenmark, B. Bastian, and J. Nilsson, "Analysis of Time Delays in Synchronous and Asynchronous Control Loops," Lund Institute of Technology, 37th CDC, Tampa, Dec. 1998.

[WLT] Wireless LAN (WiFi) Tutorial.Available: www.tutorial-reports.com/book/print/200

[WNL] WirelessLeiden.NL, Available: www.wirelessleiden.nl/english/legal.shtml

[WTG] Wireless Technologies for Persons with Disabilities www.fondazionepolitecnico.it/contenuti/file/Decina_16_05_06.pdf

[YAN 04] X. Yang, J. Liu, F. Zhao and N.H. Vaidya, "A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning," *IEEE First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services MobiQuitous*, Boston, Massachusetts, USA, Aug. 2004

[ZEI 02] V. Zeimpekis, G.M. Giaglis And G. Lekakos, "*A Taxonomy of Indoor and Outdoor Positioning Techniques for Mobile Location Services,*" ACM SIGecom Exchanges, Dec. 2002

[ZEN 05] A. Zentai, T. Daboczi, "Improving Motor Current Control Using Decoupling Technique," *Proceedings of the IEEE International Conference on "Computer as a Tool", EUROCON*, Belgrade, Serbia and Montenegro, November 2005

[ZHA 01] W. Zhang, M.S. Branicky, and S.M. Phillips, "Stability of Networked Control Systems," IEEE Control Systems Magazine, vol. 21, no. 1, pp. 84-99, Feb. 2001

REFERENCES

[ALI 08] N.A. Ali, A.M. Taha, H.S. Hassanein and H.T. Mouftah, "IEEE 802.16 Mesh Schedulers: Issues and Design Challenges," IEEE Network, Vol. 22, No. 1, JAN 2008, pp.: 58-65

[AME 04] H.H. Amer and R.M. Daoud, "Reliability and Availability of Fault-Tolerant Networked Controlled Systems," *1st International Computer Engineering Conference, ICENCO*, Cairo-Egypt, December 2004

[AME 05] H.H. Amer, M.S. Moustafa, and R.M. Daoud, "Optimum Machine Performance in Fault-Tolerant Networked Control Systems," *The IEEE International Conference on "Computer as a Tool", IEEE EUROCON*, Belgrade-Serbia and Montenegro, November 2005

[AME 06a] H.H. Amer, M.S. Moustafa and R.M. Daoud, "Availability of Pyramid Industrial Networks," *IEEE Canadian Conference on Electrical and Computer Engineering, IEEE CCECE*, Ottawa-Canada, May 2006

[AME 06b] H.H. Amer and R.M. Daoud, "Parameter Determination for the Markov Modeling of Two-Machine Production Lines," *4th International IEEE Conference on Industrial Informatics, IEEE INDIN*, Singapore, August 2006

[AME 08] H.H. Amer and R.M. Daoud, "*Increasing Network Reliability by Using Fault-Tolerant Sensors,*" To appear in the International Journal of Factory Automation, Robotics and Soft Computing, 2008

[AME 87] H.H. Amer and E.J. McCluskey, "Calculation of Coverage Parameter," *IEEE Transactions on Reliability*, June 1987, pp. 194-198

[ARN 73] T.F. Arnold, "The concept of coverage and its effect on the reliability model of a repairable system," *IEEE Trans. On Computers,* vol. C-22, No. 3, March 1973

[AZI 08] M. Aziz, B. Raouf, N. Riad, R.M. Daoud, and H.M. Elsayed, "The Use of Ethernet for Single On-board Train Network," *IEEE International Conference on Networking, Sensing and Control, ICNSC*, Sanya-China, April 2008

[BAT 06] T. ElBatt, S. Goel, G. Holland, H. Krishnan and J. Parikh "Cooperative Collision Warning Using Dedicated Short Range Wireless Communications," HRL Laboratories, LLC, ACM VANET, Los Angeles, California, USA, 2006

[BER 06] T. Berger, Y. Sallez, C. Tahon "Bio-inspired approach for autonomous routing in FMS," In Manufacturing the future, Ed. By Vedran KORDIC, Advanced Robotics Systems International, July 2006, ISBN N° 3-86611-198-3

[BIL 83] R. Billinton and R. Allan, *Reliability Evaluation of Engineering Systems: Concepts and Techniques*, Pitman, 1983

[BIS 06] S. Biswas, R. Tatchikou and F. Dion, "*Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety,*" IEEE Communications Magazine, Jan. 2006

[BLA 01] M. Blanke, M. Staroswiecki, and N. Wu, "Concepts and Methods in Fault-Tolerant Control," *Proceedings of the American Control Conference*, Arlington, VA, June 2001, pp. 2608-2620

[BLU 04] J.J. Blum, A. Eskandarian and L.J. Hoffman, "*Challenges of Intervehicle Ad Hoc Networks,*" IEEE Transactions on Intelligent Transportation Systems, Vol. 5, No. 4, Dec. 2004

[BRA 06] B. Brahimi, C. Aubrun, E. Rondeau, "Modelling and Simulation of Scheduling Policies Implemented in Ethernet Switch by Using Coloured Petri Nets," Proceedings of the 11th IEEE International Conference on Emerging Technologies and Factory Automation, Prague, Czech Republic Sept. 2006

[BRA 07] B. Brahimi, "Proposition d'une approche intégrée basée sur les réseaux de Petri de Haut Niveau pour simuler et évaluer les systèmes contrôlés en réseau," *PhD Thesis*, Université Henri Poincaré, Nancy I, Dec. 2007.

[BRE 01] E.A. Bretz, "*By-Wire Cars Turn the Corner,*" IEEE Spectrum, April 2001

[BRI 06] R. Brignolo, "Infrastructure/Vehicle Communication," Second International Symposium Safe & Reliable Tunnels. Innovative European Achievements, Lausanne 2006

[BRU 05] R. Bruno, M. Conti and E. Gregori, "*Mesh Networks: Commodity Multihop Ad Hoc Networks,*" IEEE Communications Magazine, March 2005

[CAL] Website of CALM: www.fischer-tech.de

[CHA 05] B. Chakraborty, T. Maeda and G. Chakraborty, "Multiobjective Route Selection for Car Navigation System using Genetic Algorithm," *IEEE Mid-Summer Workshop on Soft Computing in Industrial Applications, IEEE SMCia/05*, Espoo-Finland, June 2005

[CHE 05] W. Chen and S. Cai, "*Ad Hoc Peer-to-Peer Network Architecture for Vehicle Safety Communications,*" IEEE Communications Magazine, April 2005

[CHE 08] L. Cheng, B.E. Henty, R. Cooper and D. Stancil, "A Measurement Study of Time-Scaled 802.11a Waveforms over the Mobile-to-Mobile Vehicular Channel at 5.9GHz," IEEE Communication Magazine, Vol. 46, No. 5, May 2008, pp.: 84-91

[CRO 06] M. Crocker, J. Baranski, and G.Y. Lazarou, "*Fault-Tolerant Reconfigurable Ethernet-Based IP Network Proxy*," International Journal of Computers and Applications, Issue 3, 2006

[CYB] Cyber Cars: www.cybercar.org

[DAO 03] R.M. Daoud, H.M. Elsayed, H. H. Amer, and S.Z. Eid, "Performance of Fast and Gigabit Ethernet in Networked Control Systems," *Proceedings of the IEEE International Mid-West Symposium on Circuits and Systems, MWSCAS*, Cairo, Egypt, December 2003

[DAO 04a] R.M. Daoud, *Performance of Gigabit Ethernet in Networked Control Systems*, MSc Thesis, Electronics and Communications Department, Faculty of Engineering, Cairo University, 2004

[DAO 04b] R.M. Daoud, H.M. Elsayed, and H.H. Amer, "Gigabit Ethernet for Redundant Networked Control Systems," in *Proceedings of the IEEE International Conference on Industrial Technology, ICIT*, Hammamet, Tunis, December 2004.

[DAO 05a] R.M. Daoud, H.H. Amer, and H.M. Elsayed, "Fault-Tolerant Networked Control Systems under Varying Load," *IEEE Mid-Summer Workshop on Soft Computing in Industrial Applications, IEEE SMCia/05*, Espoo-Finland, June 2005

[DAO 05b] R.M. Daoud, H.H. Amer, and H.M. Elsayed, "Fault-Tolerant Two-Level Pyramid Networked Control Systems," *10th IEEE International Conference on Emerging Technologies and Factory Automation, IEEE ETFA*, Catania-Italy, September 2005

[DAO 06a] R.M. Daoud and H.H. Amer, "Optimum Supervisor Computational Power for Small Scale In-Line Production Networked Control Machines," *IEEE Canadian Conference on Electrical and Computer Engineering, IEEE CCECE*, Ottawa-Canada, May 2006

[DAO 06b] R.M. Daoud, H.H. Amer, H.M. Elsayed and Y. Sallez, "Ethernet Based Car Control Network," *IEEE Canadian Conference on Electrical and Computer Engineering, IEEE CCECE*, Ottawa-Canada, May 2006

[DAO 06c] R.M. Daoud, H.H. Amer, H.M. Elsayed and Y. Sallez, "Fault-Tolerant On-Board Ethernet-Based Vehicle Networks," *32nd Annual Conference of the IEEE Industrial Electronics Society, IEEE IECON*, Paris-France, November 2006

[DAO 06d] R.M. Daoud, M.A. El-Dakroury, H.M. Elsayed, H.H. Amer, M. El-Soudani and Y. Sallez, "Wireless Vehicle Communication for Traffic Control in Urban Areas," *32nd Annual Conference of the IEEE Industrial Electronics Society, IEEE IECON*, Paris-France, November 2006

[DAO 06e] R.M. Daoud and H.H. Amer, "*Heavy-Traffic Model for Pyramid Networked Control Systems,*" International Journal of Factory Automation, Robotics and Soft Computing, June 2006

[DAO 07a] R.M. Daoud, M.A. El-Dakroury, H.H. Amer, H.M. Elsayed and M. El-Soudani, "WiFi Architecture for Traffic Control using MIPv6," *15th IEEE Mediterranean Conference on Control and Automation, IEEE MED*, Athens-Greece, June 2007

[DAO 07b] R.M. Daoud and H.H. Amer, "Analysis of Pyramid In-Line Production at Higher-than-Nominal Speeds," *15th IEEE Mediterranean Conference on Control and Automation, IEEE MED*, Athens-Greece, June 2007

[DAO 07c] R.M. Daoud, M.A. El-Dakroury, H.M. Elsayed, H.H. Amer, M. El-Soudani and Y. Sallez, "Burst Communication for Traffic Control in Light Urban Areas," *International Workshop on Logistics and Transportation 2007, IEEE LT*, Sousse-Tunis, November 2007

[DAO 07d] R.M. Daoud and H.H. Amer, "*Ethernet for Heavy Traffic Networked Control Systems*," International Journal of Factory Automation, Robotics and Soft Computing, January 2007

[DAO 07e] R.M. Daoud and H.H. Amer, "*Fast Ethernet Implementation of Cost Effective Vehicle On-Board Networks,*" (Refereed/Invited Contribution), Journal of Factory Automation, Robotics and Soft Computing, June 2007

[DAO 08] R.M. Daoud and H.H. Amer, "Fault-Tolerant Access Points in a Mobile IPv6 WiFi Light Urban Traffic Communication Model," *IEEE 21st Canadian Conference on Electrical and Computer Engineering, CCECE*, Niagara Falls-Ontario Canada, May 2008

[DEC 05] J.-D. Decotignie, "*Ethernet-Based Real-Time and Industrial Communications,*" Proceedings of the IEEE, vol. 93, No. 6, June 2005

[EKE 99] J. Eker and A. Cervin, "A Matlab Toolbox for Real-Time and Control Systems Co-Design," *Department of Automatic Control, Lund Institute of Technology, 6th International Conference on Real-Time Computing Systems and Applications*, Hong Kong, P.R. China, Dec. 1999.

[ELC] "Summary of some of the key standards regulating the use and design of WLAN products," Available: http://www.elcard.fi/standards.htm

[ELP] "Performance of Different Frequency Bands," ELPRO Technologies, Technical Article, Available: http://www.elprotech.com/UserFiles/File/PDFs/white_paper_-_frequencies_1.3.pdf

[ERC] Official website of ERCIM: www.ercim.org/

[FAR 05] P.B. Farradyne, "Vehicle Infrastructure Integration (VII) Architecture and Functional Requirements," ITS Joint Program Office, US Department of Transportation, 2005

[FCC] Official Site for FCC regulations: www.fcc.gov

[FEL 05] M. Felser, "*Real-Time Ethernet – Industry Prospective,*" Proceedings of the IEEE, vol. 93, No. 6, June 2005.

[FRE 06] G. Fremont, "Systemes Coopératifs pour la Sécurité Routière Le Projet européen SAFESPOT," Saint-Brieuc – Côtes d'Armor 3ème Congrès ITS, 2006

[FRO 06] A. Froetscher, M. Boehm, "coopers – Co-operative Systems for Intelligent Road Safety," ITS World Conference, London, 2006

[FUJ] Official Site for Fujitsu: www.fujitsu.com

[GAR] "GPS Guide for Beginners," GARMIN Official Website: www.garmin.com

[GEO 05] J.-P. Georges, "Systèmes contrôles en réseau: Evaluation de performances d'architectures Ethernet commutées," *PhD thesis*, Centre de Recherche en Automatique de Nancy CRAN, Nov. 2005

[GEO 06] J.-P. Georges, N. Vatanski, E. Rondeau and S.-L. Jämsä Jounela, "Use of Upper Bound Delay Estimate in Stability Analysis and Robust Control Compensation in Networked Control Systems," 12th IFAC Symposium on Information Control Problems in Manufacturing, INCOM 2006, St-Etienne, France, Mai 2006

[GRI 04] J. Grieu, "Analyse et évaluation de techniques de commutation Ethernet pour l'interconnexion des systèmes avioniques," PhD Thesis, Institut National Polytechnique de Toulouse, Ecole doctorale informatique et telecommunications, Sep. 2004

[HEN 07] K. Henain, M. Milad, R. Morgan, S. Ramzy, R.M. Daoud and H.H. Amer, "Optimization of 802.11b/g Networks for High Mobility and Dynamic Data Applications," *9th IEEE International Conference on Telecommunications, IEEE ConTel*, Zaghreb-Coratia, June 2007

[HIR 99] H. Hiraishi, H. Ohwada, F. Mizoguchi, "Intercommunicating CarNavigation System with Dynamic Route Finding," *Proceedings of the Intelligent Transportation Systems,* Tokyo-Japan, 1999

[HOL 06] W. Holfelder, "Wireless Communication The next logical step in Vehicle Safety," IEEE Communications Society Joint Meeting, Oakland-East Bay and Santa Clara Valley Chapter, May 2006

[ITS] "Towards Smart Mobility Society," SMARTWAY Project, ITS official website: http://www.its.go.jp/ITS/topindex/topindex_smartway.html

[JAS 04a] J. Jasperneite and E. Elsayed, "Investigations on a Distributed Time-triggered Ethernet Realtime Protocol used by PROFINET," *3rd International Workshop on Real-Time Networks (RTN 2004)*, Catania, Sicily, Italy , Jun 2004

[JAS 04b] J. Jasperneite, K. Shehab and K. Weber, "Enhancements to the time synchronization standard IEEE-1588 for a system of cascaded bridges," Proceedings of the IEEE International Workshop on Factory Communication Systems, WFCS.2004, Sept. 2004, pp.: 239- 244.

[JOH 89] B.W. Johnson, "*Design and Analysis of Fault-Tolerant Digital Systems*", Addison-Wesley, 1989.

[KAT 02] S. Kato, S. Tsugawa, K. Tokuda, T. Matsui, and H. Fujii, "*Vehicle Control Algorithms for Cooperative Driving With Automated Vehicles and Intervehicle Communications,*" IEEE Transactions on Intelligent Transportation Systems, Vol. 3, No. 3, Sep. 2002

[KUM01] P.R. Kumar, "New Technological Vistas for Systems and Control: The Example of Wireless Networks," IEEE Control Systems Magazine, vol. 21, no. 1, pp. 24-37, 2001.

[LEA 04] J. Leary, P. Roshan, "*Wireless LAN Fundamentals: Mobility,*" CISCO Press, 2004. Available: www.ciscopress.com/articles/article.asp?p=102282&rl=1

[LEE 01] S.H. Lee and K.H. Cho, "Congestion Control of High-Speed Gigabit-Ethernet Networks for Industrial Applications," *Proceedings of IEEE International Symposium on Industrial Electronics*, vol. 1, pp. 260-265, 12-16 June 2001.

[LIA 01a] F.L. Lian, J.R. Moyne, and D.M. Tilbury, "*Performance Evaluation of Control Networks: Ethernet, ControlNet, and DeviceNet,*" IEEE Control Systems Magazine, Vol. 21, No. 1, pp.66-83, Feb. 2001

[LIA 01b] Lian, F. L., Moyne, J. R., and Tilbury, D. M., "*Networked Control Systems Toolkit: A Simulation Package for Analysis and Design of Control Systems with Network Communication,*" Tech. Rep., UM-ME-01-04, July 2001.

Available: http://www.eecs.umich.edu/~impact

[LKS] Official Site of Linksys: www.linksys.com

[LOR 03] S. Lorkowski, P. Mieth and R.-P. Schäfer, "*New ITS applications for metropolitan areas based on Floating Car Data,*" German Aerospace Center, 2003

[LOU] Musee du Louvre, Available: www.louvre.fr

[LOU 01] B. Lounsbury and J. Westerman, "Ethernet: Surviving the Manufacturing and Industrial Environment," White Paper, May 2001.
Available: http://www.ab.com/networks/enetpaper.html

[MAR 06a] G. Marsal, "Evaluation of time performances of Ethernet-based Automation Systems by simulation of High-level Petri Nets," *PhD Thesis,* Ecole Normale Superieure De Cachan, Dec. 2006

[MAR 06b] G. Marsal, B. Denis, J.-M. Faur and G. Frey, "Evaluation of Response Time in Ethernet-based Automation Systems," Proceedings of the 11th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA'06, Prague (Czech Republic), pp. 380-387, Sep. 2006

[MAT 08] D.W. Matolak, "*Channel Modeling for Vehicle-to-Vehicle Communications,*" IEEE Communications Magazine, Vol. 46, No. 5, pp.:76-83, May 2008

[MIC 96] L.B. Michael and M. Nakagawa, "Multi-Hop for Inter-Vehicle Communication over Multiple Lanes," *Proceedings of the Intelligent Vehicles Symposium, Tokyo-Japan, 1996*

[MOK 06] E. Mok, G. Retscher and L. Xia,, "Investigation of Seamless Indoor and Outdoor Positioning Integrating WiFi and GNSS," *Proceedings, XXIII International FIG Congress*, Munich, Oct. 2006

[MOL 07] D. Molta, "802.11r Holds Promise Of Secure Wi-Fi Mobility," Apr 16, 2007 Available: http://i.cmpnet.com/nc/design07/0416/0416tt_file.pdf

[MOR 05] S. B. Morriss, *Automated Manufacturing Systems Actuators, Controls, Sensors, and Robotics*, McGraw-Hill, 1995

[MOU 98] A. Moukas, K. Chandrinos and P. Maes, "Trafficopter: A Distributed Collection System for Traffic Information," *Proceedings of Cooperative Information Agents*, volume 1435 of *Lecture Notes in Artificial Intelligence*. Springer-Verlag, 1998

[NAV 05] N. Navet, Y. Song, F. Simonot-Lion, and C. Wilwert, "*Trends in Automotive Communication Systems,*" Proceedings of the IEEE, vol. 93, no. 6, June 2005

[NeSCT] "Systèmes contrôlés en réseau tolérants aux fautes (NeCST : Networked Control Systems Tolerant to fault," Projet Européen STREP n° IST – 2004-004303, Available: http://www.strep-necst.org

[NIL 98] J. Nilsson, "Real-Time Control Systems with Delays," *PhD thesis*, Department of Automatic Control, Lund Institute of Technology, Lund, Sweden, 1998,

Available: http://home.case.edu/ncs

[NTC] Official Site of NetworkChemistry: www.networkchemistry.com/

[NXP 06] "*The Vital Link in the Interconnected Car,*" Founded by Philips, 2006, Official website: www.nxp.com

[OPN] Official Site of OPNET: www.opnet.com

[PRA 86] D.K. Pradhan, *Fault-Tolerant Computing: Theory and Techniques*, Prentice-Hall, 1986

[PRO 05] M. Provera, "Activities and Applications of the vehicle to vehicle and vehicle to infrastructure communication to enhance road safety," Centro Ricerche FIAT, 2005

[RAP 02] Th.S Rappaport, *Wireless communications : Principles and Practice*, Prentice Hall, 2nd Edition, 2002

[REU 05] H.-J. Reumerman, M. Roggero and M. Ruffini, "*The Application-Based Clustering Concept and Requirements for Intervehicle Networks,*" IEEE Communications Magazine, April 2005

[RFC 02] RFC3344, August 2002

[RFC 04] RFC3775, June 2004

[RFC 05a] RFC4068, July 2005

[RFC 05b] RFC4260, November 2005

[RFC 83] RFC 879, 1983

[RFP] Datasheet Available at: www.butlertech.ie/products

[RUN] Official website of RUNES: www.ist-runes.org

[SCH 06] A. P. Schalk, "CVIS-CORTECH Core Technologies and Architecture," CVIS-Forum, Brussels 2006.

[SHA] SHARPE. Available: http://www.qualitybooks.co.uk/software/reliability_modeling_software.htm

[SIE 98] D.P. Siewiorek and R.S. Swarz, *Reliable Computer Systems – Design and Evaluation.* A K Peters, Natick, Massachusetts, 1998.

[SKE 02] T. Skeie, S. Johannessen, and C. Brunner, "*Ethernet in Substation Automation,*" IEEE Control System Magazine, Vol. 22, No. 3, pp. 43-51, June 2002

[SOL 05] H. Soliman, *Mobile IPv6 Mobility in a Wireless Internet*, Pearson Education, 2005

[STD 11] IEEE Std 802.11

[STD 11P] IEEE Official 802 Standards website: http://ieee802.org

[STD 15] IEEE Std 802.15.4

[STD 16] IEEE Std 802.16

[STD 3] IEEE Std 802.3

[SUN 05] B. Sundararaman, U. Buy and A.D. Kshemkalyani, "Clock Synchronization for Wireless Sensor Networks: a survey," Ad Hoc Networks, vol. 3, 2005, pp: 281-323

[TAN 03] Tanenbaum, Andrew S., Computer Networks, 2003, 4th edition.

[THE 99] G. Theraulaz and E. Bonabeau, "*A brief history of stigmergy,*" Journal of Artificial Life, vol. 5, No 2, pp. 97-116, 1999

[THO 06] J.S. Thomsen and M. Blanke, "Fault-Tolerant Actuator System for Electrical Steering of Vehicles," *Proceedings of the the 32nd Annual Conference of the IEEE Industrial Electronics Society, IECON*, Paris, France, November 2006

[TOL 97] K. Tolly, "*The Great Networking Correction: Frames Reaffirmed,*" Industry Report, The Tolly Group, IEEE Internet computing, 1997

[TOM] Official website of TomTom: www.tomtom.com

[TRI 02] K. S. Trivedi, *Probability and Statistics with Reliability, Queuing and Computer Science Applications*, 2nd ed, John Wiley and Sons, 2002

[UPE 96] B.P. Upender, "*Analyzing the Real-Time Characteristics of Class C Communications in CAN through Discrete Event Simulations,*" Advanced Digital Systems, United Technologies Research Center, 1996.

[VAT 06] N. Vatanski, J.P. Georges, C. Aubrun, E. Rondeau. and S.-L. Jämsä-Jounela, "Control Compensation Based on Upper Bound Delay in Networked Control Systems," *17th International Symposium on Mathematical Theory of Networks and Systems, MTNS 2006*, Kyoto, Japan, July 2006.

[VEC 03] Vector CANtech Inc., "Overview of Current Automotive Protocols," 2003, Available: www.vector-cantech.com

[VMN] Official website of ViaMichelin: www.viamichelin.com

[WAL 01] G.C. Walsh, and H. Ye, "*Scheduling of Networked Control Systems,*" IEEE Control Systems Magazine, vol. 21, no. 1, pp. 57-65, Feb. 2001

[WAN 99] J. Wang and S. Keshav, "Efficient and Accurate Ethernet Simulation," Cornell Network Research Group (C/NRG), Department of Computer Science, Cornell University, May 1999.

[WEC] Official Site: www.connected-egypt.org

[WIL 05] C. Wilwert, F. Simonot-Lion, Y. Song and F. Simonot, "Quantitative Evaluation of the Safety of X-by-Wire Architecture subject to EMI Perturbations," *10th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA,* Catania-Italy, September 2005

[WIS 06] L. Wischhof, H. Rohling and A. Ebner, "Self-Generated Road Status Maps based on Vehicular Ad Hoc Communication," *Proceedings of the 3rd International Workshop on Intelligent Transportation, WIT,* Hamburg, Germany, Mar. 2006

[WIT 98] B. Wittenmark, B. Bastian, and J. Nilsson, "Analysis of Time Delays in Synchronous and Asynchronous Control Loops," Lund Institute of Technology, 37th CDC, Tampa, Dec. 1998.

[WLT] Wireless LAN (WiFi) Tutorial.Available: www.tutorial-reports.com/book/print/200

[WNL] WirelessLeiden.NL, Available: www.wirelessleiden.nl/english/legal.shtml

[WTG] Wireless Technologies for Persons with Disabilities www.fondazionepolitecnico.it/contenuti/file/Decina_16_05_06.pdf

[YAN 04] X. Yang, J. Liu, F. Zhao and N.H. Vaidya, "A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning," *IEEE First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services MobiQuitous*, Boston, Massachusetts, USA, Aug. 2004

[ZEI 02] V. Zeimpekis, G.M. Giaglis And G. Lekakos, "*A Taxonomy of Indoor and Outdoor Positioning Techniques for Mobile Location Services,*" ACM SIGecom Exchanges, Dec. 2002

[ZEN 05] A. Zentai, T. Daboczi, "Improving Motor Current Control Using Decoupling Technique," *Proceedings of the IEEE International Conference on "Computer as a Tool", EUROCON*, Belgrade, Serbia and Montenegro, November 2005

[ZHA 01] W. Zhang, M.S. Branicky, and S.M. Phillips, "Stability of Networked Control Systems," IEEE Control Systems Magazine, vol. 21, no. 1, pp. 84-99, Feb. 2001

APPENDIX A

This appendix includes 2 major parts. The first part introduces the control system equations of [WAL 01]. The second part explains the Markov Model of Chapter 2.

The state space representation of [WAL 01] includes:

- plant states $\sum_p (A_p, B_p, C_p, 0)$

  with state $x_p \in \Re^{n_p}$ and output $y \in \Re^{n_r}$,

- network states $\hat{n}(t) = [\hat{y}(t) \quad \hat{u}(t)]^T$,

- network-induced errors $e(t) = \hat{n}(t) - [y(t) \quad u(t)]^T$, and

- controller states $\sum_c (A_c, B_c, C_c, D_c)$

  with state $x_c \in \Re^{n_c}$ and output $u(t) \in \Re^{n_q}$.

$$\dot{z}(t) = \begin{bmatrix} \dot{x}(t) \\ \dot{e}(t) \end{bmatrix} = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \begin{bmatrix} x(t) \\ e(t) \end{bmatrix}$$

where:

$$A_{11} = \begin{bmatrix} A_p + B_p D_c C_p & B_p C_c \\ B_c C_p & A_c \end{bmatrix} \qquad A_{12} = \begin{bmatrix} B_p D_c & B_p \\ B_c & 0 \end{bmatrix}$$

$$A_{21} = -\begin{bmatrix} C_p & 0 \\ 0 & C_c \end{bmatrix} A_{11} \qquad A_{22} = -\begin{bmatrix} C_p & 0 \\ 0 & C_c \end{bmatrix} A_{12}$$

As the matrices in this paper are of compact dimensions, calculations are made very easy. Also, under the assumption of having no network delays $e(t) = 0$ the dynamics reduce to $\dot{x}(t) = A_{11}x(t)$, and Lyaponuv function, $V(x) = x^T Px$ was tested on the available states, that is $A_{11}^T P + PA_{11} = -Q$. Wei et al. [ZHA 01] elaborated on Gregory et al. work and gave a limit on the network induced delay as to satisfy Lyaponuv criteria.

$$\tau < \frac{\lambda_{\min}(Q)}{16\lambda_2 \sqrt{\frac{\lambda_2}{\lambda_1}} \|A\|^2 \left(\sqrt{\frac{\lambda_2}{\lambda_1}} + 1\right) \sum_{i=1}^{p} i}$$

where: τ, maximum allowable transfer interval (MATI)

$\lambda_1 = \lambda_{\min}(P)$, minimum eigen value of matrix P

$\lambda_2 = \lambda_{\max}(P)$, maximum eigen value of matrix P

$\lambda_{\min}(Q)$, minimum eigen value of matrix Q

Matrix P and Q are positive-definite symmetric matrices

p, number of nodes on a NCS

$\|A\|$, is the Euclidian norm of matrix A

In the Markov model of [AME 04], let λ_i be the failure rate of sensor i, λ_j the failure rate of actuator j and λ_{cont} the failure rate of any of the two controllers (for simplicity, assume that the 2 controllers have identical failure rates). Also, assume that all failure rates are constant, i.e., all failure times are exponentially distributed.

The system will go from state 0 to state 1 if one of the two controllers fails. Hence, the transition rate is λ_{cont}. Of course, the failure of one of the controllers must be successfully detected and diagnosed so that the other controller can take over. Let the probability of successful switchover be c. c is known in the literature as the coverage [JOH 89, PRA 86, AME 87]. In order to incorporate the coverage in the Markov model, the transition from state 0 to state 1 becomes $(2c)$ (λ_{cont}) instead of just $(2\lambda_{cont})$. In other words:

$$B = 2c\lambda_{cont}$$

While the system is in state 1 (one controller has failed and the other controller is managing BOTH machines), the failure of the remaining controller will cause a system failure; consequently, the system will move from state 1 to state 2. Furthermore, while in state 1, any sensor or actuator failure will also cause a system failure. Hence, the transition rate from state 1 to state 2 is:

$$E = \lambda_{cont} + \sum_{i=1}^{32} \lambda_i + \sum_{j=1}^{8} \lambda_j$$

As mentioned above, if any of the 32 sensors or 8 actuators fails, the entire system fails. Consequently, the transition rate from state 0 to state 2 is:

$$A = \sum_{i=1}^{32} \lambda_i + \sum_{j=1}^{8} \lambda_j + (1-c)(2\lambda_{cont})$$

The term $(1\text{-}c)(2\lambda_{cont})$ describes the situation where one controller has failed but switchover to the remaining operational controller was not successful. When the system is in state 1, it may return to state 0 when the failed controller is repaired. Let the repair rate be μ. Hence,

$$D = \mu$$

The Markov model can be represented by a set of linear differential equations with constant coefficients (Chapman-Kolmogorov equations [TRI 02]). Let P_0, P_1 and P_2 be the probabilities (as functions of time) of being in states 0, 1 and 2 respectively. Also, let P_0', P_1' and P_2' be the derivatives with respect to time of P_0, P_1 and P_2.

$$P_0' = -(A+B)P_0 + DP_1$$

$$P_1' = BP_0 - (D+E)P_1$$

$$P_2' = AP_0 + EP_1$$

Also, at any time t: $P_0 + P_1 + P_2 = 1$

And assuming the system was initially failure-free, then:

At time $t = 0$: $P_0 = 1, \quad P_1 = P_2 = 0$

These equations can be solved using the Laplace Transform or by numerical techniques. Matrices can also be very helpful in the solution [BIL 83]. Using the Laplace transform techniques is only practical for small systems. Larger systems are usually solved by using software based on numerical techniques [BIL 83, PRA 86]. The reliability $R(t)$ of the system is the probability that it is in states 0 or 1. Hence,

$$R(t) = P_0(t) + P_1(t)$$

The Markov model in Fig. A can be used in a variety of ways. The most obvious use of the model is to calculate the reliability of an already installed and running system. Another extremely important use of the Markov model is as a design tool. Following are some examples to illustrate the use of the model during the design phase.

The choice of the switching mechanism (software) will have a great effect on reliability. The switching mechanism is responsible for the coverage factor c in the model. It is well

known in the literature that a small change in the value of c will generally have a great effect on reliability [JOH 89, AME 87]. The Markov model can therefore be used to quantitatively measure the effect of the efficiency of the switching mechanism. Efficiency is, of course, related to cost. The system designer can start with a certain reliability requirement. Using the Markov model, the coverage is calculated and the appropriate switching mechanism can be determined.

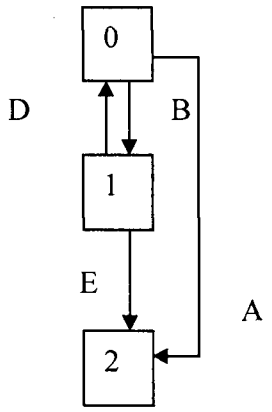


Fig. A, Reliability Model

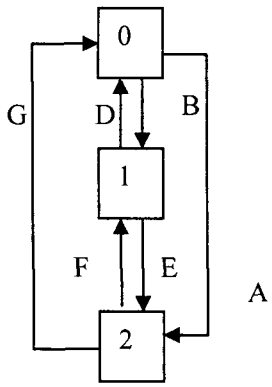


Fig. B, Availability Model

The repair rate will also affect system reliability. It is very possible (especially in developing countries) that spare parts are not available locally; they have to be imported upon the occurrence of a failure. This can take a fairly long time which will be reflected in the parameter D=μ in Fig. B. If the spare parts are imported after the occurrence of a failure, the value of μ may be such that system reliability is unacceptable. A possible solution to this problem is to stock some spare parts within the premises. The repair time

will be greatly reduced and its effect on system reliability can be quantitatively determined by using the Markov model.

If two repairmen are available [SIE 98],

$$F = 2\mu$$

Let this repair rate be represented by the parameter ξ. Hence,

$$G = \xi$$

The differential equations describing the Markov model in Fig. B are:

$$P_0' = -(A+B)P_0 + DP_1 + GP_2$$

$$P_1' = BP_0 - (D+E)P_1 + FP_2$$

$$P_2' = AP_0 + EP_1 - (G+F)P_2$$

At any time t, $P_0 + P_1 + P_2 = 1$

And at $t = 0, \quad P_0 = 1, \quad P_1 = P_2 = 0$

The solution of this system of differential equations will lead to the system availability $\mathrm{AV}(t) = P_0(t) + P_1(t)$

System availability is a function of time. Sometimes, all that is required is the steady state availability $\mathrm{AV_{ss}}$. It can be calculated by setting $P_0' = P_1' = P_2' = 0$ in the equations above and solving for P_0, P_1 and P_2 [BIL 83]. The calculations are much simpler in this case because the equations are algebraic and not differential. Again, $\mathrm{AV_{ss}} = P_0 + P_1$

In order to use the Markov model in Fig. B as a design tool, the steady-state availability can be determined before hand and the appropriate values of c, μ and ξ calculated from the model. The values of μ and ξ are determined by the maintenance policy. As in the previous section, stocking spare-parts in the premises will be more expensive but will

also increase system availability. An optimum trade off can be obtained by comparing cost and availability (quantitatively).

Let the probability of successful detection and recovery be c. The parameter c is known in the literature as the coverage and has to be taken into account in the Markov model. One of the earliest papers that defined the coverage was [ARN 73]. It defined the coverage as the proportion of faults from which a system automatically recovers. In [TRI 02], it was shown that a small change in the value of the coverage parameter had a big effect on system MTTF. The importance of the coverage was further emphasized in [AME 87]. In [BLA 01], the coverage was again defined in the context of fault-tolerant control systems. In this research, the controller software is responsible for detecting a controller failure and switching the control of that machine to the operational controller on the other machine [AME 06b]. Consequently, the value of the coverage depends on the quality of the switching software on each controller.

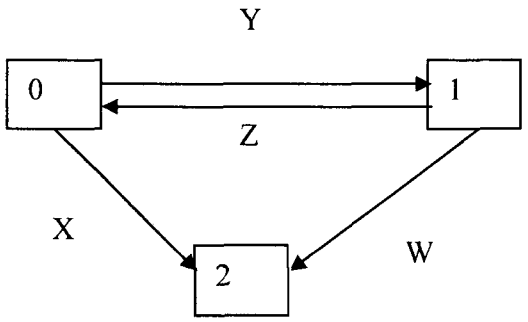


Fig. C. Markov Model

Assuming, for simplicity, that both controllers have the same failure rate λ, the transition rate from state 0 to state 1 will be equal to $Y=2c\lambda$.

As mentioned above, the system will move from state 0 to state 2 if a controller failure is not detected or if the recovery software does not transfer control to the operational controller. Due to a software problem in one of the controllers, for example, sensor data is incorrectly processed and the packet sent to the actuator has incorrect data but correct CRC. The actuator verifies the CRC, processes the data and the system fails. Another potential problem that cannot be remedied by the fault-tolerant architecture described in

this research is as follows: Both controllers are operational but their inter-communication fails. Each controller assumes that the other has failed and takes control of the entire production line. This conflict causes a production line failure. Consequently, the transition rate from state 0 to state 2 will be equal to $X=(1-c)(2\lambda)$.

If the failed controller is repaired while the system is in state 1, a transition occurs to state 0. Let the rate of this transition be $Z=\mu$. While in state 1, the failure of the remaining controller (before the first one is repaired) will take the system to state 2. Hence, the transition rate from state 1 to state 2 is equal to $W=\lambda$. In summary, the transition rates for the Markov model in Fig. C are:

$$X = (1-c)(2\lambda)$$

$$Y = 2c\lambda$$

$$Z = \mu$$

$$W = \lambda$$

The Markov model in Fig. C can be used to calculate the reliability R(t) of the 1-out-of-2 system under study.

$$R(t) = P_0(t) + P_1(t)$$

where $P_0(t)$ is the probability of being in state 0 at time t and $P_1(t)$ is the probability of being in state 1 at time t. The model can also be used to obtain the Mean Time To Failure (MTTF) of the system. $MTTF_{fault\text{-}tolerant}$ can be calculated as follows [BIL 83]: First, the Stochastic Transitional Probability Matrix P for the model in Fig. C is obtained:

$$P = \begin{bmatrix} 1-(X+Y) & Y & X \\ Z & 1-(W+Z) & W \\ 0 & 0 & 1 \end{bmatrix}$$

where element p_{ij} is the transition rate from state i to state j. So, for example, p_{01} is equal to Y=2cλ as in Fig. C. But state 2 is an absorbing state. Consequently, the truncated matrix Q is obtained from P by removing the rightmost column and the bottom row. So,

$$Q = \begin{bmatrix} 1-(X+Y) & Y \\ Z & 1-(W+Z) \end{bmatrix}$$

Let matrix M = $[I-Q]^{-1}$

$$M = \begin{bmatrix} \frac{(W+Z)}{L} & \frac{Y}{L} \\ \frac{Z}{L} & \frac{(X+Y)}{L} \end{bmatrix}$$

where L = {(X+Y)(W+Z)}-YZ

M is generally defined as the fundamental matrix in which element m_{ij} is the average time spent in state j given that the system starts in state i before being absorbed. Since the system under study starts in state 0 and is absorbed in state 2,

$$MTTF_{\text{fault-tolerant}} = m_{00} + m_{01}$$

For the system under study in this research,

$$MTTF_{\text{fault-tolerant}} = \frac{Y+W+Z}{XW+XZ+YW}$$

Expanding again in terms of λ, μ and c:

$$MTTF_{\text{fault-tolerant}} = \frac{\lambda+\mu+2c\lambda}{[(2\lambda)(1-c)][\lambda+\mu]+[(2c\lambda)(\lambda)]}$$

This is the same expression found in [TRI 02]. Furthermore, if c=1, the model represents the classical 1-out-of-2 fault-tolerant system and

$$MTTF_{\substack{\text{fault-tolerant} \\ \text{c=1}}} = \frac{3\lambda+\mu}{2\lambda^2}$$

This is the same expression found in [BIL 83].

Improving MTTF can be done by one of the following two approaches, *Complex Approach* and *Brute Force Approach.*

This section shows how to use the Markov model to improve system MTTF in a cost-effective manner using brute force approach. Let the 2-machine fault-tolerant production line described above, have the following parameters:

λ_1: controller failure rate

μ_1: controller repair rate

c_1: coverage

Increasing MTTF can be achieved by decreasing λ_1, increasing μ_1, increasing c_1 or a combination of the above. A possible answer to this question can be obtained by using operations research techniques in order to obtain a triplet ($\lambda_{optimal}$, $c_{optimal}$, $\mu_{optimal}$) that will lead to the highest MTTF. Practically, however, it may not be possible to find a controller with the exact failure rate $\lambda_{optimal}$ and/or the coverage $c_{optimal}$. Also, it may be difficult to find a maintenance plan with $\mu_{optimal}$. Upon contacting the machine's manufacturer, the factory will be offered a few choices in terms of better software versions and/or better maintenance plans. Better software will improve λ and c; the maintenance plan will affect μ. As mentioned above, let the initial value of λ, μ and c be $\{\lambda_1, c_1, \mu_1\}$. Better software will change these values to $\{\lambda_j, c_j, \mu_1\}$ for $2 \leq j \leq n$. Here, n is the number of more sophisticated software versions. Practically, n will be a small number. Changing the maintenance policy will change μ_1 to μ_k for $2 \leq k \leq m$. Again, m will be a small number. In summary, system parameters $\{\lambda_1, c_1, \mu_1\}$ can only be changed to a small number of alternate triplets $\{\lambda_j, c_j, \mu_k\}$. If n=3 and m=2, for example, the number of scenarios that need to be studied is *(mn-1)*=5. Running the Markov model 5 times will produce 5 possible values for the improved MTTF. Each scenario will obviously have a cost associated with it.

Let $\psi = \dfrac{MTTF_{new} - MTTF_{old}}{cost}$

$MTTF_{old}$ is obtained by plugging (λ_1, c_1, μ_1) in the Markov model while $MTTF_{new}$ is obtained using one of the other 5 triplets. ψ represents the improvement in system MTTF with respect to cost. The triplet that produces the highest ψ is chosen.

In the complex approach, it is shown that λ, μ and c are not totally independent of each other. Let *Qs* be the quality of the software installed on the controller and let *Qop* represent the operator's expertise. A better version of the software (higher *Qs*) will affect all three parameters simultaneously. Obviously, a better version of the software will have a lower software failure rate, thereby lowering λ. Furthermore, this better version is expected to have more sophisticated error detection and recovery mechanisms. This will increase the coverage c. Finally, the diagnostics capabilities of the software should be enhanced in this better version. This will reduce troubleshooting time; decrease the Repair time and increase μ.

Another important factor is the operator's expertise *Qop*. The controller is usually an industrial PC [DAO 03]. The machine manufacturer may be able to supply the hardware and software failure rates but the operator's expertise has to be factored in the calculation of the controller's failure rate on site. The operator does not just use the controller to operate the machine but also uses it for HTTP, FTP, e-mail, etc, beneficiating of its capabilities as a PC. Operator errors (due to lack of experience) will increase the controller failure rate. An experienced operator will make fewer mistakes while operating the machines. Hence, λ will decrease. Furthermore, an experienced operator will require less time to repair a controller, i.e., μ will increase.

In summary, an increase in *Qs* produces a decrease in λ and an increase in c and μ. Also, an increase in *Qop* reduces λ and increases μ. Next, it is shown how to use *Qs* and *Qop* to calculate λ, μ and *c*.

The parameter λ can now be written as follows:

$$\lambda = \lambda_{hardware} + \lambda_{software} + \lambda_{operator}$$

The manufacturer determines $\lambda_{hardware}$. In general, let $\lambda_{software} = g(Qs)$. The function f is determined by the manufacturer. Alternatively, the manufacturer could just have a table indicating the software failure rate for each of the software versions. Similarly, let $\lambda_{operator} = g(Qop)$. The function g has to be determined on site.

For an exponentially-distributed repair time, μ will be the inverse of the Mean Time To Repair (MTTR). There are two cases to be considered here. First, the factory does not stock controller spare parts on premises. Upon the occurrence of a controller failure, the agent of the machine manufacturer imports the appropriate spare part. A technician may also be needed to install this part. Several factors may therefore affect the MTTR including the availability of the spare part in the manufacturer's warehouse, customs, etc. Customs may seriously affect the MTTR in the case of developing countries, for example; in this case the MTTR will be in the order of two weeks. In summary, if the factory does not stock spare parts on site, the MTTR will be dominated by travel time, customs, etc. The effects of *Qs* and *Qop* can be neglected.

Second, the factory does stock spare parts on site. If a local technician can handle the problem, the repair time should be just several hours. However, this does depend on the quality of the software and on the expertise of the technician. The better the diagnostic capabilities of the software, the quicker it will take to locate the faulty component. On the other hand, if the software cannot easily pinpoint the faulty component, the expertise of the technician will be essential to quickly fix the problem. If a foreign technician is needed, travel time has to be included in the repair time which will not be in the orders of several hours anymore. Let

$$\mu = P\{\text{foreign} - \text{tech}\}\mu_{\text{foreign}} + (1 - P\{\text{foreign} - \text{tech}\})\mu_{\text{local}}$$

μ_{local} is the expected repair time in case the failure is repaired locally. It is in the order of several hours. μ_{local} is obviously a function of *Qs* and *Qop*. Let $\mu_{local} = h(Qs, Qop)$. The function h has to be determined on site. If a foreign technician is required, travel time and the technician's availability have to be taken into account. $\mu_{foreign}$ should be in the order of days. Again, here, the travel time is expected to dominate the actual repair time on site;

in other words, the effects of *Qs* and *Qop* can be neglected. The probability of requiring a foreign technician to repair a failure can be calculated as a first approximation as the number of times a foreign technician was required in the near past. The coverage parameter c has to be determined by the machine manufacturer.

As in the previous section, the options are not numerous. The production manager will only have a few options to choose from. This approach is obviously more difficult to implement than the previous one. The determination of the function *f, g* and *h* is not an easy task. On the other hand, using these functions permits the incorporation of the effect of software quality and operator expertise on λ, *c* and μ. The Markov model is used again to determine the MTTF for each triplet (λ, *c*, μ) and ψ determines the most cost-effective scenario.

APPENDIX B

Msg ID	Name	Frequency	Class	Type
0	Crash_Sensor1	200	C	S
1	Crash_Sensor2	200	C	S
2	Crash_Sensor3	200	C	S
3	Spark_Output_Timing_Signal	200	C	C
4	ABS_Pump_Speed_Control	200	C	C
5	Wheel_Speed_Sensor1	200	C	S
6	Wheel_Speed_Sensor2	200	C	S
7	Wheel_Speed_Sensor3	200	C	S
8	Wheel_Speed_Sensor4	200	C	S
9	Stearing_Rotation_Rate_Sensor	200	C	S
10	Hydraulic_Stearing_Assist	200	C	C
11	Speed_Control_Signal	200	C	C
12	Clutch_Position_sensor	200	C	S
13	Crankshaft_Postion_Sensor	200	C	S
14	Profile_Ignition_Pickup	200	C	C
15	Brake_Position_Sensor	200	C	S
16	Break_Presure_Sensor	200	C	S
17	Rear_Wheel_Spin_Sensor1	100	C	S
18	Rear_Wheel_Spin_Sensor2	100	C	S
19	Linear_Height_Sensor1	100	C	S
20	Transmission_Speed_Sensor	100	C	S
21	Vehicle_Speed_Sensor	100	C	S
22	Accelerator_Position_Rate_Sensor	100	C	S
23	Trans_Clutch_Line_Press	100	C	S
24	Ignition_Diagnostic_Monitor	50	B	C
25	Cylinder_Id_Sensor	50	B	S
26	Manual_Lever_Position	50	B	S
27	Delta_Pressure_Feedback_Electronic	50	B	S
28	Heated_Exhaust_Gas_Oxygen_Sensor	50	B	S
29	Mass_Air_Flow_Sensor	50	B	S
30	Throttle_Postion_Sensor	50	B	S
31	Engine_RPM	50	B	S
32	Handbrale_Position_Sensor	10	B	S
33	Radio_Control_on_Steering	10	B	S

Msg ID	Name	Frequency	Class	Type
34	Battery_Current	10	B	S
35	Battery_Voltage	10	B	S
36	Shift_PRNODL_Sensor	10	B	S
37	Transmission_Oil_Temperature	10	B	S
38	A/C_Compressor_Clutch	10	B	S
39	Engine_Coolant_Temperature	10	B	S
40	Transmission_Lube_Pressure	10	B	S
41	Intake_Air_temperature	5	B	S
42	Suspension_Status	1	A	C
43	Outside_Temperature	1	A	S
44	Desired_Temperature	1	A	S
45	Cabin_Temperature	1	A	S
46	Rear_Window_Defrost	1	A	S
47	Blowe_Speed_Control	1	A	C
48	Damper_Control	1	A	C
49	Heat/Cool_Control	1	A	C
50	SET/ACCEL/RESUME	1	A	S
51	Cruise_Control_Indicator	1	A	C
52	Auto_Headlamp_Sensor	1	A	S
53	Ignition_Switch_Position	1	A	S
54	Horn_Sensor	1	A	S
55	Hazard_Sensor	1	A	S
56	L/R_Signal	1	A	S
57	Control_to_Tone_Maker	1	A	S
58	Oil_Pressure	1	A	S
59	Fuel_Level_Sensor	1	A	S
60	Alternator_Warning_Indicator	1	A	C
61	Octane_Adjust_Plug	1	A	S
62	Transmission_Control_Switch (OD)	1	A	S
63	Engine_Idle_Speed	1	A	S
64	Engine_Satus	1	A	C
65	Fuel_Flow	1	A	C
66	Transmission_Control_Indicator	1	A	C
67	EGR_Vaccuum_Regulator	1	A	C
68	Check_Engine_Indicator	1	A	C
69	ABS_Fluiud_Level_Sensor	1	A	S
70	Master_Brake_Fluid_Level_Sensor	1	A	S
71	Power_Locks	1	A	S
72	Power_Seats	1	A	S
73	Power_Windows	1	A	S
74	Shift_Inhibit_Signal	1	A	S
75	Shift_In_Progress	1	A	S
76	Seatbelt_Sensor	1	A	S
77	Door_Sensor1	1	A	S

o

Msg ID	Name	Frequency	Class	Type
78	Door_Sensor2	1	A	S
79	Door_Sensor3	1	A	S
80	Door_Sensor4	1	A	S
81	Door_Sensor5	1	A	S
82	Anti-theft_Sensor	1	A	S
83	ABS_Status_Lamp	1	A	C
84	ABS_Brake_Lamp	1	A	C
85	Airbag_Indicator_Lamp	1	A	C
86	Seatbelt_Lamp	1	A	C
87	Door_Lamps_ON/OFF	1	A	C
88	Airbag_Status	1	A	C
89	Washer_Fluid_Sensor	0.1	A	S

APPENDIX C

This appendix has more details regarding the IEEE STD 802.11.

The 802.11 legacy is the original version of WiFi (standard IEEE 802.11 released in 1997). It specifies two raw data rates of 1 and 2 megabits per second (Mbit/s or Mbps) to be transmitted via infrared (IR) signals or by either Frequency hopping or Direct Sequence Spread Spectrum (DSSS) in the Industrial Scientific Medical (ISM) frequency band at 2.4GHz. The original standard also defines Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as the medium access method.

A weakness of this original specification was that it offered so many choices that interoperability was sometimes challenging to realize. It is not a rigid specification, allowing individual product vendors the flexibility to differentiate their products. Legacy 802.11 was rapidly supplemented by 802.11b.

The 802.11a standard uses the same core protocol as the original standard, operates in the 5GHz band, and uses a 52-subcarrier Orthogonal Frequency Division Multiplexing (OFDM) with a maximum raw data rate of 54Mbit/s, which yields realistic net achievable throughput in the mid-20Mbit/s. Since the 2.4GHz band is heavily used, using the 5GHz band gives 802.11a the advantage of less interference. However, this high carrier frequency also brings disadvantages. It restricts the use of 802.11a to almost line of sight, necessitating the use of more access points; it also means that 802.11a cannot penetrate as far as 802.11b since it is absorbed more readily, other things (such as power) being equal.

The 802.11b has a maximum raw data rate of 11Mbps and uses the same CSMA/CA media access method defined in the original standard. Due to the CSMA/CA protocol

overhead, in practice the maximum 802.11b throughput that an application can achieve is about 5.9Mbps over TCP and 7.1Mbps over UDP. 802.11b is usually used in a point-to-multipoint configuration, wherein an access point communicates via an omni-directional antenna with one or more clients that are located in a coverage area around the access point. With high-gain external antennas, the protocol can also be used in fixed point-to-point arrangements, typically at ranges up to 8Km although some report success at ranges up to 80–120Km, where line of sight can be established. Extensions have been made to the 802.11b protocol in order to increase speed to 22, 33, and 44Mbps, but the extensions are proprietary and have not been endorsed by the IEEE. Many companies call enhanced versions "802.11b+". These extensions have been largely obviated by the development of 802.11g, which has data rates up to 54Mbps and is backwards-compatible with 802.11b.

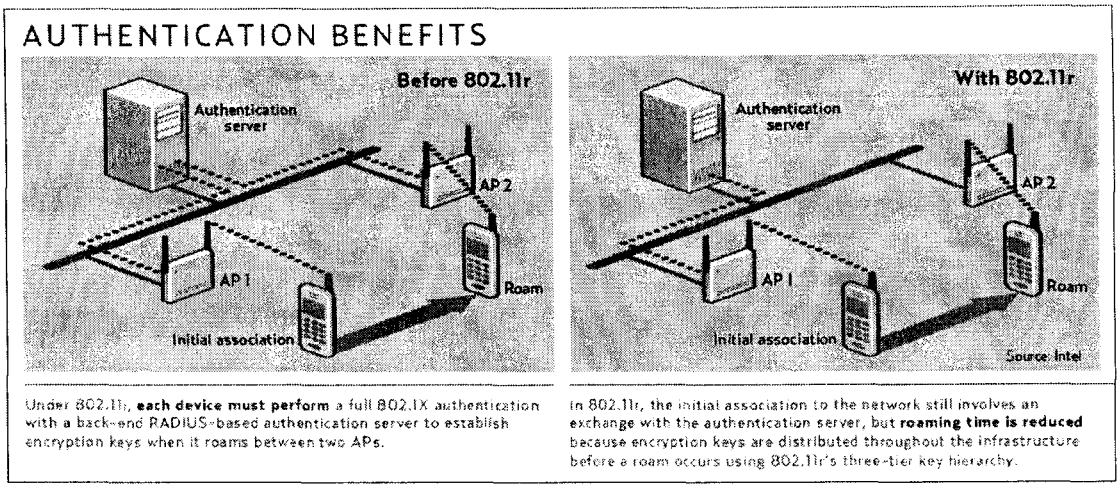
The 802.11g works in the 2.4GHz band (like 802.11b) but operates at a maximum raw data rate of 54Mbps, or about 24.7Mbps net throughput like 802.11a. 802.11g hardware will work with 802.11b hardware. The maximum range of 802.11g devices is slightly greater than that of 802.11b devices, but the range in which a client can achieve full (54Mbit/s) data rate speed is much shorter than that of 802.11b.

For 802.11n, the real data throughput is estimated to reach a theoretical 74Mbit/s.

802.11r provides security as well as QoS for fast roaming voice applications (roaming transitions of about 50ms). In other words it includes both 802.11i and 802.11e and takes into consideration VoIP restrictions [MOL 07].

802.11r includes a new mechanism to distribute security keys. This is a hierarchical method where the highest-level key holder (WLAN controller for example) is the only node having access to the original cryptography material and it is in charge to deliver keys to lower-level key holders (APs). The key derivation algorithm is based on a way to prevent the derivation of the master key using lover-level keys.

Regarding QoS considerations, 802.11r includes the option that a client requests QoS resource on a destination AP before performing roaming. This option was not present in the original 802.11 standard (figure).



The data link Layer in all 802 protocols is split into two or more sub-layers: Logical Link Control (LLC) and Media Access Control (MAC). In 802.11, the MAC sub-layer determines how the channel is allocated, meaning who gets to transmit next. Above it is the LLC sub-layer, whose job is to hide the differences between the different 802 variants and make them indistinguishable as far as the network layer is concerned. 802.11 uses the same 802.2 LLC and 48bit addressing as other 802 LANs, allowing very simple bridging from wireless to IEEE wired networks, but the MAC is unique in the WiFi. The 802.11 MAC is designed to support multiple users on a shared medium by putting the restriction that the sender must sense the medium before access. The inherent complexity of the wireless environment compared to that of a wired one is what makes the 802.11 MAC sub-layer quite different from that of the Ethernet.

For 802.3 Ethernet LANs [STD 3], the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol regulates how Ethernet stations establish access to the medium (wire). It also specifies how the stations detect and handle collisions that occur when two or more devices try to simultaneously communicate over the LAN. In an 802.11 WLAN, collision detection is not possible due to what is known as the "near/far" problem: to detect a collision, a station must be able to transmit and listen at the same time, but in radio systems the transmission drowns out the ability of the station to "hear" a collision.

To solve this problem, the 802.11 uses a modified version of the protocol known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Any station, working using CSMA/CA, wishing to send data senses the medium (air) first, and then checks if the medium is clear, i.e. no activity is detected (no other station is sending data on the medium). Having a clear medium, the station waits for an additional randomly selected period and rechecks if the medium is still free, it transmits the data. When the packet is received correctly, the receiving station issues an acknowledgment frame (ACK) that completes the process when received by the sender station. The ACK frame might not be received by the transmitting station due to either of two reasons: the original data packet was not received correctly or the ACK frame was not received correctly.

In either case, a collision is assumed to have happened and the data packet is retransmitted after waiting another random amount of time. Thus, CSMA/CA solves the problem of inability to detect collisions by providing a way of sharing access over the air. However, the disadvantage of this method is that the ACK frame adds an overhead to the WLAN which will make it always slower than an Ethernet.

Another MAC-layer problem specific to wireless is the "hidden node" issue, in which two stations on opposite sides of an access point can both "hear" activity from an access point, but not from each other, usually due to distance or an obstruction. This problem is illustrated in Fig. A.

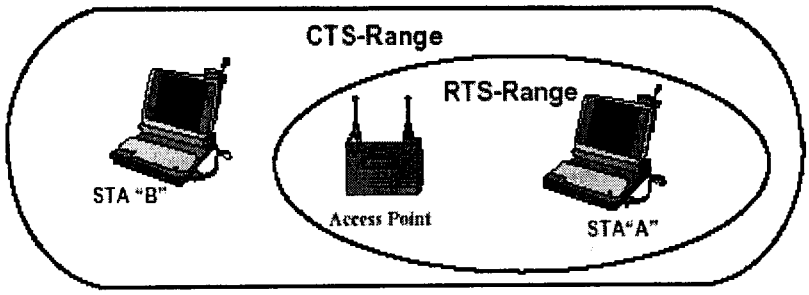


Fig. A, Hidden Node Problem and Solution RTS/CTS

To solve this problem, the 802.11 standard specifies an optional Request to Send/Clear to Send (RTS/CTS) protocol at the MAC layer. When this feature is activated, the sending station transmits an RTS signal and waits for the access point to reply with a CTS signal. Since all stations in the network can hear the access point, the CTS causes them to delay

any intended transmissions, allowing the sending station to transmit and receive a packet acknowledgment without any chance of collision. But again this adds another overhead on the network. Thus, to reduce its effect on the network, it is only used for large-sized packets because retransmission for these packets would be more costly than the RTS/CTS.

APPENDIX D

This appendix groups some simulation results that complement those presented in Chapter 4.

Figures A and B illustrates the results for a congested model simulation in MIPv4 for an IPT of 90sec. Fig. A shows the results for a MN moving at the high (maximum) speed of 60Km/hr. Fig. B presents the results when the MN is moving at the medium speed of 33Km/hr.

In both figures, the first graph is the AP connectivity chart: the vertical axis indicates the BSS number of the AP in communication with the MN. (-1) means that the MN is not connected to any AP. This happens during the break before make mechanism of the handoff. The second graph shows the traffic sent from the CN to the WNs in bytes per seconds. The last graph illustrates the received traffic by the MN again in bytes per seconds. In all graphs, the horizontal axis is the simulation time in minutes and seconds.

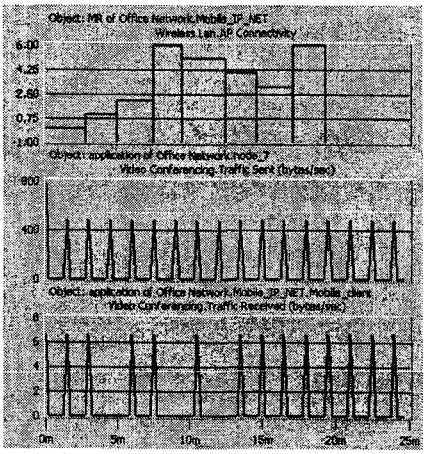


Fig. A, MN V=60Km/hr; IPT 90; MIPv4, Congested Model

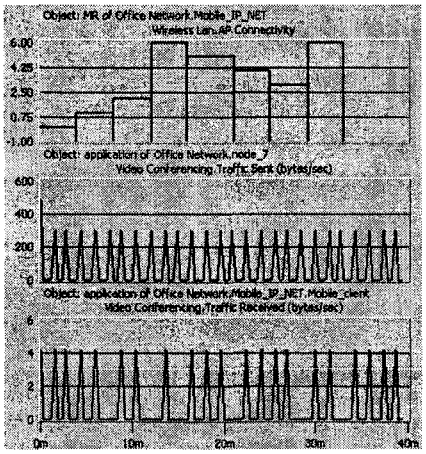


Fig. B, MN V=33Km/hr; IPT 90; MIPv4, Congested Model

Figures C and D show the simulation results for Burst Communication in MIPv4 congested model scenario. The MN speed in both figures is 33Km/hr. The number of packets per burst is 3. Fig. C shows that a complete burst loss is probable, while Fig. D shows that complete burst loss is less probable. Statistical analysis are presented in Chapter 4.

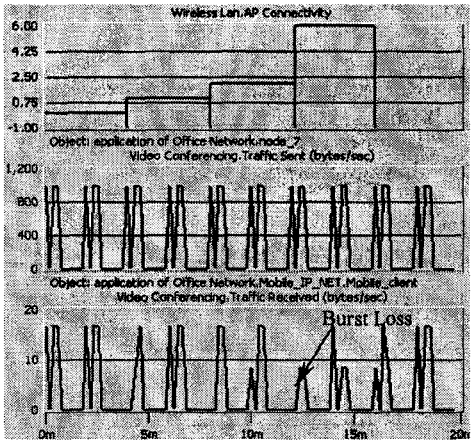


Fig. C, MN V=33Km/hr, MIPv4, t_{packet}=18sec, 3PB

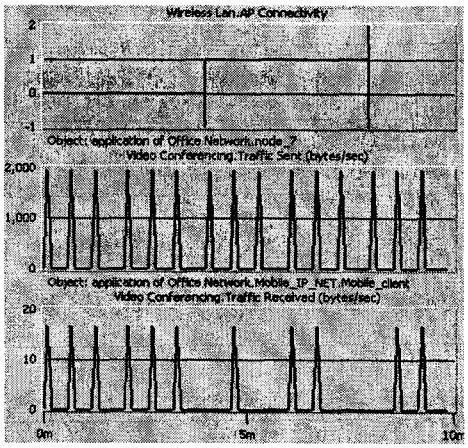


Fig. D, MN V=33Km/hr, MIPv4, t_{packet}=36sec, 3PB

In both figures, the first graph is the AP connectivity chart: the vertical axis indicates the BSS number of the AP in communication with the MN. The second graph shows the traffic sent from the CN to the WNs in bytes per seconds. The last graph illustrates the received traffic by the MN again in bytes per seconds. In all graphs, the horizontal axis is the simulation time in minutes and seconds.

Figures E illustrates the simulation results for MIPv6 MN moving at 33Km/hr and communicating with the CN with IPT 120sec in a congested scenario. It can be seen that the amount of packet loss is less than in the case of using MIPv4 as handoff mechanism.

The first graph is the AP connectivity chart. The second graph shows the traffic sent from the CN to the WNs in bytes per seconds. The last graph illustrates the received traffic by the MN again in bytes per seconds. In all graphs, the horizontal axis is the simulation time in minutes and seconds.

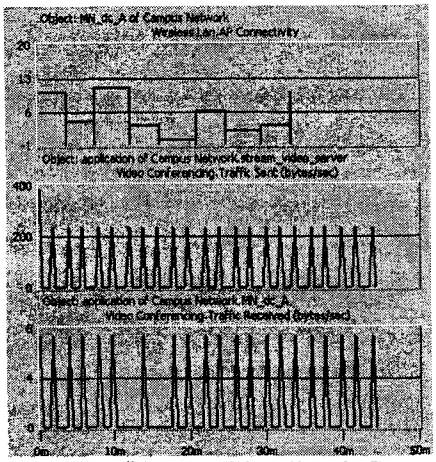


Fig. E, MN V=33Km/hr; IPT120; MIPv6, Congested Model

Figures F and G presents the simulation results for MIPv6 MN burst communication: 2-packet and 3-packet burst respectively. It is shown that for 3PB and t_{F2L}=36sec, complete burst loss occurs (Fig. G).

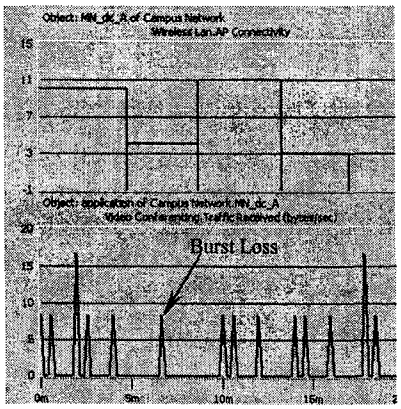


Fig. F, Complete Burst Loss in 2PB

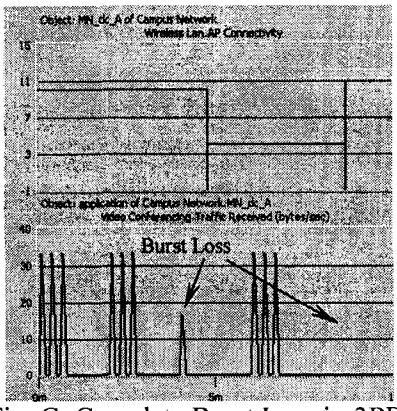


Fig. G, Complete Burst Loss in 3PB; t_{F2L}=36sec

The first graph is the AP connectivity chart. The second illustrates the received traffic by the MN in bytes per seconds. In the two graphs, the horizontal axis is the simulation time in minutes and seconds.

Figure H is produced during Fault-Tolerant AP simulations. It can be shown that the AP connectivity graph (the first graph) has -1 regions. This means that the MN is not

connected to any AP in the system. This is the result of the center AP (AR) failure. Although the AP-P_t=10mW, the blind area (due to no coverage) still exists. The second graph is shows the data sent from the CN to the WNs. The third graph indicates the data received at the MN. The horizontal axis in all three graphs is the simulation time in minutes and seconds.

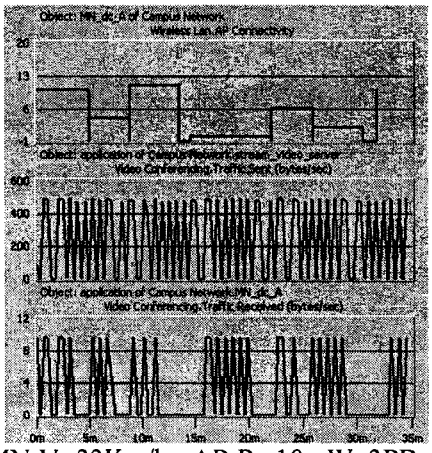


Fig. H, MN V=33Km/hr, AP-P_t=10mW, 3PB, 120/36-3

During the Protocol Comparison simulations, results of Fig. I illustrates the results for MN moving at 33Km/hr for 802.11g architecture and AP-P_t=4mW, while Fig. J shows the results for MN moving at 33Km/hr for 802.11g architecture and AP-P_t=80mW.

In both figures, the first graph is the data received in packets per seconds while the second is the AP connectivity. The horizontal axis is the simulation time.

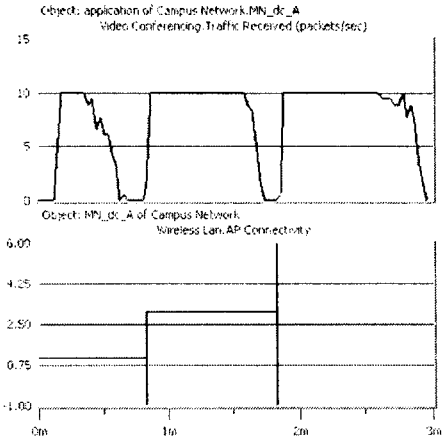


Fig. I, Traffic received in packets/second and AP connectivity for a mobile node moving at 33Km/hr in 802.11g architecture, transmit power 4mW

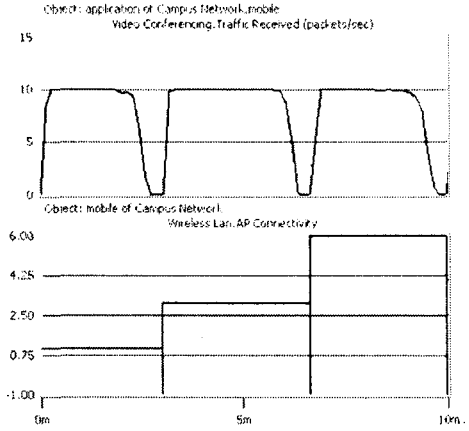


Fig. J, Traffic received in packets/second and AP connectivity for a mobile node moving at 33Km/hr in 802.11g architecture, transmit power 80mW

Bibliothèque Universitaire de Valenciennes
00900540