UNIVERSIDADE DO ALGARVE

IP/Optical Integration in Access Network Infrastructures: Key Issues on Resource Provisioning

José António Marques Coimbra

PhD thesis in Computer Science

Work done under the supervision of:
Prof. Dr. Noélia Correia

2013

UNIVERSIDADE DO ALGARVE

IP/Optical Integration in Access Network Infrastructures: Key Issues on Resource Provisioning

José António Marques Coimbra

PhD thesis in Computer Science

Work done under the supervision of:
Prof. Dr. Noélia Correia

2013

Statement of Originality

IP/Optical Integration in Access Network Infrastructures:
Key Issues on Resource Provisioning

Statement of authorship: The work presented in this thesis is, to the best of my knowledge and belief, original, except as acknowledged in the text. The material has not been submitted, either in whole or in part, for a degree at this or any other university.

Candidate:

____

(José António Marques Coimbra)

FCT
Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

This work had the financial support of Fundação para a Ciência e Tecnologia through the PhD grant SFRH/BD/37808/2007.

NETWORKING

Work done at Research Center of Electronics Optoelectronics and Telecommunications (CEOT)

To my parents: José Coimbra and Natália Coimbra.
Para os meus pais: José Coimbra e Natália Coimbra.

Acknowledgements

Completing a PhD is truly a journey, which I completed with the priceless help of many people. First and foremost, I would like to thank my supervisor Dr. Noélia Correia. Her mentorship was vital to keep me on track and motivated during these years. Working with her has been very enjoyable and fruitful. I look forward to keep working with her on possible future projects.

I would also like to thank Dr. Gabriela Schütz for her helpful input on many of my articles. It is always good to have a knowledgeable mathematician to work with and learn from.

This thesis would not have been possible without the support from Fundação para a Ciência e Tecnologia, through their funding of my doctoral years (scholarship reference: SFRH/BD/37808/2007). Also, I would like to thank the directors of Centro de Eletrónica, Optoeletrónica e Telecomunicações (CEOT), Dr. Henrique Gomes, Dr. Carmo Medeiros and Dr. Rui Guerra, for all the institutional support. A special thank to all the teachers, colleagues and friends from CEOT and Faculdade de Ciência e Tecnologia for all the interesting discussions and fun times. Namely, Dr. Álvaro Barradas, Dr. Peter Stallinga, Artur Neves, Ricardo Avó, Paulo Rocha, Mark Guerreiro, Hugo Amorim, Asal Kiazadeh, Bruno Romeira, Dr. José Figueiredo, Dr. Paula Laurêncio, Dr. Marielba Zacarias, Dr. Fernando Lobo... I am sorry if I forgot to name someone.

I would also like to thank my beloved wife, Adriana Santos. Thank you for all the love and care. You have been very patient with me for all the hours that I spent in front of the computer reading, writing and researching.

I owe a big part of what I am to my parents. One of the things they taught me, through example, is that achievements require hard work. To them I dedicate this thesis. Hope you are proud of me. The rest of my family, too numerous to name them all, has also been of great support to me. Thank you all. Specially my godson, whose happiness is truly contagious. Also, to my mother-in-law who always receives me at her home with great kindness.

At last but not least, I would like to thank all my friends for all the encouragement and fun times. Namely, Pedro Nave, Eva Oliveira, João Bispo, Jani Négrier, Ruben Gomes, Daniel Nunes, Emanuel Ramalho, Bianca Brito, Nina Vieira, Rui Afonso, Rui Cristina... and many others. I am sorry, it is just not possible to name you all.

Abstract

This thesis contributes to the advancement of Fiber-Wireless (FiWi) access technologies, through the development of algorithms for resource allocation and energy efficient routing. FiWi access networks use both optical and wireless/cellular technologies to provide high bandwidth and ubiquity, required by users and current high demanding services.

FiWi access technologies are divided in two parts. In one of the parts, fiber is brought from the central office to near the users, while in the other part wireless routers or base stations take over and provide Internet access to users. Many technologies can be used at both the optical and wireless parts, which lead to different integration and optimization problems to be solved. In this thesis, the focus will be on FiWi access networks that use a passive optical network at the optical section and a wireless mesh network at the wireless section. In such networks, two important aspects that influence network performance are: allocation of resources and traffic routing throughout the mesh section. In this thesis, both problems are addressed. A fair bandwidth allocation algorithm is developed, which provides fairness in terms of bandwidth and in terms of experienced delays among all users. As for routing, an energy efficient routing algorithm is proposed that optimizes sleeping and productive periods throughout the wireless and optical sections.

To develop the stated algorithms, game theory and networks formation theory were used. These are powerful mathematical tools that can be used to solve problems involving agents with conflicting interests. Since, usually, these tools are not common knowledge, a brief survey on game theory and network formation theory is provided to explain the concepts that are used throughout the thesis. As such, this thesis also serves as a showcase on the use of game theory and network formation theory to develop new algorithms.

Keywords: Fiber-Wireless Access Networks, Wireless Mesh Network, Bandwidth Allocation, Routing, Energy Efficiency, Game Theory, Network Formation Theory.

Resumo

Esta tese é uma contribuição para o desenvolvimento das redes de acesso. Mais especificamente, contribui para o avanço das redes de acesso híbridas *fiber-wireless* (FiWi) através do desenvolvimento de algoritmos para a alocação de recursos e para um encaminhamento de tráfego energeticamente eficiente. As redes de acesso FiWi usam uma mistura de tecnologias: tecnologia ótica, com capacidade para fornecer a elevada largura de banda requerida pelos novos serviços, e tecnologia sem fios (ou celular) para responder à ubiquidade exigida pelos utilizadores. Devido à sua flexibilidade e elevado potencial, este tipo de redes tem recebido muita atenção por parte da comunidade científica.

As redes de acesso FiWi possuem duas secções principais. Numa delas, a fibra ótica é trazida da central até à vizinhança dos utilizadores; na outra, roteadores sem fios ou estações de base espalhados por uma determinada área proporcionam aos utilizadores o acesso à Internet. Qualquer das secções pode incorporar várias tecnologias e o uso de diferentes combinações dessas tecnologias acaba por levantar diferentes problemas de integração. Esta tese foca-se em redes FiWi que exploram, numa das secções, uma rede ótica passiva, e na outra, uma rede em malha sem fios. Os pacotes que circulam neste tipo de redes em malha podem ter que passar por múltiplos roteadores, consumindo recursos em todos eles. Assim, tanto a alocação de recursos como o roteamento do tráfego pela rede em malha sem fios são componentes importantes para a obtenção de um bom desempenho, sendo ambas estudadas nesta tese.

Para estudar e melhorar as componentes descritas foram usadas ferramentas matemáticas, nomeadamente, teoria de jogos e teoria de formação de redes. Tratam-se de ferramentas com enorme potencial e que podem ser usadas para estudar e perceber como otimizar situações que envolvem vários agentes com interesses conflituosos. Embora maioritariamente utilizadas no domínio das aplicações económicas, são ferramentas suficientemente ágeis para utilização noutros terrenos, como já foi demonstrado, por exemplo, em trabalhos de biologia e de ciências da computação. No entanto, tratam-se de ferramentas pouco utilizadas no âmbito das redes de computadores e das telecomunicações, terreno onde ainda são pouco conhecidas. Por esse motivo é apresentada nesta tese uma breve explicação de todos os conceitos de teoria de jogos

e formação de redes que foram utilizados ao longo dos estudos efetuados. Deste modo, a partir dos exemplos nela descritos, a tese contribui também como ferramenta de estudo para quem precise de perceber como se resolvem problemas envolvendo agentes com conflitos de interesse e, com base nessas aquisições, desenvolver algoritmos para a obtenção dos resultados desejados, aplicáveis, neste caso, às redes FiWi.

Após a apresentação de todos os conceitos matemáticos utilizados, é apresentada uma primeira aplicação desses conceitos a uma rede FiWi onde todos os roteadores são agentes interessados, sobretudo, em encaminhar tráfego dos seus próprios utilizadores, ignorando tráfego pertencente a utilizadores conectados a outros roteadores. Isto significa que os roteadores não vão querer usar os seus recursos com utilizadores com os quais não estejam diretamente conectados. É desenvolvido um modelo matemático do problema baseado em teoria de jogos, e são extraídas as condições para que exista um equilíbrio onde os roteadores cooperam encaminhando tráfego uns dos outros.

Como já mencionado, a alocação inteligente de recursos é um dos fatores-chave para melhorar o desempenho das redes de acesso FiWi. Com o objetivo de conceber um algoritmo de alocação de largura de banda é desenvolvido um modelo baseado em teoria de jogos no qual os roteadores pretendem maximizar a quantidade de tráfego entregue com sucesso e minimizar a perda de pacotes. O objetivo de minimizar a perda de pacotes está relacionado com o facto de tais pacotes já terem consumido alguns recursos dos roteadores por onde passaram, recursos esses que terão sido desperdiçados ou, por outras palavras, não terão sido produtivos. Acresce que estes pacotes provocam ainda algum atraso no envio de outros pacotes. O modelo desenvolvido fornece as bases para um algoritmo de alocação de largura de banda eficiente e justo, isto é, onde todos os roteadores têm as mesmas oportunidades de acesso à largura de banda. Deste modo, os roteadores com mais tráfego não irão consumir todos os recursos, deixando os outros roteadores sem nenhuma largura de banda disponível. Para além de iguais oportunidades no acesso à largura de banda, o algoritmo é também capaz de fornecer tempos de espera equivalentes entre os utilizadores. Esta característica facilita a implementação de sistemas que forneçam qualidade de serviço. No entanto, se o fornecedor do serviço assim o desejar, é possível definir algum nível de desigualdade nas oportunidades de acesso através da configuração de um parâmetro.

Quanto ao encaminhamento de tráfego, primeiro é estudado o estabelecimento de rotas de modo a aumentar a eficiência energética e a quantidade de tráfego entregue com sucesso. Para tal é desenvolvido um modelo baseado em teoria de formação de redes cujo objetivo é perceber como podem ser estabelecidas as rotas de maneira a otimizar os tempos produtivos, aqueles

em que os dispositivos estão a enviar ou receber tráfego, e os tempos em *standby*, aqueles em que os dispositivos estão em modo de poupança de energia. Para ser possível contabilizar a energia consumida a abordagem adotada neste modelo foi diferente. Uma vez que a rede na secção sem fios é em malha, o tráfego pertencente aos utilizadores de um roteador influencia a energia consumida em todos os roteadores por onde esse tráfego passa. Assim, o roteador de origem (no caso de tráfego *upstream*) ou destino (no caso de tráfego *downstream*), deverá ser responsabilizado por parte da energia consumida nos roteadores por onde o seu tráfego é encaminhado. O modelo desenvolvido permite perceber quais as rotas que têm um impacto mais positivo na eficiência energética e, sempre que possível, que permitam aumentar a quantidade de tráfego entregue com sucesso. Com esse conhecimento foi possível desenvolver uma heurística para o estabelecimento de rotas eficientes tanto do ponto de vista energético como da entrega bem sucedida de tráfego. Este algoritmo consegue ser computacionalmente eficiente, uma vez que se dedica a otimizar os tempos produtivos e em *standby* nos dispositivos onde surte mais efeito.

Palavras chave: Redes de Acesso Híbridas de Fibra e Sem Fios, Redes Sem Fios em Malha, Alocação de Largura de Banda, Roteamento, Eficiência Energética, Teoria de Jogos, Teoria de Formação de Redes.

Contents

Statement of Originality **ii**

Acknowledgements **v**

Abstract **vi**

Resumo **vii**

Nomenclature **xvi**

1 Introduction **1**

1.1 Motivation and Scope 1

1.2 Objectives 2

1.3 Contributions 2

1.4 Thesis Outline 3

2 Game Theory **5**

2.1 Introduction 5

2.2 One-Stage Games 6

2.2.1 Normal and Strategic Form Representations 7

2.2.2 Dominated Strategies 8

2.2.3 Nash Equilibrium 10

2.2.4 Mixed Strategies 12

2.3 Dynamic Games 13

2.3.1 Nash Equilibrium and Backward Induction 14

2.4 Repeated Games 16

2.4.1 Finite-Horizon Games and Nash Equilibrium 16

2.4.2 Infinite-Horizon Repeated Games and Nash Equilibrium 17

2.5 Network Formation Theory 20

2.5.1 Network Structure 21
2.5.2 Network and Allocation Value 21
2.5.3 Formation Process 22
2.6 Summary 26

3 Fiber-Wireless Access Networks 27
3.1 Introduction 27
3.2 Enabling Technologies for FiWi Access Networks 28
3.2.1 Wireless Networks 28
3.2.2 Optical Access Networks 29
3.2.3 FiWi Topologies and Approaches Proposed in Literature 31
3.3 Network Model and Nomenclature 33
3.3.1 Independent Networks 34
3.4 Summary 36

4 Traffic Forwarding Game 37
4.1 Introduction 37
4.2 Repeated Game Model 38
4.2.1 Bandwidth Sharing 38
4.2.2 Stage Game 39
4.2.3 Repeated Game 42
4.3 Simulation 43
4.3.1 Simulation Setup 43
4.3.2 Analysis of Results 44
4.4 Conclusions 48
4.5 Summary 48

5 Fair Bandwidth Allocation Algorithm 49
5.1 Introduction 49
5.2 Game Theoretical Model 50
5.2.1 Players and Actions 50
5.2.2 Stage Payoff 53
5.2.3 Strategies and Repeated Game 55
5.3 Equilibrium 56
5.3.1 Nash Equilibrium 56

5.3.2 Plain Strategy and Proposed Algorithm 58
5.4 Simulation and Results 64
5.4.1 Simulation Setup 64
5.4.2 Results Discussion 67
5.5 Conclusions 72
5.6 Summary 72

6 Energy Efficient Routing Algorithm 73
6.1 Introduction 73
6.2 Routing through Network Formation 74
6.2.1 Network Formation Processes 76
6.3 Energy Efficient Routing Model 79
6.3.1 Energy Consumption 79
6.3.2 Network Model 83
6.4 Comparison of Network Formation Processes 84
6.4.1 Simulation Setup 84
6.4.2 Analysis of Results 85
6.4.3 Computational Time 90
6.5 Network Formation Heuristic Algorithm 92
6.5.1 Heuristic Algorithm 92
6.5.2 Simulation and Results 94
6.6 Conclusions 101
6.7 Summary 101

7 Conclusions and Future Work 102
7.1 Conclusions 102
7.2 Future Work 103

References 104

List of Publications 113

List of Figures

2.1 Forwarder's dilemma representation. 6
2.2 Difference between two alternative iterative eliminations of weakly dominated strategies. 10
2.3 Two stage version of the forwarder's dilemma. 14
2.4 Example of a dynamic game. 15
2.5 Backward induction technique applied to the game in Figure 2.4. 16
2.6 Illustration of the min-max and feasible payoffs. 20
2.7 Network example with $\mathcal{P} = \{1, 2, 3\}$, $\mathcal{L}^E = \{13, 23\}$ and $\mathcal{L}^T = \{12, 13, 23\}$. 21

3.1 FiWi access network composition. 32
3.2 FiWi access network example. 35

4.1 Independent networks created by the shortest paths calculation. 40
4.2 Impact on δ when cooperating or defecting cooperation levels are increased. . 47

5.1 FiWi access network example. 50
5.2 Example of the sharing levels for a gateway router. 52
5.3 Generic independent network. 59
5.4 Upward procedure of the bandwidth allocation algorithm, executed on a router upon arrival of a REQUEST message. 62
5.5 Downward procedure of the bandwidth allocation algorithm, executed on a router upon arrival of a RESPONSE message. 63
5.6 Simulated independent networks. 65
5.7 Node modules implemented in simulation. 66
5.8 Average throughput ratio obtained by FIFO, proposed algorithm and WFQ. . 67
5.9 Comparison of packet average time in queue obtained by the proposed algorithm and WFQ. 68

5.10 Effect of the weight increase of over demanding nodes relative to the weight of less demanding nodes in terms of average waiting time in queue and throughput ratio. 69
5.11 Average throughput ratio experienced by the less demanding nodes when a different number of over demanding nodes exist. 70
5.12 Average throughput ratio experienced by the less demanding nodes in the various independent networks tested. 71
5.13 Example of the protection provided to less demanding nodes at the moment of the load increase by an over demanding node. 71

6.1 Average results of the tested formation processes and SP. 86
6.2 Effect that the parameter ϵ of SNF has on network value, energy efficiency and allocation ratio. 87
6.3 Effect that the number of wireless routers per gateway routers has on network value, energy efficiency and bandwidth allocation. 89
6.4 Effect that the tested loads have on network value, energy efficiency and bandwidth allocation ratio. 90
6.5 Percentage of uplink changes made by the second stage of FNF, which involved at least one node that belongs to: *i*) the component with the highest average traffic load; *ii*) the component highest average node degree; *iii*) the components with either the highest average traffic load or highest average node degree. . . 91
6.6 Illustration of dependency set. 93
6.7 Heuristic algorithm to update uplink connection of $i \in \mathcal{R}$. 95
6.8 Comparison between heuristic algorithm, DNF and FNF. 96
6.9 Effect that the number of wireless routers per gateway router has on the heuristic algorithm results in terms of network value, energy efficiency and bandwidth allocation. 97
6.10 Effect that the tested loads has on the heuristic algorithm in terms of network value, energy efficiency and bandwidth allocation. 98
6.11 Average time that DNF, FNF and HA take until no more path changes are made. 99

List of Tables

2.1 Forwarder's dilemma in normal form. 7
2.2 Example of a game with one strongly dominated strategy, taken from [29]. . . 9
2.3 Game from Table 2.2 with the strongly dominated strategy eliminated. 9
2.4 Example of a game with weakly dominated strategies. 10
2.5 Example of a game without dominated strategies, taken from [29]. 11
2.6 Example of a game without pure Nash equilibrium, taken from [37]. 12
2.7 Normal form equivalent for the game in Figure 2.4 15

4.1 Strategy profiles in equilibrium. 45

6.1 Parameters of generated networks. 84
6.2 Energy consumption during one byte time. 85
6.3 Average number of hops of the paths obtained by the several formation processes and SP. 88

Nomenclature

Abbreviations

10G-EPON	10 Gigabit EPON
4G	Fourth Generation
Al-C	Always Cooperate
Al-D	Always Defect
ATM	Asynchronous Transfer Mode
ATFT	Anti-Tit-For-Tat
CO	Central Office
DBA	Dynamic Bandwidth Allocation
DNF	Dynamic Network Formation
DSL	Digital Subscriber Line
DWDM-PON	Wavelength Division Multiplexing PON
EPON	Ethernet PON
FIFO	First In First Out
FiWi	Fiber-Wireless
FNF	Farsighted Network Formation
FTTB	Fiber To The Building
FTTC	Fiber To The Cabinet
FTTH	Fiber To The Home
FTTX	Fiber To The Premises
GPON	Gigabit PON
GT	Grim Trigger
GW	Gateway Router
HA	Heuristic Algorithm
HDTV	High-Definition Television

IEEE	Institute of Electrical and Electronics Engineers
IMT-Advanced	International Mobile Telecommunications-Advanced
IP	Internet Protocol
IPTV	Internet Protocol Television
ITU-T	International Telecommunications Union, Telecommunication Standardization Sector
LSA	Link State Advertisement
LR-PON	Long Reach PON
LTE	Long Term Evolution
MAC	Media Access Control
MIMO	Multi-Input Multi-Output
MPCP	Multi-Point Control Protocol
OFDM	Orthogonal Frequency Division Multiplexing
OLT	Optical Line Terminal
ONU	Optical Network Unit
PDV	Packet Delay Variation
PON	Passive Optical Network
QoS	Quality of Service
RoF	Radio over Fiber
SFNet	San Francisco Network
SNF	Stochastic Network Formation
SP	Shortest Path
TDMA	Time Division Multiple Access
TFT	Tit-For-Tat
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WDM	Wavelength Division Multiplexing
WDM-PON	Wavelength Division Multiplexing PON
WFQ	Weighted Fair Queuing
WiMAX	Worldwide Interoperability for Microwave Access
WMN	Wireless Mesh Networks
WR	Wireless Router
WRR	Weighted Round Robin
XG-PON	10 Gigabit GPON

Sets

Ω	Strategic game representation.
$\mathcal{P}$	Set of players in a game.
$\mathcal{V}$	A subset of all players, $\mathcal{V} \subseteq \mathcal{P}$.
$\mathcal{S}$	Set of all strategy profiles in a game.
$\mathcal{S}_i$	Set of strategies available to player i.
Σ	Set of all mixed strategy profiles in a game.
Σ_i	Set of mixed strategies available to player i.
$\mathcal{U}$	Set of utility functions.
$h\left(t\right)$	Set of all actions prior to stage t.
$\mathcal{L}^E$	List of all established connections among players in $\mathcal{P}$, also termed network or network structure.
$\mathcal{L}^T$	List of all possible connections among players in $\mathcal{P}$.
$\mathcal{L}$	Set of all possible networks, i.e. all possible $\mathcal{L}^E$.
$\mathcal{P}^{\mathcal{L}^E}$	Set of all players with at least one established connection, $\mathcal{P}^{\mathcal{L}^E} = \left\{i \middle| \exists ij \in \mathcal{L}^E, j \neq i\right\}$.
$\mathcal{C}^{\mathcal{L}^E}$	Set of all components in network $\mathcal{L}^E$.
$\Pi^{\mathcal{L}^E}$	Set of all components plus players without any connection, $\Pi^{\mathcal{L}^E} = \mathcal{C}^{\mathcal{L}^E} \cup \left\{i \middle| i \notin \mathcal{P}^{\mathcal{L}^E}\right\}$.
$\mathcal{G}$	Set of all gateway routers in a FiWi access network.
$\mathcal{R}$	Set of all wireless routers in a FiWi access network.
$\mathcal{W}$	Set of all wireless nodes, $\mathcal{W} = \mathcal{G} \cup \mathcal{R}$.
$\mathcal{O}$	Set of all ONUs in a FiWi access network.
$\mathcal{N}$	Set of all nodes in a FiWi access network, $\mathcal{N} = \mathcal{O} \cup \mathcal{W}$.
Γ_i^+	All descendants of node i, considering an independent network.
Γ_i^-	All ancestors of node i, considering an independent network.
γ_i^+	Set of children of a node i, i.e. the nodes immediately below i, considering an independent network in particular.
γ_i^-	Parent node of node i, considering an independent network in particular.
$\mathcal{F}$	Set of forwarding wireless routers, $\mathcal{F} = \left\{i \middle| \gamma_i^+ \neq \emptyset\right\}$.
μ^j	Set of cooperation levels of gateway j at stage t.
$\mathcal{D}_i$	Dependency super-set of wireless router i.

Set elements

s	A strategy profile.
s_i	A strategy being used by player i.
a^{PR}	Prescribed cooperating action profile of the plain strategy.
a^i	Punishment action profile used to punish player i.
σ	A mixed strategy profile.
σ_i	A mixed strategy being used by player i.
ij	A connection between player i and player j.

Variables

br_i	Best response function of player i.
u_i	Utility function of player i in a one-stage game.
U_i	Discounted utility function of player i in a repeated game.
Υ	Value function, used to calculate the network value.
υ_i	Allocation rule, used to assign values to every player i.
δ	Discounting factor used in the discounted utility function.
$\underline{u_i}$	Min-max payoff of player i.
t	Stage in a repeated game or iteration in a formation process.
θ_i	Cooperation level of forwarding router i.
μ_i^j	Cooperation level of gateway j, applied to traffic belonging to wireless router i.
cap_i	Highest attainable byte rate between node $i \in \mathcal{R}$ and γ_i^-. For $i \in \mathcal{G}$, cap_i is the attainable byte rate of the optical link.
α^i_j	Sharing level of wireless node i representing the fraction of cap_i that is reserved for local traffic of wireless node $j \in \gamma_i^+$.
$\alpha^i_{\Gamma^+_j}$	Sharing level of wireless node i representing the fraction of cap_i that is reserved for foreign traffic of wireless node $j \in \gamma_i^+$.
$\alpha^i_{j\cup\Gamma^+_j}$	Sharing level of wireless node i representing the fraction of cap_i that is reserved for local and foreign traffic of wireless node $j \in \gamma_i^+$, $\alpha^i_{j\cup\Gamma^+_j} = \alpha^i_j + \alpha^i_{\Gamma^+_j}$.
$\alpha^i_{\Gamma^+_i}$	Sharing level of wireless node i representing the fraction of cap_i that is reserved for its foreign traffic, $\alpha^i_{\Gamma^+_i} = \sum_{j\in\gamma_i^+}\left[\alpha^i_{j\cup\Gamma^+_j}\right]$.
χ^i	Trust level that wireless node i applies to its local traffic.

ψ_j^i	Trust level that wireless node i applies to the local traffic of wireless node $j \in \gamma_i^+$.
$\psi_{\Gamma_j^+}^i$	Trust level that wireless node i applies to the foreign traffic of wireless node $j \in \gamma_i^+$.
η_i	Drop component of wireless node i, which represents the resources wasted by packets that were dropped.
η_i^{th}	Drop component threshold of wireless node i, which represents the maximum allowed waste of resources due to packet drops.
e_i^{DLV}	Energy consumed to deliver traffic belonging to i.
e_i^{SLP}	Sleep energy consumed at i and nodes in Γ_i^- that i is held accountable for.
e_i^{UNP}	Unproductive energy consumed at i and nodes in Γ_i^- that i is held accountable for.
e_i	Energy consumed by all transceivers in order to send and receive traffic belonging to wireless node i.
E^O	Energy per byte time that is consumed by the transceiver of an ONU in wake mode.
E^T	Energy per byte time that is consumed by a wireless radio in transmit mode.
E^R	Energy per byte time that is consumed by a wireless radio in receive mode.
E_i^S	Energy per byte time that is consumed by the transceiver of a node i in sleep mode.
E_i^W	Energy per byte time that is consumed by the transceiver of a node i when waking up.
h_i	Number of hops between wireless router i and the gateway to which i is associated.
τ_i^S	Average number of byte times per second that a node i spends in sleep mode.
τ_i^W	Average number of byte times per second that a node i takes to wake up.
τ_i^{UR}	Average number of byte times per second that the radio of a wireless node i spends in receive mode without receiving traffic. That is, unproductive time while in receive mode.
τ_i^{UT}	Average number of byte times per second that the radio of a wireless node i spends in transmit mode without actually transmitting traffic. That is, unproductive time while in transmit mode.
τ_i^{UW}	Average number of byte times per second that the optical transceiver of the ONU i spends in wake mode without actually transmitting or receiving any traffic. That is, unproductive time in wake mode.
d	Average node degree in a network.
ϵ	Probability parameter given to the stochastic network formation.
I	Number of iterations run by the first stage of the stochastic network formation.
M	Maximum number of simultaneous uplink changes of the farsighted network formation.
t_{DNF}	Execution time (seconds) of the dynamic network formation.
t_{FNF}	Execution time (seconds) of farsighted network formation.

t_{HA}	Execution time (seconds) of the heuristic algorithm.
P	Average power (Watts) used during the execution of the formation process.
ρ_{DNF}	Joules per byte sent/received when the dynamic network formation was used to establish the routes.
ρ_{FNF}	Joules per byte sent/received when the farsighted network formation was used to establish the routes.
ρ_{HA}	Joules per byte sent/received when the heuristic algorithm was used to establish the routes.
ζ_i^{DNF}	Bandwidth allocation of wireless node i obtained with the routes established by the dynamic network formation.
ζ_i^{FNF}	Bandwidth allocation of wireless node i obtained with the routes established by the farsighted network formation.
ζ_i^{HA}	Bandwidth allocation of wireless node i obtained with the routes established by the heuristic algorithm.
ϕ	A certain amount of bytes sent/received by all wireless nodes.
B_i^d	Downstream local traffic (amount of bytes) destined to wireless node i.
β_i^d	Byte rate required by downstream local traffic of wireless node i.
B_i^{d*}	Downstream local traffic (amount of bytes) destined to wireless node i that successfully reached the destination.
B_i^u	Upstream local traffic (amount of bytes) sent by wireless node i.
β_i^u	Byte rate required by upstream local traffic of wireless node i.
B_i^{u*}	Upstream local traffic (amount of bytes) sent by wireless node i that successfully reached the optical link.
B_i	Downstream and upstream local traffic (amount of bytes) belonging to wireless node i, $B_i = B_i^d + B_i^u$.
β_i	Byte rate required by downstream and upstream local traffic of wireless node i, $\beta_i = \beta_i^d + \beta_i^u$.
B_i^*	Downstream and upstream local traffic (amount of bytes) belonging to wireless node i that successfully reached the destination, $B_i^* = B_i^{d*} + B_i^{u*}$.
β_i^*	Byte rate for downstream and upstream local traffic of i, after applying the trust level χ^i.
$B^*_{\Gamma_i^+}$	Downstream and upstream foreign traffic forwarded by wireless node i.
$\beta^*_{\Gamma_i^+}$	Byte rate for downstream and upstream foreign traffic of i, after applying the trust levels ψ_j^i and $\psi^i_{\Gamma_j^+}$, $\forall j \in \gamma_i^+$.

β_i^A	Bandwidth allocation at node i for its local traffic.
$\beta_{\Gamma_i^+}^A$	Bandwidth allocation at node i for foreign traffic.
g_i	Gain function of wireless node i.
c_i	Cost function of forwarding router i.

CHAPTER 1

Introduction

1.1 Motivation and Scope

Bandwidth requirements of multimedia services have been constantly growing and, as a result, current copper based access technologies will no longer be able to cope with the needed requirements [1, 2]. Optical fiber was chosen as the preferred medium to replace copper wires. The reason behind this preference is related with its huge bandwidth capacity and long range communication without needing amplifiers or signal regenerators [1, 2]. As such, many optical access networks have already been installed, either to replace older copper installations or in new installations where no network infrastructures existed before [3–5].

Passive optical networks (PONs) are the most common optical access networks, either Ethernet PONs (EPONs) or Gigabit PONs (GPONs). These technologies provide the needed bandwidth for demanding services such as the internet protocol television (IPTV), high-definition television (HDTV), voice over internet protocol (VoIP) and Internet, all coexisting and being served by the same network structure [3–6]. Moreover, these protocols are future proof and new generations of these technologies are under heavy development, which will coexist with current PON installations [7–12].

Albeit all the advantages of optical fiber, users also want Internet access everywhere and fiber can not provide it. One possible solution is to combine fiber with wireless or cellular technologies. This way, high bandwidth and ubiquity will be provided [13–15]. These networks are termed Fiber-Wireless (FiWi) access networks and have been receiving considerable research attention in recent years due to their potential. In these cross-domain access networks, the optical and wireless domains can have different levels of integration [15–19]. Nevertheless, all FiWi access networks are divided in two parts. The first part is termed back end, which is where fiber is brought from the central office (CO) to near the users. From there, at the front end, wireless routers or base stations take over, providing Internet access to users. Many different technologies can be used at both front and back end. The most common approach is to use a PON at the back end and 802.11, worldwide interoperability for microwave access (WiMAX) or long term evolution (LTE) at the front end [14, 16].

This thesis focuses on studying and contributing to the state of the art of FiWi access networks with a wireless mesh front end. Such front end provides great flexibility in terms of coverage, bandwidth allocation and routing, which is exploited in this thesis [14, 15]. For instance, in such front end, packets may have to travel through several wireless hops before they reach the optical link at the back end. Two major building blocks to increase the performance on such networks are the design of efficient routing schemes and the design of efficient packet scheduling policies [14, 15]. To pursue such demand, game theory and network formation theory were used. These are powerful mathematical tools that have been extensively used in many other fields but have rarely been used in network communications research. However, they can also be applied to communication networks, FiWi access networks in our case, to help solve problems and improve the performance [20, 21].

1.2 Objectives

This thesis is intended to contribute to the advance of FiWi access networks by:

- Showcasing the use of game theory and network formation theory as powerful mathematical tools to help in the analysis of several problems and development of new algorithms.
- Developing a bandwidth allocation algorithm that provides fairness both in terms of bandwidth and delays to all wireless routers. Such fairness among users opens way for traffic differentiation and quality of service (QoS) provisioning.
- Developing an energy efficient routing algorithm. Such algorithm tries to choose the routes that most optimize active and sleeping periods at all nodes in order to improve the number of bytes sent/received per each Joule consumed.

1.3 Contributions

Several research articles have been published or are being finalized as a result of the work developed in this thesis. In [22], it is shown how repeated game theory can be used as a framework for the development of algorithms to be applied in communication networks. Game theory is usually used as an analytical tool, however, in this article, its potential as a tool to help in the development of algorithms is highlighted and explored.

The object of study in this thesis is the FiWi access network technology. Lately, much attention is being devoted to such networks, due to their high bandwidth, ubiquity and flexibility. In [23] a survey on FiWi access networks is presented along with all the enabling technologies. That is, current and developing optical, wireless and cellular technologies are surveyed in order to understand their importance and potential when used together in FiWi access networks.

In [24, 25], game theory was applied to the problem of traffic forwarding in FiWi access networks where every wireless router is a selfish player mainly interested in forwarding traffic that belongs to its directly connected users. Nash equilibrium was then obtained, as well as the necessary conditions for such equilibrium to occur. These articles served as an initial study on how to apply game theory concepts to FiWi access networks.

Besides predicting outcomes, game theory can also be used as a framework to develop new algorithms. In [26], game theory was used to help in the development of a fair bandwidth allocation algorithm. The algorithm is efficient and is able to provide fairness among all wireless nodes, both in terms of access to bandwidth and experienced delays. Such fairness is important because it opens way to the QoS provisioning that new services require.

Energy efficiency has also been receiving much attention by the research community. In [27, 28], the establishment of energy efficient routes is studied through network formation theory. Instead of taking into consideration the total energy expenditure, it was decided that the average amount of sent/received bytes per Joule would be the focus. Insights are given on how energy efficiency can be improved by establishing routes that optimize active and sleeping periods. In [28], the work from [27] is improved and more energy efficient methods are proposed, including an heuristic algorithm.

More details on the contributions will be given in every chapter.

1.4 Thesis Outline

This thesis consists of seven chapters. Chapter 1 introduces the motivation for this work, clarifies what is the scope, states the objectives, exhibits the contributions and details the outline.

Chapter 2 presents theoretical concepts that are used throughout. More specifically, game theory and network formation theory. Note that, only the needed concepts to understand the forthcoming chapters are given in order to avoid an extensive exposure of concepts.

Chapter 3 introduces FiWi access networks. It starts by introducing the current state of the art of optical and wireless networks. Afterwards, the attention is focused on FiWi access networks, i.e. on the different integrations considered and architectures proposed in the literature.

Chapter 4 shows a direct application of game theoretical concepts to a FiWi access network. Nash equilibrium is derived along with the necessary conditions. This chapter is based on the work published in [24, 25].

Chapter 5 presents the development of a fair bandwidth allocation algorithm. In order to achieve that goal, a repeated game model was created to serve as a basic structure. This chapter is based on the work published in [26].

Chapter 6 studies energy efficient routing and develops a heuristic algorithm for the establishment of such efficient routes. A network formation model is presented, which is used to gain insights on how energy efficient routes can be established. Based on the obtained insights, a heuristic algorithm is then developed to establish energy efficient routes with a small execution time. This chapter is based on the work published in [27, 28].

Chapter 7 finalizes the thesis with some conclusions and presents some topics for future work.

CHAPTER 2

Game Theory

2.1 Introduction

Game theory is a mathematical tool that can be used to study situations with two or more agents with conflicting interests. That is, it allows to predict the outcome of situations where individual decisions can influence other agents. Game theory has mainly been used for economical studies and practical decision-making [29]. It has also been applied in many other fields such as biology or, more recently, computer science and computer networks [20, 29]. Moreover, it laid down the foundations for modern disciplines such as mechanism/market design and algorithmic game theory [30, 31]. In computer networks, it can be used to model and study situations where different devices have different interests that may affect each other. Various kinds of problems can be modeled for analytical purposes or to act as a support model for algorithm development [20, 32, 33].

In this chapter, an introduction to game theory and network formation is given. Only the concepts needed to understand the forthcoming chapters are introduced, in order to avoid an excessively and unnecessarily exposure of concepts. The next section starts by introducing one-stage games and how the outcome of a game can be predicted. Afterwards, in Section 2.3, games composed of many stages are presented and their differences from the one-stage games are highlighted. In Section 2.4, finite-horizon and infinite-horizon repeated games are explained, as well as how the predicted outcome of an infinite-horizon repeated game can be different from the finite-horizon equivalent. The chapter ends with a short summary of all the introduced notions.

Contributions:

i) Survey on game theory and network formation theory.

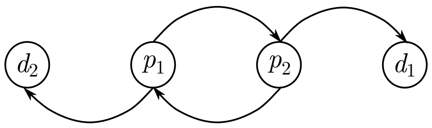


Figure 2.1: Forwarder's dilemma representation.

Publications:

The work in this chapter is to be published in [22].

2.2 One-Stage Games

As aforementioned, game theory can be used to model and study situations where agents have conflicting interests. One example of such a situation is the widely known *prisoner's dilemma*, which is usually presented as follows [29]. Two men are arrested, but the police does not have enough information for them to be convicted. Both prisoners are then interrogated separately and at the same time. Each prisoner can choose to stay silent or betray the other. If both stay silent, both will go to prison for just 1 month. If one prisoner betrays the other, while the other stays silent, then the silent prisoner goes to prison for 12 months and the betrayer goes free for cooperating with the police. Finally, if both prisoners betray each other, then both will go to prison for 3 months. The question is what will prisoners do, assuming that none of them can be sure if the other will betray or stay silent. If both stay silent, both get a minor sentence of one month. However, each prisoner may feel tempted to betray the other in order to be freed. As a result, both may end up betraying each other. Hence the dilemma.

In [34], a conceptually similar version of the prisoner's dilemma is presented. It is called the *forwarder's dilemma* and will be used throughout this chapter to help explaining some definitions. The game can be explained as follows. There are two players, router p_1 and router p_2, that want to send a packet to d_1 and d_2, respectively. As shown in Figure 2.1, for d_1 to receive the packet from p_1, p_2 will have to cooperate and forward the packet. Conversely, the same applies for the packet from p_2 sent to d_2. If a packet reaches its destination, then the player who sent it receives a payment of 1. A player that chooses to forward the packet of the opponent is incurred a cost of C, where $0 < C << 1$. This cost represents the consumption of resources to forward foreign traffic.

The question is whether or not players in the forwarder's dilemma will cooperate with each other by forwarding packets. If both players cooperate, then both will receive a payoff of $1-C$. However, a player might feel tempted to defect in order to receive a payoff of 1, which is

Table 2.1: Forwarder's dilemma in normal form.

		p_2: F	p_2: D
p_1	F	$(1-C, 1-C)$	$(-C, 1)$
	D	$(1, -C)$	$(0, 0)$

the highest payoff in this game, leaving a payoff of $-C$ for the opponent. In non-cooperative one-stage games, it is assumed that players decide at the same time what will be their actions without any communication or coordination among them. That is, neither of the players knows beforehand what will the the action of the opponent. As a safe precaution, both players might defect by not forwarding the packet of the opponent. This way, a defecting player can rest assured that at least he will not receive a negative payoff, $-C$. However, both could receive a higher payoff by cooperating. Hence the dilemma.

2.2.1 Normal and Strategic Form Representations

Games can be represented in many different forms. One of the most common is the *normal form* representation, which is very useful for simple games with two players and only a few available actions to each player [29,35]. This representation consists of a table, where the lines represent the strategies of one player and the columns represent the strategies of the other player. The cell that results from the intersection of the row and column contains the payoffs that both players will receive. Considering the just presented forwarder's dilemma, there are two players, p_1 and p_2, which can forward or drop the packet, represented by F and D, respectively. The normal form representation of the forwarder's dilemma is shown in Table 2.1. The rows represent the actions available to p_1, while the columns represent the actions available to p_2. As already told, the cell resulting from the chosen line and column contains the payoffs that both players will receive. For instance, if p_1 forwards and p_2 drops the packet, then the resulting cell contains $(-C, 1)$, which means that p_1 receives a payoff of $-C$ and p_2 receives a payoff of 1. The tuple including the strategy chosen by each player is called *strategy profile*. In the example just used, where p_1 forwards and p_2 drops, the strategy profile is (F, D).

The normal form representation is good for simple examples, however, for games with many players and multiple strategies, it is impossible to use the normal representation. For those cases, the *strategic form* is the most suited. In this form, a game is represented by $\Omega = \{\mathcal{P}, \mathcal{S}, \mathcal{U}\}$, where $\mathcal{P}$ represents the set of players, $\mathcal{S}$ represents the set of all strategy profiles and $\mathcal{U}$ represents the set of utility functions, explained next [29,34,35].

The set of all strategy profiles can be obtained by $\mathcal{S} = \times_{i \in \mathcal{P}} \mathcal{S}_i$, where $\mathcal{S}_i$ is the set of all strategies available to player i.[1] In game theory literature, for convenience, the set of all players except i is denoted by $-i$. This way, one can represent a strategy profile (s_i, s_{-i}) that is composed of a specific strategy from i, $s_i \in \mathcal{S}_i$, and any combination of strategies from all other players, $s_{-i} \in \mathcal{S}_{-i}$. As for the set of utility functions, $\mathcal{U} = \{u_i | i \in \mathcal{P}\}$, it includes the payoffs that each player receives as a result from the chosen strategy profile, i.e. $u_i : \mathcal{S} \to \mathbb{R}$ [29,34,35].

Players in a game can have *complete* or *incomplete* information. In a complete information game, every player $i \in \mathcal{P}$ knows everything about the game he is involved in. More specifically, every player $i \in \mathcal{P}$ knows all the other players, their available strategies and the respective payoffs. Moreover, every player knows that the opponents also have that information. This knowledge can be used to intelligently choose strategies that provide the highest possible payoffs [29, 34, 35].

On the other hand, in a game with incomplete information, players do not know which strategies are available to the opponents, neither the resulting payoffs. Certain beliefs might be known about the opponents but those are not accurate and, as such, the behavior of players can be different. In this thesis, only complete information games will be used.

Definition 2.1 (Complete Information Game) *A game with complete information is a game where every player $i \in \mathcal{P}$ knows all the other players, their available strategies and all payoffs that they receive as result from the chosen strategy profiles.*

2.2.2 Dominated Strategies

In game theory, players choose their strategies in order to receive the highest possible payoff. Thus, it can be expected that strategies that never lead to high payoffs will never be chosen. Considering the game from Table 2.2, taken from [29], player p_2 will never choose strategy z_2. That is because greater payoffs can be obtained by p_2, either by choosing x_2 or y_2, no matter how his opponent plays. In this case, it is said that strategy z_2 is *strongly dominated* [29,34,35].

Definition 2.2 (Strong Dominance) *Strategy s'_i of player i is strongly dominated if for any $s_{-i} \in \mathcal{S}_{-i}$, there exists at least one $s_i \neq s'_i$ such that $u_i(s'_i, s_{-i}) < u_i(s_i, s_{-i})$.*

---

[1] The symbol $'\times'$ represents the Cartesian product. Hence, $\times_{i \in \mathcal{P}} \mathcal{S}_i = \{(s_1, s_2, \ldots, s_{|\mathcal{P}|}) : s_1 \in \mathcal{S}_1 \wedge s_2 \in \mathcal{S}_2 \wedge \ldots \wedge s_{|\mathcal{P}|} \in \mathcal{S}_{|\mathcal{P}|}\}$.

Table 2.2: Example of a game with one strongly dominated strategy, taken from [29].

		p_2		
		x_2	y_2	z_2
p_1	x_1	$(2,3)$	$(3,0)$	$(0,1)$
	y_1	$(0,0)$	$(1,6)$	$(4,2)$

Table 2.3: Game from Table 2.2 with the strongly dominated strategy eliminated.

		p_2	
		x_2	y_2
p_1	x_1	$(2,3)$	$(3,0)$
	y_1	$(0,0)$	$(1,6)$

Strongly dominated strategies can be removed from the game, since intelligent players would never choose them. In the case of the game from Table 2.2, if strategy z_2 is eliminated, then the resulting game will be the one in Table 2.3. Note that in the resulting game, after elimination of z_2, strategy y_1 of p_1 also becomes strongly dominated and, therefore, can be removed. This elimination process of strongly dominated strategies is called *iterative elimination* [29, 34, 35]. At the end, for the given example, only one strategy for each player will remain, x_1 for p_1 and x_2 for p_2. Since strategy profile (x_1, x_2) is expected to be chosen, p_1 will receive a payoff of 2 and p_2 will receive a payoff of 3.

Strategies can also be weakly dominated [29, 34, 35].

Definition 2.3 (Weak Dominance) *Strategy s'_i of player i is weakly dominated if for any $s_{-i} \in \mathcal{S}_{-i}$, there exists at least one $s_i \neq s'_i$ such that $u_i\left(s'_i, s_{-i}\right) \leq u_i\left(s_i, s_{-i}\right)$, with strict inequality for at least one $s_{-i} \in \mathcal{S}_{-i}$.*

Removing weakly dominated strategies by iterative elimination can also be done, however, it can lead to unexpected results. Considering the game from Table 2.4, taken from [36], p_1 has two weakly dominated strategies, x_1 and y_1. In Figure 2.2, it is possible to see how eliminating x_1 or y_1 first can lead to different results. That is, the order in which weakly dominated strategies are eliminated can lead to different outcomes. Such situation does not happen with strongly dominated strategies, because elimination does not cause strongly dominated strategies to cease being strongly dominated. On the other hand, a weakly dominated strategy can cease being dominated if other strategies are removed.

Table 2.4: Example of a game with weakly dominated strategies, taken from [36].

		p_2	
		x_2	y_2
p_1	x_1	$(1,0)$	$(0,2)$
	y_1	$(0,2)$	$(2,0)$
	z_1	$(1,1)$	$(2,1)$

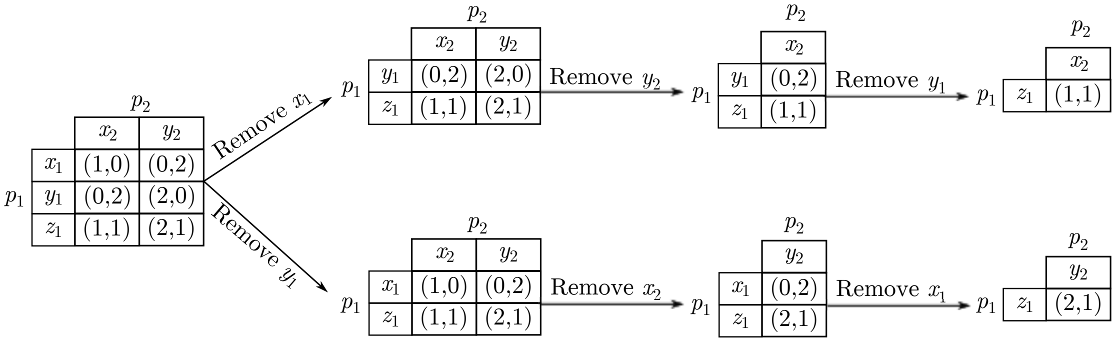


Figure 2.2: Difference between two alternative iterative eliminations of weakly dominated strategies.

2.2.3 Nash Equilibrium

It is not always possible to predict the outcome of a game through iterative elimination. For instance, the game in Table 2.5, taken from [29], has no dominated strategies. Nevertheless, it is still possible to predict what will be the outcome of the game. For that, the notion of *best response* needs to be introduced [29, 34, 35].

Definition 2.4 (Best Response) *The best response of player i is a function $br_i\left(s_{-i}\right)$ that outputs which strategy should be chosen by player i in order to receive the highest possible payoff, given that the opponents will play s_{-i}. That is, $br_i\left(s_{-i}\right)=\arg\max_{s_i \in \mathcal{S}_i} u_i\left(s_i, s_{-i}\right)$.*

In the game from Table 2.5, the strategy x_1 from p_1 is the best response to strategy x_2 from p_2. Strategy x_2, in its turn, is the best response to strategy z_1. One interesting strategy profile is the one where p_1 plays y_1 and p_2 plays y_2, with the payoff $(1,1)$. In this case, y_1 is the best response to y_2 and, conversely, y_2 is the best response to y_1. This strategy profile is actually the expected outcome of this game, since none of the players has any incentive to unilaterally choose a different strategy. That is, if p_1 plays x_1 or y_1, its payoff will decrease, considering that p_2 does not change its strategy. Similarly, p_2 will also not change to x_2 or z_2 because its payoff will decrease, since p_1 is playing y_1. This type of strategy profiles, where no player has any incentive to deviate, is termed *Nash equilibrium* [29, 34, 35].

Table 2.5: Example of a game without dominated strategies, taken from [29].

			p_2	
		x_2	y_2	z_2
	x_1	$(3, 0)$	$(0, 2)$	$(0, 3)$
p_1	y_1	$(2, 0)$	$(1, 1)$	$(2, 0)$
	z_1	$(0, 3)$	$(0, 2)$	$(3, 0)$

Definition 2.5 (Nash Equilibrium) *A strategy profile s^* is a Nash equilibrium if $u_i\left(s_i^*, s_{-i}^*\right) \geq u_i\left(s_i, s_{-i}^*\right), \forall s_i \in \mathcal{S}_i, s_i \neq s_i^*, \forall i \in \mathcal{P}$, with at least one strict inequality.*

It is possible to have more than one Nash equilibrium in one game. In the example from Table 2.4, both strategies obtained through iterative elimination of weakly dominated strategies, (z_1, x_2) and (z_1, y_2), are actually Nash equilibrium strategies. Indeed, strategy profiles obtained by iterative elimination are always Nash equilibrium profiles. Note, however, that in the case of iterative elimination of weakly dominated strategies, the resulting profiles are a subset of the Nash equilibrium profiles, meaning that there might be more Nash equilibrium profiles [29]. As for iterative elimination of strongly dominated strategies, the resulting profile is the only Nash equilibrium, as in the game from Table 2.2 [29].

Nash equilibrium, as shown, predicts what will be the outcome of a game. For example, in the forwarder's dilemma from Table 2.1, the Nash equilibrium profile is (D, D). Note that this outcome is not the most efficient, since both players could receiver greater payoffs if the profile (F, F) was played instead. However, any player might feel tempted do defect in order to receive the highest payoff of 1. As a precaution, both players end up choosing D in order to avoid receiving $-C$. This means that Nash equilibrium only predicts what will be the natural choices of intelligent players that do not trust each other or have no prior arrangement related to which strategies will be used. As such, Nash equilibrium, in many games, is not the most efficient outcome. The challenge resides in designing systems where players, routers in the case of the forwarder's dilemma, have incentives to cooperate, forward traffic from each other in the case of the forwarder's dilemma [30, 31, 33].

In game theory, the strategy profile (F, F) of the forwarder's dilemma is said to be *Pareto superior* to the other profiles.

Definition 2.6 (Pareto Superior) *A strategy profile $s \in \mathcal{S}$ is Pareto superior to $s' \in \mathcal{S}$ if $u_i\left(s_i, s_{-i}\right) \geq u_i\left(s_i', s_{-i}'\right), \forall i \in \mathcal{P}$, with at least one strict inequality.*

The most efficient outcome in a game would be one with the highest payoffs for every player, (F, F) in the case of the forwarder's dilemma. This efficient outcome has the particularity that

Table 2.6: Example of a game without pure Nash equilibrium, taken from [37].

		p_2	
		x_2	y_2
p_1	x_1	$(1,-1)$	$(-1,1)$
	y_1	$(-1,1)$	$(1,-1)$

there is no other profile that is Pareto superior to it [29,34,35].

Definition 2.7 (Pareto Optimal) *A strategy profile $s \in \mathcal{S}$ is Pareto optimal if there is no other strategy that is Pareto superior to s.*

There are cases where Nash equilibrium is Pareto optimal. In such cases, it is said that Nash equilibrium is *Pareto efficient*. Naturally, the most desired Nash equilibrium is the Pareto efficient one, since payoffs are higher.

2.2.4 Mixed Strategies

Until now, in this chapter, it has been assumed that players choose one specific strategy to be played and the expected outcome of the game is a Nash equilibrium profile. However, in some games, Nash equilibrium may not exist, as shown in the example from Table 2.6, taken from [37].

Instead of specifically choosing which strategy should be played, players can define a probabilistic distribution over their available strategies. In the example from Table 2.6, a Nash equilibrium would exist if both players define a probability of $1/2$ over each of their strategies, as it will become clear next. Such distribution is termed *mixed strategy* [37].

Definition 2.8 (Mixed Strategy) *A mixed strategy σ_i is a distribution over the strategies of i, $\mathcal{S}_i$.*

The set of all mixed strategies from a player $i \in \mathcal{P}$ is denoted by Σ_i (capital of σ). Similarly to strategy profiles, $s \in \mathcal{S}$, *mixed strategy profiles* can be defined by $\Sigma = \times_{i \in \mathcal{P}} \Sigma_i$. From here on, to avoid confusion, the set of profiles in $\mathcal{S}$ will be called *pure strategy profiles*, while the profiles in Σ will be termed *mixed strategy profiles*.

Since mixed strategies define probabilities over the set of available pure strategies, the utility function in this case reveals the expected payoff based on the chosen mixed profile σ [29,35,37]:

$$u_i(\sigma) = \sum_{s \in \mathcal{S}} \left[u_i(s) \prod_{j \in \mathcal{P}} \sigma_j(s_j) \right], \tag{2.1}$$

where s_j is the strategy of j in profile s and, $\sigma_j\left(s_j\right)$ represents the probability of s_j being chosen. Since $u_i\left(s\right)$ is the payoff of i when the pure strategy profile $s = \left(s_1, s_2, \ldots, s_{|\mathcal{P}|}\right)$ is played and, $\prod_{j \in \mathcal{P}} \sigma_j\left(s_j\right)$ is the probability of s being chosen if the mixed profile $\sigma = \left(\sigma_1, \sigma_2, \ldots, \sigma_{|\mathcal{P}|}\right)$ is used, then $u_i\left(s\right) \prod_{j \in \mathcal{P}} \sigma_j\left(s_j\right)$ represents the expected payoff of i.

Reconsidering the game from Table 2.6, assuming p_1 chooses x_1 with probability q_{x_1} and p_2 chooses x_2 with probability q_{x_2}, then the expected payoff for p_1 can be calculated by:

$$u_{p_1}\left(\sigma\right) = \left[1 q_{x_1} q_{x_2}\right] + \left[-1 q_{x_1}\left(1 - q_{x_2}\right)\right] + \left[-1\left(1 - q_{x_1}\right) q_{x_2}\right] + \left[1\left(1 - q_{x_1}\right)\left(1 - q_{x_2}\right)\right], \quad (2.2)$$

where 1 and -1 are the payoffs that p_1 would receive according to the different pure strategy profiles, shown in Table 2.6. As aforementioned, Nash equilibrium will exist, in this case, for $q_{x_1} = q_{x_2} = 1/2$, meaning that in this mixed Nash equilibrium both players will receive a payoff of 0. According to [29, 35], every game with a finite set of strategies has at least one pure or mixed Nash equilibrium. Note that a mixed Nash equilibrium profile is never Pareto optimal. That is because a mixed profile is, in fact, a linear combination of pure strategies and, as such, could not result in higher payoffs than the ones obtained by pure strategies.

2.3 Dynamic Games

One-stage games can only model situations where all players take their decisions at the same time. However, many situations may be better modeled with games composed of several stages [29, 35, 38]. For instance, in the forwarder's dilemma, players may not have packets to send at the same time. Let us assume that p_2 is the first player with a packet to be sent, which p_1 may or may not forward. Immediately after, p_1 also sends a packet, which p_2 can choose to forward or not. Such games are termed *dynamic games* or *multi-stage games*. In this chapter, and throughout the thesis, only dynamic games with *perfect information* are considered.

Definition 2.9 (Perfect Information) *A dynamic game with perfect information is one where every player $i \in \mathcal{P}$ knows all the actions taken in previous stages by all opponents.*

In the previous multi-stage forwarder's dilemma example, p_2 can decide whether or not to forward based on the action of p_1 in the previous stage.

Naturally, dynamic games need a different representation that must be capable of showing the order in which players make their moves [29]. The *extensive form* representation, shown in Figure 2.3 for the forwarder's dilemma, is the most suited for these situations. The extensive form consists of a tree structure where the root node represents the first decision in the game. In

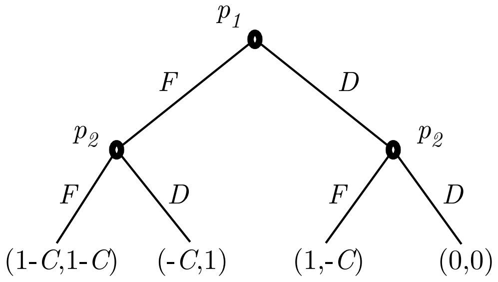


Figure 2.3: Two stage version of the forwarder's dilemma, where p_1 is the first player to move.

the previous example, the first decision belongs to p_1. The lines with labels (F and D) represent the actions available to the players. Player p_1, at the first stage, can decide to forward, F, or to drop, D, the packet from p_2. The leafs of the tree contain the payoffs that players will receive according to their decisions.

In multi-stage games, the player to move in the first stage has a set of strategies equal to the ones available in the one-stage game. For instance, p_1 from Figure 2.3 has the following strategies available: $\mathcal{S}_{p_1} = \{F, D\}$. The players in the subsequent stages can take their decisions based on the actions from previous stages. Player p_2 from Figure 2.3, can decide its action based on the move of p_1 in the previous stage. For this reason, strategies for p_2 will be different in the multi-stage game. In this case, p_2 has the following strategies available: $\mathcal{S}_{p_2} = \{FF, FD, DF, DD\}$. The first character in a strategy for p_2 represents the action that p_2 takes if p_1 chooses F in the first stage and the second character represents the action that p_2 takes if p_1 chooses D. For instance, strategy (FD) means that p_2 will forward if p_1 has forwarded in the previous stage and will drop if p_1 has dropped.

2.3.1 Nash Equilibrium and Backward Induction

The concept of Nash equilibrium in dynamic games is not different from one stage games. That is, a strategy profile is Nash equilibrium if no player can increase its payoff by unilaterally deviating. Considering the example from Figure 2.4, taken from [37], the pure Nash equilibrium strategy profiles are: (H, DD), (H, DH) and (D, HH). These Nash equilibria can be found more easily from the normal form equivalent game shown in Table 2.7. Note that the rows of the table include the current possible moves for p_1 (H and D) and the columns include the current possible moves for p_2 (HH, HD, DH and DD) that are based on the previous action of p_1. In strategy profile (D, HH), which is one of the Nash equilibrium profiles, p_2 threatens to play H regardless of the move from p_1. Player p_1 is aware of this threat and, as a result, could play

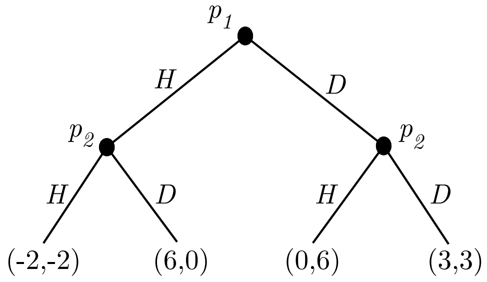


Figure 2.4: Example of a dynamic game taken from [37].

Table 2.7: Normal form equivalent for the game in Figure 2.4

		p_2			
		HH	HD	DH	DD
p_1	H	$(-2,-2)$	$(-2,-2)$	$(6,0)$	$(6,0)$
	D	$(0,6)$	$(3,3)$	$(0,6)$	$(3,3)$

his best response to HH, which is strategy D. However, looking more closely at Figure 2.4, if p_1 chooses H in the first stage, then p_2 is really not willing to choose H in the second stage, since D would give p_2 a better payoff. This kind of threats are termed *empty threats*, since p_2 is actually bluffing and HH does not represent a real threat [35, 37].

Finding Nash equilibrium strategy profiles in multi-stage games can lead to empty threats, and their removal can be done through *backward induction* [35, 37]. This technique starts by analyzing the most profitable action in the last stage and then, based on the most profitable actions at the last stage, it is analyzed which is the most profitable action at the penultimate stage. This analysis keeps proceeding upward in the tree structure until the root node is reached. To exemplify this, let us assume the game from Figure 2.4. First, the action that results in the highest payoff for p_2 is determined, considering all the possible previous actions of p_1. If p_1 played H, then the best choice is for p_2 to choose D. On the other hand, if p_1 chose D, then p_2 will be better with H. Given the best moves of p_2, it is possible decide which action results in the highest payoff for p_1. Clearly, p_1 will be better by playing H, since it will give him a higher payoff. In Figure 2.5, it is possible to see the result of the backward induction, where the thick lines mark the best actions in every stage. The continuous route of thick lines from the root to the leaf represents the predicted outcome of the game. Hence, (H, DD) and (H, DH) are the predicted outcomes, since both these strategies lead to the actions chosen by backward induction.

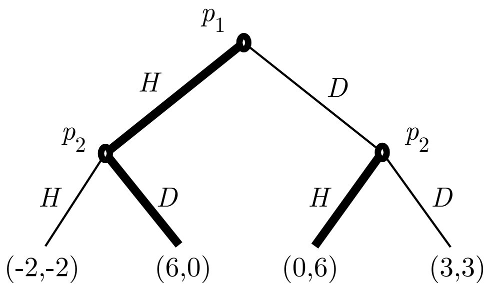


Figure 2.5: Backward induction technique applied to the game in Figure 2.4. The continuous route of thick lines from the root node to the leaf represents the predicted outcome of the game.

2.4 Repeated Games

Repeated games are a specific type of dynamic games where players face the same one-stage game repeatedly [29, 35, 37, 38]. An example of a repeated game would be the repeated forwarder's dilemma, where the game in Table 2.1 is played repeatedly over several stages.

At every stage t, every player $i \in \mathcal{P}$ has to choose his action. In the case of the forwarder's dilemma, in every stage t, every player chooses to forward or drop the packet. Since in this thesis, only repeated games with perfect information are considered, the action at every stage t can be chosen by considering the history of all previous moves, $h(t)$. That is, the history of previous moves is given as input to the strategy of every player to decide what will be the next action, $s_i(h(t))$. Naturally, the strategy profile outputs the next profile of actions, $s(h(t)) = \left(s_{p_1}(h(t)), s_{p_2}(h(t)), \ldots, s_{p_{|\mathcal{P}|}}(h(t))\right)$.

2.4.1 Finite-Horizon Games and Nash Equilibrium

Repeated games can be *finite-horizon*, which means that the number of stages is limited, or *infinite-horizon*, which means that players interact over an infinite number of stages [29, 37]. The payoff attributed to every player $i \in \mathcal{P}$ of finite-horizon games can be calculated by summing the stage payoffs of all stages:

$$U_i(s) = \sum_{t=0}^{T} u_i(s(h(t))), \tag{2.3}$$

where T is the last stage, u_i is the stage payoff of player i and U_i is the total payoff. Exemplifying with the repeated forwarder's dilemma, and considering that both players are using a strategy that chooses F at every stage, the payoff attributed to both players would be $\sum_{t=0}^{T}(1-C) = (T+1)(1-C)$.

To understand Nash equilibrium in finite-horizon games, let us keep considering the repeated forwarder's dilemma. If both players played F until stage $T-1$, then one of the players could deviate to D at the last stage T to increase his payoff. The opponent knows that, and to avoid receiving $-C$ at the last stage, he can also play D. Moreover, since it is predicted that both players will play D at the last stage, then players can also deviate at the penultimate stage in order to increase their payoff. Following this reasoning, the strategy profile that chooses the action (D, D) at every stage is a Nash equilibrium of the finite-horizon repeated forwarder's dilemma. Note that this method, used to find Nash equilibrium, is similar to the backward induction introduced in Section 2.3.1. Hence, any strategy profile that produces the outcome predicted by the backward induction is a Nash equilibrium.

2.4.2 Infinite-Horizon Repeated Games and Nash Equilibrium

Infinite-horizon repeated games, as aforementioned, are played on forever. As such, the payoff function of the finite-horizon game, shown in equation 2.3, can not be used for infinite-horizon games because it could result in infinite payoffs. Instead, a weighted sum, termed *discounted payoff*, is used [29,37,38]:

$$U_i\left(s\right) = \left(1-\delta\right)\sum_{t=0}^{\infty}\delta^t u_i\left(s\left(h\left(t\right)\right)\right), \tag{2.4}$$

where δ is a weighting factor, termed *discounting factor*, that receives values between 0 and 1, $0 < \delta < 1$. As for $(1-\delta)$, it is responsible for normalizing the payoffs, allowing the comparison between discounted payoffs and the payoffs received at every stage. For instance, in an infinite-horizon repeated game where player i receives a stage payoff of 1 at all stages, the discounted payoff for i will be 1. Note that as t grows, δ^t decreases. Hence, stage payoffs become less important as t grows, since the stage payoff is being multiplied by δ^t. Furthermore, assigning different values to δ will influence how fast the stage payoffs loose importance, altering the behavior of players and the Nash equilibrium profiles, as will be demonstrated next.

In infinite-horizon games, similarly to one-stage games, a strategy profile $s^* \in \mathcal{S}$ is a Nash equilibrium if:

$$U_i\left(s_i^*, s_{-i}^*\right) \geq U_i\left(s_i, s_{-i}^*\right), \forall s_i \in \mathcal{S}_i, \forall i \in \mathcal{P}. \tag{2.5}$$

However, in the case of infinite-horizon games, Nash equilibrium is greatly influenced by the discounting factor and by the fact that the game is played on forever [29,37,38]. To exemplify it, let us introduce the *grim trigger* strategy, which is widely used in game theoretical literature [29, 37,38]. A player i using this strategy will exert effort in every stage, as long as the opponent also cooperates. If the opponent shirks even only once, then i will stop cooperating from thereafter. Applying this strategy to the forwarder's dilemma, and labeling one of the players by i and the opponent by j (if $i = p_1$ then $j = p_2$, if $i = p_2$ then $j = p_1$), grim trigger can be defined by the following expression:

$$s_i\left(h\left(t\right)\right) = \begin{cases} F, & \text{if } \left(s_i\left(h\left(t-1\right)\right) = F\right) \text{ and } \left(s_j\left(h\left(t-1\right)\right) = F\right) \\ D, & \text{otherwise} \end{cases} \tag{2.6}$$

If both players in the infinite-horizon repeated forwarder's dilemma play this strategy, then they will play F at all stages. The outcome of such strategy profile for both players will be:

$$\begin{gathered}\left(1-\delta\right)\left[\left(1-C\right)\delta^0 + \left(1-C\right)\delta^1 + \ldots\right] = \left(1-\delta\right)\left[\left(1-C\right)\textstyle\sum_{t=0}^{\infty}\delta^t\right] = \\ = \left(1-\delta\right)\left[\left(1-C\right)\tfrac{1}{1-\delta}\right] = \left(1-C\right),\end{gathered}$$

If player i deviates at some stage t^*, then i will receive a higher payoff in that stage but will receive zero thereafter. The resulting discounted payoff for the deviating player can be calculated by:

$$\begin{gathered}\left(1-\delta\right)\left[\left(1-C\right)\delta^0 + \left(1-C\right)\delta^1 + \ldots + 1\delta^{t^*} + 0\delta^{t^*+1} + 0\delta^{t^*+2} + \ldots\right] = \\ = \left(1-\delta\right)\left[\left(1-C\right)\textstyle\sum_{t=0}^{t^*-1}\delta^t + \delta^{t^*}\right] = \left(1-\delta\right)\left[\left(1-C\right)\tfrac{1-\delta^{t^*}}{1-\delta} + \delta^{t^*}\right] = \\ = \left(1-C\right)\left(1-\delta^{t^*}\right) + \left(1-\delta\right)\delta^{t^*} = \left(1-C\right) - \delta^{t^*}\left(1-C\right) + \delta^{t^*}\left(1-\delta\right) = \\ = \left(1-C\right) + \delta^{t^*}C - \delta^{t^*}\delta = \left(1-C\right) + \delta^{t^*}\left(C-\delta\right).\end{gathered}$$

For the profile, where both players use grim trigger, to be Nash equilibrium, the deviation can not be profitable for i. That is:

$$1 - C \geq 1 - C + \delta^{t^*}\left(C-\delta\right) \Leftrightarrow 0 \geq \delta^{t^*}\left(C-\delta\right).$$

Since $0 < \delta < 1$, then $\delta \geq C$ for the inequality to hold. As long as the cost of forwarding a packet, C, is lower than the discounting factor, δ, it is more profitable to follow the grim trigger than deviating from it. This results in a Nash equilibrium profile where both players exert effort by forwarding packets from each other.

As aforementioned and exemplified, the discounting factor is an important piece in the Nash equilibrium of infinite-horizon repeated games. If δ is close to 0, players are impatient. That is, players will give more relevance to the payoff of the current stage than payoffs in future stages. In the forwarder's dilemma example, if the cost is too high or δ is too low, then players will feel compelled to receive a higher immediate payoff, even if they will receive a lower payoff thereafter. On the other hand, if δ is close to 1, players will be more patient by giving more relevance to future payoffs and, as such, will not deviate because it would result in lower payoffs in future stages.

Folk Theorem

Many Nash equilibrium strategy profiles exist in infinite-horizon repeated games that do not exist in one-stage games. This allows for certain payoffs to be obtained that would not be possible in Nash equilibrium of one-stage games. To understand which payoff values are possible, let us introduce the *min-max payoff* [37, 38].

Definition 2.10 (Min-max Payoff) *The min-max payoff for player* i*,* $\underline{u_i}$*, is defined as:* $\underline{u_i} = \min_{s_{-i}} \max_{s_i} u_i\left(s_i, s_{-i}\right)$.

That is, the min-max payoff is the lowest payoff that some player i can receive, provided that all opponents will choose a strategy to minimize the payoff of i and i will choose the best response to such strategy to maximize his payoff. In the case of the forwarder's dilemma, this corresponds to the payoff $(0, 0)$, earned when both players play D. Any payoff greater or equal than the min-max is possible to obtain by a Nash equilibrium strategy profile in an infinite-horizon repeated game. In Figure 2.6, the min-max payoff in the infinite-horizon forwarder's dilemma is shown with thick lines. The gray area represents all *feasible payoffs* by Nash equilibrium strategies [37, 38].

Definition 2.11 (Feasible Payoffs) *The set of feasible payoff profiles is given by:* $\left\{u = \left(u_1,\ u_2,\ \ldots,\ u_{|\mathcal{P}|}\right) : u_i \geq \underline{u_i}, \forall i \in \mathcal{P}\right\}$.

Provided that δ is high enough, then any payoff in the feasible area can be obtained by a Nash equilibrium strategy profile.

Theorem 2.1 (Folk Theorem) *For every feasible payoff profile* $u^* \in \left\{u = \left(u_1,\ u_2,\ \ldots,\ u_{|\mathcal{P}|}\right) :\ u_i \geq \underline{u_i}, \forall i \in \mathcal{P}\right\}$*, there exists a discounting factor* $\underline{\delta} < 1$ *such that for all* $\delta \in \left]\underline{\delta}, 1\right[$*, there is a Nash equilibrium profile with payoffs* u^*.

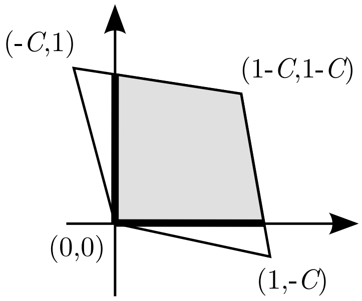


Figure 2.6: Illustration of the min-max and feasible payoffs of the infinite-horizon repeated forwarder's dilemma. The thick lines represent the min-max payoffs, while the gray area represents all feasible payoffs.

2.5 Network Formation Theory

The formation of networks plays a significant role in many fields. Thus, it may be helpful to study how such networks are formed, which connections are more important or which ones are more likely to be established, and how efficient are the resulting network structures. For instance, in labor economics, social networks are the main source of information about jobs and, ultimately, many jobs are found through personal contacts [21, 39]. Understanding who should be connected and how many connections should be established is important. In the context of computer networks, wireless routers in a wireless mesh can establish connections with neighbor wireless routers to route traffic in the most efficient way [27, 28].

Two different categories of network formation can be identified. In one of the categories, connections are formed to serve one single entity. For instance, the routing of planes by an airline or the establishment of distribution networks fall into this category [21,40]. In the second category, connections are formed among several individuals or entities acting on their own. That is, the entities themselves decide on what connections should be established or severed [21]. For instance, the establishment of connections by wireless routers in a wireless mesh network, where every router decides which connections should be established, in a decentralized manner, to route traffic. In this chapter, the focus will be on this second category.

Network formation theory is distinct from cooperative game theory. The outcome of cooperative games depends solely on the formed coalitions and on which players are involved in each coalition. Network formation theory, on the other hand, takes the full network structure into account, i.e. who is connected to whom [21].

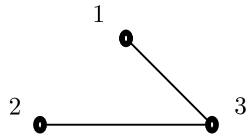


Figure 2.7: Network example with $\mathcal{P} = \{1, 2, 3\}$, $\mathcal{L}^E = \{13, 23\}$ and $\mathcal{L}^T = \{12, 13, 23\}$.

2.5.1 Network Structure

In network formation theory, the individuals establishing connections among them are also termed players, which may be people, organizations or wireless routers in a mesh network. Like in previous sections of this chapter, let us denote the set of players by $\mathcal{P}$.

An established connection between player $i \in \mathcal{P}$ and player $j \in \mathcal{P}$, $i \neq j$, is denoted by ij. The set of all established connections, i.e. all ij pairs, forms a network structure, which is denoted by $\mathcal{L}^E$. In this thesis, it is assumed that all connections are undirected, i.e. $ij \Leftrightarrow ji, \forall i \in \mathcal{P}, \forall j \in \mathcal{P}$ and $i \neq j$. Considering the example from Figure 2.7, $\mathcal{P} = \{1, 2, 3\}$ and $\mathcal{L}^E = \{13, 23\}$. The set of all possible connections involving all possible pairs of players from $\mathcal{P}$ is denoted by $\mathcal{L}^T$. Reconsidering the example from Figure 2.7, $\mathcal{L}^T = \{12, 13, 23\}$. The set of all possible networks, denoted by $\mathcal{L}$, is defined by $\mathcal{L} = \left\{\mathcal{L}^E | \mathcal{L}^E \subset \mathcal{L}^T\right\}$. All players with at least one established connection belong to set $\mathcal{P}^{\mathcal{L}^E}$, which is defined as $\mathcal{P}^{\mathcal{L}^E} = \left\{i | \exists ij \in \mathcal{L}^E, j \neq i\right\}$. As a result from the establishment of connections, *paths* and disconnected sub-networks, termed *components*, may emerge [21].

Definition 2.12 (Path) *A path between a player $i \in \mathcal{P}$ and a player $j \in \mathcal{P}$ is a sequence of connections $\{i_1 i_2, i_2 i_3, \ldots, i_{K-1} i_K\}$, where $i_1 = i$, $i_K = j$ and $i_k i_{k+1} \in \mathcal{L}^E, k = \{1, 2, \ldots, K-1\}$.*

Definition 2.13 (Component) *A component in a network $\mathcal{L}^E$ is a sub-network $\mathcal{L}^{E'} \subset \mathcal{L}^E$ such that:*

- *if $i \in \mathcal{P}^{\mathcal{L}^{E'}}$ and $j \in \mathcal{P}^{\mathcal{L}^{E'}}$, for $i \neq j$, then there exists a path between i and j, and*
- *if $i \in \mathcal{P}^{\mathcal{L}^{E'}}$ and $ij \in \mathcal{L}^E$, then $ij \in \mathcal{L}^{E'}$.*

All components in $\mathcal{L}^E$ are denoted by $\mathcal{C}^{\mathcal{L}^E}$. Note that according to this definition of component, an isolated player without any connections, i.e. $i \notin \mathcal{P}^{\mathcal{L}^E}$, is not considered a component. To denote the set of all components plus lone players, $\Pi^{\mathcal{L}^E} = \mathcal{C}^{\mathcal{L}^E} \cup \{i | i \notin \mathcal{P}_L\}$ is used.

2.5.2 Network and Allocation Value

All established and possible connections in a network structure define how valuable a network is. This value is termed *network value* and can be calculated by a *value function* [21].

Definition 2.14 (Network Value) *The network value represents the worth of a network structure and can be calculated by a value function* $\Upsilon : \mathcal{L} \rightarrow \mathbb{R}$*.*

Value functions can have interesting properties. For instance a value function is *component additive* if $\sum_{c \in \mathcal{C}^{\mathcal{L}^E}} \Upsilon(c) = \Upsilon\left(\mathcal{L}^E\right)$. This property rules out externalities across components, i.e. components do not interfere with each other [21].

Another interesting property is the *anonymity*. An anonymous value function assigns value to a network $\mathcal{L}^E$ based on its structure, independently of the labels of players involved in the connections. For instance, let us consider a permutation of players $\pi : \mathcal{P} \rightarrow \mathcal{P}$ (a bijection from $\mathcal{P}$ to $\mathcal{P}$). For any $\mathcal{L}^E \in \mathcal{L}$, $\mathcal{L}^{E,\pi} = \left\{i^\pi j^\pi | ij \in \mathcal{L}^E\right\}$. That is, $\mathcal{L}^{E,\pi}$ shares the same structure as $\mathcal{L}^E$ with players permuted. A value function Υ is anonymous if $\Upsilon\left(\mathcal{L}^{E,\pi}\right) = \Upsilon\left(\mathcal{L}^E\right)$ [21].

The network value is distributed among all players by means of an *allocation rule*.

Definition 2.15 (Allocation Rule) *An allocation rule is a function,* $\upsilon_i\left(\mathcal{L}^E, \Upsilon\right)$*, that assigns a value to each player* $i \in \mathcal{P}$*, such that* $\sum_{i \in \mathcal{P}} \upsilon_i\left(\mathcal{L}^E, \Upsilon\right) = \Upsilon\left(\mathcal{L}^E\right), \forall \mathcal{L}^E \in \mathcal{L}$*.*

Note that the allocation rule depends on the network structure, $\mathcal{L}^E$, and on the value function, Υ. This allows the allocation rule to calculate the role that every player has on the network, considering the network structure and network value [21].

Allocation rules, similarly to value functions, can also be anonymous. An anonymous allocation rule assigns values to players independently of their labels. Considering a permutation of players $\pi : \mathcal{P} \rightarrow \mathcal{P}$ and $\Upsilon\left(\mathcal{L}^{E,\pi}\right) = \Upsilon\left(\mathcal{L}^E\right), \forall \mathcal{L}^E \in \mathcal{L}$, an allocation rule is anonymous if for any $\mathcal{L}^E \in \mathcal{L}$ and any permutation of players π, $\upsilon_{i^\pi}\left(\mathcal{L}^{E,\pi}, \Upsilon\right) = \upsilon_i\left(\mathcal{L}^E, \Upsilon\right)$.

2.5.3 Formation Process

Value functions and allocation rules measure the outcome of networks and how that outcome can be assigned to players. A method to actually establish connections is still needed and, in the literature, many approaches have been proposed [21, 41]. One of such approaches uses non-cooperative game theory. However, important aspects in network formation, such as the order in which connections are established, are not taken into consideration by non-cooperative games [29]. Another approach is to model the objective of network formation in terms of *stability* and *efficiency* [42].

In a stable network, players have no incentive to add or remove connections. Many stability definitions have been proposed [21,42,43]. One of the most common is the *pairwise stability*.

Definition 2.16 (Pairwise Stability) *A network* $\mathcal{L}^E$ *is pairwise stable with respect to* υ *and* Υ *if:*

1. *for all* $ij \in \mathcal{L}^E, \upsilon_i\left(\mathcal{L}^E, \Upsilon\right) \geq \upsilon_i\left(\mathcal{L}^E \setminus \{ij\}, \Upsilon\right)$ *and* $\upsilon_j\left(\mathcal{L}^E, \Upsilon\right) \geq \upsilon_j\left(\mathcal{L}^E \setminus \{ij\}, \Upsilon\right)$*, and*
2. *for all* $ij \notin \mathcal{L}^E$*, if* $\upsilon_i\left(\mathcal{L}^E \cup \{ij\}, \Upsilon\right) > \upsilon_i\left(\mathcal{L}^E, \Upsilon\right)$ *then* $\upsilon_j\left(\mathcal{L}^E \cup \{ij\}, \Upsilon\right) < \upsilon_j\left(\mathcal{L}^E, \Upsilon\right)$.

Condition 1 of this definition dictates that both players involved in a connection must agree on maintaining it. As for condition 2, it dictates that if a connection does not exist in $\mathcal{L}^E$, then it means that at least one of the players would not benefit from establishing that connection. It is implicit in this definition that any player can unilaterally sever any of its connections and, for a connection to be established, the consent of both players involved in the establishment is needed.

The pairwise stability is simple and easy to work with [21]. However, it has one limitation. The definition only checks for stability among pairs of players, ignoring more complex changes that involve more than two players or more than one connection simultaneously. *Strong stability* addresses such limitation by considering all possible combinations of connection establishments or dissolutions [43]. Prior to define strong stability, the notion of deviation by a subgroup of players needs to be introduced. A network $\mathcal{L}^{E'} \in \mathcal{L}$ is obtainable from $\mathcal{L}^E \in \mathcal{L}$ via deviations by $\mathcal{V} \subseteq \mathcal{P}$ if:

1. $ij \in \mathcal{L}^{E'}$ and $ij \notin \mathcal{L}^E$ implies that $\{\{i\} \cup \{j\}\} \subseteq \mathcal{V}$, and
2. $ij \in \mathcal{L}^E$ and $ij \notin \mathcal{L}^{E'}$ implies that $\{\{i\} \cup \{j\}\} \cap \mathcal{V} \neq \emptyset$.

The deviation by a subgroup $\mathcal{V}$ implies that the establishment of new connections is allowed only within players in $\mathcal{V}$. As for connection dissolutions, at least one of the players involved in the dissolution of a connection must belong to $\mathcal{V}$.

Definition 2.17 (Strong Stability) *A network* $\mathcal{L}^E \in \mathcal{L}$ *is strongly stable with respect to* υ *and* Υ *if for:* i*) any* $\mathcal{V} \subseteq \mathcal{P}$*,* ii*) any* $\mathcal{L}^{E'}$ *that is obtainable from* $\mathcal{L}^E$ *via deviations by* $\mathcal{V}$*,* iii*) and any* $i \in \mathcal{V}$ *such that* $\upsilon_i\left(\mathcal{L}^{E'}, \Upsilon\right) > \upsilon_i\left(\mathcal{L}^E, \Upsilon\right)$*; then there exists* $j \in \mathcal{V}$ *such that* $\upsilon_j\left(\mathcal{L}^{E'}, \Upsilon\right) < \upsilon_j\left(\mathcal{L}^E, \Upsilon\right)$.

This strong stability notion is more refined than the pairwise stability. In fact, the set of strong stable networks is a subset of pairwise stable networks [21,43]. The refinement comes from the fact that strong stability checks for possible profitable deviations involving more than two players. Strong stability may be useful for small networks where there are only a few players with established connections and efforts to improve the allocation value can be easily coordinated.

For instance, in a wireless mesh network, with wireless routers establishing wireless connections between them, the strong stability would require all possible combinations of connection establishments, or dissolutions, to be considered. In small networks with only a few wireless routers, the number of combinations would not be too high and, hence, strong stability would not be too demanding. However, in larger networks with many wireless routers, it would be very demanding since too many possibilities of wireless connection establishments and dissolutions exist [21].

Besides finding and improving the allocation values for every player, knowing which network has the greatest network value may also be important. That is, which network brings the greatest overall benefit, independently of the individual interests of every player. A network $\mathcal{L}^E$ is said to be *efficient* if it has the greatest possible network value.

Definition 2.18 (Efficient Network) *A network* $\mathcal{L}^E$ *is efficient, relative to* Υ*, if* $\Upsilon\left(\mathcal{L}^E\right) \geq \Upsilon\left(\mathcal{L}^{E'}\right)$ *for all* $\mathcal{L}^{E'} \in \mathcal{L}$.

Note that there exists always at least one efficient network [21]. Having these definitions in mind, different formation process methods are discussed next.

Dynamic Network Formation (DNF)

In this approach, introduced in [44], networks are dynamically formed over several iterations. This process can be described as follows:

Step 1: The process begins with an empty network, $\mathcal{L}^E = \emptyset$.

Step 2: At each iteration $t = \{1, 2, \ldots\}$, a pair of players i and j is randomly chosen.

Step 3: If $ij \notin \mathcal{L}^E$, i.e. a connection between i and j does not exist, proceed to Step 3.1. Otherwise, $ij \in \mathcal{L}^E$, proceed to Step 3.2.

Step 3.1: If establishing the connection ij increases the allocation value of at least one of the chosen players, without decreasing the allocation value of the other, then establish the connection and proceed to Step 4. Otherwise, i.e. establishing the connection does not increase allocation values, do nothing and proceed to Step 4.

Step 3.2: If severing ij increases the allocation value of at least one of the chosen players, regardless of the other, then sever the connection and continue to Step 4. Otherwise, i.e. severing the connection does not increase any of the allocation values, do nothing and proceed to Step 4.

Step 4: If all pairs of players have been chosen and no connections have been added or severed, then end the process. Otherwise, go back to Step 2 for the next iteration.

With this method, either a pairwise stable network or a *cycle* of network modifications is reached [21, 44]. A cycle is a sequence of networks $\left\{\mathcal{L}_1^E, \mathcal{L}_2^E, \ldots, \mathcal{L}_K^E\right\}$, where $\mathcal{L}_1^E = \mathcal{L}_K^E$ and $\forall k = \{1, 2, \ldots, K-1\}, \exists i : v_i\left(\mathcal{L}_k^E, \Upsilon\right) < v_i\left(\mathcal{L}_{k+1}^E, \Upsilon\right)$. That is, there always exists at least one player that will have its allocation value increased by establishing or severing one connection.

Besides being stuck in a cycle, it is also possible to remain stuck at an empty network, $\mathcal{L}^E = \emptyset$. Such situation happens when establishing any connection does not lead to immediate higher allocation values, even if future connection establishments, beyond the first one, will give rise to allocation value improvements. This is related with the myopic behavior of players when establishing or severing connections. Two different approaches can be used to overcome such empty network. The first one is a stochastic approach, while the other tries to forecast better future conditions that may lie behind less favorable networks [21, 45–48].

Stochastic Network Formation **(SNF)**

This process, similarly to DNF, starts from an empty network. Then, at each iteration $t = \{1, 2, \ldots\}$, a pair of players, i and j, is randomly chosen. Then, like in DNF, it is decided whether or not the connection is established or severed. The difference from DNF is that the decision on establishing a connection will only be carried with a probability of $1 - \epsilon$, and the reverse will happen with probability ϵ. Likewise, if it was decided that the connection should be severed, then the decision will only be carried with probability $1 - \epsilon$, and the reverse will be done with probability ϵ. This way it is possible to get out of empty networks, where DNF can get stuck. This process can continue on forever, since random perturbations are always possible, and many pairwise stable networks can be visited. An examination can then be done to understand which networks are more likely to be formed [21, 45].

Farsighted Network Formation **(FNF)**

As aforementioned, there is another alternative to DNF and SNF that tries to forecast better future conditions that may lie behind less favorable immediate networks. This alternative is termed *farsighted network formation* (FNF) and tries to overcome the myopic nature of the decisions on establishing or severing connections. In large networks, players might have little ability to guess how other players will react to the establishment or dissolution of a connection, since many players and possible connections exist that have to be considered. However, in small networks, players may have good predictions about future moves and reachable networks. Many approaches have been proposed to achieve this type of farsighted formation [21, 46–48]. For instance, in [49] a method similar to repeated game theory is proposed, where future outcomes are weighted by means of a discounting factor.

2.6 Summary

This chapter introduced essential topics on game theory that are used throughout this thesis. It starts with one-stage games and how their outcome can be predicted. Afterwards, multi-stage games are introduced, as well as their main differences from one-stage games. Besides multi-stage games, where players play according to a specific order, repeated games are a good way to model situations where all players interact repeatedly over many stages. In this case, special emphasis is given to the Nash equilibrium of infinite-horizon repeated games, with which it is possible to obtain equilibrium profiles where all players cooperate, leading to an overall better outcome.

Network formation theory, which is a sub-field of game theory, is also introduced. This approach is usually used to study the formation of social or economic networks, however, it can also be applied to the establishment of wireless connections in a wireless mesh network.

CHAPTER 3

Fiber-Wireless Access Networks

3.1 Introduction

Bandwidth requirements of new services have been growing rapidly. To cope with such demand, fiber is being deployed to provide Internet access to users in fiber to the home (FTTH) or to the premises (FTTX) [1–3]. Fiber has several advantages over other technologies (e.g. digital subscriber line (DSL)), such as the huge bandwidth capacity and long range communication without needing active devices for signal recovery. Moreover, it is a low maintenance technology and, because of that, it is currently the medium of choice in most of today greenfield installations [1, 2]. However, fiber cannot go everywhere and users want Internet access wherever they are. To provide this kind of ubiquity, wireless and cellular networks are the technologies of choice. Despite the initial purpose of wireless technology, which is to provide low bandwidth and short distance communications, recent developments allowed wireless technology to achieve higher bandwidths. The fact that fiber is the medium of choice for new installations, being continuously preferred over other wired technologies, and the ubiquity required by users makes the joining of both these technologies a very interesting approach. FiWi access networks join both technologies in order to provide the required high bandwidth of new services and applications, while also providing the required ubiquity that users demand [13–16].

The rest of this chapter is organized as follows. Section 3.2 introduces the enabling technologies of both wireless and optical environments and how they can be combined to build FiWi access networks. In Section 3.3, network related notation and some assumptions, that are used throughout the thesis, are presented and explained.

Contributions:

***i*)** Survey on FiWi access networks through a careful explanation of all enabling technologies.

Publications:

The work in this chapter is to be published in [23].

3.2 Enabling Technologies for FiWi Access Networks

3.2.1 Wireless Networks

Wireless communication technology has been evolving considerably. Data rates up to hundreds of Mbps and ranges up to hundreds of meters are common nowadays [50–53]. Such improvements were possible due to great advances at the physical, media access control (MAC) and network layers. At the physical layer, the most common techniques used to improve data rate and signal quality are the multi-input multi-output (MIMO) and the orthogonal frequency division multiplexing (OFDM) [51, 53]. MIMO uses multiple antennas at the transmitter and/or receiver to improve spectral efficiency or link reliability. As for OFDM, it is used to encode data on multiple orthogonal carrier frequencies, leading to a higher spectral efficiency. Both of these techniques have been extensively used on many new wireless protocols, such as, 802.11n, LTE and WiMAX [50, 52, 54–58].

At the MAC layer, new time division multiple access (TDMA) schemes and dynamic bandwidth allocation (DBA) schemes with QoS concerns have been proposed and released by new wireless and cellular protocols. Providing the needed QoS for all types of traffic in wireless and cellular networks is one of the most important challenges [59]. The same distribution network needs to be able to accommodate all kinds of traffic, such as VoIP, video conferencing, audio and video streaming, online gaming, virtual private networking (VPN), web browsing, file transfers, etc. Both LTE and WiMAX provide mechanisms to identify all QoS parameters, prioritize traffic and control data rates, delays and packet delay variations (PDV), according to the needs of different types of traffic [57–60].

As for the network layer, cellular networks have been experiencing changes in network structure. For instance, LTE has a flatter network structure with fewer nodes when compared to previous cellular networks, such as universal mobile telecommunications system (UMTS) [58, 61]. Due to this structural change, the new base stations of LTE are more complex and take care of functionalities such as radio resource management and handoff procedures. This way, LTE has a more distributed management, unlike previous cellular networks that use less capable base stations and have a centralized management. Moreover, cellular networks are moving away from circuit switched communications to all-IP packet networks, which eases the integration of different multimedia services in the same distribution network [51, 58, 61].

Still relating the network layer, considerable research efforts have been applied on wireless mesh networks (WMNs). In such networks, wireless routers, connected wirelessly in a mesh topology, can be scattered around an area to provide Internet access to users. This topology can be easily used to provide great coverage, since wireless routers can be promptly deployed where they are most needed and integrated with the rest of the wireless mesh. In addition, due to its structure, mesh networks provide great flexibility in terms of resource provisioning and survivability [62–64]. The 802.11s standard has already been released to support WMNs. It introduces changes to 802.11 in terms of multihop routing, medium access and security [65–67]. The drawback of 802.11s is that it is not the most suited technology for high data rates and long distance communications, when compared to LTE or WiMAX [50–54].

To further increase the capacity of WiMAX and LTE, and to cope with the requirements of the International Mobile Telecommunications-Advanced (IMT-Advanced) specifications, also termed as the fourth generation (4G), WiMAX 2.0 and LTE-Advanced were proposed [51, 53, 68–71]. These protocols introduce techniques to improve data rates up to 1 Gbps for nomadic access and 100 Mbps for mobile users. Other aspects, such as mobility, latency and handover were also significantly improved [58, 69, 72]. One of the techniques implemented by LTE-Advanced and WiMAX 2.0 is the aggregation of non-contiguous carriers. This contributes to a high impact on the achievable data rates since, in practice, greater bandwidth usage will be possible. For instance, LTE-Advanced can use up to 100 MHz, while LTE only allows up to 20 MHz [53, 73]. Concerning the network structure, LTE-Advanced and WiMAX 2.0 also implement relay techniques to improve coverage and signal quality [69, 74–76].

3.2.2 Optical Access Networks

As aforementioned, new services and applications are becoming more and more demanding, requiring higher data rates and stricter QoS parameters. Existing copper access networks, such as DSL, can not cope with such demands. The optical fiber, on the other hand, seems to fit perfectly, since it is an excellent transmission medium with great longevity, low attenuation and high cost effectiveness. In fact, many optical access networks have already been deployed in many countries [1–3].

In optical access networks, different configurations are possible according to how close the fiber is to the users: FTTH, fiber to the building (FTTB) or fiber to the cabinet (FTTC). In FTTB and FTTC, the final connections are made with copper technologies, such as DSL or Ethernet, depending on how far fiber is from users [3,4]. These new optical access networks fulfill current requirements and open way for new demanding services, such as triple play, video on demand, HDTV, online gaming, etc.

The most famous optical technology used at the access section is the PON. It consists of deploying fiber from the CO to several optical network units (ONUs), near the users. At the CO, fiber is connected to an optical line terminal (OLT) and up to 32 ONUs can be served by the same OLT, depending on the specific PON protocol that is being used. If more ONUs need to be served, then more OLTs need to be added at the CO. No active devices exist between the ONUs and the OLT, hence the name passive optical network. The signal to/from the OLT is joined/split by means of a passive splitter, meaning that all ONUs share the same optical medium. The downstream transmission is broadcast to all ONUs and each ONU selects its own traffic. In the upstream, transmissions are synchronized in a TDMA manner. The high data rates and the inexistence of active components between the OLT and the ONUs contribute to the high cost effectiveness and high energy efficiency of PONs [77–80].

Currently commercialized PONs use either the EPON or GPON protocol. EPON, as the name suggests, aims at bringing the existing low cost Ethernet standard to the access network. The advantage of EPON is that most traffic is generated and terminated at Ethernet local networks, hence, translation among different data frame formats is not necessary. As for the GPON, it is an evolution of the asynchronous transfer mode (ATM) technology. GPON has the advantage of achieving higher data rates than EPON, 2.488 Gbps in downstream and 1.244 Gbps in upstream against the symmetrical 1.25 Gbps of EPON. Moreover, GPON is more scalable and flexible, since it allows up to 64 ONUs, whereas EPON allows up to 32 ONUs, and different downstream and upstream asymmetrical data rates are possible [78, 79, 81–83].

Like any other technology, optical access networks continue to evolve in order to meet future requirements. Next generation PONs have been widely researched and, currently, evolutions of GPON and EPON are actively being specified by the International Telecommunications Union, Telecommunication Standardization Sector, (ITU-T) and Institute of Electrical and Electronics Engineers (IEEE), respectively. The evolution of GPON, 10G-PON (XG-PON), will be able to operate at a symmetrical 10 Gbps or at an asymmetrical 10 Gbps in downstream and 2.5 Gbps in upstream. The split ratio is also expected to be increased and several chained splitters will also be possible, which will improve flexibility. Reach will also be improved through the use of reach extenders [7, 9–12, 84, 86, 89].

As for the 10 Gigabit EPON (10G-EPON), the evolution of EPON, it will operate symmetrically at 10 Gbps or asymmetrically at 10 Gbps in downstream and 1 Gbps in upstream. Both XG-PON and 10G-EPON can coexist with their previous versions, GPON and EPON, respectively. XG-PON will use wavelength division multiplexing (WDM) to coexist with GPON, while 10G-EPON will use dual-rate TDMA and WDM for coexistence to be possible. These new generation PONs, due to their high capacities, may be used as common access infrastructures to support residential and business applications. Furthermore, they can also be used as a backhaul for cellular or wireless networks [7, 9–12, 84, 86, 89].

Beyond XG-PON and 10G-EPON, other technologies can be exploited to further improve PON capabilities. Dense wavelength division multiplexing PON (DWDM-PON) is one possible approach. It will enable the transmission of many wavelengths in a limited spectrum region, providing high bandwidth to many subscribers [87].

Long reach PON (LR-PON) is another PON technology that has also been receiving some research effort. This will enable the reach of PONs to be increased from 20 km to 100 km through the use of optical amplifiers. Moreover, this will also allow greater split ratios, meaning that more ONUs can be served by the same OLT. As a result, this can lead to a lower number of COs and, therefore, higher cost savings, since less COs and OLTs will be needed. XG-PON, actually, specifies that longer reaches will be achieved through the use of reach extenders [88, 89].

3.2.3 FiWi Topologies and Approaches Proposed in Literature

Optical access networks meet current and future service/application requirements. However, users also want Internet access everywhere. FiWi access networks use both optical and wireless technologies to take advantage of the optical high capacity and wireless ubiquity [13–15].

FiWi access networks are composed of two parts, termed *back end* and *front end*. At the back end, optical links are brought from the CO toward end users and, at the front end, wireless routers take over and provide Internet, as exhibited in Figure 3.1. The main optical technology considered at the back end is the PON, due to its high deployment, high capacity and growing potential. At the front end, any radio frequency technology can be used, such as 802.11, WiMAX or LTE [13–16].

Deploying different technologies at the back and front end may bring additional challenges, since different protocols and architectures may be in use. For instance, in [90], a FiWi prototype was developed, which consists of an EPON at the back end and 802.11g wireless routers at the front end. Modifications at EPON and 802.11 protocols were not needed for the FiWi network to function. However, performance could be significantly improved if a closer integration was developed. For instance, the multi-point control protocol (MPCP) based DBA at the EPON and the routing protocol at the wireless section were unaware of each other, leading to a loosely

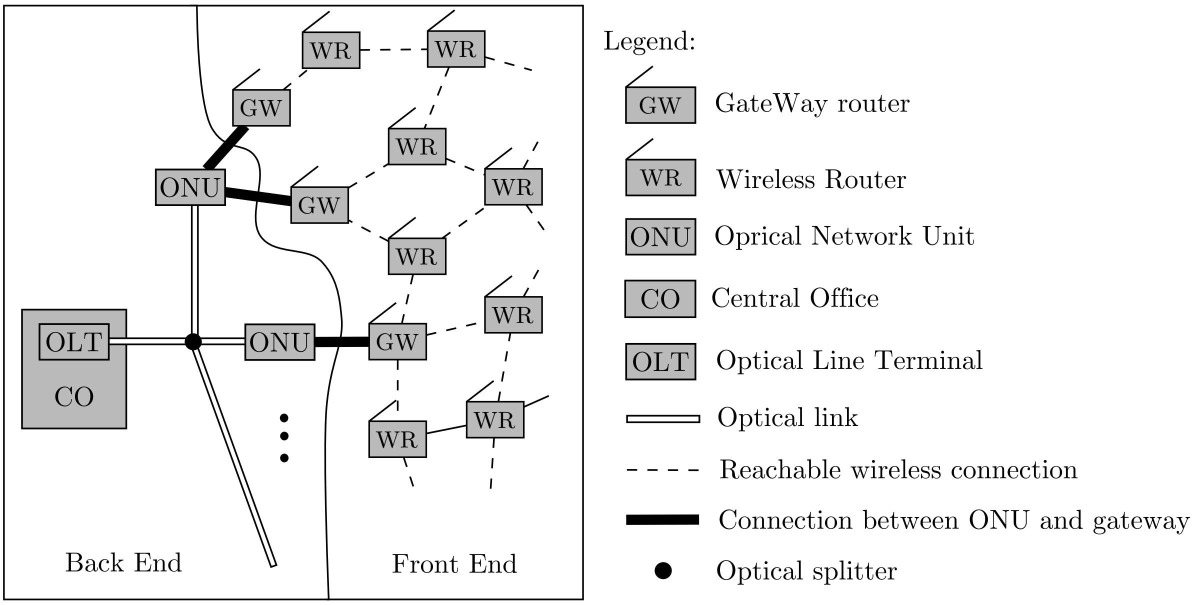


Figure 3.1: FiWi access network composition.

integrated architecture and control. The development of a closer integration was left for future work.

Given the architectural and operational requirements of LTE, its integration in a FiWi access network needs careful planning. More specifically, certain components of the LTE network architecture, such as the mobile management entity, serving gateway and packet data network, need to be integrated in the FiWi architecture [16, 58]. Furthermore, PONs are typically deployed as tree topologies, which can not easily support a fully distributed mesh structure of decentralized base stations, which is required by the LTE specification [58, 91]. In [16], the integration between a wavelength division multiplexing PON (WDM-PON) and LTE is studied and these integration issues, among others, are addressed.

Research on FiWi access networks can be mainly classified in three groups [16]: *i*) radio over fiber (RoF) systems [17]; *ii*) hybrid optical/WMN access networks [15]; *iii*) specific integration of PONs and 802.11/WiMAX technologies [18, 19]. The first group, RoF, mainly studies the transmission of radio signals directly through fiber. As a result, wireless protocol management can be centralized at the CO and antenna units will simply radiate through air the received signals from fiber, and send through fiber the signals received wirelessly. These antenna units have low requirements in terms of circuitry, since resource management and signal generation is centralized, and, as such, are more simple and more cost effective than regular access points, wireless routers and base stations. Furthermore, antenna units can handle any wireless technology. The RoF contributions have been mainly focused on transmission characteristics and modulation techniques, considering primarily physical layer issues [16, 17]. The drawback of this approach is that sending radio signals over long fibers increases delays, which can exceed certain timeouts of wireless MAC protocols [13, 92, 93]. In centralized polling and scheduling systems, the delays can be taken into account by interleaved polling. However, distributed MAC protocols may not work as expected [13].

The second group has mainly focused on FiWi access networks with a WMN at the front end. Research efforts at this group have mainly focused on performance issues of the multihop front end through the development of routing algorithms and optimal placement of ONUs and gateways [15, 90, 94, 95]. These architectures are very flexible, scalable and can easily provide the needed coverage [14, 15, 62]. In fact, due to their flexibility, some have already been deployed as municipal access solutions to eliminate the need for wired connections [15]. In [90], a prototype was developed, using an EPON at the back end and 802.11g wireless routers at the front end, and a performance study was conducted. Several key aspects were identified that can significantly improve performance, such as integrating the routing protocol used at the front end with resource allocation of the back end, and using TDMA MAC protocols at the wireless section instead of collision avoidance ones.

As for the third group, its contributions have been mainly focused on the integration between PON and WiFi/WiMAX protocols. For instance, how can different classes of service, specified by different protocols, be integrated. The challenge relies on merging both standards in use at front and back end in the most scalable and seamless possible way. In [18], a module is introduced between an ONU and a WiMAX base station to coordinate joint resource allocation.

3.3 Network Model and Nomenclature

This thesis will focus on FiWi access networks with a wireless mesh network at the front end. These networks are considered to be the most promising due to their cost effectiveness, bandwidth efficiency, wide coverage, high flexibility and scalability [14, 15, 62]. In such networks, there are many issues to be solved in terms of routing schemes, energy efficiency and resource provisioning, which will be addressed in this thesis [14].

The mesh front end of FiWi access networks is composed of gateways and wireless routers. The gateways are responsible for the frontier between the optical and wireless environment and for forwarding traffic to/from the optical link. Users willing to send/receive traffic to/from the Internet, will connect to either a wireless router or a gateway. From here on, the term *wireless* *node* will be used when referring to either a wireless router or a gateway. As for the back end, as aforementioned, the most common technology is the PON.

In these FiWi mesh architectures, traffic from users might need to traverse several wireless routers in a multihop manner in order to reach its destination. Traffic that a wireless node forwards from its directly connected users is termed *local traffic* throughout this thesis. Traffic being forwarded, at a wireless node, that belongs to users connected to other wireless nodes is termed *foreign traffic*.

To denote the set of nodes in a FiWi access network, the following notation will be used throughout this thesis:

$\mathcal{G}$**:** Set of gateways at the front end of the FiWi access network.

$\mathcal{R}$**:** Set of wireless routers at the front end of the FiWi access network, gateways not included.

$\mathcal{W}$**:** Set of wireless nodes. This set includes both gateways and wireless routers, $\mathcal{W} = \mathcal{G} \cup \mathcal{R}$.

$\mathcal{O}$**:** Set of ONUs at the back end of the FiWi access network.

$\mathcal{N}$**:** Set of nodes in the FiWi access network, $\mathcal{N} = \mathcal{W} \cup \mathcal{O}$.

3.3.1 Independent Networks

Every wireless router in $\mathcal{R}$ needs to be associated with a gateway from $\mathcal{G}$ in order to provide Internet access to its users. Since it is assumed that routers forward traffic to/from its associated gateway using a single upward/downward network connection, the wireless mesh will be partitioned into $|\mathcal{G}|$ smaller networks with a tree structure, called *independent networks* in this thesis. Figure 3.2 shows a FiWi access network taken from [95], the San Francisco Network (SFNet), already with independent networks drawn according to a shortest path criterion that also balances the number of routers per gateway in case of alternative shortest paths. Note that the independent networks are a result of the routing protocol being used. If the routing protocol changes routes according to network conditions, then the independent networks will change accordingly. In this thesis, the gateway routers are always the root nodes of the independent networks, i.e. ONUs are not part of the independent network. The only exception is in Chapter 6, where the ONUs are the roots of the independent networks.[1]

---

[1] In Chapter 6, the reader will be reminded of this difference and an explanation will be given for such distinction.

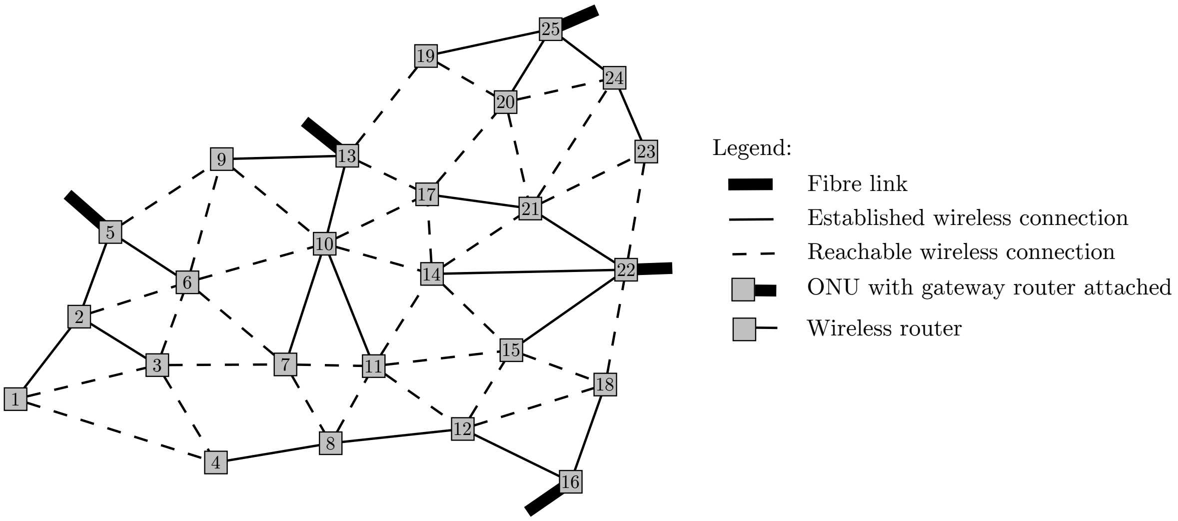


Figure 3.2: FiWi access network, taken from [95], with independent networks drawn.

Throughout the thesis, Γ_i^+ and Γ_i^- are used to represent the descendants and ancestors, respectively, of a node $i \in \mathcal{N}$ included in an independent network. For instance, Γ_i^+, for $i \in \mathcal{G}$, will be the set of wireless routers associated with gateway i. To represent the set of children of node i, i.e. the nodes immediately below i, γ_i^+ is used, and to represent the parent node of i, i.e. the node immediately above, γ_i^- is used. For instance, in the independent network of gateway 5 in Figure 3.2, nodes 1 and 3 make the set γ_2^+, while γ_2^- denotes node 5. A specific independent network can be identified by the wireless gateway that is serving all wireless routers included in the independent network. That is, for a $i \in \mathcal{G}$, the set of all nodes in the independent network served by gateway i can be represented by $\{i\} \cup \Gamma_i^+, \forall i \in \mathcal{G}$.

A wireless node $i \in \mathcal{W}$ will only forward local traffic (both downstream and upstream) to/from the users directly connected to it, and foreign traffic to/from wireless nodes in Γ_i^+, according to the independent network structure. The downstream and upstream local traffic of a wireless node $i \in \mathcal{W}$ at time t is denoted by $B_i^d(t)$ and $B_i^u(t)$, respectively. Note that these are amount of bytes to be transmitted. To represent the byte rate of a wireless node $i \in \mathcal{W}$ at time t, that is required for downstream and upstream local traffic, $\beta_i^d(t)$ and $\beta_i^u(t)$ are used, respectively. When needed, the joint amount of local downstream and upstream bytes to be transmitted/received by $i \in \mathcal{W}$ at time t is represented by $B_i(t)$ throughout this thesis, $B_i(t) = B_i^d(t) + B_i^u(t)$. Similarly, the joint byte rate required for downstream and upstream local traffic of $i \in \mathcal{W}$ at time t is represented by $\beta_i(t)$ throughout this thesis, $\beta_i(t) = \beta_i^d(t) + \beta_i^u(t)$.

For an easier reference, the notation introduced is summarized as follows:

Γ_i^+: All descendants of a node $i \in \mathcal{N}$, considering an independent network in particular.

Γ_i^-: All ancestors of a node $i \in \mathcal{N}$, considering an independent network in particular.

γ_i^+: Set of children of a node $i \in \mathcal{N}$, i.e. the nodes immediately below i, considering an independent network in particular.

γ_i^-: Parent node of node $i \in \mathcal{N}$, considering an independent network in particular.

cap_i: Highest attainable byte rate between node $i \in \mathcal{R}$ and γ_i^-. For $i \in \mathcal{G}$, cap_i is the attainable byte rate capacity of the optical link.

$B_i^d(t)$: Downstream local traffic (amount of bytes) destined to wireless node i at time t.

$\beta_i^d(t)$: Byte rate required by downstream local traffic of wireless node i at time t.

$B_i^u(t)$: Upstream local traffic (amount of bytes) sent by wireless node i at time t.

$\beta_i^u(t)$: Byte rate required by upstream local traffic of wireless node i at time t.

$B_i(t)$: Downstream and upstream local traffic (amount of bytes) belonging to wireless node i at time t, $B_i(t) = B_i^d(t) + B_i^u(t)$.

$\beta_i(t)$: Byte rate required by downstream and upstream local traffic of wireless node i at time t, $\beta_i(t) = \beta_i^d(t) + \beta_i^u(t)$.

3.4 Summary

This chapter presents FiWi access networks. It starts by introducing the current state of the art of wireless and optical networks. Currently used standards, as well as technologies under heavy development and research, were presented along with their features and potential. FiWi access networks were then introduced. Several possible approaches for the integration between wireless and optical technologies, and their main challenges, were explained. In this thesis, FiWi access networks with a mesh front end are the main focus of study. The chapter ends with some notation definitions that will be used throughout all the next chapters.

CHAPTER 4

Traffic Forwarding Game

4.1 Introduction

In FiWi access networks, packets have to travel through several hops in order to reach the optical link, in case of upstream traffic, or to reach the wireless router to which users are connected, in case of downstream traffic. Hence, wireless routers have to forward local and foreign traffic for communication to become possible. This chapter presents a repeated game to model bandwidth sharing among selfish wireless routers that are mainly interested in forwarding traffic from their own users. Subsequently, through Nash equilibrium, it can be verified under which conditions will wireless routers cooperate. This model serves as an initial study to understand whether or not cooperation is possible among wireless routers in FiWi access networks with a wireless mesh front end.

There are already some contributions that apply game theory to WMNs [33, 96]. However, the purpose of a traditional WMN is different from the purpose of a FiWi access front end. In traditional WMNs, nodes inside the mesh can send traffic to each other and, consequently, all nodes are potential sources, destinations and intermediaries. On the other hand, in FiWi access networks, there is little or no interest in sending traffic to nodes inside the access network since its main purpose is to provide Internet access. Therefore, it can be considered that most of its traffic is sent/received to/from gateways connected to ONUs.

The next section presents the repeated game model along with the used notation. Section 4.3 explains how Nash equilibrium was calculated and discusses the obtained results. The chapter ends with a brief summary in Section 4.5.

Contributions:

i) Showcase of a first application of game theoretical concepts to the problem of traffic forwarding in a FiWi access network where wireless routers are selfish players interested only in forwarding their own local traffic.

***ii*)** Development of a game theoretical model.

***iii*)** Demonstrate existence of Nash equilibrium.

Publications:

The work in this chapter has been published in [24, 25].

4.2 Repeated Game Model

4.2.1 Bandwidth Sharing

In FiWi access networks with a mesh front end, as aforementioned in Section 3.2, the interface with the user is made using a multi-hop wireless mesh network. As such, for Internet communication to be possible, wireless routers have to forward both local and foreign traffic.[1]

In this chapter, it is assumed that routes at the mesh front end are already established by a routing algorithm and independent networks with tree structures emerge from the established routes as previously explained in Section 3.3.1. Also, the notation introduced in Section 3.3 will be used in this chapter to denote all node sets, such as routers, gateways and ONUs.

Every router $i \in \mathcal{R}$ has a set of users connected to it that together receive $B_i^d\left(t\right)$ of downstream traffic and generate $B_i^u\left(t\right)$ of upstream traffic, throughout time t. Wireless routers that are not leafs in the tree structure, which i belongs to, $\gamma_i^+ \neq \emptyset$, have to forward foreign traffic belonging to users connected to routers in Γ_i^+, besides their own local traffic. These wireless routers, are termed *forwarding routers* and the set of all such routers is denoted by $\mathcal{F}$. Note that $\mathcal{F} \subset \mathcal{R}$. As for the leaf routers, they are termed *non forwarding routers* and forward only local traffic.

Each forwarding router $i \in \mathcal{F}$, forwards traffic from foreign users according to a variable called *cooperation level*, $\theta_i\left(t\right) \in [0, 1]$, that represents the fraction of foreign traffic that should be forwarded. The value 0 and 1 represent full defection and full cooperation, respectively. A forwarding router has the freedom to set its cooperation level and change it according to its wishes throughout time t. As a result, and since forwarding routers are selfish players only interested in forwarding their own local traffic, it is expected that they will set their cooperation levels to 0. That is, forwarding routers will defect, unless they have some sort of incentive to cooperate.

---

[1] See Section 3.3 for the definition of local and foreign traffic.

The incentive that forwarding routers need to cooperate can be provided by assigning a different objective to the gateways. Every gateway $j \in \mathcal{G}$ wants to forward as much traffic as possible from all wireless routers. Moreover, if some forwarding router does not cooperate, then the gateway can apply a punishment by forwarding less traffic from the defecting router. Every gateway $j \in \mathcal{G}$ decides how much traffic to forward from each wireless router $i \in \Gamma_j^+$ through a cooperation level $\mu_i^j(t)$. The set of all cooperation levels of a gateway j is represented by $\mu^j(t)$. Similarly to cooperation levels of forwarding routers, each cooperation level of the gateways can have any value in the interval $[0, 1]$, where 0 means full defection and 1 means full cooperation. Note that in this case, gateways would solely be responsible for the frontier between front and back end, without accepting user connections. However, it is possible to consider user connections by assuming that gateways are composed of two connected parts: a regular non forwarding router, which accepts connections from users and forwards traffic according to its own cooperation level, and a gateway, which is responsible for the frontier between front and back end.

Forwarding routers and gateways are the only nodes that can make decisions in the game, since they are the ones that can decide how much foreign traffic to forward. Hence, it can be considered that forwarding routers and gateways are the only players in the game.

Before proceeding into the details of the model, the notation just introduced is resumed in the following list:

$\mathcal{F}$: Set of forwarding routers, i.e. $\mathcal{F} = \left\{i \in \mathcal{R} : \gamma_i^+ \neq \emptyset\right\}$.

$\theta_i(t)$: Cooperation level of a forwarding router $i \in \mathcal{F}$ throughout time t.

$\mu_i^j(t)$: Cooperation level of a gateway $j \in \mathcal{G}$ applied to wireless router i throughout time t.

4.2.2 Stage Game

In this chapter, the time t being used does not refer to continuous time but rather to stages. Let us consider the independent network of gateway 5 in Figure 4.1. Node 1 has $B_1^d(t)$ of downstream traffic destined to it. However, the gateway only forwards a fraction, $\mu_1^5(t)$, of the traffic $B_1^d(t)$ and router 2 only forwards a fraction, $\theta_2(t)$, of the traffic $B_1^d(t)\,\mu_1^5(t)$. So, router 1 receives $B_1^d(t)\,\mu_1^5(t)\,\theta_2(t)$ of downstream traffic. Generalizing, the received downstream traffic for any

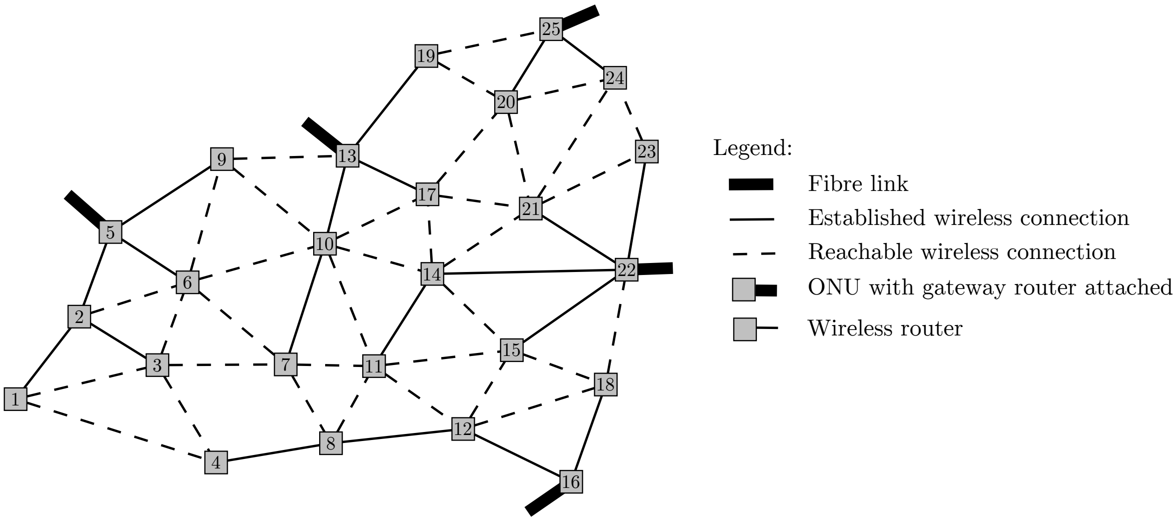


Figure 4.1: Independent networks created by the shortest paths calculation.

router $i \in \mathcal{R}$, associated with gateway $j \in \left(\Gamma_i^- \cap \mathcal{G}\right)$, can be calculated using:[2]

$$B_i^{d*}(t) = B_i^d(t)\,\mu_i^j(t) \prod_{k \in \left\{\Gamma_i^- \setminus \{j\}\right\}} \theta_k(t). \tag{4.1}$$

The same happens for upstream. Considering router 1, only $B_1^u(t)\,\theta_2(t)\,\mu_1^5(t)$ of traffic from router 1 arrives the optical section. To calculate the upstream traffic, for any router $i \in \mathcal{R}$ associated with gateway $j \in \left(\Gamma_i^- \cap \mathcal{G}\right)$, the following expression can be used:

$$B_i^{u*}(t) = B_i^u(t)\,\mu_i^j(t) \prod_{k \in \left\{\Gamma_i^- \setminus \{j\}\right\}} \theta_k(t). \tag{4.2}$$

The total traffic (downstream and upstream), belonging to the users of a router i, successfully received and transmitted, at stage t, will be:

$$B_i^*(t) = B_i^{d*}(t) + B_i^{u*}(t), \forall i \in \mathcal{R}. \tag{4.3}$$

Forwarding routers will have to forward traffic besides their own, as already explained in Section 4.2.1. Such foreign traffic, forwarded by a forwarding router $i \in \mathcal{F}$, can be calculated

---

[2] Note that $\prod \emptyset = 1$.

by:

$$\begin{aligned} B^*_{\Gamma_i^+}(t) &= \theta_i(t)\left[\sum_{k\in\Gamma_i^+}\left(B_k^u(t)\prod_{m\in\left\{\Gamma_i^+\cap\Gamma_k^-\right\}}\theta_m(t)\right)+\right. \\ &\left.+\sum_{k\in\Gamma_i^+}\left(B_k^d(t)\,\mu_k^j(t)\prod_{m\in\left\{\Gamma_i^-\cap\Gamma_j^+\right\}}\theta_m(t)\right)\right], j=\left(\Gamma_i^-\cap\mathcal{G}\right). \end{aligned} \tag{4.4}$$

Concerning the gateway, the forwarded foreign traffic can be calculated using the following expression:

$$B^*_{\Gamma_j^+}(t)=\sum_{i\in\Gamma_j^+}\left[B_i^d(t)\,\mu_i^j(t)\right]+\sum_{i\in\Gamma_j^+}\left[B_i^u(t)\,\mu_i^j(t)\prod_{k\in\left(\Gamma_j^+\cap\Gamma_i^-\right)}\theta_k(t)\right], \forall j\in\mathcal{G}. \tag{4.5}$$

To measure the interests of players, *stage payoff functions* are used. The stage payoff functions for forwarding and gateway routers will not be the same due to their different objectives. The stage payoff of forwarding routers is calculated by the sum of two functions. The first is a gain function $g_i\left(B_i^*(t)\right), \forall i\in\mathcal{F}$, dependent on the traffic successfully sent and received. The second is a negative cost function $c_i\left(B^*_{\Gamma_i^+}(t)\right), \forall i\in\mathcal{F}$, that depends on the traffic forwarded to other routers. Thus, the stage payoff of a forwarding router will be given by the following utility function:

$$u_i(t)=g_i\left(B_i^*(t)\right)+c_i\left(B^*_{\Gamma_i^+}(t)\right), \forall i\in\mathcal{F}. \tag{4.6}$$

Therefore, in order to have a high payoff, it is in the interest of the forwarding routers to forward a low amount of foreign traffic, and send a high amount of local traffic.

For the gateway, whose objective is to forward as much traffic as possible, the stage payoff is calculated using just a gain function $g_j\left(B^*_{\Gamma_j^+}(t)\right), \forall j\in\mathcal{G}$, that depends on the total amount of foreign traffic the gateway forwards. Thus, the stage payoff of a gateway will be given by the following utility function:

$$u_j(t)=g_j\left(B^*_{\Gamma_j^+}(t)\right), \forall j\in\mathcal{G}. \tag{4.7}$$

Note that gateways have a higher payoff if they forward more traffic. Therefore, it is in the interest of the gateway that forwarding routers forward a high amount of traffic.

4.2.3 Repeated Game

A repeated game consists in a number of repetitions of some stage game, as already explained in Section 2.4. In every stage, players decide which actions to take based on the stage payoff they get. A player can decide not to cooperate with the opponents, earning a higher immediate payoff. However, that action can cause losses to other players in the game, and these other players can, in future stages, punish that player. Therefore, in a repeated game, players have to worry about present and future stage payoffs when deciding which action to take. A forwarding router might choose to defect in order to have a higher immediate payoff, however, the gateway can punish the defecting forwarding router in future stages, leading to lower future stage payoffs. The discounted payoff function can help players to know if some action will lead to higher or lower future payoffs:

$$U_k = (1-\delta)\sum_{t=0}^{\infty}\delta^t u_k(t), \forall k \in (\mathcal{F} \cup \mathcal{G}), \tag{4.8}$$

where δ is the discounting factor, already introduced in Section 2.4.2. Note that, high values of δ characterize players more concerned with future payoffs, whereas low values of δ characterize players interested in the payoff of the current stage.

In each stage t, players have to choose their cooperation levels based on their strategies. In this case, the strategy adopted by a player outputs the cooperation level to use in every stage t. For the forwarding routers, the strategy, $s_i(.)$, depends on the downstream and upstream traffic perceived in the previous stage, $B_i^*(t-1), \forall i \in \mathcal{F}$. Thus:

$$\theta_i(t) = s_i\left(B_i^*(t-1)\right). \tag{4.9}$$

For the gateways, the strategy depends on the cooperation levels of the forwarding routers in the previous stage, $\theta_i(t-1), \forall i \in \Gamma_j^+, \forall j \in \mathcal{G}$. The gateways treat non forwarding routers as always cooperating forwarding routers. Thus, $\forall j \in \mathcal{G}$ and $\forall i \in \Gamma_j^+$:

$$\mu_i^j(t) = s_j\left(\theta_j(t-1)\right). \tag{4.10}$$

Whenever a forwarding router defects, the gateway will be able to punish it by decreasing the respective cooperation level. This conflict of interests, where forwarding routers are mainly interested in forwarding their local traffic and gateways are mainly interested in forwarding as much traffic as possible from all wireless routers, is responsible for the balance of the game.

4.3 Simulation

4.3.1 Simulation Setup

Simulations were done for SFNet in Figure 4.1. We consider that nodes receive three times more traffic than they send, since downstream traffic in access networks is usually higher [97].

The gain and cost functions, used in (4.6), are shown to be dependent on $B_i^*(t)$ and $B_{\Gamma_i^+}^*(t)$, $\forall i \in \mathcal{F}$, respectively. For simplicity, the gain is assumed to be the amount of traffic successfully sent and received, $B_i^*(t)$, while the cost is the symmetric of the amount of forwarded traffic, $B_{\Gamma_i^+}^*(t)$. As such, the stage payoff of forwarding routers in the simulations is:

$$u_i'(t) = B_i^*(t) + \left[-B_{\Gamma_i^+}^*(t)\right], \forall i \in \mathcal{F}. \tag{4.11}$$

Depending on the objective of the simulation, other possibilities exist, e.g. a gain and cost function that mimics signal interference or fading as in [32]. The same was considered for the gateway, i.e. the payoff is considered to be the actual amount of traffic that the gateway forwards:

$$u_j'(t) = B_{\Gamma_j^+}^*(t), \forall j \in \mathcal{G}. \tag{4.12}$$

To study equilibrium in a FiWi access mesh network, the following known strategies were used [34, 38]:

Tit-For-Tat (TFT): The player mimics the previous action of the opponent. The first action is to cooperate.

Anti-Tit-For-Tat (ATFT): The player mimics the previous action of the opponent. The first action is not to cooperate.

Grim Trigger (GT): The player cooperates by default. If an opponent does not cooperate, then the player will punish the opponent forever.

Always Cooperate (Al-C): Whatever the opponent does, the player always cooperates.

Always Defect (Al-D): Whatever the opponent does, the player never cooperates.

These strategies rely on two possible actions: cooperation and non-cooperation [34, 38]. However, the cooperation levels in our game can have any value in the interval $[0, 1]$. In order to make these strategies compatible with the developed model, forwarding routers are set with a low cooperation level, 0.1, when defecting and are set with a high cooperation level, 0.8, when cooperating.

Special attention is needed with the cooperation levels of the gateways. Let us consider the independent network from gateway 5 in Figure 4.1. If gateway 5 sets all its cooperation levels to 1, then it will not be able to punish a defecting router without hurting itself. For instance, if router 2 from Figure 4.1 defects, then gateway 5 can punish router 2. However, by punishing router 2, the gateway will forward less traffic and, as a result, gateway 5 receives a lower payoff. That is, the threat from gateway 5 toward router 2 is an empty threat. To avoid this, gateway 5 can set its cooperation levels to lower values, instead of setting them to 1, when cooperating.[3] This way, if router 2 defects, then gateway 5 can punish it by lowering the respective cooperation level and increase the cooperation levels of routers 6 and 9 to compensate for the smaller amount of traffic that the gateway will forward from router 2.

4.3.2 Analysis of Results

Table 4.1 shows the strategy profiles in equilibrium considering the cooperation levels of 0.1 and 0.8 for defecting and cooperating, respectively, along with the necessary δ intervals for each player. Nash equilibrium was tested by checking if any of the forwarding routers or gateways would receive a greater payoff by deviating from the strategy, similar to what was exemplified in Section 2.4.2. Note that in the independent network of gateway 16, the gateway can make a deviation against router 12 or router 8. In Table 4.1, only the δ intervals for the deviation against router 8 are presented since these δ intervals were smaller and more limitative than the δ intervals for the deviation against 12.

Notice that the equilibrium strategies are the same for independent networks of gateways 5, 14 and 22. This happens because these networks have a similar structure: one gateway, one forwarding router directly connected to the gateway and some non forwarding routers. For the independent network of gateway 16, the set of equilibrium strategy profiles is different because of its different structure, both in terms of number of forwarding routers and their position in relation to the gateway, as shown in Figure 4.1.

The δ intervals for which the strategy profiles are in equilibrium are very large in the independent networks of gateways 5, 13 and 22. Almost all profiles in Table 4.1 can have any value for δ, except strategy profile (Al-C, GT). That makes sense because (Al-C, GT) requires the forwarding router to always cooperate no matter what happens in the game, making the devia-

---

[3] The actual values could change for different independent networks, according to the number of forwarding and non forwarding routers.

Table 4.1: Strategy profiles in equilibrium.

	strategy profiles			δ interval for equilibrium		
Independent network of gateway 16	node 8 strategy	node 12 strategy	node 16 strategy	node 8	node 12	node 16
	TFT	ATFT	TFT	0.69 - 1	0 - 1	0.70 - 1
	ATFT	ATFT	TFT	0 - 0.69	0 - 1	0.48 - 1
	GT	ATFT	TFT	0.69 - 1	0 - 1	0.58 - 1
	ATFT	ATFT	GT	0 - 1	0 - 1	0.48 - 1
	ATFT	ATFT	Al-C	0 - 1	0 - 1	0.76 - 1
	ATFT	Al-C	GT	0 - 1	0 - 1	0 - 1
	Al-D	Al-C	GT	0 - 1	0.57 - 1	0 - 1

	node 2 strategy	node 5 strategy	node 2	node 5
Independent network of gateway 5	ATFT	TFT	0 - 1	0 - 1
	ATFT	GT	0 - 1	0 - 1
	ATFT	All-C	0 - 1	0 - 1
	Al-C	GT	0.72 - 1	0 - 1
	Al-D	TFT	0 - 1	0 - 1
	Al-D	GT	0 - 1	0 - 1
	Al-D	Al-C	0 - 1	0 - 1

	node 10 strategy	node 13 strategy	node 10	node 13
Independent network of gateway 13	ATFT	TFT	0 - 1	0 - 1
	ATFT	GT	0 - 1	0 - 1
	ATFT	All-C	0 - 1	0 - 1
	Al-C	GT	0.55 - 1	0 - 1
	Al-D	TFT	0 - 1	0 - 1
	Al-D	GT	0 - 1	0 - 1
	Al-D	Al-C	0 - 1	0 - 1

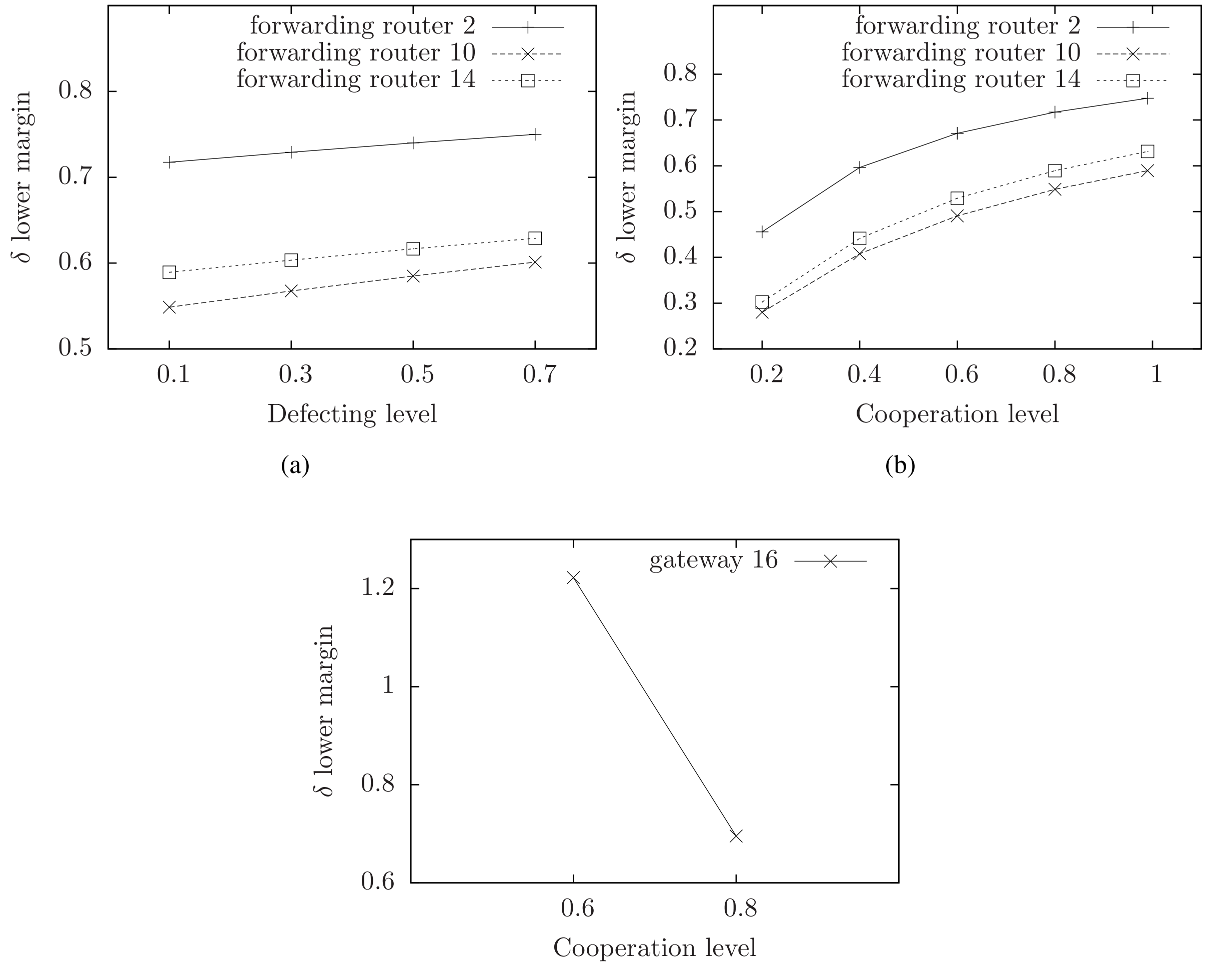
	node 14 strategy	node 22 strategy	node 14	node 22
Independent network of gateway 22	ATFT	TFT	0 - 1	0 - 1
	ATFT	GT	0 - 1	0 - 1
	ATFT	All-C	0 - 1	0 - 1
	Al-C	GT	0.59 - 1	0 - 1
	Al-D	TFT	0 - 1	0 - 1
	Al-D	GT	0 - 1	0 - 1
	Al-D	Al-C	0 - 1	0 - 1

tion more appealing. This means that there are less possible values for δ to achieve equilibrium. Also, when using (Al-C, GT), the δ interval required for equilibrium is smaller for forwarding router 2, which belongs to the independent network of gateway 5, than for forwarding routers 10 and 14. This is due to the fact that more non forwarding routers depend on node 2, than on nodes 10 or 14. Still for the same strategy profile, (Al-C, GT), the forwarding router 14, from the network of gateway 22, also has a slightly smaller δ interval, when comparing it with forwarding router 10, of independent network with gateway 13, due to the higher number of non forwarding routers dependent on the gateway in that network, as shown in Figure 4.1. Hence, having more non forwarding routers dependent on forwarding routers or gateways impacts negatively the equilibrium, i.e. shortens the δ interval for which equilibrium is still possible.

In what concerns to the use of specific strategies by certain players, it can be seen that ATFT and Al-D are never used by any of the gateways in a Nash equilibrium profile. The sole objective of gateways is to forward as much traffic as possible from all wireless routers. Hence, the gateway is interested in cooperating, unless it is punishing some forwarding router. When a gateway uses ATFT, for instance, its first action is not to cooperate, resulting in lower payoffs, independently of the strategies of the forwarding routers.

Results presented in Table 4.1 were obtained using cooperation levels of 0.1 and 0.8 for defecting and cooperating, respectively. However, changing the cooperation level values may change the δ intervals and can even turn the equilibrium of a strategy profile into non equilibrium. Considering the strategy profile (Al-C, GT) in the independent networks of gateways 5, 13 and 22, Figure 4.2(a) and Figure 4.2(b) show the increase of the lower margin of the δ interval when the defecting and cooperating cooperation levels increase, respectively. Increasing either the cooperating or the defecting cooperation level leads into a narrower δ interval. This makes sense since higher cooperation levels force forwarding routers to forward more traffic, as can be inferred from expression (4.4).

In Figure 4.2(c), it is shown that changing cooperation levels can even turn a strategy profile into non-equilibrium. It shows what happens to the lower margin of the δ interval of gateway 16, with strategy profile (TFT, ATFT, TFT), when the cooperation level is too low for the cooperating action. When it is lower than approximately 0.7, the lower margin of the δ interval becomes higher than 1 and, as explained in Section 2.4.2, δ can only have values between 0 and 1. Notice that, contrarily to the forwarding routers, high cooperating and defecting levels in gateways lead to larger δ intervals, since their main objective is to forward traffic.



(a)

(b)

(c)

Figure 4.2: Impact on δ interval when: (a) defecting level of forwarding routers is increased and the strategy profile (Al-C, GT) is used; (b) cooperation level of the forwarding routers is increased and the strategy profile (Al-C, GT) is used; (c) when cooperation level of gateway 16 is increased and the strategy profile (TFT, ATFT, TFT) is used.

4.4 Conclusions

According to the analysis, it can therefore be stated that it is possible to design a game theoretical model of traffic forwarding in FiWi access networks, in which Nash equilibrium exists for a scenario where wireless routers have incentives to cooperate. This happens despite the selfish nature of wireless routers, which are only interested in forwarding their own local traffic. For the equilibrium to exist, some conditions have to be fulfilled. More specifically, gateways need to have the purpose of forwarding as much traffic as possible from all wireless routers. This way, gateways are able to control and punish wireless routers that do not cooperate. Without such gateways, wireless routers at deeper positions in the independent network structure would not have any traffic successfully delivered. Another important condition, for Nash equilibrium to be possible, is the discounting factor. It is shown that as long as the discounting factor is high enough, Nash equilibrium profiles where all routers cooperate is possible.

4.5 Summary

This chapter presents a first showcase of the application of game theoretical concepts to the problem of traffic forwarding at the front end section of FiWi access networks. A repeated game model is presented where wireless routers and gateways are players with opposing objectives. Wireless routers are selfish players interested mainly in forwarding traffic from their directly connected users, while gateways are interested in forwarding as much traffic as possible from/to all wireless routers. Equilibrium profiles are then derived for the presented model, showing that equilibrium in such networks is possible, provided that certain conditions exist. More precisely, the gateway needs to have a different role, which is to forward as much traffic as possible from all wireless routers and to punish any defecting forwarding routers. Without such gateways, forwarding routers would not have any incentive to cooperate. It is also shown that the discounting factor, δ, has to be within a certain interval. Such interval depends on the number of non forwarding routers, which traffic has to be forwarded by forwarding routers and gateway.

CHAPTER 5

Fair Bandwidth Allocation Algorithm

5.1 Introduction

Wireless routers at the wireless mesh section of FiWi access networks have to forward both local and foreign traffic. In the previous chapter, it was studied whether or not cooperation is possible in FiWi access networks where wireless routers are mainly interested in forwarding local traffic. In this chapter, a different approach is pursued. It is assumed that wireless routers want their resources to be as productive as possible. That is, every wireless router wants to forward as much traffic as possible, either local or foreign, with as few packet drops as possible. Reducing the number of packet drops is important since packets being dropped may have traveled through one or more hops and consumed bandwidth without being successfully delivered. Besides bandwidth consumption, the dropped packets may also consume processing time and impose queuing delay to other packets. The conflict between routers arises when a certain traffic congestion level is reached and the available bandwidth is not enough to forward all the traffic. In that case, players with more resource requirements may become too greedy and capture all the available bandwidth, leading to starvation of routers with less bandwidth needs. In this chapter, besides building a repeated game model, a bandwidth allocation algorithm is also developed, which provides fairness among all wireless and gateway routers in FiWi access networks.

This chapter starts by outlining a generic game theoretical model, where players, actions and stage payoff functions are defined. Afterwards, in Section 5.3, conditions for Nash equilibrium to exist are presented and an algorithm to achieve that equilibrium is proposed. Simulation and results are then presented and discussed in Section 5.4. The chapter finalizes with a summary.

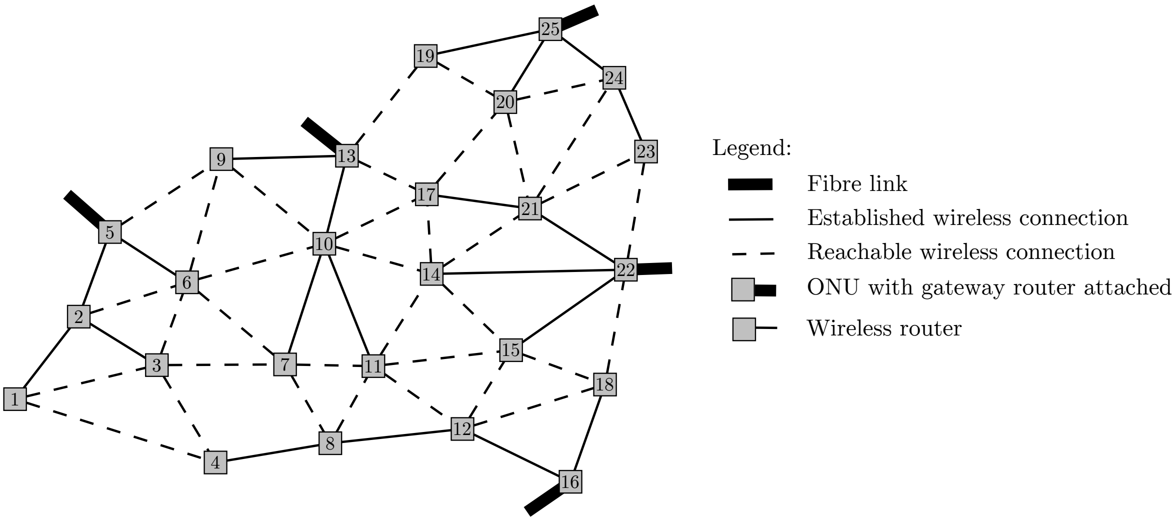


Figure 5.1: FiWi access network from Figure 3.2, reproduced here for convenience.

Contributions:

***i*)** Development of a game theoretical model that can serve as a framework for the development of a bandwidth allocation algorithm.
***ii*)** Development of a fair bandwidth allocation algorithm.

Publications:

The work in this chapter has been published in [26].

5.2 Game Theoretical Model

In this chapter, similarly to the previous one, it is assumed that routes have been established by routing protocols. As a result, independent networks with a tree structure emerge from the established routes, as explained in Section 3.3.1. The notation introduced in Section 3.3 will be used to denote any set of nodes in the FiWi access network.

5.2.1 Players and Actions

The model developed in this chapter is inspired on repeated game theory [29, 38]. It consists of successive stage game repetitions over a discrete time t. Throughout this chapter the term *stage* is used when referring to a time slot. The players in this model are all the wireless nodes in $\mathcal{W}$ and their objective is to forward as much traffic as possible, which can be local or foreign traffic.[1] Reducing the number of packet drops will also be part of the objective of every player, as packets being dropped may have traveled through one or more hops and consumed bandwidth without being successfully delivered. There will be an independent game per independent network, meaning that several games will be played in parallel. The discussion that follows applies to each independent network.

At all stages, every player has to choose a value for a variable called *sharing level*, $\alpha^i_{\Gamma_i^+}, \forall i \in \mathcal{W}$.[2] The sharing level can assume any real value between 0 and 1, and it represents the fraction of bandwidth reserved in i for foreign traffic, which is traffic belonging to routers in Γ_i^+. Besides choosing a sharing level for foreign traffic, players also choose how much of it will be assigned to each player in γ_i^+ and players in $\Gamma_i^+ \setminus \gamma_i^+, \forall i \in \mathcal{W}$. In Figure 5.2, such sharing level assignment is illustrated for gateway 5 from Figure 5.1, where $\alpha^i_{\Gamma_i^+}$, $1 - \alpha^i_{\Gamma_i^+}$, $\alpha^i_{j \cup \Gamma_j^+}$, α^i_j, $\alpha^i_{\Gamma_j^+}$ denote:

$\alpha^i_{\Gamma_i^+}$**:** Bandwidth fraction at wireless node i reserved for foreign traffic.

$1 - \alpha^i_{\Gamma_i^+}$**:** Bandwidth fraction at wireless node i reserved for local traffic.

$\alpha^i_{j \cup \Gamma_j^+}$**:** Bandwidth fraction at wireless node i reserved for local and foreign traffic of node $j, \forall j \in \gamma_i^+$.

α^i_j**:** Bandwidth fraction at wireless node i reserved for local traffic of node $j, \forall j \in \gamma_i^+$.

$\alpha^i_{\Gamma_j^+}$**:** Bandwidth fraction at wireless node i reserved for foreign traffic of node $j, \forall j \in \gamma_i^+$. This value is split proportionally among all players in Γ_j^+. In the example of Figure 5.2, $\alpha^5_{\Gamma_2^+}$ is split between players 1 and 3 according to the amount of upstream and downstream traffic of these players.

Clearly, $\alpha^i_{j \cup \Gamma_j^+} = \alpha^i_j + \alpha^i_{\Gamma_j^+}, \forall j \in \gamma_i^+, \forall i \in \mathcal{W}$, and $\alpha^i_{\Gamma_i^+} = \sum_{j \in \gamma_i^+} \left[\alpha^i_{j \cup \Gamma_j^+} \right], \forall i \in \mathcal{W}$. Leaf nodes, such as nodes 1, 3 and 6 from the independent network of gateway 5 in Figure 5.1, for example, have $\alpha^i_{\Gamma_i^+} = 0$, since no foreign traffic exists.

According to the estimated future bandwidth needs of players in Γ_i^+, player $i \in \mathcal{W}$ will use the sharing levels, shown above, to divide its bandwidth capacity, cap_i, among Γ_i^+ and itself. However, i is still vulnerable to its opponents in the following situations: *i)* wireless nodes in

---

[1] See Section 3.3 for definitions of local and foreign traffic.

[2] Not to be confused with the cooperation level from Chapter 4. Cooperation levels define the fraction of foreign traffic to be forwarded, while the sharing levels, introduced in this chapter, define the fraction of the bandwidth that is dedicated to foreign traffic.

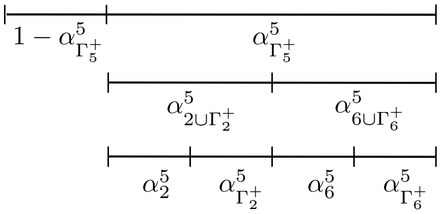


Figure 5.2: Sharing levels used by gateway router 5 from Figure 5.1.

Γ_i^- may have sharing levels that are too small, resulting in packets being dropped further along the path and, therefore, waste of resources at i; *ii)* wireless nodes in Γ_i^+ may actually need less bandwidth than what was reserved at i, resulting in unused bandwidth that could be used for local traffic instead; *iii)* traffic from nodes in Γ_i^+, arriving at wireless node i, may be more than the bandwidth reserved at i for foreign traffic, leading to the drop of packets and, therefore, waste of resources. In summary, the opponents of i may be unpredictable or not trustworthy.

To protect themselves from traffic fluctuations of users connected to them, and from the unknown actions of their opponents, every player $i \in \mathcal{W}$ chooses a set of variables that reveal the confidence that i has on its users and on its opponents, termed *trust levels*. These follow a nomenclature similar to the one used by the sharing levels:

χ^i**:** Trust level that i has on the fact that it will not receive excessive local traffic from its users, or that sharing levels applied by wireless nodes in Γ_i^- to its local traffic will not be too small.

ψ^i_j**:** Trust level that i has on the fact that j will not receive excessive local traffic from its directly connected users, or that sharing levels applied by wireless nodes in Γ_i^- to the local traffic of j will not be too small, $\forall j \in \gamma_i^+$.

$\psi^i_{\Gamma_j^+}$**:** Trust level that i has on the fact that j will not receive excessive foreign traffic, or that sharing levels applied by wireless nodes in Γ_i^- to foreign traffic of j will not be too small, $\forall j \in \gamma_i^+$.

In other words, χ^i, ψ^i_j and $\psi^i_{\Gamma_j^+}$ represent the confidence that player i has on the fact that it will not receive excessive traffic, or that wireless nodes in Γ_i^- will not use small sharing levels, which would cause packet drops. All trust levels assume a real value between 0 and 1, where 1 means full trust and 0 means full mistrust.

Whenever a player $i \in \mathcal{W}$, at some stage t, suspects that its directly connected users will generate too much traffic, then it may protect itself by lowering χ^i. This means that player i, at some stage t, will only be worried with providing the following bitrate to its connected users:

$$\beta^*_i(t) = \chi^i \left(\beta^d_i(t) + \beta^u_i(t)\right), \tag{5.1}$$

where $\beta^d_i(t)$ and $\beta^u_i(t)$ represent the downstream and upstream byte rates required by users connected to node $i \in \mathcal{W}$ at stage t. Analogously, if player i believes there will be too much traffic belonging to users connected to players in Γ^+_i, then player i can lower the corresponding trust levels, ψ^i_j or $\psi^i_{\Gamma^+_j}$. This would mean that player i, at some stage t, is only worried with providing the following bitrate for foreign traffic:

$$\beta^*_{\Gamma^+_i}(t) = \sum_{j \in \gamma^+_i} \left(\psi^i_j \beta^*_j(t) + \psi^i_{\Gamma^+_j} \beta^*_{\Gamma^+_j}(t)\right). \tag{5.2}$$

In practice, whenever trust levels are lowered, the responsibility for excessive traffic and packet drops is being discarded to the sources. The exact amount of traffic that successfully reaches its destination will depend on trust and sharing levels of all players in the independent network and will be explained in Section 5.2.2.

At every stage, a player will choose an action based on the beliefs that it has on the behavior of the opponents. In our case, every player $i \in \mathcal{W}$ chooses trust and sharing levels based on the expected traffic from users connected to i and on the expected traffic from users connected to players in Γ^+_i. More specifically, player i chooses sharing levels to divide cap_i among the expected local and foreign traffic and adjusts the trust levels according to its beliefs.

5.2.2 Stage Payoff

At all stages, every player receives a stage payoff that depends on the traffic delivered with success. To explain how the successfully delivered traffic can be calculated, let us assume the independent network of gateway 5 from Figure 5.1. The local traffic successfully sent and received by gateway 5 depends on the available bandwidth for its local traffic, i.e. it depends on its bandwidth capacity, cap_5, its sharing level, $\left(1 - \alpha^5_{\Gamma^+_5}\right)$, and the trust level applied to its users, χ^i, as follows: on one hand, the bandwidth available for local traffic, that depends on the sharing level and capacity, can not be exceeded, which means that in high load scenarios no more than $\mathrm{cap}_5 \left(1 - \alpha^5_{\Gamma^+_5}\right)$ can be used for local traffic; on the other hand, if there is not much local traffic to forward, or the trust level is a restraining factor, then no more than $\beta^*_5(t)$ can be used for local traffic delivery. Hence, we can state that gateway 5 will have $\min\left(\mathrm{cap}_5 \left(1 - \alpha^i_{\Gamma^+_i}\right), \beta^*_i(t)\right)$ of bandwidth for local traffic. Let us now assume wireless router 4, in the independent network of gateway 16 from Figure 5.1, whose traffic must cross several hops to reach the optical link. In this case, the available bandwidth for the local traffic of node 4 will depend on the sharing and trust levels of players in set Γ_4^-, which will be:

$$\min\left(\beta_4^*\left(t\right), \mathrm{cap}_4\left(1-\alpha_{\Gamma_4^+}^4\right), \mathrm{cap}_8\alpha_4^8, \psi_4^8\beta_4^*\left(t\right), \mathrm{cap}_{12}\alpha_{\Gamma_8^+}^{12}\frac{\beta_4^*\left(t\right)\psi_4^8\psi_{\Gamma_8^+}^{12}}{\beta_4^*\left(t\right)\psi_4^8\psi_{\Gamma_8^+}^{12}}, \beta_4^*\left(t\right)\psi_4^8\psi_{\Gamma_8^+}^{12},\right.$$
$$\left.\mathrm{cap}_{16}\alpha_{\Gamma_{12}^+}^{16}\frac{\beta_4^*\left(t\right)\psi_4^8\psi_{\Gamma_8^+}^{12}\psi_{\Gamma_{12}^+}^{16}}{\beta_4^*\left(t\right)\psi_4^8\psi_{\Gamma_8^+}^{12}\psi_{\Gamma_{12}^+}^{16}+\beta_8^*\left(t\right)\psi_8^{12}\psi_{\Gamma_{12}^+}^{16}}, \beta_4^*\left(t\right)\psi_4^8\psi_{\Gamma_8^+}^{12}\psi_{\Gamma_{12}^+}^{16}\right).$$

Note that the amount of traffic from players 4 and 8 to be forwarded by player 16 will be in proportion to their needs, $\beta_4^*\left(t\right)\psi_4^8\psi_{\Gamma_8^+}^{12}\psi_{\Gamma_{12}^+}^{16} + \beta_8^*\left(t\right)\psi_8^{12}\psi_{\Gamma_{12}^+}^{16}$. Generalizing, the available bandwidth to wireless node i over time t can be obtained by[3]:

$$\begin{aligned}\beta_i^A\left(t\right) &= \min\left[\beta_i^*\left(t\right), \mathrm{cap}_i\left(1-\alpha_{\Gamma_i^+}^i\right), \mathrm{cap}_{\gamma_i^-}\alpha_i^{\gamma_i^-}, \psi_i^{\gamma_i^-}\beta_i^*\left(t\right), \min_{j\in\Gamma_{\gamma_i^-}^-}\left(\mathrm{cap}_j\alpha_{\Gamma_{\gamma_j^+}^+\cap\Gamma_i^-}^j\right.\right.\\ &\left.\frac{\beta_i^*\left(t\right)\psi_i^{\gamma_i^-}\prod_{l\in j\cup\left\{\Gamma_j^+\cap\Gamma_{\gamma_i^-}^-\right\}}\psi_{\Gamma_{\gamma_l^+}^+\cap\Gamma_i^-}^l}{\sum_{k\in\Gamma_{\gamma_j^+}^+\cap\Gamma_i^-}\left(\beta_k^*\left(t\right)\psi_k^{\gamma_k^-}\prod_{l\in j\cup\left\{\Gamma_j^+\cap\Gamma_{\gamma_i^-}^-\right\}}\psi_{\Gamma_{\gamma_l^+}^+\cap\Gamma_i^-}^l\right)}\right),\\ &\left.\beta_i^*\left(t\right)\psi_i^{\gamma_i^-}\prod_{l\in j\cup\left\{\Gamma_j^+\cap\Gamma_{\gamma_i^-}^-\right\}}\psi_{\Gamma_{\gamma_l^+}^+\cap\Gamma_i^-}^l\right], \forall i\in\mathcal{W}.\end{aligned} \tag{5.3}$$

Concerning the foreign traffic, of some wireless node i, being successfully delivered, this also depends on the sharing and trust levels of players. For instance, player 2, in the independent network of gateway 5 from Figure 5.1, forwards traffic from players 1 and 3, whose successful traffic delivery depends on the bandwidth that they have available, $\beta_1^A\left(t\right)$ and $\beta_3^A\left(t\right)$, respectively. Hence, the bandwidth actually available to the foreign traffic of player i, over time t, is given by:

$$\beta_{\Gamma_i^+}^A\left(t\right) = \sum_{j\in\Gamma_i^+}\beta_j^A\left(t\right), \forall i\in\mathcal{W}. \tag{5.4}$$

As already stated, the objective of all players is to forward as much traffic as possible while

---

[3] Note that $\min\left(\emptyset\right)=+\infty$. We defined $\mathrm{cap}_\emptyset=+\infty$.

avoiding packet drops. Hence, both expressions (5.3) and (5.4) can be used to calculate the *stage payoff*, that a player i gets at every stage, as follows:

$$u_i\left(t\right) = \begin{cases} \eta_i\left(t\right) + \beta_i^A\left(t\right)\beta_{\Gamma_i^+}^A\left(t\right), & \gamma_i^+ \neq \emptyset \\ \eta_i\left(t\right) + \beta_i^A\left(t\right), & \gamma_i^+ = \emptyset \end{cases}, \forall i \in \mathcal{W}, \tag{5.5}$$

where $\eta_i\left(t\right)$ represents the resources that were wasted due to packet drops, termed *drop component*. This value is zero if no drops exist and negative if drops occur. The following expression is used to calculate $\eta_i\left(t\right)$:

$$\eta_i\left(t\right) = \begin{cases} \log\left(\frac{\beta_i^A(t)}{\beta_i^*(t)}\right) + \log\left(\frac{\beta_{\Gamma_i^+}^A(t)}{\beta_{\Gamma_i^+}^*(t)}\right), & \gamma_i^+ \neq \emptyset \\ \log\left(\frac{\beta_i^A(t)}{\beta_i^*(t)}\right), & \gamma_i^+ = \emptyset \end{cases}, \forall i \in \mathcal{W}. \tag{5.6}$$

Note that, due to its logarithmic nature, a small amount of packet drops will only slightly reduce the stage payoff, while high amounts of packet drops can greatly reduce the stage payoff. From a network perspective, a small amount of packet drops can be tolerated while a high amount of drops can be unbearable and greatly affect the services being provided by the FiWi access network.

5.2.3 Strategies and Repeated Game

In a repeated game, players have to choose their actions at every stage according to their strategies. The strategy of a player $i \in \mathcal{W}$ is a function that depends on the history of previous actions, $s_i\left(h_t\right)$, where h_t is the set of all action profiles taken by all players prior to stage t. In our case, each player of an independent network will have a strategy toward its opponents, the other nodes of the independent network. Note that each independent network is a separate game, as already introduced in Section 5.2.1. Such strategy outputs the sharing and trust levels to be used at every stage, which will be based on the sharing and trust levels used by all players at previous stages. Expressions (5.3), (5.4) and (5.5) vary over time and depend on the sharing and trust levels chosen by all players. Since the strategy profile[4] outputs the sharing and trust levels to use at every stage t, we can write the previous expressions, from now on, as being dependent on the strategy profile in use, $\beta_i^A\left(s\left(h_t\right)\right), \beta_{\Gamma_i^+}^A\left(s\left(h_t\right)\right), u_i\left(s\left(h_t\right)\right), \forall i \in \mathcal{W}$.

Throughout stages, players receive a stream of payoffs, $u_i\left(s\left(h_0\right)\right), u_i\left(s\left(h_1\right)\right), u_i\left(s\left(h_2\right)\right),$

---

[4] As introduced in Section 2.2.1, the tuple of strategies being used by all players in the game is called strategy profile.

$\ldots, \forall i \in \mathcal{W}$, which can be used to calculate the average discounted payoff:

$$U_i(s) = (1-\delta)\sum_{t=0}^{\infty} \delta^t u_i(s(h_t)), \forall i \in \mathcal{W}, \tag{5.7}$$

where $0 < \delta < 1$ is the discounting factor already introduced in Section 2.4.2.

5.3 Equilibrium

5.3.1 Nash Equilibrium

A set of strategies and corresponding payoffs constitute a Nash equilibrium if no player benefits by deviating from its strategy while others keep their strategies unchanged, as aforementioned in Section 2.4.2:

$$U_i\left(s_i^*, s_{-i}^*\right) \geq U_i\left(s_i, s_{-i}^*\right), \forall s_i \in \mathcal{S}_i, \forall i \in \mathcal{W}, \tag{5.8}$$

where s^* is the Nash equilibrium strategy profile. Nash equilibria in stage games are generically inefficient and exhibit suboptimal results, as exemplified in Section 2.2.3. That is because players can not know beforehand what will be the actions of their opponents and will, therefore, play safe. In the game presented in this chapter, players do not know what will be the sharing and trust levels of their opponents. Because of that, nodes will play safe by choosing low values for their trust levels. This way they can be sure that their stage payoff, $u_i(t)$, will not be negative due to high packet drops.

In the repeated game version, which is our case, Nash equilibrium greatly depends on the discount factor, δ, from the average discounted payoff function (5.7). The parameter δ represents how much a player is concerned with future or immediate payoffs, where the immediate payoff is the payoff obtained for the current stage, $t = 0$, and future payoffs are the sequence of payoffs obtained for future stages, $t = 1, 2, \ldots$. Players with a value of δ near 1 are more concerned with future payoffs, whereas players with δ near 0 are more concerned with immediate payoffs. If the player is more concerned with the immediate payoff, then the game is identical to a one-stage game and the player will play safe in order not to receive payoffs below zero. On the other hand, if future payoffs are important, the player may take the risk to get smaller immediate payoffs in order to receive higher payoffs in the long run. As a result, efficient payoffs that cannot be reached by a Nash equilibrium in a stage game, might be reached in the corresponding repeated game version. This is similar to the Nash equilibrium of the repeated forwarder's dilemma example in Section 2.4.2.

For the problem studied in this chapter, we are interested in values of δ near 1, since this will lead to an outcome where routers forward as much traffic as possible and the successfully delivered traffic is the highest possible[5]. Such situation happens whenever $\beta_i^A(t) = \beta_i^*(t)$, $\beta_{\Gamma_i^+}^A(t) = \beta_{\Gamma_i^+}^*(t)$ and $\chi^i = \psi_j^i = \psi_{\Gamma_j^+}^i = 1$, for all $i \in \mathcal{W}$. That is, when all traffic reaches the destination and all trust levels are set to the highest value. According to (5.3), this can be achieved when the following conditions are met:

$$\begin{aligned}
\beta_i^*(t) &= \beta_i^d(t) + \beta_i^u(t), \forall i \in \mathcal{W} && (5.9)\\
\beta_i^*(t) &\leq \mathrm{cap}_i\left(1 - \alpha_{\Gamma_i^+}^i\right), \forall i \in \mathcal{W} && (5.10)\\
\beta_i^*(t) &\leq \mathrm{cap}_{\gamma_i^-}\alpha_i^{\gamma_i^-}, \forall i \in \mathcal{W} && (5.11)\\
\beta_i^*(t) &\leq \mathrm{cap}_j\alpha_{\Gamma_{\gamma_j^+\cap\Gamma_i^-}^+}^j\\
&\quad \frac{\beta_i^*\psi_i^{\gamma_i^-}\prod_{l\in j\cup\left\{\Gamma_j^+\cap\Gamma_{\gamma_i^-}^-\right\}}\psi_{\Gamma_{\gamma_l^+\cap\Gamma_i^-}^+}^l}{\sum_{k\in\Gamma_{\gamma_j^+\cap\Gamma_i^-}^+}\left(\beta_k^*\psi_k^{\gamma_k^-}\prod_{l\in j\cup\left\{\Gamma_j^+\cap\Gamma_{\gamma_i^-}^-\right\}}\psi_{\Gamma_{\gamma_l^+\cap\Gamma_i^-}^+}^l\right)}, \forall i \in \mathcal{W}, \forall j \in \Gamma_{\gamma_i^-}^-, && (5.12)
\end{aligned}$$

where $\alpha_{\Gamma_i^+}^i = \sum_{j\in\gamma_i^+}\left(\alpha_j^i + \alpha_{\Gamma_j^+}^i\right)$. These conditions can be further simplified into:

$$\begin{aligned}
\frac{\beta_i^d(t) + \beta_i^u(t)}{\mathrm{cap}_i} &\leq 1 - \alpha_{\Gamma_i^+}^i, \forall i \in \mathcal{W} && (5.13)\\
\frac{\beta_i^d(t) + \beta_i^u(t)}{\mathrm{cap}_{\gamma_i^-}} &\leq \alpha_i^{\gamma_i^-}, \forall i \in \mathcal{W} && (5.14)\\
\frac{\beta_{\Gamma_{\gamma_j^+\cap\Gamma_i^-}^+}^*(t)}{\mathrm{cap}_j} &\leq \alpha_{\Gamma_{\gamma_j^+\cap\Gamma_i^-}^+}^j, \forall i \in \mathcal{W}, \forall j \in \Gamma_{\gamma_i^-}^-, && (5.15)
\end{aligned}$$

where:

$$\begin{aligned}
\beta_{\Gamma_{\gamma_j^+\cap\Gamma_i^-}^+}^*(t) &= \sum_{k\in\Gamma_{\gamma_j^+\cap\Gamma_i^-}^+}\beta_k^*\psi_k^{\gamma_k^-}\prod_{l\in j\cup\left\{\Gamma_j^+\cap\Gamma_{\gamma_i^-}^-\right\}}\psi_{\Gamma_{\gamma_l^+\cap\Gamma_i^-}^+}^l,\\
&= \sum_{k\in\Gamma_{\gamma_j^+\cap\Gamma_i^-}^+}\left(\beta_k^d(t) + \beta_k^u(t)\right).
\end{aligned}$$

---

[5] The objective is to develop a bandwidth allocation algorithm, hence, the calculation of the exact values for sharing levels, trust levels and δ for which Nash equilibrium exists is out of the scope of this chapter.

These conditions reveal that the sharing levels will be conditioned by traffic over capacity ratios and will serve as a basis for the strategy discussed next.

5.3.2 Plain Strategy and Proposed Algorithm

Plain strategy works like a recipe for constructing equilibrium in repeated games. They consist of a prescribed stream of cooperating action profiles, a^{PR}, and a punishment action profile, $a^i = \left(a_1^i, a_2^i, \dots, a_{|\mathcal{P}|}^i\right)$, to be applied by all opponents of i when punishing i, $\forall i \in \mathcal{W}$. As long as no player deviates from the prescribed stream, the action profile at every stage t is a^{PR}. A player i may want to deviate from the prescribed stream by defecting at some stage t in order to increase its payoff, causing smaller payoffs to all the others. When that happens, all players, except i, respond by switching to the punishment action profile a^i at the next stage. This strategy is in equilibrium as long as the punishment is severe enough, deterring any deviation [38].

The algorithm proposed in this chapter adopts such plain strategy behavior. Players will cooperate by choosing appropriate sharing levels in accordance to conditions (5.13), (5.14) and (5.15) and high values for trust levels. Whenever, a player $i \in \mathcal{W}$ detects that its drop component, $\eta_i(t)$, falls bellow a *drop component threshold*[6], η_i^{th}, then either $\beta_i^*(t)$ or $\beta_{\Gamma_i^+}^*(t)$ is too high and must be reduced by adjusting the respective trust level until $\eta_i \geq \eta_i^{th}$. If $\beta_i^*(t)$ is the one that is too high, then i will have to reduce the trust level for the directly connected users, χ^i. In practical terms, this means that router i will have to reduce the number of connected users or certain quality parameters of the provided services will have to be reduced, e.g. video resolution or sound bit rate, in order not to overload the FiWi front end. If $\beta_{\Gamma_i^+}^*(t)$ is the one that is too high, then at least one player in Γ_i^+ is being too greedy and is lowering the payoff of i. When a player is responsible for lowering the drop component of other players below the specified threshold, and as a consequence is lowering their payoffs, it is considered a defection. To safeguard itself, player i will have to lower the trust level of the source having excessive traffic. From here on, this trust level reduction will be termed *punishment* or simply *bandwidth reduction*. The exact value of the drop component threshold can be determined according to the amount of packet drops that can be tolerated without affecting the services being provided by the FiWi access network, which will be explained further on when presenting the algorithm details.

During the algorithm execution, every router will try to optimize β_i^A, $\beta_{\Gamma_i^+}^A$ and η_i by choosing the appropriate sharing and trust levels[7]. More specifically, every router i chooses values for

---

[6] Note that the drop component is zero if no drops exist and negative if drops occur.

[7] From here on, for briefness, β_i^A, $\beta_{\Gamma_i^+}^A$, β_i^* and $\beta_{\Gamma_i^+}^*$ will be used instead of $\beta_i^A(t)$, $\beta_{\Gamma_i^+}^A(t)$, $\beta_i^*(t)$ and $\beta_{\Gamma_i^+}^*(t)$.

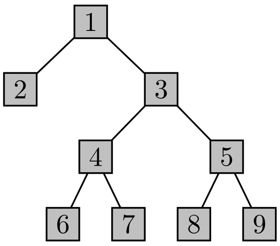


Figure 5.3: Generic independent network.

α^i_j, $\alpha^i_{\Gamma^+_j}$, χ^i, ψ^i_j and $\psi^i_{\Gamma^+_j}$. For instance, router 3 in Figure 5.3.2 chooses values for the following variables: α^3_4, α^3_5, $\alpha^3_{\Gamma^+_4}$, $\alpha^3_{\Gamma^+_5}$, χ^3, ψ^3_4, ψ^3_5, $\psi^3_{\Gamma^+_4}$ and $\psi^3_{\Gamma^+_5}$. Leaf routers, i.e. any router i with $\gamma^+_i = \emptyset$, only need to determine a value for χ^i and set everything else to zero. Similarly, any router i with $\gamma^+_i = \Gamma^+_i$, i.e. routers with only one level below, can set $\alpha^i_{\Gamma^+_j}$ and $\psi^i_{\Gamma^+_j}$ to zero, $\forall j \in \gamma^+_i$.

General Algorithm Behavior

In order to determine the just mentioned values/allocations, every router needs to communicate its bandwidth needs for local and foreign traffic, β^*_i and $\beta^*_{\Gamma^+_i}$. That can be done through the use of REQUEST messages sent by routers. Note that we are not concerned here with signaling protocol specifications. At this stage we just want to prove that the algorithm provides a fair and efficient bandwidth allocation. When the time arrives, a leaf router i would send a REQUEST message to its parent node γ^-_i. In the case of Figure 5.3.2, nodes 2, 6, 7, 8 and 9 send a REQUEST message to their respective parent nodes. Upon reception of REQUEST messages, a router must analyze all requests, its own bandwidth needs, and then send a new REQUEST message to the router above containing all bandwidth requirements adjusted to the transfer capacity between itself and the router above. For instance node 4 from Figure 5.3.2, after receiving the requests from nodes 6 and 7, would analyze these requests, its own bandwidth needs and adjust bandwidth requirements as follows: if node 4 can forward all traffic then a REQUEST message for all the requested bandwidth is sent to node 3; otherwise, bandwidth requirements are decreased accordingly and a REQUEST message is sent to router 3. Note that it is not worth making higher requests than it is possible to forward, since this would lead to lower payoffs.

The REQUEST messages keep being sent to the upper levels until the gateway is reached, i.e. router i with $\gamma^-_i = \emptyset$. The gateway then decides the values for its sharing levels, $\alpha^i_{\Gamma^+_i}$, α^i_j and $\alpha^i_{\Gamma^+_j}, \forall j \in \gamma^+_i$, together with possible punishments, and sends RESPONSE messages to all its children nodes notifying the bandwidth allocated to them, β_j^A and $\beta_{\Gamma_j^+}^A, \forall j \in \gamma_i^+$. Any router receiving a RESPONSE checks the bandwidth allocated to itself, proceeds to a proportional bandwidth distribution among nodes in Γ_i^+, and then sends a RESPONSE message for every node in γ_i^+ to notify the bandwidth allocated to them. This is done until all leaf routers receive response messages. Any router trying to use more than the allocated bandwidth will suffer packet losses.

Algorithm Details

We now present how the sharing levels are calculated by the algorithm, how the drop component threshold is calculated and how a defecting router is detected. Concerning sharing levels, a router i requesting β_i^*, for local traffic, and $\beta_{\Gamma_i^+}^*$, for foreign traffic, calculates its sharing level $\alpha_{\Gamma_i^+}^i$ using expression $\frac{\beta_{\Gamma_i^+}^*}{\beta_i^*+\beta_{\Gamma_i^+}^*}$. As for α_j^i and $\alpha_{\Gamma_j^+}^i, \forall j \in \gamma_i^+$, these are calculated using $\alpha_{\Gamma_i^+}^i \frac{\beta_j^*}{\beta_{\Gamma_i^+}^*}$ and $\alpha_{\Gamma_i^+}^i \frac{\beta_{\Gamma_j^+}^*}{\beta_{\Gamma_i^+}^*}$, respectively. These expressions ensure that conditions (5.13), (5.14) and (5.15) are met when $\beta_i^* + \beta_{\Gamma_i^+}^* \leq \text{cap}_i$. Considering condition (5.13), for example, and since $\frac{\beta_i^d(t)+\beta_i^u(t)}{\text{cap}_i} = \frac{\beta_i^*}{\text{cap}_i}$, we obtain $\frac{\beta_i^*}{\text{cap}_i} \leq 1 - \alpha_{\Gamma_i^+}^i \Leftrightarrow \frac{\beta_i^*}{\text{cap}_i} \leq 1 - \frac{\beta_{\Gamma_i^+}^*}{\beta_i^*+\beta_{\Gamma_i^+}^*} \Leftrightarrow \frac{\beta_i^*}{\text{cap}_i} \leq \frac{\beta_i^*}{\beta_i^*+\beta_{\Gamma_i^+}^*}$, which is valid when $\beta_i^* + \beta_{\Gamma_i^+}^* \leq \text{cap}_i$. On the other hand, if $\beta_i^* + \beta_{\Gamma_i^+}^* > \text{cap}_i$, it means that losses will occur. If the drop component is still greater than or equal to the threshold, $\eta_i \geq \eta_i^{th}$, then no punishments will be done. Otherwise, when $\eta_i < \eta_i^{th}$, punishments will be done.

The calculation of the drop component threshold to use can be based on the following relation:

$$\begin{aligned}
\eta_i &\geq \eta_i^{th} \Leftrightarrow && (5.16)\\
\Leftrightarrow \log\left(\frac{\beta_i^A}{\beta_i^*}\right) + \log\left(\frac{\beta_{\Gamma_i^+}^A}{\beta_{\Gamma_i^+}^*}\right) &\geq \eta_i^{th} \Leftrightarrow && (5.17)\\
\Leftrightarrow \frac{\beta_i^A \beta_{\Gamma_i^+}^A}{\beta_i^* \beta_{\Gamma_i^+}^*} &\geq 10^{\eta_i^{th}}, \forall i : \gamma_i^+ \neq \emptyset. && (5.18)
\end{aligned}$$

This means that as long as the product of the ratios $\frac{\beta_i^A}{\beta_i^*}$ and $\frac{\beta_{\Gamma_i^+}^A}{\beta_{\Gamma_i^+}^*}$ is greater than or equal to $10^{\eta_i^{th}}$, no punishments will be done. The drop component threshold for router i will be set according to the amount of local and foreign traffic that must be protected. For instance, a drop component threshold equal to -0.0969 means that at least 80% of either the local or foreign traffic will be provided, since $\frac{\beta_i^A \beta_{\Gamma_i^+}^A}{\beta_i^* \beta_{\Gamma_i^+}^*} \geq 10^{-0.0969} \simeq 0.8$. A drop component threshold equal to zero, $\eta_i^{th} = 0$, ensures full protection. As for leaf routers, a similar relation is obtained, $\frac{\beta_i^A}{\beta_i^*} \geq 10^{\eta_i^{th}}, \forall i : \gamma_i^+ = \emptyset$.

In what concerns to the detection of defecting routers, a router i with $\eta_i < \eta_i^{th}$ is able to identify these defecting routers by finding the highest values among β_i^*, β_j^* and $\frac{\beta_{\Gamma_j^+}^*}{|\Gamma_j^+|}, \forall j \in \gamma_i^+$. The highest values will then be reduced through trust level reductions until expression $\eta_i \geq \eta_i^{th}$ becomes valid. This way, cooperating nodes will not be affected by defecting nodes.

The algorithm implementation details are summarized in the procedures of Figure 5.4 and Figure 5.5, termed *upward* and *downward procedure*, respectively. The upward procedure is executed at every node upon the reception of REQUEST messages coming from wireless routers, and flowing toward the gateway, while the downward procedure is executed at every router upon the reception of RESPONSE messages, with bandwidth allocations assigned to users, flowing toward the leaf nodes. In both these procedures, the function `punishDefectingRouter` is responsible for reducing the highest values among β_i^*, β_j^* and $\frac{\beta_{\Gamma_j^+}^*}{|\Gamma_j^+|}, \forall j \in \gamma_i^+$, ensuring $\eta_i \geq \eta_i^{th}$, as previously described. The function `lowerExcessiveRequests`, used in the upward procedure, detects whether requests will lead to situations where $\eta_i < \eta_i^{th}$, independently of the RESPONSE messages coming from γ_i^-. That is, it detects situations where one or more nodes are certainly requesting too much traffic. In that case, adjustments equal to the ones in function `punishDefectingRouter` are made until $\eta_i \geq \eta_i^{th}$. This way router i will not request bandwidth to routers in Γ_i^- that i can not forward for sure, e.g. when $\mathrm{cap}_i < \beta_i^* + \beta_{\Gamma_i^+}^*$, preventing allocation of bandwidth at Γ_i^- that will not be used.

According to the model and algorithm presented in this chapter, bandwidth is allocated proportionally among all wireless nodes in conformity with their requirements, as long as the drop component is greater than or equal to the threshold. If the drop component falls below the established threshold, then bandwidth will stop being allocated proportionally. That is, more demanding routers will not be able to increase their allocations and the less demanding routers will always have a minimum allocation, according to the value of the drop component threshold. Here, this allocation is called *limited proportional allocation*, since bandwidth is provided proportionally up until the limit specified by the drop component threshold.

```
Procedure upwardAlgorithm ($q_k$):

arrivedRequests ← $q_k$
if |arrivedRequests| = $\left|\gamma_i^+\right|$ then
    /*Sum all the bandwidth requests received.*/
    $\beta^*_{\Gamma_i^+} = \sum_{j \in \gamma_i^+} \left(\beta_j^* + \beta^*_{\Gamma_j^+}\right)$
    if $\gamma_i^- \neq \emptyset$ then /*$i$ is not a gateway.*/
        /*Reduce excessive requests among $\beta_i^*$, $\beta_j^*$, and $\beta^*_{\Gamma_j^+}$, that are not possible to forward.*/
        lowerExcessiveRequests(arrivedRequests)
        /*Send a REQUEST message to $\gamma_i^-$.*/
        sendRequestTo$\gamma_i^-$ $\left(\beta_i^*, \beta^*_{\Gamma_i^+}\right)$
    else /*$i$ is a gateway*/
        /*Calculate the drop component, check defections and punish defecting routers until $\eta_i \geq \eta_i^{th}$, if needed.*/
        repeat
            /*Calculate the sharing levels and drop component.*/
            $\alpha^i_{\Gamma_i^+} = \frac{\beta^*_{\Gamma_i^+}}{\beta_i^* + \beta^*_{\Gamma_i^+}}$
            $\beta^A_{\Gamma_i^+} = \mathrm{cap}_i \alpha^i_{\Gamma_i^+}$
            $\beta_i^A = \mathrm{cap}_i \left(1 - \alpha^i_{\Gamma_i^+}\right)$
            $\eta_i = \log\left(\frac{\beta_i^A}{\beta_i^*}\right) + \log\left(\frac{\beta^A_{\Gamma_i^+}}{\beta^*_{\Gamma_i^+}}\right)$
            if $\eta_i < \eta_i^{th}$ then /*Defection detected.*/
                punishDefectingRouter (arrivedRequests)
            end if
        until $\eta_i < \eta_i^{th}$
        /*Send a RESPONSE message to every $j \in \gamma_i^+$.*/
        for all $j \in \gamma_i^+$ do
            $\alpha^i_j = \alpha^i_{\Gamma_i^+} \frac{\beta_j^*}{\beta^*_{\Gamma_i^+}}$
            $\alpha^i_{\Gamma_j^+} = \alpha^i_{\Gamma_i^+} \frac{\beta^*_{\Gamma_j^+}}{\beta^*_{\Gamma_i^+}}$
            sendResponseTo$j$ $\left(\mathrm{cap}_i \alpha^i_j, \mathrm{cap}_i \alpha^i_{\Gamma_j^+}\right)$
        end for
    end if
end if
```

Figure 5.4: Executed on router i upon arrival of a REQUEST message q_k from any child router $k \in \gamma_i^+$.

```
Procedure downwardAlgorithm ($r_k$):

$\beta_i^A = \text{extractBandwidthToItself}(r_k)$
$\beta_{\Gamma_i^+}^A = \text{extractBandwidthToFwd}(r_k)$
if $\mathrm{cap}_i < \beta_i^A + \beta_{\Gamma_i^+}^A$ then /*$k$ allocated more than $\mathrm{cap}_i$ (could happen if $\mathrm{cap}_k > \mathrm{cap}_i$). Reduce allocation accordingly.*/
    $\beta_i^A = \mathrm{cap}_i \frac{\beta_i^A}{\beta_i^A + \beta_{\Gamma_i^+}^A}$
    $\beta_{\Gamma_i^+}^A = \mathrm{cap}_i \frac{\beta_{\Gamma_i^+}^A}{\beta_i^A + \beta_{\Gamma_i^+}^A}$
end if
/*Calculate the drop component, check defections and punish defecting routers until $\eta_i \geq \eta_i^{th}$, if needed.*/
repeat
    if $\gamma_i^+ \neq \emptyset$ then /*$i$ is not a leaf*/
        $\eta_i = \log\left(\frac{\beta_i^A}{\beta_i^*}\right) + \log\left(\frac{\beta_{\Gamma_i^+}^A}{\beta_{\Gamma_i^+}^*}\right)$
    else /*$i$ is a leaf*/
        $\eta_i = \log\left(\frac{\beta_i^A}{\beta_i^*}\right)$
    end if
    if $\eta_i < \eta_i^{th}$ then /*Defection detected.*/
        punishDefectingRouter (arrivedRequests)
    end if
until $\eta_i < \eta_i^{th}$
/*Calculate sharing levels and send a RESPONSE message for every child.*/
$\alpha_{\Gamma_i^+}^i = \frac{\beta_{\Gamma_i^+}^A}{\mathrm{cap}_i}$
for all $j \in \gamma_i^+$ do
    $\alpha_j^i = \alpha_{\Gamma_i^+}^i \frac{\beta_j^*}{\beta_{\Gamma_i^+}^*}$
    $\alpha_{\Gamma_j^+}^i = \alpha_{\Gamma_i^+}^i \frac{\beta_{\Gamma_j^+}^*}{\beta_{\Gamma_i^+}^*}$
    sendResponseTo$j$ $\left(\mathrm{cap}_i \alpha_j^i, \mathrm{cap}_i \alpha_{\Gamma_j^+}^i\right)$
end for
```

Figure 5.5: Executed on router i upon arrival of a RESPONSE message r_k from parent router $k = \gamma_i^-$.

5.4 Simulation and Results

To analyze the performance of the proposed algorithm, a network simulation model has been implemented. The objective of simulations is to evaluate the performance of the proposed algorithm in terms of protection given to less demanding nodes, throughput and delay. For that purpose, our algorithm was tested alongside two other algorithms: *first in first out* (FIFO) and *weighted fair queuing* (WFQ) [98]. With FIFO, no allocations or priorities are set and, as such, less demanding routers have no protection against more demanding ones. This is one of the most widely used scheduling protocols in packet switching networks, mainly due to its simple queuing policy. In the context of our simulations, it will allow us to get a sense of the degree of protection that the other algorithms give to less demanding nodes.

The WFQ and the *weighted round robin* (WRR) are two scheduling policies typically used in PONs. In WRR, every stream of packets has its own queue and these queues are then served with respect to their weights in a round robin fashion. However, WRR has a packet granularity problem since size of packets is not considered [99]. That is, streams with larger packets will have a higher bit rate and consume more bandwidth. WFQ solves this granularity problem by considering the size of packets [98]. A bit-wise decision, instead of packet-wise, on the next queue being served is made, also in a round robin manner. In summary, both WRR and WFQ methods serve the queues with respect to their weights, but WFQ does it in a more complex and accurate way. For this reason, and for a clearer analysis, only WFQ has been implemented for comparison with the proposed algorithm.

When implementing the WFQ at some node, the downstream traffic directed to a specific wireless node will have its own queue. Note that traffic is being differentiated on a per node basis and not on a service stream basis. Since our algorithm seeks for fair bandwidth allocation, we should compare it with WFQ having equal weights for every queue, so that equal bandwidth access opportunities is promoted. The same happens for upstream traffic coming from a certain wireless source, which must reach the optical section. For instance, the uplink connection of node 1 from Figure 5.6(a) will have 5 queues, one for each source using this uplink. If fair bandwidth is to be provided, then all 5 queues at the uplink of node 1 will have weights equal to $\frac{1}{5}$.

5.4.1 Simulation Setup

The networks used in our simulations are exhibited in Figure 5.6. The structures of the network in Figures 5.6(a), 5.6(b) and 5.6(c) are similar to the independent networks identified in the FiWi

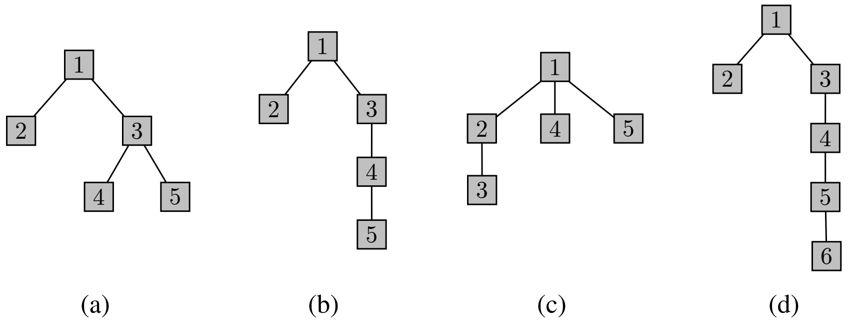


Figure 5.6: Simulated independent networks.

access network of Figure 5.1. As for Figure 5.6(d), it is used to test the protection provided to less demanding routers in structures with a higher depth. Note that, in FiWi access networks, it is not desirable to have too many wireless routers per gateway or to have wireless routers that are too many hops away from a gateway, since this would negatively affect the QoS. The optical link capacity is assumed to be five times the wireless transfer capacity.

The network simulation model was implemented using the OMNet++ discrete event platform [100]. Basically, every wireless node is composed of five modules, as illustrated in Figure 5.7: Receiver, Sink, Statistics, Queue Logic and Traffic Generator. The Receiver is responsible for directing packets either to the Sink module, for local absorption, or to the Queue Logic module, for forwarding. That is, if the packet is destined to the node itself, then it is sent to the Sink module. On the other hand, if the packet is destined to some other node, then it will be sent to the Queue Logic for forwarding. The Queue Logic module implements the scheduling policies being tested: the proposed algorithm, FIFO and WFQ. Both Sink and Queue Logic modules will send statistical messages to the Statistics module. These messages include information related to successful packet deliveries, packet drops and waiting times in queue. The Statistics module is responsible for storing the information delivered by the Sink and Queue Logic modules for further analysis. As for the Traffic Generator, this module is responsible for generating traffic with the statistical behavior described next.

The traffic modeling in our simulations was accomplished through the Pareto and exponential distributions. The Pareto distribution was used to model packet size and the exponential distribution to model inter arrival times [97]. The Pareto distribution was configured with a scale of 2025.7833 and a shape of 5.1430, to emulate the HTTP traffic behavior, according to [97]. The λ parameter of the exponential distribution was calculated based on an intended load. That is, the mean inter arrival time will be $\lambda_i^{-1} = \frac{\bar{p}}{\text{cap}_i L_i}$, where $\bar{p}$ is the Pareto mean and L_i is the intended load for node i, $0 < L_i \leq 1$ ($0 =$ no load; $1 =$ full capacity utilization).

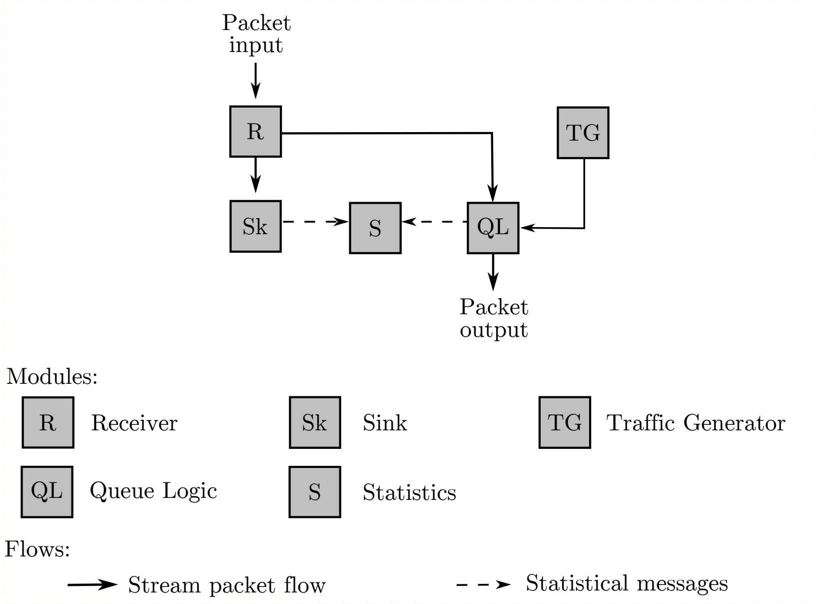


Figure 5.7: Node modules implemented in simulation.

An exception is made for local traffic generation at gateways, for which a mean inter arrival time equal to $\lambda_i^{-1} = \frac{\bar{p}}{\frac{\text{cap}_i}{5} L_i}$ is used. This is because the capacity of optical links is considered to be five times the capacity of wireless connections, and this fact should not have impact on local traffic generation at gateways. The downstream load was considered to be three times the upstream load, since downstream traffic in access networks is usually higher [97].

To demonstrate that our algorithm is able to detect defecting nodes with excessive loads, that could penalize the QoS of others, some nodes of the independent networks were set with a high load of 0.8, while the others were set with a load of 0.25. The average of the results obtained, considering all possible combinations of high and low load assignment to nodes, are compared for the different scheduling algorithms. Also, simulations were run for two drop component threshold values, $\eta_i^{th} = 0$ and $\eta_i^{th} = -0.17$, to test different levels of protection. Note that router 2 from Figure 5.6(a), Figure 5.6(b) and Figure 5.6(d), and routers 4 and 5 from Figure 5.6(c) are not potential defecting nodes because the optical link was assumed to have sufficiently high bandwidth to accommodate the traffic from all directly connected wireless routers, meaning that routers directly connected to the gateway will never compete for bandwidth. Hence, only the remaining routers will be set with different high and low bandwidth needs.

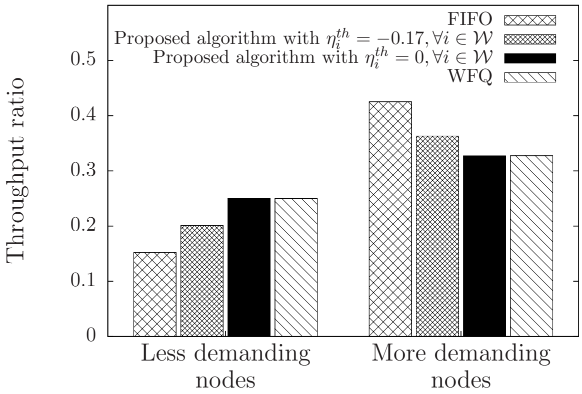


Figure 5.8: Average throughput ratio obtained by FIFO, proposed algorithm and WFQ. WFQ was set with equal weights among all queues and the proposed algorithm was tested with $\eta_i^{th} = 0$ and $\eta_i^{th} = -0.17$. Load of less demanding nodes = 0.25; Load of over demanding nodes = 0.8. Queues with a maximum capacity of 40 packets were used.

5.4.2 Results Discussion

In Figure 5.8, it is possible to compare the average throughput ratios obtained by FIFO, the proposed algorithm and WFQ, assuming that the throughput ratio of a wireless node i was calculated using the expression $\frac{throughput\,experienced\,by\,i}{\text{cap}_i}$. For the proposed algorithm, simulations were done for $\eta_i^{th} = 0$ and $\eta_i^{th} = -0.17$, $\forall i \in \mathcal{W}$, where $\eta_i^{th} = 0$ means that requests from less demanding nodes will be fully protected and $\eta_i^{th} = -0.17$ ensures that the less demanding receive an allocation of at least 66% (approximately two thirds) of the requested bandwidth, $10^{-0.17} \simeq 0.66$, (see Section 5.3.2). WFQ was set with equal queue weights as previously stated.

Results show that, when FIFO is used, the less demanding nodes are severely penalized, obtaining a throughput much lower than the assigned load. More specifically, the effective throughput of less demanding nodes was approximately half of the load set for these nodes (0.25), while the remaining packets were dropped. The proposed approach and the WFQ were both able to protect less demanding nodes from the greediness of nodes with excessive traffic. For $\eta_i^{th} = 0, \forall i \in \mathcal{W}$, the throughput obtained by these two schemes was, in fact, similar. An advantage of the proposed algorithm is that it is flexible and can be configured to provide the level of protection desired by the network administrators. In the case of Figure 5.8, when $\eta_i^{th} = -0.17$ is used, it is guaranteed that the less demanding nodes will receive at least 66% of their throughput needs. For WFQ to change the level of protection of less demanding nodes, all weights would need to be recalculated to reflect load changes. Our algorithm provides

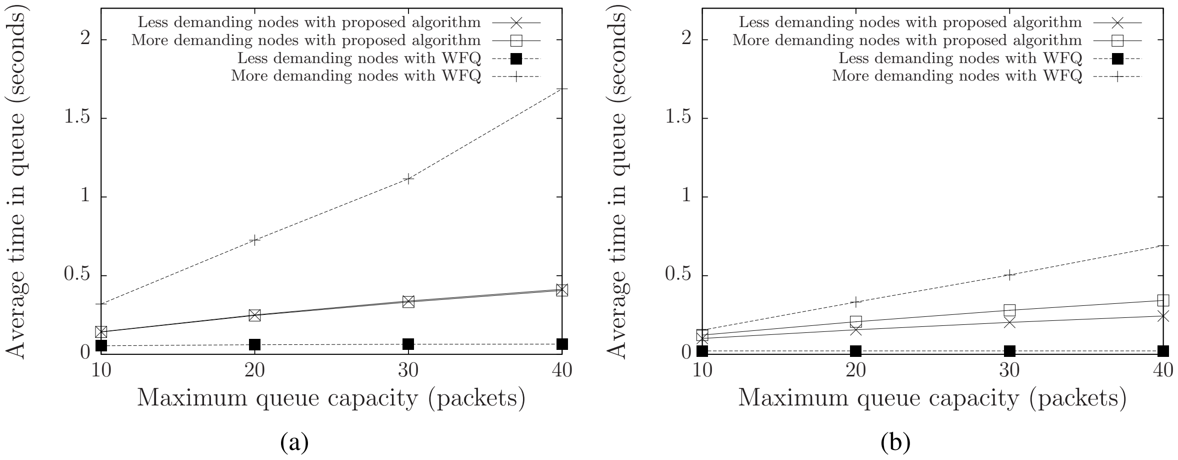
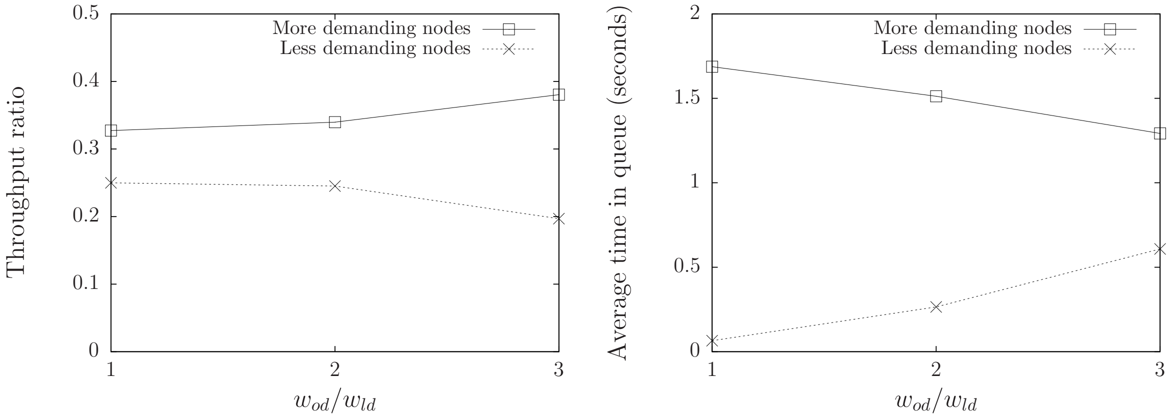


Figure 5.9: Packet average time in queue. The proposed algorithm was set with $\eta_i^{th} = 0, \forall i \in \mathcal{W}$ and WFQ with equal weights among all queues. Loads of more demanding nodes and less demanding nodes are set to: (a) 0.8 and 0.25, respectively; (b) 0.5 and 0.1, respectively.

protection to less demanding nodes according to $\eta_i^{th}, \forall i \in \mathcal{W}$, regardless of which wireless nodes are the less demanding.

In what concerns to queuing delay, the proposed algorithm presents much better results in terms of fairness than WFQ, as shown in Figure 5.9(a). This has to do with two issues. First of all, WFQ will forward packets in queues according to the weights of these queues. Since equal weights were given, packets from less demanding nodes will more often get ahead of already queued packets from more demanding nodes. With the proposed algorithm, packets are inserted in queue according to their arrival and, as such, contrarily to what happens when WFQ is used, queuing delays of packets belonging to more demanding wireless nodes are not affected. Besides this, our algorithm adopts a preventive behavior when dealing with excessive packets of over demanding nodes, which WFQ does not. That is, our algorithm discards excessive packets that are expected to be dropped at some point later in the path, avoiding unfruitful use of resources and increased queuing delay that these excessive packets cause to other packets. WFQ, on the other hand, does not have this preventive behavior. That is, packets will be accepted and forwarded as long as there is capacity, even if there is a high probability of being dropped at subsequent nodes, due to insufficient resources. As a result, with WFQ, resources are wasted when packets do not reach their destination and unnecessary queuing delays are added. A smaller gap on average delay exists between the WFQ and the proposed algorithm if loads are reduced, as can be seen in Figure 5.9(b).

In order to ensure fairness in delay when using WFQ, one might think that weights could be



(a) (b)

Figure 5.10: Effect of the weight increase of over demanding nodes, w_{od}, relative to the weight of less demanding nodes, w_{ld}, in terms of: (a) average waiting time in queue; (b) throughput ratio. Over demanding nodes were set with a load of 0.8 and less demanding nodes with 0.25. Queues with a maximum capacity of 40 packets were used.

adjusted. This approach, however, would decrease the protection provided to less demanding nodes, as can be seen in Figure 5.10. For this reason, WFQ seems to be more appropriate to control the waiting time in queue of specific streams, rather than finding an equilibrium in both bandwidth access and delay for every node. For example, WFQ would be suitable to control waiting times of different types of streams, such as VoIP, IPTV and data traffic. On the other hand, the algorithm being proposed here is suitable for bandwidth access control while providing similar queuing delay conditions to users.

Another observation is related with the effect that the number of over demanding nodes has on results. Results show that full protection is still provided to less demanding routers even when there are many over demanding routers, which does not happen with FIFO. Figure 5.11 compares the average throughput ratio of the less demanding nodes when using the proposed algorithm, WFQ and FIFO. As the number of over demanding nodes increases, the throughput of less demanding nodes reduces when using FIFO, while the proposed algorithm and WFQ were able to keep the throughput of less demanding nodes. This means that, despite the congestion increase, caused by the higher number of over demanding nodes, the less demanding ones can still maintain a steady throughput.

Concerning the depth of the independent network structure, and according to Figure 5.12, results show that this has no influence on the throughput achieved by the less demanding nodes when the proposed algorithm is used. For instance, the throughput of the less demanding nodes

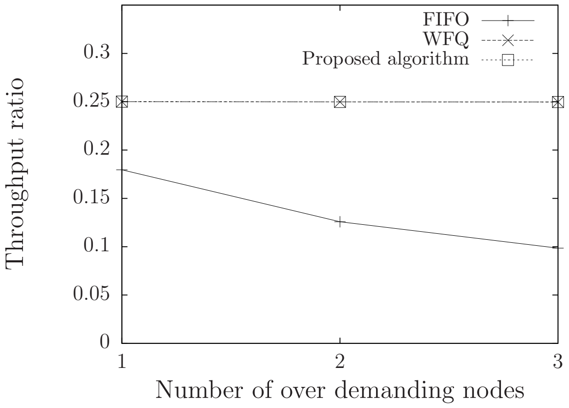


Figure 5.11: Average throughput ratio experienced by the less demanding nodes when a different number of over demanding nodes exist. The proposed algorithm was set with $\eta_i^{th} = 0, \forall i \in \mathcal{W}$ and WFQ with equal weights among all queues. Loads of more demanding nodes and less demanding nodes are set to 0.8 and 0.25, respectively. Queues with a maximum capacity of 40 packets were used.

in the independent networks of Figure 5.6(a) and Figure 5.6(d) are similar, despite the structure from Figure 5.6(d) being deeper.

It is worth noting the similar gap between FIFO and the other two approaches in Figure 5.12 for the independent networks of Figure 5.6(a) and Figure 5.6(b), despite the structure from Figure 5.6(b) being deeper. That is because the number of routers sharing the same connection to the gateway is the same. In the independent network from Figure 5.6(c), the gap between FIFO and the other two approaches is the smallest of all tested networks, since only two routers share the same connection with the gateway. A small gap means that the less demanding nodes require a low protection, while a high gap means that a great protection is needed. As such, and according to Figure 5.12, the protection needed by the less demanding nodes depends on the number of routers sharing the same connection to a gateway.

To better understand that our algorithm will not allow nodes to hurt the QoS of others, we have simulated a scenario where node 3 from the independent network in Figure 5.6(b) increases its load from 0.25 to 0.8 at the simulation time $t = 3000$s, while others keep their load of 0.25. In Figure 5.13, it is possible to see the effect that such increase has on nodes 4 and 5. If FIFO is used, the throughput of nodes 4 and 5 drops immediately. Our algorithm is able to recognize that the increase in load by node 3 would hurt the performance of other nodes, and node 3 is obligated to deny the excessive requests so that other nodes are not affected.

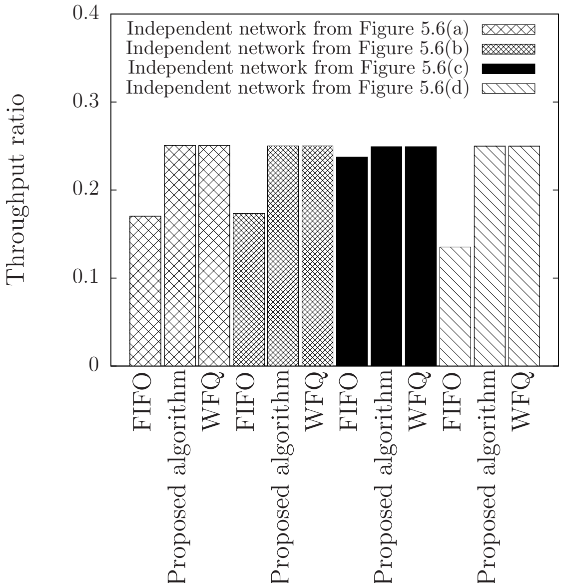


Figure 5.12: Average throughput ratio experienced by the less demanding nodes in the various independent networks tested. The proposed algorithm was set with $\eta_i^{th} = 0, \forall i \in \mathcal{W}$ and WFQ with equal weights among all queues. Loads of more demanding nodes and less demanding nodes are set to 0.8 and 0.25, respectively. Queues with a maximum capacity of 40 packets were used.

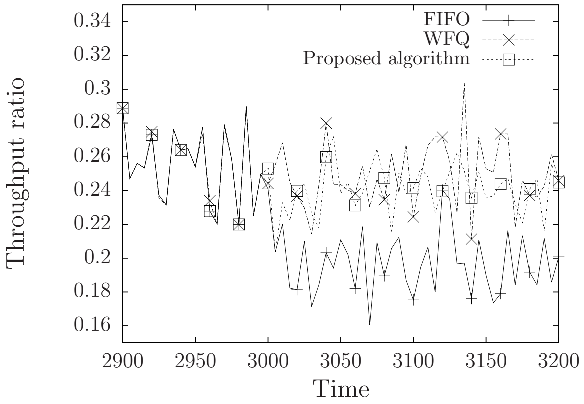


Figure 5.13: Average throughput ratio of nodes 4 and 5 from independent network of Figure 5.6(b) when node 3 increases its load from 0.25 to 0.8 at 3000s. The proposed algorithm was set with $\eta_i^{th} = 0, \forall i \in \mathcal{W}$ and WFQ with equal weights among all queues. Queues with a maximum capacity of 40 packets were used.

5.5 Conclusions

The analysis proves that the proposed algorithm is able to protect the less demanding nodes from the greediness of the over demanding nodes, avoiding starvation for bandwidth. Moreover, delays are kept similar among all users, easing further development of QoS schemes that are able to prioritize traffic with different requirements (IPTV, VoIP, web, etc.) in the same distribution network.

5.6 Summary

In this chapter, a repeated game model is presented, where all wireless routers are players that want to forward as much traffic as possible. This model led to the development of a bandwidth allocation algorithm with fairness concerns. With this algorithm, bandwidth is allocated proportionally among all wireless nodes, according to their requirements, as long as fairness is being provided to less demanding wireless nodes. This type of allocation was termed limited proportional allocation, since bandwidth is proportionally allocated as long as less demanding routers receive a minimum bandwidth. The level of protection, i.e. the minimum bandwidth that less demanding routers receive, is specified by a parameter, meaning that the algorithm can be configured according to the network needs. Moreover, the proposed algorithm is also able to obtain fairness in terms of queuing delays. This opens way for implementation of QoS support since it becomes easier to ensure the correct operation of services in networks with fair conditions, both in terms of bandwidth and experienced delays.

CHAPTER 6

Energy Efficient Routing Algorithm

6.1 Introduction

Energy efficiency is becoming an increasingly important issue. In communication infrastructures, the majority of the energy is consumed at the access section, where new technologies have been proposed recently to fulfill the growing demands for bandwidth and ubiquity [80, 101]. One of such technologies is the FiWi access network. The front end of FiWi access networks can be a wireless mesh with wireless routers scattered throughout an area. This mesh topology provides great routing flexibility, which can be exploited to improve energy efficiency [94,102]. For instance, routes longer than the shortest ones can be used in order to improve sleeping periods of devices throughout the network.

In this chapter, an energy efficient routing algorithm is proposed for FiWi access networks. To achieve such goal, firstly, a network model is developed, based on network formation theory. This model needs to be aware of features and capabilities of wireless and optical technologies to achieve overall energy efficiency at front and back end. With the model in place, several formation processes were then tested in order to obtain insights on how energy efficient routes can be created, and where in the network it is more likely that route changes will improve energy efficiency. Based on the obtained insights, a heuristic algorithm is proposed, tested and analyzed.

The rest of this chapter is organized as follows. In Section 6.2, some network formation theory concepts are adjusted to the problem in question. An energy consumption model is presented in Section 6.3. Then, all formation processes are tested and analyzed in Section 6.4. Based on this analysis, a heuristic algorithm is developed, tested and analyzed in Section 6.5. Finally, this chapter ends with a summary.

Contributions:

***i*)** Development of a model based on network formation theory to study the establishment of energy efficient routes in FiWi access networks with a WMN front end.

***ii*)** Development of a new stability concept and adapt dynamic network formation processes in order to be compatible with the objective of building energy efficient routes.

***iii*)** Analysis of the results of the network formation processes and obtain insights on how routes can be established to increase energy efficiency and traffic delivered with success.

***iv*)** Development of an energy efficient heuristic algorithm to establish efficient routes, both in terms of energy efficiency and in terms of traffic delivered successfully.

Publications:

The work in this chapter has been published in [27, 28].

6.2 Routing through Network Formation

Unlike to the previous two chapters, here independent networks will be formed, i.e., are not given in advance. This formation of the tree structured independent networks resembles co-operative games, where players form coalitions in order to improve their outcome. However, coalition game theory considers only which players form the coalitions, while in our case the connections actually established between players are important, i.e. who is connected to whom. Network formation theory addresses such kind of formation, examining which players are part of each group and which connections are actually established inside each group [21].

In this chapter, unlike the previous ones, the ONUs are the root nodes of the independent networks. Hence, gateway routers still have one node above them, $\gamma_i^- \neq \emptyset, \forall i \in \mathcal{G}$. The reason for this difference is that, both energy expenditures of the optical and radio transceivers need to be considered. Note, however, that ONUs will not be players. Wireless routers and gateways, collectively called wireless nodes, will be the players in this chapter.

Every wireless node, $i \in \mathcal{W}$, is a player trying to establish the best wireless connections in order to obtain energy efficient routes. In accordance to Definition 2.13, the term *component* will be used when referring to a group of players with established connections among them. More specifically, each independent network will be a component, which can be redefined using the nomenclature from Section 3.3.

Definition 6.1 (Component) *A component is a group of wireless routers/players where, for any combination of two of its elements* $i \in \mathcal{W}$ *and* $j \in \mathcal{W}$, $i \neq j$, *the following condition is true:* $\left\{\{i\} \cup \Gamma_i^-\right\} \cap \left\{\{j\} \cup \Gamma_j^-\right\} \neq \emptyset$.

A connection established between wireless nodes $i \in \mathcal{W}$ and $j \in \mathcal{W}$, $i \neq j$, is denoted by ij. The set of all the established connections form a network $\mathcal{L}^E$, and the set of all possible networks is represented by $\mathcal{L}$. Each network $\mathcal{L}^E \in \mathcal{L}$, as a result of the established connections, has its own network value that can be calculated using a value function, introduced in Definition 2.14. For the problem addressed in this chapter, the network value will measure the energy efficiency obtained by the established routes. Therefore, the objective is to reach a network $\mathcal{L}^E \in \mathcal{L}$ with the highest possible network value. Such network is termed efficient network, as in the Definition 2.18.

A network value is a common value that may be distributed among players, wireless nodes in our case. This is done by means of an allocation rule, already introduced in Definition 2.15. Every wireless node will try to improve its allocation value as much as possible by carefully establishing and severing wireless connections. This will be done by fulfilling some network formation process, discussed in the following section. When no player is able to increase its allocation value, following such network formation process, then the network is said to be stable. According to Section 2.5.3, stability has been modeled in many different ways in the literature. However, those stability models allow stable networks to have unconnected players. Such situation is not desirable for the problem addressed in this chapter because it would allow the existence of unconnected wireless routers, which would not be able to send/receive traffic. Here, a new stability notion, termed *complete connection stability*, is presented.

Definition 6.2 (Complete Connection Stable Network) *A network* $\mathcal{L}^E \in \mathcal{L}$ *is complete connection stable if all the following conditions hold:*

1. *for all* $i \in \mathcal{R}$, *there exists one path* $n_1, n_2, \ldots, n_K$ *such that* $\forall k \in \{1, \ \ldots, \ K-1\}$, $n_k n_{k+1} \in \mathcal{L}^E, n_1 = i$ *and* $n_K \in \mathcal{G}$,
2. *for all* $ij \in \mathcal{L}^E$ *and all* $z \in \mathcal{W}$:
    - *(a)* $v_i\left(\mathcal{L}^E\right) \geq v_i\left(\left\{\mathcal{L}^E \setminus \{ij\}\right\} \cup \{iz\}\right)$ *and* $v_z\left(\mathcal{L}^E\right) \geq v_z\left(\left\{\mathcal{L}^E \setminus \{ij\}\right\} \cup \{iz\}\right)$,
    - *(b)* $v_j\left(\mathcal{L}^E\right) \geq v_j\left(\left\{\mathcal{L}^E \setminus \{ij\}\right\} \cup \{jz\}\right)$ *and* $v_z\left(\mathcal{L}^E\right) \geq v_z\left(\left\{\mathcal{L}^E \setminus \{ij\}\right\} \cup \{jz\}\right)$.

The complete connection stability dictates through condition 1 that every wireless router has one uplink wireless connection that leads to a gateway router. Also, through conditions 2a and

2b, wireless nodes can not increase their allocation values by switching their current uplink connection by another one.

Wireless nodes will keep improving their allocation values until a stable network is reached. However, if the stability model of Definition 6.2 is assumed, then the resulting network may not be the most efficient one because only pairs of directly connected players are being checked for better allocation values at conditions 2a and 2b of Definition 6.2. As explained in Section 2.5.3, some allocation improvements may only be achieved by establishing and/or severing two or more wireless connections simultaneously, which by themselves alone do not bring any benefit. The strong stability from Definition 2.17 could be used instead. However, it would be computationally too expensive, since all combinations of connections would have to be tested for allocation value improvements. Note that the objective is to develop an energy efficient routing algorithm and computing the algorithm also consumes energy. Therefore, a computationally expensive routing algorithm could deter any efficiency gained by careful route choices [103]. A stable and non efficient network will be termed, from here on, as *hidden profitable network*.

Definition 6.3 (Hidden Profitable Network) *A network $\mathcal{L}^E \in \mathcal{L}$ is a hidden profitable network if it is complete connection stable, according to Definition 6.2, while not being efficient, according to Definition 2.18.*

6.2.1 Network Formation Processes

Complete connection stability merely indicates the desired network configuration properties. A process is still needed to actually achieve a complete connection stable and, if possible, efficient network. That is, connections will have to be established or severed to create routes that are as energy efficient as possible. Here, the focus will be on dynamic approaches where networks are formed over several iterations.

Before introducing the formation processes considered in this chapter, it is important to note that different schemes can be used by the MAC layer for bandwidth access. In this chapter, a MAC layer based on a bandwidth allocation scheme is assumed, instead of a collision avoidance one. This assumption is related with the fact that bandwidth allocation based MACs are more energy efficient than the collision avoidance schemes. This is so because collisions may still be frequent in a collision avoidance scheme, leading to retransmissions and unfruitful use of bandwidth and energy [103]. Moreover, formation processes require accurate information on the length of scheduled transmission, reception and sleep periods, which can be easily obtained if a bandwidth allocation based MAC is used. With a collision avoidance scheme, such information would be less precise or difficult to obtain.

The dynamic network formation processes under analysis are discussed next.

Dynamic Network Formation (DNF)

This approach, introduced in Section 2.5.3, starts from an empty network, with no established connections, and then establishes or severs connections, at each iteration, in order to increase the allocation values of the players involved in the connection establishment/dissolution. The process ends when a stable network is reached.

The DNF has one drawback. There is no guarantee that every wireless router will have one established uplink connection, i.e. a wireless connection that leads to a gateway router in order to send traffic to/from the Internet. Moreover, it is even possible to get stuck at an empty network, i.e. a network without any established connection. Such scenarios contradict the first condition of the complete connection stability from Definition 6.2, which dictates that every wireless router $i \in \mathcal{R}$ needs to have one established connection that leads to a gateway router. That is, a complete connected stable network may not be reached. Hence, a modified version of DNF is presented. This modified DNF starts from a network $\mathcal{L}^E$ where every wireless router has already one established uplink connection. From this starting point, and at each iteration, one established uplink connection may be replaced by another one that is not in use, ensuring that every wireless router has one established uplink connection. Its operation can be described as follows:

Step 1: Randomly choose a wireless router $i \in \mathcal{R}$.

Step 2: Determine if i can have its allocation value increased by replacing its current uplink connection, $ij \in \mathcal{L}^E$, by another one that is not in use, $ik \notin \mathcal{L}^E$. Note that the wireless node k, at the other end of the new uplink connection, will only accept this new connection if it does not decrease its own allocation value. If there is more than one wireless connection that satisfies this condition, then the one that provides the highest allocation value increase to i is used. In case the uplink connection of i is changed, allocation values of wireless nodes affected by this change will have to be recalculated.

Step 3: If the current network, $\mathcal{L}^E \in \mathcal{L}$, is complete connection stable, then the process ends. Otherwise, go back to Step 1.

From here on, this modified DNF will simply be called DNF.

A drawback of DNF, however, is that it may get stuck in a hidden profitable network. Two possible approaches to overcome this issue are: *i*) a stochastic approach similar to the one introduced in Section 2.5.3; *ii*) a farsighted approach similar to the one introduced in Section 2.5.3. These two approaches are discussed next.

Stochastic Network Formation (SNF)

This approach randomizes decisions in order to disrupt hidden profitable networks and unlock further improvements. Here, an SNF, based on the DNF just presented, is proposed. It is composed of two stages. At the first stage, DNF is run until a complete connected stable network is reached. Then an iterative second stage starts where, similarly to DNF, a wireless router is randomly chosen at each iteration. If the chosen wireless router has a link that provides a greater bandwidth allocation, then that link may be chosen to become the next uplink connection with probability ϵ. If more than one connection can improve the bandwidth allocation, then the first to be found, and chosen with probability ϵ, will be the one used. Note that only connections improving the bandwidth allocation are considered. This avoids pure random choices that could result in meaningless connection changes. Whenever a change is made at the second stage, the first stage will be run again. The SNF ends when no changes occur at the second stage or after the first stage has run for a maximum number of specified times. SNF can be described as follows:

Step 1: Run DNF.

Step 2: Start second stage:

Step 2.1: Randomly choose a wireless router $i \in \mathcal{R}$.

Step 2.2: Search for wireless connections of i that are not being used and can increase the bandwidth allocation of i if used as its new uplink. The first of such connections to be found, and selected with probability ϵ, will become the new uplink of i. In case the uplink connection of i has changed, allocation values of wireless nodes affected by this change will have to be recalculated and the process will move on to the next step. Otherwise, if no changes occurred, then the process will end.

Step 2.3: If DNF, at step 1, ran already for the maximum number of times, then end the process. Otherwise, go back to Step 1.

Farsighted Network Formation (FNF)

This approach tries to predict connection changes that are not immediately profitable but will allow higher improvements in the future. Here, a DNF composed of two stages is proposed. At the first stage, DNF is run until a complete connection stable network is reached. Then a second iterative stage starts where a group of wireless routers are randomly chosen at each iteration. If that group of wireless routers can increase their allocation values by simultaneously changing their uplink connections, then the uplink connections will be changed accordingly. Note that these uplink changes would not be profitable if done individually. Only a limited number of simultaneous uplink changes can be tested, otherwise the processing time would be very long. The objective of this second stage is to get out of hidden profitable networks, where DNF gets stuck, improving allocation and network values. When a change is made at the second stage, the first stage will then be run again. If no changes occur at the second stage, then FNF ends execution. FNF can be described as follows:

Step 1: Run DNF.

Step 2: Start second stage:

Step 2.1: Randomly choose a group of wireless routers, either belonging to the same component or different components. The number of wireless routers to choose is equal to the number of allowed simultaneous uplink changes.

Step 2.2: Calculate the allocation values for all combinations of uplink changes involving the chosen wireless routers.

Step 2.3: If there are combinations of uplink changes that lead to allocation value increases, then choose the combination that provides the highest aggregate increase to all wireless routers and go back to Step 1. Otherwise, proceed to the next step. In case of uplink connection changes, allocation values of wireless nodes affected by these changes will have to be recalculated.

Step 2.4: If all combinations of wireless routers were already chosen in Step 2.1 without any uplink connection change, then the process will end. Otherwise, go back to Step 2.1 to choose another group of wireless routers.

6.3 Energy Efficient Routing Model

6.3.1 Energy Consumption

Energy efficient routing methods in FiWi access networks should be aware of the capabilities of optical and wireless technologies in an integrated manner. That is, routes at the wireless front end should be established by taking into consideration the energy consumption of optical and wireless transceivers, as well as the scheduling policy for sleeping periods. Here, it will be assumed that nodes will always go to sleep whenever there are no scheduled transmissions or receptions of local or foreign traffic. The only exception is when the time until the next scheduled transmission or reception is shorter than the time needed to switch to sleep mode and wake up again. This time, during which a node is in wake mode without transmitting or receiving traffic, is called *unproductive time* and the energy consumed during this period is termed *unproductive energy*.

When accounting for the total energy expenditure, one has to consider that traffic from/to a source/sink will be forwarded through several hops, affecting wake, sleep and unproductive periods of several nodes. Hence, each wireless node $i \in \mathcal{W}$ will be held accountable for part of the energy consumed at nodes in Γ_i^-. More specifically, $i \in \mathcal{W}$ will be accountable for: *i*) the energy that nodes in Γ_i^- consume to transmit/receive traffic belonging to i; *ii*) part of the energy that nodes in Γ_i^- consume while in sleep mode; *iii*) part of the unproductive energy that nodes in Γ_i^- consume. These three constituents of the energy consumption will be denoted by e_i^{DLV}, e_i^{SLP} and e_i^{UNP}, respectively. The total energy consumed by all transceivers, in order to send and receive traffic emanating/arriving from/to a node $i \in \mathcal{W}$, can be calculated by:

$$e_i = e_i^{DLV} + e_i^{SLP} + e_i^{UNP}. \tag{6.1}$$

When determining e_i^{DLV}, e_i^{SLP} and e_i^{UNP}, the term *byte time* will be used to refer to the time that one byte takes to be transmitted or received by a device, which can be a wireless radio or an optical transceiver, with its meaning and value being changed accordingly. The following notation is assumed for values that do not change during network lifetime:

E^O: Energy per byte time that is consumed by the transceiver of an ONU in wake mode.

E^T: Energy per byte time that is consumed by a wireless radio in transmit mode.

E^R: Energy per byte time that is consumed by a wireless radio in receive mode.

E_i^S: Energy per byte time that is consumed by the transceiver of node $i \in \mathcal{N}$ in sleep mode.

E_i^W: Energy per byte time that is consumed by the transceiver of node $i \in \mathcal{N}$ when waking up.

Besides the just mentioned notation, additional variables become necessary, which may change according to network conditions such as the currently established routes:

β_i: Local traffic load of wireless node $i \in \mathcal{W}$.

β_i^A: Bandwidth allocation at $i \in \mathcal{W}$ for downstream and upstream local traffic. It is assumed that TDM is used by transmissions within the interference range, hence, β_i^A will be adjusted according to the load and bandwidth allocation of interfering nodes, so that the medium is shared and interferences are avoided.

h_i: Number of hops between wireless router $i \in \mathcal{R}$ and its gateway along the corresponding component.

τ_i^S: Average number of byte times per second that a node $i \in \mathcal{N}$ spends in sleep mode.

τ_i^W: Average number of byte times per second that a node $i \in \mathcal{N}$ takes to wake up.

τ_i^{UR}: Average number of byte times per second that the radio of a wireless node $i \in \mathcal{W}$ spends in receive mode without actually receiving traffic. That is, unproductive time while in receive mode.

τ_i^{UT}: Average number of byte times per second that the radio of a wireless node $i \in \mathcal{W}$ spends in transmit mode without actually transmitting traffic. That is, unproductive time while in transmit mode.

τ_i^{UW}: Average number of byte times that the optical transceiver of an ONU $i \in \mathcal{O}$ spends in wake mode without actually transmitting or receiving any traffic. That is, unproductive time in wake mode.

Energy consumed when delivering traffic

As aforementioned, packets will have to go through several hops in order to reach a specific ONU or wireless router, considering upstream and downstream transmissions respectively. This means that an average of β_i^A bytes per second, emanating/arriving from/to wireless router i, will consume $\beta_i^A \left(h_i \left(E^T + E^R\right)\right)$ Joules per second at the front end, assuming that wireless radio transceivers consume E^T Joules per byte time in transmit mode, E^R Joules per byte time in receive mode and that i is h_i hops away from its gateway router. As for the back end, it is considered that the transceiver of an ONU consumes E^O Joules per byte time when in wake mode to send/receive packets. Therefore, the energy expenditure per second to ensure a deliver of β_i^A bytes per second to/from node i is:

$$e_i^{DLV} = \beta_i^A \left(E^O + h_i \left(E^T + E^R\right)\right). \tag{6.2}$$

For simplicity, the energy consumed to transfer packets between gateway routers and ONUs is not taken into consideration, as gateway routers can be connected or attached to ONUs in many different ways and can support many different working modes [13, 104].

Energy consumed when in sleep mode

Assuming that the transceiver of a node $i \in \mathcal{N}$ consumes E_i^S Joules per byte time in sleep mode and, on average, stays in that mode for τ_i^S byte times per second, then i will consume an average of $\tau_i^S E_i^S$ Joules per second while in sleep mode. The time that i takes to wake up from sleep/standby needs also to be considered. If node $i \in \mathcal{N}$ takes an average of τ_i^W byte times per second to wake up and uses E_i^W Joules per byte time, then it will consume $\tau_i^S E_i^S + \tau_i^W E_i^W$ Joules per second during sleep mode and while waking up.

The time that a node $i \in \mathcal{N}$ stays in sleep mode depends on local traffic and on traffic to/from nodes in Γ_i^+. Therefore, the energy spent in sleep mode should be divided among all nodes in $\Gamma_i^+ \cup \{i\}$. Similarly, i also influences the sleeping periods of nodes in Γ_i^- and, as such, should be held accountable for a portion of the energy that those nodes consume while in sleep mode and waking up. Hence, node $i \in \mathcal{W}$ is responsible for the consumption of the following amount of sleep mode energy:

$$e_i^{SLP} = \left[\sum_{j \in \left\{ \left(\Gamma_i^- \cup \{i\} \right) \cap \mathcal{W} \right\}} \frac{\tau_j^S E_j^S + \tau_j^W E_j^W}{\left| \Gamma_j^+ \cup \{j\} \right|} \right] + \frac{\tau^S_{\Gamma_i^- \cap \mathcal{O}} E^S_{\Gamma_i^- \cap \mathcal{O}} + \tau^W_{\Gamma_i^- \cap \mathcal{O}} E^W_{\Gamma_i^- \cap \mathcal{O}}}{\left| \Gamma^+_{\Gamma_i^- \cap \mathcal{O}} \right|}, \qquad (6.3)$$

where the first part accounts for the consumption at wireless nodes in $\left\{ \left(\Gamma_i^- \cup \{i\} \right) \cap \mathcal{W} \right\}$, that will be required to forward traffic belonging to i, and the second part accounts for the consumption at the ONU being used by i, $\Gamma_i^- \cap \mathcal{O}$.

Unproductive energy consumed in wake mode

Assuming that the radio of a wireless node $i \in \mathcal{W}$ spends an average of τ_i^{UT} and τ_i^{UR} byte times per second in transmit and receive mode, respectively, without sending or receiving traffic, then the unproductive energy consumed per second at i will be: $\tau_i^{UR} E^R + \tau_i^{UT} E^T$. Similarly to wireless nodes, ONUs may also have unproductive time periods. Considering that the transceiver of the ONU, used by a wireless router $i \in \mathcal{W}$, stays in wake mode for $\tau^{UW}_{\Gamma_i^- \cap \mathcal{O}}$ byte times per second on average without sending or receiving traffic, then the ONU will consume $\tau^{UW}_{\Gamma_i^- \cap \mathcal{O}} E^O$ Joules of unproductive energy per second. Similarly to what was done in expression (6.3), the unproductive energy consumed at node $i \in \mathcal{N}$ should be divided among all nodes in $\Gamma_i^+ \cup \{i\}$, and a portion of the unproductive energy of nodes in Γ_i^- should be assigned to i. Hence, every node $i \in \mathcal{W}$ is responsible for the consumption of the following amount of unproductive energy:

$$e_i^{UNP} = \left[\sum_{j \in \left\{ \left(\Gamma_i^- \cup \{i\} \right) \cap \mathcal{W} \right\}} \frac{\tau_j^{UR} E^R + \tau_j^{UT} E^T}{\left| \Gamma_j^+ \cup \{j\} \right|} \right] + \frac{\tau^{UW}_{\Gamma_i^- \cap \mathcal{O}} E^O}{\left| \Gamma^+_{\Gamma_i^- \cap \mathcal{O}} \right|}, \tag{6.4}$$

where the first part accounts for the consumption at wireless nodes in $\left\{ \left(\Gamma_i^- \cup \{i\} \right) \cap \mathcal{W} \right\}$, that will be required to forward traffic belonging to i, and the second part accounts for the consumption at the ONU being used by i, $\Gamma_i^- \cap \mathcal{O}$.

6.3.2 Network Model

Since our goal is to find the most energy efficient routes, expressions (6.2), (6.3) and (6.4) will become part of the value function, $\Upsilon\left(\mathcal{L}^E\right)$, so that a network value is obtained (see Definition 2.14 in Section 2.5.2). One might think that $\frac{\sum_{i \in \mathcal{W}} \beta_i^A}{\sum_{i \in \mathcal{W}} e_i}$ should be used to calculate the network value. However, the use of such function may lead to paths that, although energy efficient, would forward just a small fraction of the intended traffic. To avoid this, the fraction of traffic successfully delivered, $\frac{\sum_{i \in \mathcal{W}} \beta_i^A}{\sum_{i \in \mathcal{W}} \beta_i}$, should also be taken in consideration. Hence, the network value of a network $\mathcal{L}^E \in \mathcal{L}$ is calculated using:

$$\Upsilon\left(\mathcal{L}^E\right) = \frac{\sum_{i \in \mathcal{W}} \beta_i^A}{\sum_{i \in \mathcal{W}} e_i} \frac{\sum_{i \in \mathcal{W}} \beta_i^A}{\sum_{i \in \mathcal{W}} \beta_i}. \tag{6.5}$$

As for the allocation rule used to distribute the network value among all wireless nodes, an *egalitarian allocation rule* is used:

$$v_i\left(\mathcal{L}^E\right) = \frac{\Upsilon\left(\mathcal{L}^E\right)}{|\mathcal{W}|}. \tag{6.6}$$

This allocation rule distributes the network value equally among all players, aligning the network value with the individual interests of players and avoiding cycles [42]. In the context of FiWi access networks, the existence of such cycles, which were introduced in Section 2.5.3, would mean that wireless routers would always be changing their uplink connections without ever stabilize.

Table 6.1: Parameters of generated networks.

Number of wireless nodes, $\|\mathcal{W}\|$	$15; 19; 23; 27$
Number of gateways, $\|\mathcal{G}\|$	$3; 4; 5$
Load ranges of wireless nodes	0-0.5; 0.2-0.7; 0-1; 0.5-1
Average node degree	4.5

6.4 Comparison of Network Formation Processes

6.4.1 Simulation Setup

In order to identify the formation process that gives rise to the most energy efficient network, and to understand how each process changes the network in order to increase energy efficiency, which will be useful to develop an efficient heuristic algorithm, a set of simulations were done. For this purpose, several random networks were generated using the weighted proximity algorithm in [105]. The parameters used to build these networks are summarized in Table 6.1. Different combinations of network size, gateway set and load range were tested. Ten different networks of each size were created and, for each network, five different gateway placements were done, for $|\mathcal{G}| = 3$, 4 and 5. A uniform distribution was used to select gateway routers among network nodes. For each combination of network size, gateway placement and load, five simulations were done using different seeds for random number generation. ONUs and gateways are directly attached.

In what concerns to network formation processes, as explained in Section 6.2.1, a starting point is needed where every wireless router has already one established uplink connection that leads to a gateway. In these simulations, the shortest path (SP) was used as the input for all formation processes since it is a widely used routing method and may serve as a reference. FNF was set to test at most three uplink changes simultaneously and to run until no changes occur at the second stage. As for SNF, different experiments were done for different values of ϵ (from 0.1 to 0.5, in steps of 0.1) and it was set to run the first stage up to five iterations.

The considered energy consumptions per byte time are shown in Table 6.2. Such values were obtained considering that ONUs have a bandwidth capacity of 1Gbps for upstream and 1Gbps for downstream, consume 3.85W in wake mode, 0.75W in sleep mode and take 3.5ms to wake up [77, 106]. Radios have a bandwidth capacity of 100Mbps, which has to be shared among downstream and upstream, consume 1.75W in transmit mode, 0.75W in receive mode, 0.01W in standby and take 5ms to wake up [103]. Therefore, the transceiver of an ONU takes

Table 6.2: Energy consumption during one byte time.

Transceiver of ONU in wake mode $\left(E^{O}\right)$	30.8×10^{-9}J
Transceiver of ONU in sleep mode $\left(E_i^{S}, i \in \mathcal{O}\right)$	6×10^{-9}J
Transceiver of ONU when waking up $\left(E_i^{W}, i \in \mathcal{O}\right)$	30.8×10^{-9}J
Radio of a wireless node in transmit mode $\left(E^{T}\right)$	140×10^{-9}J
Radio of a wireless node in receive mode $\left(E^{R}\right)$	60×10^{-9}J
Radio of a wireless node in standby $\left(E_i^{S}, i \in \mathcal{W}\right)$	0.8×10^{-9}J
Radio of a wireless node when waking up $\left(E_i^{W}, i \in \mathcal{W}\right)$	140×10^{-9}J

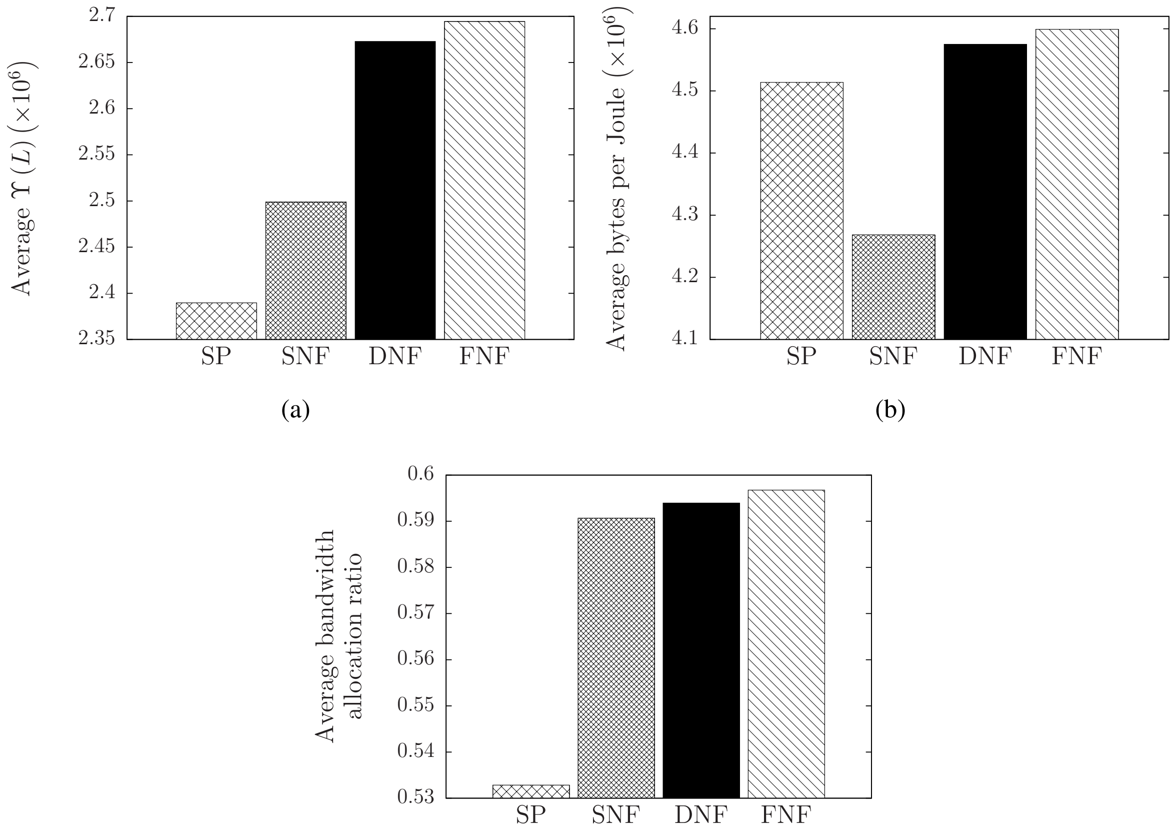
437500 byte times to wake up, while the transceiver of a wireless node takes 62500 byte times to wake up.

6.4.2 Analysis of Results

In this section, the average network value, average energy efficiency and average bandwidth allocation of the results obtained by formation processes, when applied to all the tested network scenarios, will be analyzed. Conclusions will allow us to obtain insights on how energy efficient routes can be created and where in the network it is more likely that route changes will produce energy efficiency improvements. This will serve as a basis for the development of a heuristic algorithm.

The average network values, $\Upsilon\left(\mathcal{L}^{E}\right)$, obtained by the formation processes, are plotted in Figure 6.1(a). As can be seen, all formation processes were able to obtain higher network values than SP. FNF provides the highest average network value, approximately 0.02×10^{6} more than DNF. This means that FNF was able to overcome hidden profitable networks where DNF was stuck and, as a result, network values were improved. As for SNF, an average network value better than SP is obtained, although much smaller than the one obtained by DNF. Such result means that the random method of SNF, to surpass hidden profitable networks, is not good enough and ends up making uplink changes that do not produce network value improvements. In fact, as shown in Figure 6.2, with higher values of ϵ (see Section 6.2.1), the results of SNF get worse in terms of average network value, $\Upsilon\left(\mathcal{L}^{E}\right)$, average energy efficiency, $\frac{\sum_{i\in\mathcal{W}}\beta_i^A}{\sum_{i\in\mathcal{W}}e_i}$, and average bandwidth allocation, $\frac{\sum_{i\in\mathcal{W}}\beta_i^A}{\sum_{i\in\mathcal{W}}\beta_i}$.

Let us now look into the energy efficiency and bandwidth allocation ratio, shown in Figure 6.1(b) and Figure 6.1(c). From these plots, it is possible to state that the good network values obtained by FNF are a consequence of the increase in both energy efficiency and bandwidth



(a)

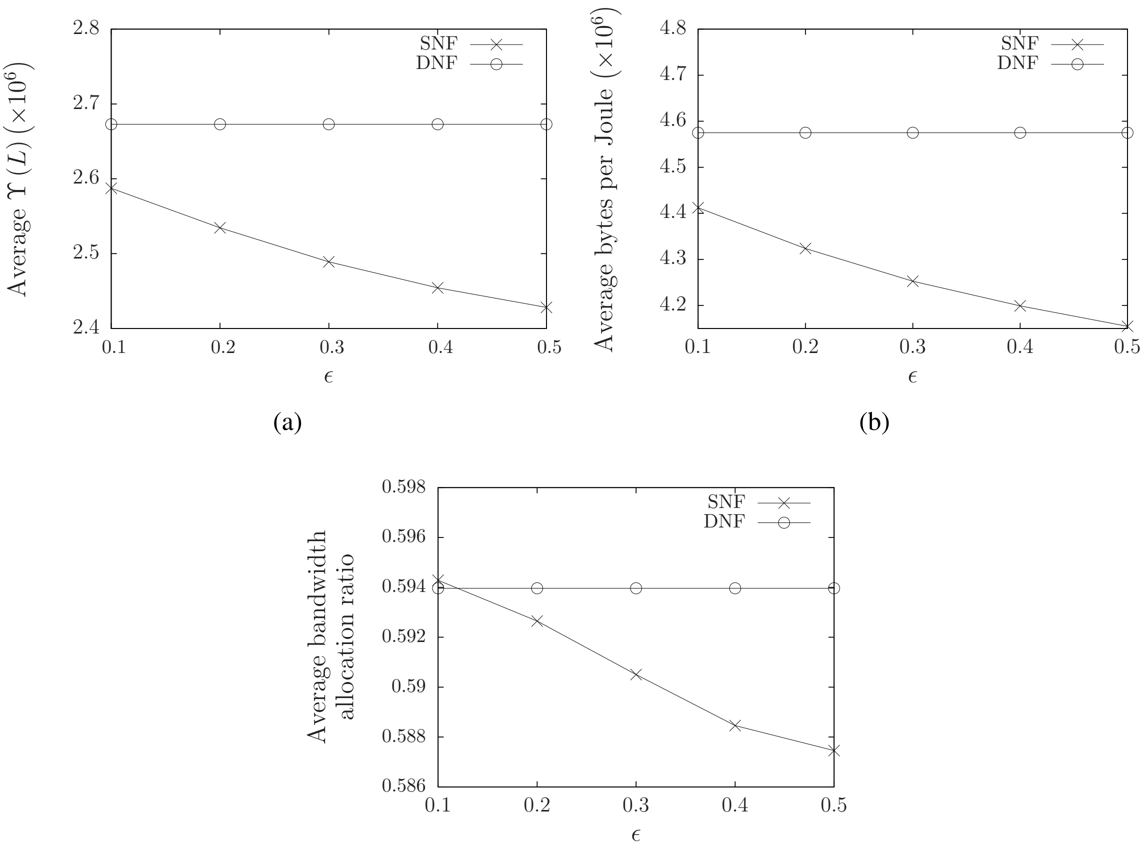
(b)

(c)

Figure 6.1: Average results of the tested formation processes and SP: (a) network value; (b) energy efficiency; (c) allocation ratio.

allocation ratio. More specifically, the energy efficiency of FNF is 0.02×10^6 higher than the one obtained by DNF. This means that FNF, in average, is able to send 20kB more than DNF for each Joule, while slightly increasing the average bandwidth allocation ratio. When compared to SP, FNF is able to send 80kB more for each Joule, while having an average bandwidth allocation ratio of almost 60% against 53% of SP.

The higher energy efficiency and higher bandwidth allocation results obtained by DNF and FNF, when compared to SP, are due to a good selection of paths. More energy efficient paths, avoiding congested areas of the network, are chosen. Concerning the number of hops, one might think that DNF and FNF paths may become too long, when compared with SP, increasing delays. However, as shown in Table 6.3, the average number of hops, of the paths obtained by the formation processes, increased only marginally when compared to SP. In fact, if the number of hops increased too much, then the energy efficiency could actually decrease, since traffic



(a) (b)

(c)

Figure 6.2: Effect that the parameter ϵ of SNF has on: (a) network value; (b) energy efficiency; (c) allocation ratio.

Table 6.3: Average number of hops of the paths obtained by the several formation processes and SP.

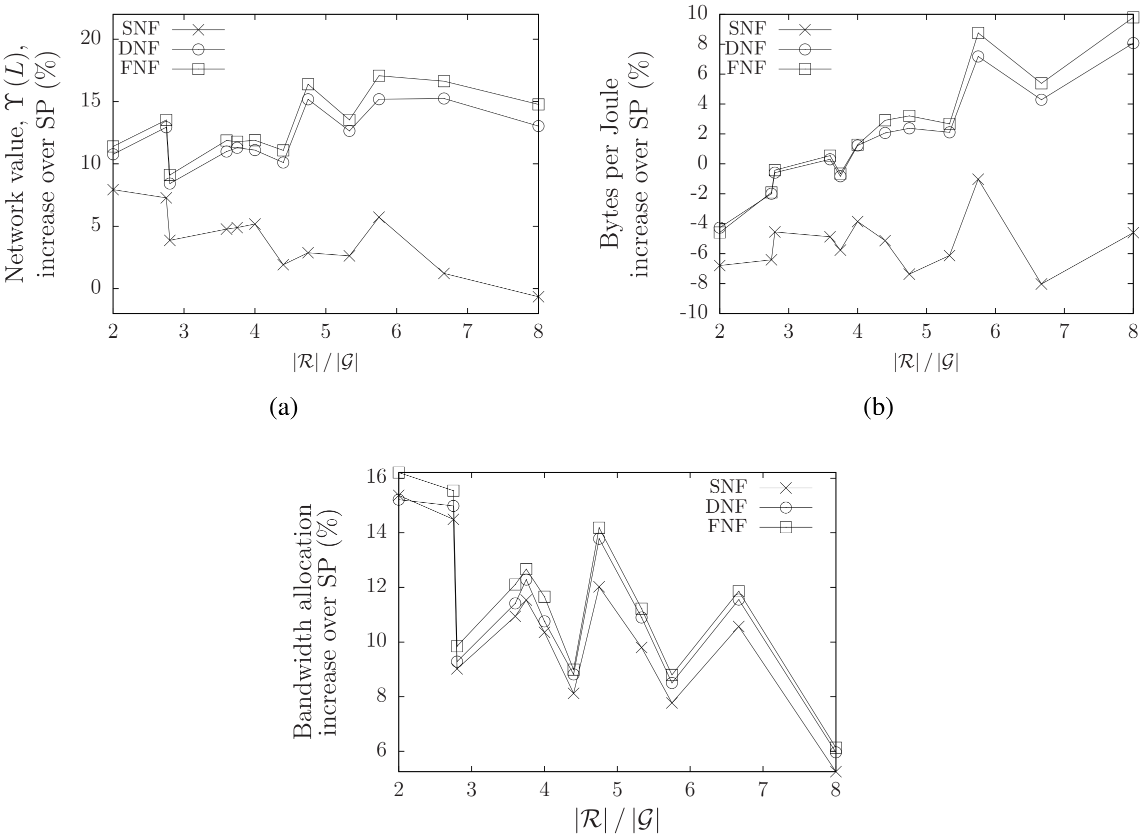
	Average number of hops
SP	1.495
DNF	1.585
SNF	1.914
FNF	1.604

would have to be forwarded through too many hops and more energy would be consumed to deliver the same amount of traffic. This means that the average delays associated with the formation processes and SP are expected to remain similar. These observations lead us to the following assumption:

Claim 6.1 *Surpassing hidden profitable networks in an accurate way, which is the case of FNF, leads to significant increases in both energy efficiency and successful traffic delivery, while maintaining similar delays.*

In average, FNF obtains the best results. However, it is necessary to check whether or not that observation still holds for different network conditions. In Figure 6.3, the results obtained by DNF, SNF and FNF are compared with the results of SP, as the ratio of wireless routers per gateway increases, $\frac{|\mathcal{R}|}{|\mathcal{G}|}$. Note that these are average results considering all tested network traffic loads. In terms of network value, Figure 6.3(a), FNF always obtains the best results for any ratio of wireless routers per gateway. As for bandwidth allocation, Figure 6.3(c), FNF also obtains the best results for any number of wireless routers per gateway, even if just by a small margin. Regarding energy efficiency, Figure 6.3(b), both DNF and FNF have negative percentages when $\frac{|\mathcal{R}|}{|\mathcal{G}|} < 3$, meaning that they were not able to get better results than SP. This is so because, in networks with a small number of wireless routers per gateway, there are not enough alternative paths that can be exploited to improve energy efficiency and the only way to improve network value is to balance traffic throughout the network, improving traffic successfully delivered. When $3 \leq \frac{|\mathcal{R}|}{|\mathcal{G}|} \leq 4$, DNF and FNF are similar to SP, i.e. there is no increase over SP. From there on, i.e. for $\frac{|\mathcal{R}|}{|\mathcal{G}|} > 4$, DNF and FNF always obtained better results than SP, while FNF obtains better results than DNF. Hence, we may conclude the following:

Claim 6.2 *FNF, in terms of network value and successful traffic delivery, always performs better than SP, DNF and SNF for any number of wireless routers per gateway. As for energy efficiency, FNF is also able to perform better, except when the network has a very low ratio of wireless routers per gateway router.*



(a)

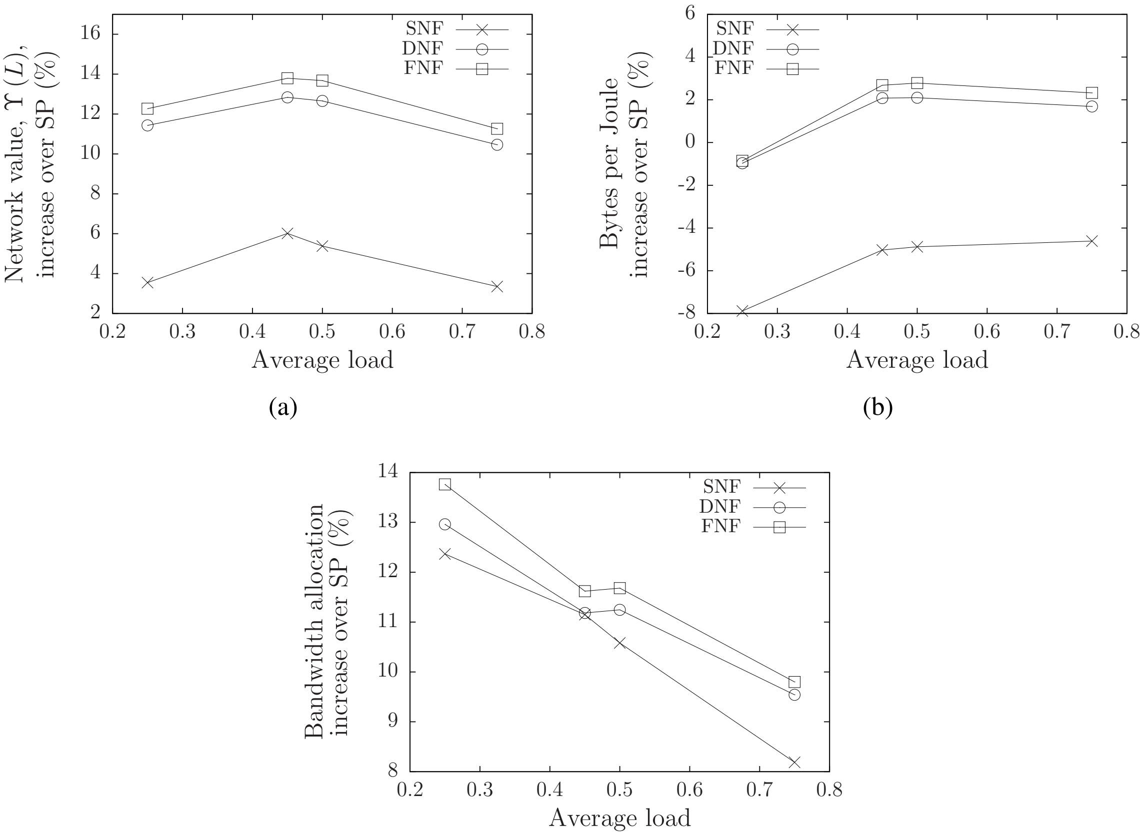
(b)

(c)

Figure 6.3: Effect that the number of wireless routers per gateway routers has on: (a) network value; (b) energy efficiency; (c) bandwidth allocation ratio.

Another network condition that may affect the results is the network traffic load. In Figure 6.4, the results obtained by DNF, SNF and FNF can be compared with the results of SP for different network traffic loads. Note that these are average results considering all possible ratios of wireless routers per gateway. In what concerns to network value, Figure 6.4(a), and traffic successfully delivered, Figure 6.4(c), FNF always obtains better results when compared to the other methods. In terms of energy efficiency, Figure 6.4(b), when average traffic is low, 0.25, DNF and FNF obtained lower results than SP. This means that when traffic load is low, it is difficult to establish routes that can efficiently optimize the scheduled transmission, reception and sleep periods. However, for higher traffic loads, FNF obtains better results than any of the other methods. Therefore, we can assume the following:

Claim 6.3 *FNF, when compared to SP, DNF and SNF, obtains better results in terms of network value and successful traffic delivery for any network traffic load. As for energy efficiency,*



(a)

(b)

(c)

Figure 6.4: Effect that the tested loads have on: (a) network value; (b) energy efficiency; (c) bandwidth allocation ratio.

the results of FNF are similar to the ones of SP and DNF when network traffic load is low, however, when network traffic load is high, FNF achieves a better energy efficiency.

6.4.3 Computational Time

In general, FNF obtains the best results in terms of network value, energy efficiency and bandwidth allocation ratio. However, it is also the most computationally expensive, even if only three wireless routers are checked for a simultaneous uplink change. More specifically, considering that the front end has $|\mathcal{R}|$ wireless routers and the average node degree is d, then, on average, the computational time of DNF depends on all possible link changes that have to be checked: $|\mathcal{R}|\, d$. As for SNF, and considering that the first stage will be run up to I iterations, its computational time depends on $|\mathcal{R}|\, dI$ possible link changes. FNF, as already told, is much

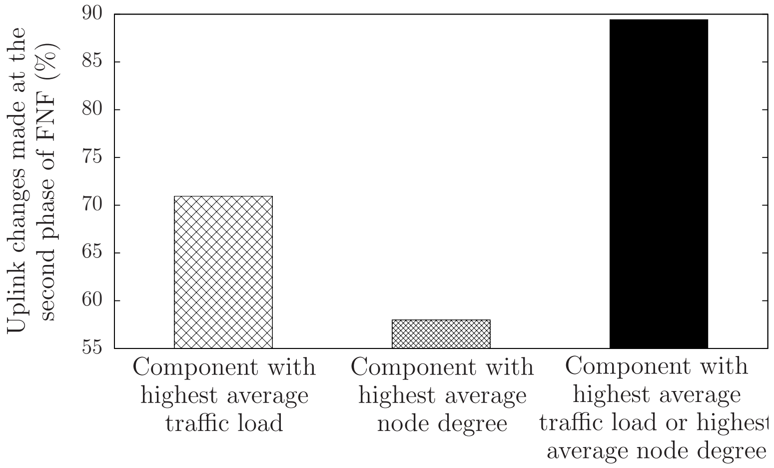


Figure 6.5: Percentage of uplink changes made by the second stage of FNF, which involved at least one node that belongs to: *i*) the component with the highest average traffic load; *ii*) the component highest average node degree; *iii*) the components with either the highest average traffic load or highest average node degree.

more computationally expensive. If FNF checks a maximum of M simultaneous changes, then it will have to consider, on average, $\binom{|\mathcal{R}|}{\mathrm{M}} d^{\mathrm{M}}$ possible link changes[1].

FNF is, undoubtedly, more computationally expensive than the other formation processes, despite also achieving the best overall results. However, it may happen that connection changes, done at the second stage of FNF, do not occur evenly across all the network. According to Figure 6.5, approximately 70% of connection changes done at the second stage of FNF involved at least one wireless router that belongs to the component with the highest average traffic load. Similarly, about 58% of connection changes done at the second stage of FNF involved at least one wireless router that belongs to the component with the highest average node degree. When combining both, almost 90% of connection changes done at the second stage of FNF involved at least one wireless router that belongs to the component with either the highest average node degree or with the highest average traffic load. Hence, we can assume the following:

Claim 6.4 *Path changes at the second stage of FNF are significantly more common at components with either the highest average node degree or with the highest average traffic load.*

---

[1] Here, $\binom{|\mathcal{R}|}{\mathrm{M}}$ refers to the number of combinations of M nodes from set $\mathcal{R}$

6.5 Network Formation Heuristic Algorithm

According to Claims 6.1, 6.2 and 6.3, the FNF, when compared to the other formation processes, obtains the best results except for a small number of situations. To tackle the high computational time that FNF requires, a heuristic algorithm can be developed that detects and improves hidden profitable networks only at components with the highest average node degree or highest average traffic load, according to Claim 6.4. This way, only nodes that belong to such components need to consume energy detecting and solving hidden profitable networks.

6.5.1 Heuristic Algorithm

For the operation of the heuristic algorithm, every node will have to acknowledge information to all the other nodes. This includes traffic load, currently allocated bandwidth and established route to the gateway. Such information can be exchanged through link state advertisements (LSAs), similarly to other link state algorithms. The time between LSAs exchange can be defined according to the network conditions. That is, a bursty network will need more LSA exchanges, for more frequent network information update, while a less bursty network can work properly with less LSA exchanges. Another possibility is to exchange LSAs whenever changes occur (e.g. traffic load, bandwidth allocation or routes).[2]

This algorithm is assumed to start from a network with the connections of shortest paths established. Every wireless router executes the heuristic algorithm, which is composed of two stages:

First stage

The wireless router checks if it can improve its allocation value by switching the current uplink to another one. Among all possible uplink changes, the one that brings the highest improvement is adopted.

At this first stage, a wireless router $i \in \mathcal{R}$, searching for the uplink connection that brings the best network value, needs to know how the other wireless nodes will be affected by its link change in order to calculate the network and allocation value. However, not all nodes of the FiWi access network will be affected by the uplink change of i. Only wireless nodes that belong to the same *dependency set* will be affected. To understand the notion of dependency set, let us consider Figure 6.6 that illustrates the switching possibilities for wireless router 1. When

---

[2] Note that the heuristic algorithm could also run centrally. In that case, every node would have to exchange control messages with the central node for routes to be computed and established.

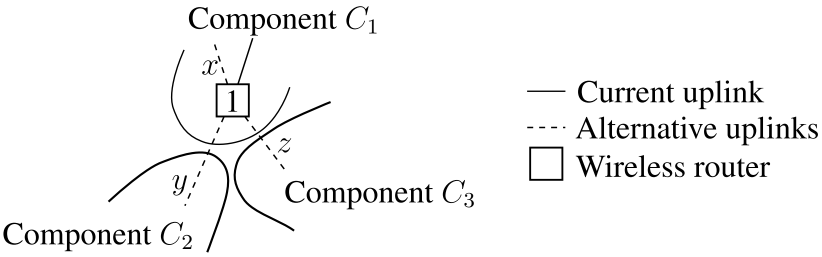


Figure 6.6: Illustration of dependency set.

this wireless router is checking if link x brings a better network value, then the dependency set includes all wireless routers in component C_1. When link y is being tested, the dependency set includes the wireless nodes from components C_1 and C_2. When link z is tested, the dependency set includes the wireless nodes from components C_1 and C_3. In summary, the components including the end nodes of links involved in the switching operation will be the ones that will make up the dependency set.

If a wireless router can not find a better uplink, and if it belongs to a component with the highest average node degree or highest average traffic load, then the algorithm will pass on to the second stage.

Second stage

The wireless router will try to discover better outcomes that can only be reached if its uplink connection is switched together with the uplink of other wireless routers, i.e. the wireless router will try to detect and solve hidden profitable networks. Similarly to FNF, the proposed heuristic algorithm considers a limited number of simultaneous uplink changes. If a better outcome is found, then the wireless router switches its uplink to the new one and informs, through special LSAs, all the affected wireless routers so that their uplinks are also changed.

At this stage, a wireless router $i \in \mathcal{R}$ does not need to check all wireless routers of the FiWi access network for simultaneous uplink connection changes. Only the wireless routers that can affect i need to be considered. To understand which wireless routers are these, let us introduce the term *dependency super-set*. The dependency super-set of a wireless router $i \in \mathcal{R}$ is denoted by $\mathcal{D}_i$ and is the union of all dependency sets that result from all possible uplink changes of i. In the example of Figure 6.6, the dependency super-set of wireless router 1 includes all nodes from components C_1, C_2 and C_3. The nodes that need to be considered for simultaneous uplink change with i are the ones whose dependency super-sets intersect. For instance, if up to three simultaneous uplink changes are allowed, $M = 3$, then only the wireless routers $j \in \mathcal{R}$

and $k \in \mathcal{R}$ that obey to the following condition will be considered for simultaneous uplink connection change with i: $\mathcal{D}_i \cap \mathcal{D}_j \cap \mathcal{D}_k \neq \emptyset$.

The computational time of the heuristic algorithm depends on the number of nodes having dependency super-sets intersection. Since the intersection of dependency super-sets is composed of entire components, the computational time depends on the number of possible link changes involving the wireless nodes belonging to those components. That is, on average, $\binom{n\frac{|\mathcal{R}|}{|\mathcal{G}|}}{M} d^M$ link changes have to be considered, where M is the maximum number of simultaneous uplink changes, $\frac{|\mathcal{R}|}{|\mathcal{G}|}$ is the expected number of wireless routers per component, n is the number of components that will be considered for simultaneous uplink changes and d is the average node degree. As it will be shown in the next section, for small networks with a low number of wireless routers and gateways, FNF and the heuristic algorithm are computationally similar. However, for larger networks, with more wireless routers and gateways, the heuristic algorithm will need less time than FNF. The algorithm is summarized in Figure 6.7.

6.5.2 Simulation and Results

The performance of the heuristic algorithm previously discussed will now be evaluated using the test bed used to evaluate the formation processes in Section 6.4.

When analyzing the network values, energy efficiencies and bandwidth allocations obtained by the heuristic algorithm (HA), DNF and FNF, shown in Figure 6.8, we can state that the performance of HA is between DNF and FNF. The only exception is for the bandwidth allocation ratio, which reflects the traffic successfully delivered. In that case, FNF and HA obtained similar results, with a difference smaller than one percent. This means that, in average, HA is able to surpass hidden profitable networks, improving energy efficiency and bandwidth allocation, when compared to DNF.

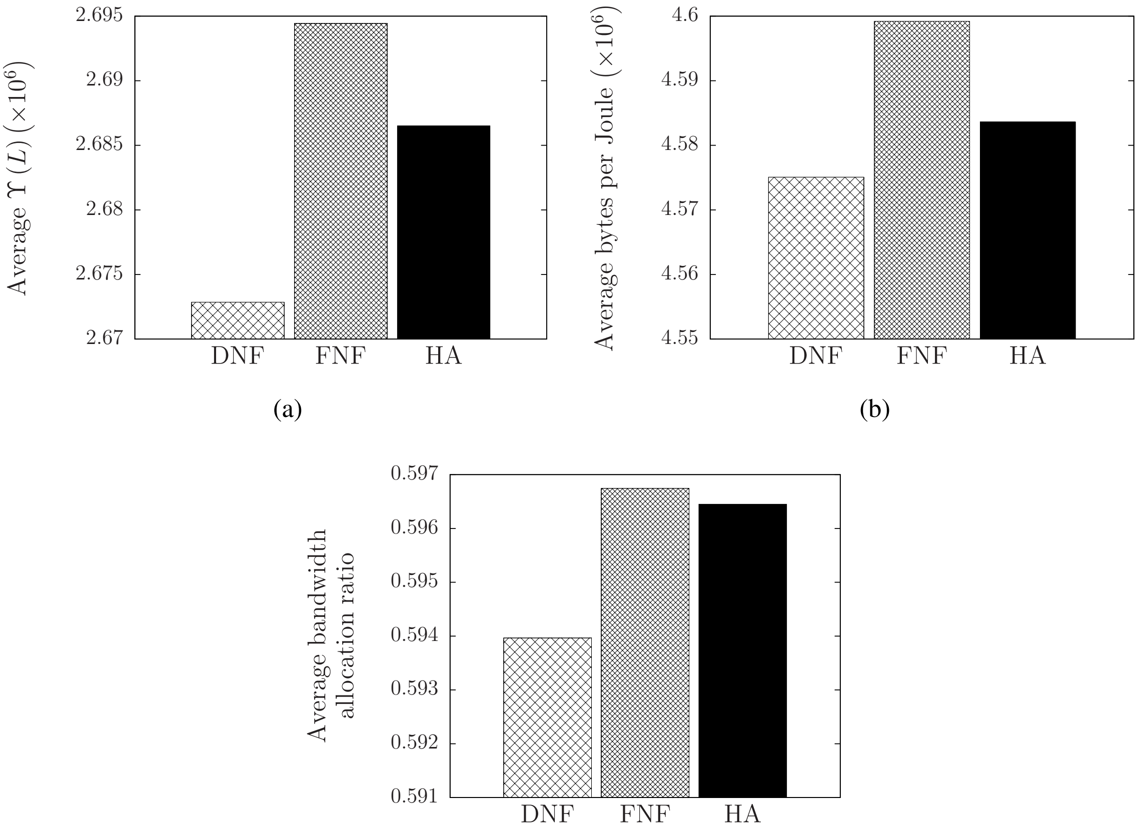
The effect that the number of wireless routers per gateway has on results is shown in Figure 6.9, while the effect of different loads is shown in Figure 6.10. Both these results are in accordance to what is observed in Figure 6.8. That is, HA provides a network value and energy efficiency (bytes per Joule) that are between DNF and FNF, while providing a successful traffic delivery that is roughly equal to the one obtained by FNF, independently of the ratio $\frac{|\mathcal{R}|}{|\mathcal{G}|}$ or network traffic load. Summarizing, HA solves many of the hidden profitable networks for any network conditions, increasing energy efficiency and delivered traffic, when compared to DNF, and gets close to the FNF results.

The computational time of formation processes, as aforementioned, is also an important issue when energy consumption is a concern. That is because executing the formation pro-

```
FirstStage $(i, M, \mathcal{L}^E)$
  /*Inputs:
  $i$ = node that will have its current uplink connection checked
  $M$ = maximum simultaneous uplink changes (required for second stage)
  $\mathcal{L}^E$ = currently established connections*/
  $l$ = current established uplink connection at $i$
  $l'$ = wireless connection at $i$ that provides the highest allocation value to $i$
  if $l \neq l'$ then
    $\mathcal{L}^E = \{\mathcal{L}^E \setminus \{l\}\} \cup \{l'\}$
  else if $i$ belongs to a component with the highest average node degree or highest average traffic load then
    $\mathcal{L}^{E\prime}$ = SecondStage $(i, M, \mathcal{L}^E)$
    if $\mathcal{L}^E \neq \mathcal{L}^{E\prime}$ then
      $\mathcal{L}^E = \mathcal{L}^{E\prime}$
    end if
  end if
  return $\mathcal{L}^E$

SecondStage $(i, M, \mathcal{L}^E)$
  /*Inputs:
  $i$ = node that will have its current uplink connection checked
  $M$ = maximum simultaneous uplink changes
  $\mathcal{L}^E$ = currently established connections*/
  for all combinations of $M$ wireless routers ($i$ included) whose dependency super-sets intersect do
    $\mathcal{X}$ = set of $M$ selected wireless routers ($i$ included)
    $l_{\mathcal{X}}$ = set of currently established uplink connections of every wireless router in $\mathcal{X}$
    $l'_{\mathcal{X}}$ = set of uplink connections involving the wireless routers in $\mathcal{X}$, that provides the highest aggregated allocation value
    if $l_{\mathcal{X}} \neq l'_{\mathcal{X}}$ then
      $\mathcal{L}^E = \{\mathcal{L}^E \setminus \{l_{\mathcal{X}}\}\} \cup \{l'_{\mathcal{X}}\}$
    end if
    return $\mathcal{L}^E$
  end for
```

Figure 6.7: Heuristic algorithm to update uplink connection of $i \in \mathcal{R}$.

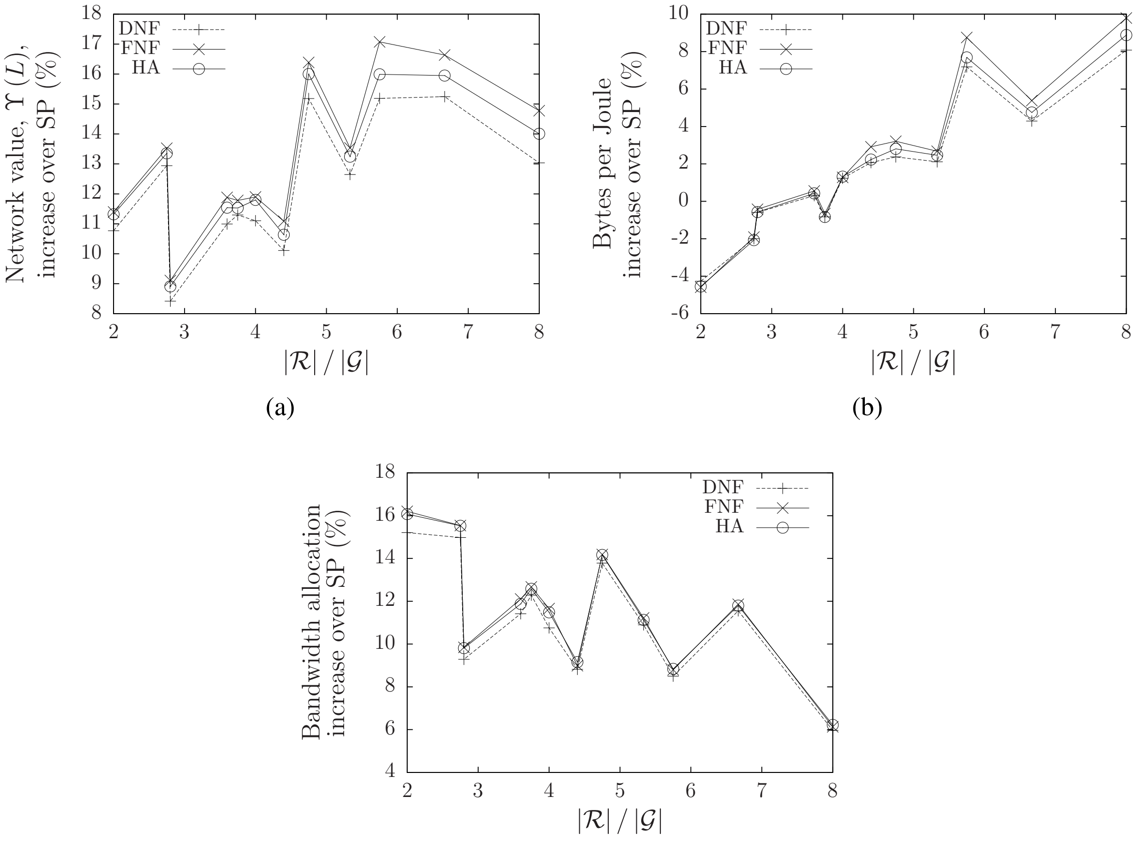


(a)

(b)

(c)

Figure 6.8: Comparison between heuristic algorithm, DNF and FNF: (a) network value; (b) energy efficiency; (c) bandwidth allocation ratio.

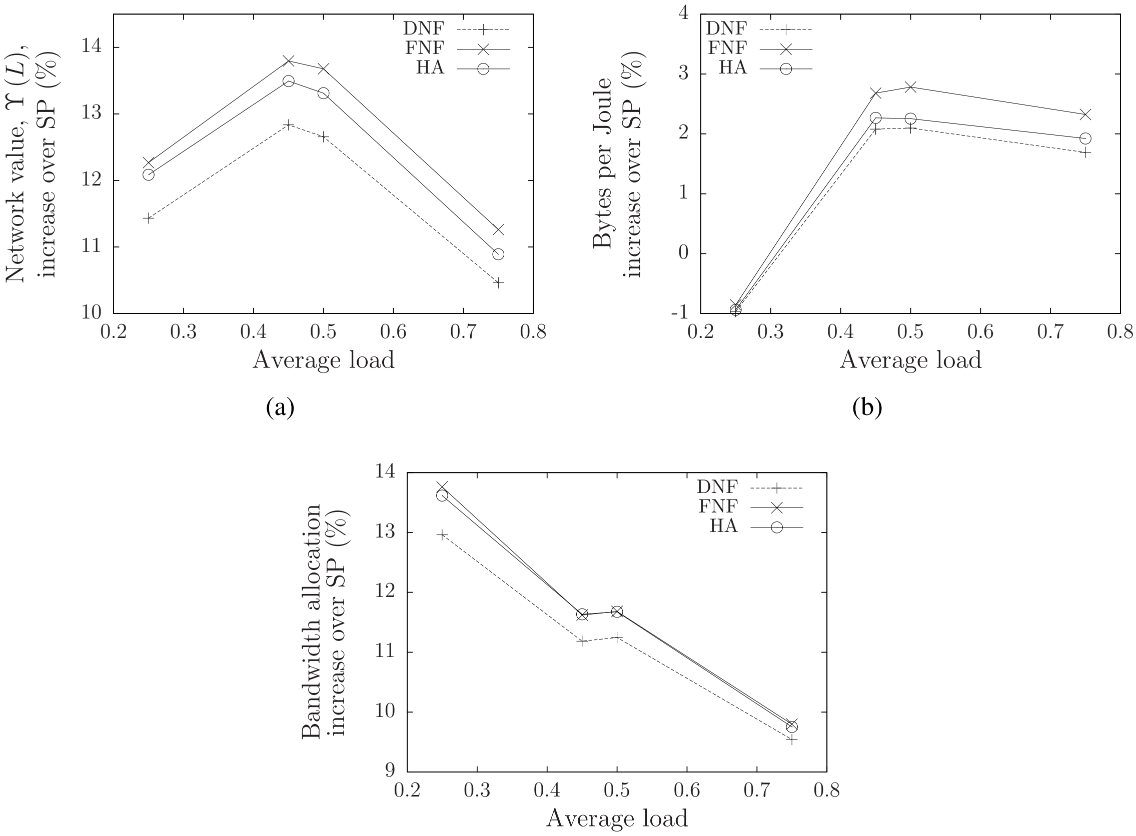


(a)

(b)

(c)

Figure 6.9: Effect that the number of wireless routers per gateway router has on the heuristic algorithm results: (a) network value; (b) energy efficiency; (c) bandwidth allocation ratio.



(a)

(b)

(c)

Figure 6.10: Effect that the tested loads has on the heuristic algorithm results: (a) network value; (b) energy efficiency; (c) bandwidth allocation ratio.

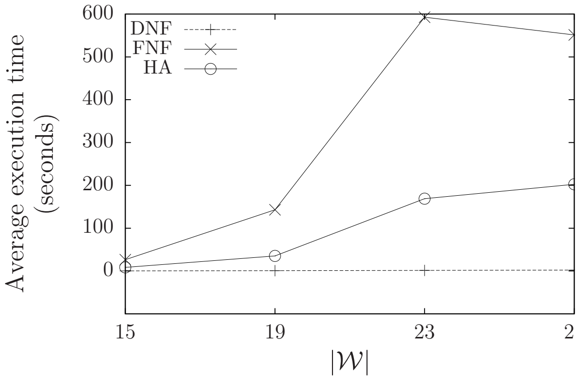


Figure 6.11: Average time that DNF, FNF and HA take until no more path changes are made.

cesses also consumes energy and, as such, longer execution times will lead to higher energy consumptions. The average processing time of the formation processes, which is the time until no more path changes are made to the network, is shown in Figure 6.11 for different network sizes. As can be observed, the HA is much faster than FNF, since only nodes that belong to the component with the highest node degree or highest traffic load pass on to the second stage of the algorithm. Also, in accordance with the expected computational time from the previous section, the difference in execution time between HA and FNF tends to increase for larger networks. DNF, in turn, is faster than HA and FNF, since hidden profitable networks are not detected. The question, however, is whether or not the higher energy efficiency obtained by FNF and HA, when compared to DNF, compensates the longer execution time. Let us recall that computing the formation processes also consumes energy, hence, longer execution times lead to higher energy consumption. In cases where infrequent traffic load variations exist and, therefore, infrequent bandwidth allocation variations also exist, the formation processes do not have to be executed very often for routes to be updated. In that case, FNF and HA can be more advantageous than DNF, since the longer execution time can be compensated by the higher energy efficiency obtained.

It is possible to estimate the time interval during which no network condition variations may occur, so that HA and FNF become more advantageous than DNF. To this end, let us introduce the following notation, where alg refers to DNF, FNF or HA:

t_{alg}**:** Execution time of alg (seconds).

P**:** Average power (Watts) used during the execution of the formation process.

ρ_{alg}: Joules per byte sent/received, which is a result of the energy efficiency obtained.[3]

ζ_i^{alg}: Bandwidth allocation of wireless node $i \in \mathcal{W}$ obtained with the routes established by alg.[4]

Using this notation, the energy consumed to execute DNF, FNF and HA can be calculated by Pt^x_{DNF}, Pt^x_{FNF} and Pt^x_{HA}, respectively. After all routes have been established, the energy needed to send/receive ϕ bytes with the routes established by DNF, FNF and HA is $\phi\rho_{DNF}$, $\phi\rho_{FNF}$ and $\phi\rho_{HA}$, respectively. Hence, HA will be more advantageous than DNF if the following condition holds:

$$\begin{aligned} Pt^x_{DNF} + \phi\rho_{DNF} &> Pt^x_{HA} + \phi\rho_{HA} \Leftrightarrow \\ \Leftrightarrow P\frac{t^x_{DNF} - t^x_{HA}}{\rho_{HA} - \rho_{DNF}} &> \phi. \end{aligned} \tag{6.7}$$

This means that if the network conditions stay the same at least for a time interval equal to the time required to send/receive ϕ bytes, then HA will be more advantageous than DNF. The time needed to send ϕ bytes can be calculated by $\frac{\phi}{\sum_{i\in\mathcal{W}}\zeta_i^{HA}}$. Naturally, the same reasoning can be applied for FNF, when compared to DNF:

$$P\frac{t^x_{DNF} - t^x_{FNF}}{\rho_{FNF} - \rho_{DNF}} > \phi.$$

The actual time interval, with no changes on network conditions, depends on the power used during the execution, the execution time, the obtained energy efficiency and the bandwidth allocation. The energy efficiency and bandwidth allocation, in turn, as analyzed in Section 6.4.2 and Section 6.5.2, depend on the ratio $\frac{|\mathcal{R}|}{|\mathcal{G}|}$ and on the average traffic load. Hence, ultimately, the time interval with no changes on network conditions is very complex to determine and depends on: the power used, the execution time, the energy efficiency variation according to $\frac{|\mathcal{R}|}{|\mathcal{G}|}$, the bandwidth allocation variation according to $\frac{|\mathcal{R}|}{|\mathcal{G}|}$, the energy efficiency variation according to the average traffic load and the bandwidth allocation variation according to the average traffic load. In our test bed, the shortest time that HA needed for the network to stay stable, in order to be more advantageous than DNF, was of 60 seconds, while the longest time was approximately 5 hours. As for FNF, when compared to DNF, the shortest time was of 128 seconds, while the longest was of approximately 11 hours. Hence, HA will be more advantageous than FNF, since

---

[3] This is the inverse of the sent/received bytes per Joule introduced in expression (6.5).

[4] This bandwidth allocation is equal to β_i^A, that results from the paths established by the respective formation process.

the time needed for the network to stay stable is shorter.

6.6 Conclusions

This chapter shows that routes in FiWi access networks can be chosen in order to optimize sleeping and productive periods of all devices, increasing energy efficiency and successful traffic delivery. The HA is able to establish those routes and it is shown that it is more energy efficient than DNF, provided that network conditions do not change too often. The network operator could choose in which conditions would DNF or HA be used, according to how often conditions change.

6.7 Summary

In this chapter, the energy efficient routing in FiWi access networks is addressed. A network formation game theoretical model for energy efficiency was presented. This model was used to test several network formation processes: DNF, SNF and FNF. From all these formation processes, FNF obtained the highest energy efficiency. However, FNF is computationally the most demanding. To address such demand, an analysis was done to understand where in the network did FNF make the route changes that led to its highest energy efficiency. With this analysis, it was possible to develop a heuristic algorithm that is computationally more efficient than FNF and obtains results close to FNF in terms of energy efficiency.

CHAPTER 7

Conclusions and Future Work

7.1 Conclusions

This thesis contributes to the state of the art of FiWi access networks. Before delving into the study and research of these networks, game theory and network formation theory are reviewed. Concepts such as Nash equilibrium, network efficiency and stability are used throughout the chapters and, as such, have been introduced. These mathematical tools revealed to be very useful and powerful. Afterwards, a detailed state of the art on FiWi access networks is presented.

Following the presentation of all fundamental theoretical concepts and state of the art, an initial study of FiWi access networks, through the use of a repeated game model, is presented. More specifically, wireless routers were considered to be selfish players, mainly interested in forwarding local traffic, and it was studied whether or not routers would cooperate by forwarding packets from each other. It was demonstrated that Nash equilibrium, where all routers cooperate, is possible as long as certain conditions are verified. Conditions include having gateways with a different objective, which is to forward as much traffic as possible from all wireless routers, and having a discounting value high enough to deter any deviations. This served as an initial showcase of a game theory application to a specific problem of FiWi access networks, i.e. packet forwarding in an environment where all routers have their own interests.

Two important factors to improve performance of FiWi access networks with a wireless mesh front end are: good resource allocation schemes and good routes establishment. Concerning the allocation of resources, a bandwidth allocation algorithm has been proposed. The proposed algorithm obtained good results, when compared to FIFO and WFQ, and revealed to be agile by allowing several levels of protection to be configured. Moreover, protection is provided to whichever routers are the less demanding, contrarily to WFQ that has to be reconfigured in case of network condition changes, i.e. in case a previously less demanding router changes its load and is now an over demanding router. The proposed algorithm is able to maintain fairness in terms of bandwidth allocation and in terms of average waiting time of packets in queue. That is because the proposed algorithm has a preventive behaviour relating excessive traffic that will be dropped at subsequent hops, avoiding the waste of resources and the increase of waiting time in queue of other packets.

Efficient routing schemes are also very important for FiWi access networks performance. Concerning this topic, energy efficient routing is investigated and a heuristic algorithm is proposed to achieve routes as energy efficient as possible without being too computationally expensive. The amount of bytes sent/received per each Joule consumed is higher when compared with the shortest path algorithm. Such routes are reached by optimising sleep and productive periods of all devices throughout the FiWi access network.

7.2 Future Work

The algorithm developed in Chapter 5 can be adjusted by means of a parameter termed drop component threshold. This parameter controls how much protection is being provided to the less demanding routers. The exact match between the drop component threshold and the protection required by different services provided by the nodes needs to be investigated.

In Chapter 5 and in Chapter 6, new algorithms are developed and it is demonstrated that good performances can be achieved. For those algorithms to be applied in real FiWi access networks, signalling and timing issues need to be addressed. For instance, how often should messages be exchanged, REQUEST and RESPONSE messages in the case of the algorithm from Chapter 5, LSAs in the case of the proposal from Chapter 6, and what should be assumed if some of these messages are lost.

In Section 6.4.2, it is shown that the alternative routes chosen by DNF, SNF and FNF are only marginally longer than the shortest paths. This means that delays are expected to remain similar. As such, special precautions related to delays may not be necessary. However, the results could be different if wireless nodes had a much smaller energy consumption when compared to the energy consumption of ONUs. That is, choosing much longer paths could be easily compensated by putting ONUs in sleep, from an energetic point of view. In such case, delays could increase considerably. It needs to be studied at which consumption levels of the wireless nodes, relative to the consumption of ONUs, should delays be a concern.

References

[1] Glen Kramer, Biswanath Mukherjee, Ariel Maislos, “Ethernet Passive Optical Networks,” in *IP over WDM*, Hoboken, New Jersey: John Wiley & Sons Inc., 2003.

[2] Glen Kramer, “Overview of PON Enabling Technologies,” in *Ethernet Passive Optical Networks*, New York City: McGraw Hill, 2005.

[3] Ton Koonen, “Fiber to the Home/Fiber to the premises: What, where, and when?,” *Proceedings of the IEEE*, vol. 94, no. 5, pp. 911–934, May 2006.

[4] A. M. J. Koonen, A. Ng’oma, G. J. Rijckenberg, M. G. Larrode, P. J. Urban, H. de Waardt, J. Yang, H. Yang, H. P. A. van den Boom, “How deep should fibre go into the access network?,” in *European Conference and Exhibition of Optical Communication*, Berlin, Germany, 2007, pp. 1–4.

[5] Branca Lakic and Marek Hajduczenia, “On optimized passive optical network (PON) deployment,” in *Second International Conference on Access Networks*, Ottawa, Ontario, Canada, 2007, pp. 1–8.

[6] Mauricio López Bonilla, Felipe Rudge Barbosa, Edson Moschim, “Techno-economical comparison between GPON and EPON networks,” in *ITU-T Kaleidoscope Innovations for Digital Inclusions*, 2009, pp. 1–5.

[7] Keiji Tanaka, Akira Agata, Yukio Horiuchi, “IEEE 802.3av 10G-EPON standardization and its research and development status,” *IEEE Journal of Lightwave Technology*, vol. 28, no. 4, pp. 651–661, Feb. 2010.

[8] Russell Davey, Junichi Kani, Fabrice Bourgart, Kent McCammon, “Options for future optical access networks,” *IEEE Communications Magazine*, vol. 44, no. 10, pp. 50–56, Oct. 2006.

[9] Frank J. Effenberger, “The XG-PON system: Cost effective 10 gb/s access,” *IEEE Journal of Lightwave Technology*, vol. 29, no. 4, pp. 403–409, Feb. 2011.

[10] Jun-ichi Kani, Fabrice Bourgart, Anna Cui, Albert Rafel, Malcolm Campbell, Russell Davey, Silvana Rodrigues, “Next-Generation PON-Part I: Technology Roadmap and General Requirements,” *IEEE Communications Magazine*, vol. 47, no. 11, pp. 43–49, Nov. 2009.

[11] Frank J. Effenberger, Hiroaki Mukai, Soojin Park, Thomas Pfeiffer, “Next-Generation PON-Part II: Candidate Systems for Next-Generation PON,” *IEEE Communications Magazine*, vol. 47, no. 11, pp. 50–57, Nov. 2009.

[12] Frank J. Effenberger, Hiroaki Mukai, Jun-ichi Kani, Michael Rasztovits-Wiech, “Next-Generation PON-Part III: System Specifications for XG-PON,” *IEEE Communications Magazine*, vol. 47, no. 11, pp. 58–64, Nov. 2009.

[13] Navid Ghazisaidi, Martin Maier, “Fiber-wireless (FiWi) access networks: Challenges and opportunities,” *IEEE Network*, vol. 25, no. 1, pp. 36–42, Jan. 2011.

[14] Navid Ghazisaidi, Martin Maier, Chadi M. Assi, “Fiber-wireless (FiWi) access networks: A survey,” *IEEE Communications Magazine*, vol. 47, no. 2, pp. 160–167, Feb. 2009.

[15] Suman Sarkar, Sudhir Dixit, Biswanath Mukherjee, “Hybrid Wireless-Optical Broadband-Access network (WOBAN): A review of relevant challenges,” *IEEE Journal of Lightwave Technology*, vol. 25, no. 11, pp. 3329–3340, Nov. 2007.

[16] Mohamed A. Ali, Georgios Ellinas, Hasan Erkan, Antonis Hadjiantonis, Roger Dorsinville, “On the vision of complete Fixed-Mobile convergence,” *IEEE Journal of Lightwave Technology*, vol. 28, no. 16, pp. 2343–2357, Aug. 2010.

[17] Chun-Ting Lin, Jason Chen, Peng-Chun Peng, Cheng-Feng Peng, Wei-Ren Peng, Bi-Shiou Chiou, Sien Chi, “Hybrid optical access network integrating Fiber-to-the-Home and Radio-Over-fiber systems,” *IEEE Photonics Technology Letters*, vol. 19, no. 8, pp. 610–612, Apr. 2007.

[18] Kun Yang, Shumao Ou, Ken Guild, Hsiao-Hwa Chen, “Convergence of ethernet PON and IEEE 802.16 broadband access networks and its QoS-aware dynamic bandwidth allocation scheme,” *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 2, pp. 101–116, Feb. 2009.

[19] Yuanqiu Luo, Ting Wang, Steve Weinstein, Milorad Cvijetic, Shinya Nakamura, “Integrating optical and wireless services in the access network,” in *IEEE Optical Fiber Communication Conference*, Anaheim, CA, USA, 2006.

[20] Frank H. P. Fitzek, Marcos D. Katz, “Cooperation in Nature and Wireless Communications,” in *Cooperation in Wireless Networks: Principles and Applications*, 1st ed. Dordrecht, Netherlands: Springer, 2006.

[21] Matthew O. Jackson, “A Survey of Network Formation Models: Stability and Efficiency,” in *Group Formation in Economics: Networks, Clubs, and Coalitions*, Cambridge, UK: Cambridge University Press, 2005.

[22] J. Coimbra, and N. Correia, “Repeated Game Theory as a Framework for Algorithm Development in Communication Networks,” to be published.

[23] J. Coimbra, and N. Correia, “Survey on Fiber-Wireless Access Networks and Enabling Technologies,” to be published.

[24] J. Coimbra, G. Schütz, N. Correia, “Forwarding repeated game for End-to-End QoS support in Fiber-Wireless access networks,” in *IEEE Global Communications Conference*, Miami, FL, USA, 2010.

[25] J. Coimbra, G. Schütz, N. Correia, “Modeling Fiber-Wireless Access Networks using Repeated Game Theory,” *IEEE European Conference on Networks and Optical Communications*, Faro, Portugal, 2010, pp. 359–366.

[26] J. Coimbra, G. Schütz, and N. Correia, “A game-based algorithm for fair bandwidth allocation in Fibre-Wireless access networks,” *Elsevier Optical Switching and Networking*, vol. 10, no. 2, pp. 149–162, Apr. 2013.

[27] J. Coimbra, G. Schütz, and N. Correia, “Network game based routing for energy efficient Fibre-Wireless access networks,” in *IEEE International Conference on Communications*, Ottawa, Ontario, Canada, 2012, pp. 1958–1963.

[28] J. Coimbra, G. Schütz, and N. Correia, “Energy Efficient Routing Algorithm for Fiber-Wireless Access Networks: A Network Formation Game Approach,” submitted to *IEEE Transactions on Networking*.

[29] Roger B. Myerson, *Game Theory: Analysis of Conflict*, 1st ed. Cambridge, MA, USA: Harvard University Press, 1997.

[30] Alvin E. Roth, “The economist as engineer: Game theory, experimentation, and computation as tools for design economics,” *Econometrica*, vol. 70, no. 4, pp. 1341–1378, Jul. 2002.

[31] Noam Nisan, Amir Ronen, “Algorithmic mechanism design (extended abstract),” in *ACM Symposium on Theory of Computing*, New York City, NY, USA, 1999, pp. 129–140.

[32] Walid Saad, Zhu Han, Tamer Basar, Mérouane Debbah, Are Hjrungnes, “A selfish approach to coalition formation among unmanned air vehicles in wireless networks,” *International Conference on Game Theory for Networks*, Istanbul, Turkey, 2009, pp. 259–267.

[33] Márk Félegyházi, Jean-Pierre Hubaux, Levente Buttyán, “Nash equilibria of packet forwarding strategies in wireless ad hoc networks,” *IEEE Transactions on Mobile Computing*, vol. 5, no. 5, pp. 463–476, Mar. 2006.

[34] Márk Félegyházi, Jean-Pierre Hubaux, “Game Theory in Wireless Networks: A Tutorial,” EPFL, Lausanne, Switzerland, Tech. Rep. LCA-REPORT-2006-002, Jun. 2006.

[35] Drew Fudenberg and Jean Tirole, *Game Theory*. Cambridge, MA: MIT Press, 1991.

[36] William Spaniel, *Game Theory 101: The Complete Textbook*, Sep. 2011.

[37] Kevin Leyton-Brown and Yoav Shoham, *Essentials of Game Theory: A Concise, Multidisciplinary Introduction*, 1st ed. Morgan and Claypool Publishers, Jun. 2008.

[38] George J. Mailath and Larry Samuelson, *Repeated Games and Reputations: Long-Run Relationships*. New York City, NY, USA: Oxford University Press, Sep. 2006.

[39] Yannis M. Ioannides and Linda Datcher Loury, "Job Information Networks, Neighborhood Effects, and Inequality," *Journal of Economic Literature*, vol. 42, no. 4, pp. 1056-1093, Dec. 2004.

[40] Ken Hendricks, Michele Piccione, and Guofu Tan, "The economics of hubs: The case of monopoly," *The Review of Economic Studies*, vol. 62, no. 1, pp. 83–99, Jan. 1995.

[41] Jan K. Brueckner, "Friendship networks," *Journal of Regional Science*, vol. 46, no. 5, pp. 847–865, Dec. 2006.

[42] Matthew O. Jackson and Asher Wolinsky, "A strategic model of social and economic networks," *Journal of Economic Theory*, vol. 71, no. 1, pp. 44–74, Oct. 1996.

[43] Matthew O. Jackson and Anne van den Nouweland, "Strongly stable networks," *Games and Economic Behavior*, vol. 51, no. 2, pp. 420–444, May 2005.

[44] Alison Watts, "A dynamic model of network formation," *Games and Economic Behavior*, vol. 34, no. 2, pp. 331–341, Feb. 2001.

[45] Matthew O. Jackson and Alison Watts, "The evolution of social and economic networks," *Journal of Economic Theory*, vol. 106, no. 2, pp. 265–295, Oct. 2002.

[46] Bhaskar Dutta, Sayantan Ghosal, Debraj Ray, "Farsighted network formation," *Journal of Economic Theory*, vol. 122, no. 2, pp. 143–164, Jun. 2005.

[47] Frédéric Deroïan, "Farsighted strategies in the formation of a communication network," *Economics Letters*, vol. 80, no. 3, pp. 343–349, Sep. 2003.

[48] Frank H. Page Jr., Myrna H. Wooders, and Samir Kamat, "Networks and farsighted stability," *Journal of Economic Theory*, vol. 120, no. 2, pp. 257–269, Feb. 2005.

[49] Alison Watts, "Non-myopic formation of circle networks," *Economics Letters*, vol. 74, no. 2, pp. 277–282, Jan. 2002.

[50] David Astély, Erik Dahlman, Anders Furuskär, Ylva Jading, Magnus Lindström, and Stefan Parkvall, "LTE: the evolution of mobile broadband," *IEEE Communications Magazine*, vol. 47, no. 4, pp. 44–51, Apr. 2009.

[51] Amitava Ghosh, Rapeepat Ratasuk, Bishwarup Mondal, Nitin Mangalvedhe, and Tim Thomas, "LTE-advanced: next-generation wireless broadband technology," *IEEE Wireless Communications*, vol. 17, no. 3, pp. 10–22, Jun. 2010.

[52] Fan Wang, Amitava Ghosh, Chandy Sankaran, Philip J. Fleming, Frank Hsieh, and Stanley J. Benes, "Mobile WiMAX systems: performance and evolution," *IEEE Communications Magazine*, vol. 46, no. 10, pp. 41–49, Oct. 2008.

[53] I-Kang Fu, Yih-Shen Chen, Paul Cheng, Youngsoo Yuk, Ronny Yongho Kim, and Jin Sam Kwak, "Multicarrier technology for 4G WiMax system," *IEEE Communications Magazine*, vol. 48, no. 8, pp. 50–58, Aug. 2010.

[54] Yang Xiao, "IEEE 802.11n: enhancements for higher throughput in wireless LANs," *IEEE Wireless Communications*, vol. 12, no. 6, pp. 82–91, Dec. 2005.

[55] *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Enhancements for Higher Throughput*, IEEE Standard 802.11n-2009, 2009.

[56] *Local and Metropolotan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems*, IEEE Standard 802.16-2004, 2004.

[57] *Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1*, IEEE Standard 802.16e-2005, 2005.

[58] *Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2*, 3GPP TS 36.300, 2012.

[59] Mehdi Alasti, Behnam Neekzad, Jie Hui and Rath Vannithamby, "Quality of service in WiMAX and LTE networks," *IEEE Communications Magazine*, vol. 48, no. 5, pp. 104–111, May 2010.

[60] Y. Ahmet Şekercioğlu, Milosh Ivanovich, and Alper Yeğin, "A survey of MAC based QoS implementations for WiMAX networks," *Elsevier Computer Networks*, vol. 53, no. 14, pp. 2517–2536, Sep. 2009.

[61] Anna Larmo, Magnus Lindström, Michael Meyer, Ghyslain Pelletier, Johan Torsner, and Henning Wiemann, "The LTE link-layer design," *IEEE Communications Magazine*, vol. 47, no. 4, pp. 52–59, Apr. 2009.

[62] Ian F. Akyildiz, Xudong Wang, and Weilin Wang, "Wireless mesh networks: a survey," *Elsevier Computer Networks*, vol. 47, no. 4, pp. 445–487, Mar. 2005.

[63] Ian F. Akyildiz and Xudong Wang, "A survey on wireless mesh networks," *IEEE Communications Magazine*, vol. 43, no. 9, pp. S23–S30, Sep. 2005.

[64] Muhammad Shoaib Siddiqui, Choong Seon Hong, "Security issues in wireless mesh networks," in *International Conference in Multimedia and Ubiquitous Engineering*, Apr. 2007, pp. 717–722.

[65] *Information Technology–Telecommunications and Information Exchange Between Systems–Local and Metropolitan Area Networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 10: Mesh Networking*, IEEE 802.11s, 2011.

[66] Joseph Camp and Edward Knightly, "The IEEE 802.11s extended service set mesh networking standard," *IEEE Communications Magazine*, vol. 46, no. 8, pp. 120–126, Aug. 2008.

[67] Guido R. Hiertz, Dee Denteneer, Sebastian Max, Rakesh Taori, Javier Cardona, Lars Berlemann, and Bernhard Walke, "IEEE 802.11s: The WLAN mesh standard," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 104–111, Feb. 2010.

[68] *Requirements Related to Technical Performance for IMT-Advanced Radio Interface(s)*, ITU-R Report M.2134, 2008.

[69] *Local and Metropolitan Area Networks Part 16: Air Interface for Broadband Wireless Access Systems, Amendment 3: Advanced Air Interface*, IEEE Standard 802.16m-2012, 2012.

[70] Stefan Parkvall, Erik Dahlman, Anders Furuskär, Ylva Jading, Magnus Olsson, Stefan Wänstedt, and Kambiz Zangi, "LTE-advanced - evolving LTE towards IMT-advanced," in *IEEE Vehicular Technology Conference*, Singapore, Oct. 2008, pp. 1–5.

[71] *Requirements for Further Advancements for Evolved Universal Terrestrial Radio Access (E-UTRA)(LTE-Advanced)*, 3GPP TR 36.913, 2012.

[72] Ronny Yongho Kim, Inuk Jung, Xiangying Yang, and Chao-Chin Chou, "Advanced handover schemes in IMT-advanced systems," *IEEE Communications Magazine*, vol. 48, no. 8, pp. 78–85, Aug. 2010.

[73] Mikio Iwamura, Kamran Etemad, Mo-Han Fong, Ravi Nory, and Robert Love, "Carrier aggregation framework in 3GPP LTE-advanced," *IEEE Communications Magazine*, vol. 48, no. 8, pp. 60–67, Aug. 2010.

[74] Kanchei Loa, Chih-Chiang Wu, Shiann-Tsong Sheu, Yifei Yuan, Mary Chion, David Huo, and Ling Xu, "IMT-advanced relay standards," *IEEE Communications Magazine*, vol. 48, no. 8, pp. 40–48, Aug. 2010.

[75] *Evolved Universal Terrestrial Radio Access (E-UTRA); Further advancements for E-UTRA physical layer aspects*, 3GPP TR 36.814, 2010.

[76] *Evolved Universal Terrestrial Radio Access (E-UTRA); Relay architectures for E-UTRA (LTE-Advanced)*, 3GPP TR 36.806, 2009.

[77] Glen Kramer, "EPON Overview," in *Ethernet Passive Optical Networks*, New York City: McGraw Hill, 2005.

[78] Ivica Cale, Aida Salihovic, and Matija Ivekovic, “Gigabit passive optical network - GPON,” in *IEEE International Conference on Information Technology Interfaces*, Jun. 2007, pp. 679–684.

[79] Glen Kramer and Gerry Pesavento, “Ethernet passive optical network (EPON): building a next-generation optical access network,” *IEEE Communications Magazine*, vol. 40, no. 2, pp. 66–73, Feb. 2002.

[80] Jayant Baliga, Robert Ayre, Kerry Hinton, and Rodney S. Tucker, “Energy consumption in wired and wireless access networks,” *IEEE Communications Magazine*, vol. 49, no. 6, pp. 70–77, Jun. 2011.

[81] *Information Technology–Telecommunications and Information Exchange Between Systems–Local and Metropolitan Area Networks–Specific Requirements Part 3: Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks*, IEEE 802.3ah, 2004.

[82] Michael McGarry, Martin Reisslein, and Martin Maier, “Ethernet passive optical network architectures and dynamic bandwidth allocation algorithms,” *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 46–60, 2008.

[83] *Gigabit-capable passive optical networks (GPON): General Characteristics, Amendment 2*, ITU-T G.984.1, 2012.

[84] *10-Gigabit-capable passive optical networks (XG-PON): General Requirements*, ITU-T G.987.1, 2010.

[85] *10-Gigabit-capable passive optical networks (XG-PON): Reach extension*, ITU-T G.987.4, 2012.

[86] *Information technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment 1: Physical Layer Specifications and Management Parameters for 10 Gb/s Passive Optical Networks*, IEEE 802.3av, 2009.

[87] Amitabha Banerjee, Youngil Park, Frederick Clarke, Huan Song, Sunhee Yang, Glen Kramer, Kwangjoon Kim, and Biswanath Mukherjee, “Wavelength-division-multiplexed passive optical network (WDM-PON) technologies for broadband access: a review,” *OSA Journal of Optical Communications and Networking*, vol. 4, no. 11, pp. 737–758, Nov. 2005.

[88] Darren P. Shea and John E. Mitchell, “Long-Reach optical access technologies,” *IEEE Network*, vol. 21, no. 5, pp. 5–11, 2007.

[89] *10-Gigabit-capable passive optical networks (XG-PON): Reach extension*, ITU-T G.987.4, 2012.

[90] Pulak Chowdhury, Biswanath Mukherjee, Suman Sarkar, Glen Kramer, and Sudhir Dixit, “Hybrid wireless-optical broadband access network(woban) : prototype development and research challenges,” *IEEE Network*, vol. 23, no. 3, pp. 41–48, May 2009.

[91] *Evolved Universal Terrestrial Radio Access Network (E-UTRAN); X2 general aspects and principles*, 3GPP TS 36.420, 2012.

[92] Bao Linh Dang and Ignas Niemegeers, “Analysis of IEEE 802.11 in radio over fiber home networks,” in *IEEE Conference on Local Computer Networks*, Sydney, Australia, Nov. 2005, pp. 744–747.

[93] Martin Maier, Navid Ghazisaidi, and Martin Reisslein, “The audacity of Fiber-Wireless (FiWi) networks,” in AccessNets, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, C. Wang, Ed. Springer Berlin Heidelberg, 2009, vol. 6, pp. 16–35.

[94] Xin Liu, Navid Ghazisaidi, Liviu Ivanescu, Rui Kang, and Martin Maier, “On the tradeoff between energy saving and QoS support for video delivery in EEE-based FiWi networks using Real-World traffic traces,” *Journal of Lightwave Technology*, vol. 29, no. 18, pp. 2670–2676, 2011.

[95] Suman Sarkar, Hong-Hsu Yen, Sudhir Dixit, and Biswanath Mukherjee, “DARA: Delay-Aware Routing Algorithm in a Hybrid Wireless-Optical Broadband Access Network (WOBAN)”, in *IEEE Internation Conference on Communications*, Glasgow, Scotland, Jun. 2007, pp. 2480–2484.

[96] Richard J. La and Venkat Anantharam, “Optimal routing control: repeated game approach,” *IEEE Transactions on Automatic Control*, vol. 47, no. 3, pp. 437–450, Mar. 2002.

[97] Roberto García, Victor García, Xabiel G. Pañeda, David Melendi, and Jesús Pérez, “Analysis and modelling of a broadband fiber access network with high peer-to-peer traffic load,” *Simulation Modelling Practice and Theory*, vol. 14, no. 5, pp. 506–526, Jul. 2006.

[98] Alan Demers, Srinivasan Keshav, and Scott Shenker, “Analysis and simulation of a fair queueing algorithm,” *ACM SIGCOMM Computer Communication Review*, vol. 19, no. 4, pp. 1–12, Aug. 1989.

[99] Manolis Katevenis, Stefanos Sidiropoulos, and Costas Courcoubetis, “Weighted round-robin cell multiplexing in a general-purpose ATM switch chip,” *IEEE Journal on Selected Areas in Communications*, vol. 9, no. 8, pp. 1265–1279, Oct. 1991.

[100] OMNet++, an advanced public source, component-based, modular and open-architecture simulation environment. ¡http://www.omnetpp.org/¿, (accessed Feb. 2013).

[101] Kenneth J. Christensen, Chamara Gunaratne, Bruce Nordman, and Alan D. George, "The next frontier for communications networks: power management," *Computer Communications*, vol. 27, no. 18, pp. 1758–1770, Dec. 2004.

[102] Pulak Chowdhury, Massimo Tornatore, Suman Sarkar Sarkar, and Biswanath Mukherjee, "Building a green Wireless-Optical broadband access network (WOBAN)," *Journal of Lightwave Technology*, vol. 28, no. 16, pp. 2219–2229, Aug. 2010.

[103] Christine E. Jones, Krishna M. Sivalingam, Prathima Agrawal, and Jyh Cheng Chen, "A survey of energy efficient network protocols for wireless networks," *Wireless Networks*, vol. 7, no. 4, pp. 343–358, Jul. 2001.

[104] Martin Maier and Navid Ghazisaidi, "QoS-aware Radio-and-Fiber (R&F) Access-Metro networks," in *IEEE Wireless Communications and Networking Conference Workshops*, Sydney, Australia, Apr. 2010, pp. 1–6.

[105] Furuzan Atay Onat and Ivan Stojmenovic, "Generating random graphs for wireless actuator networks," in *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, Helsinki, Finland, Jun. 2007, pp. 1–12.

[106] Shing-Wa Wong, Luca Valcarenghi, She-Hwa Yen, Divanilson R. Campelo, Shinji Yamashita, and Leonid Kazovsky, "Sleep mode for energy saving PONs: Advantages and drawbacks," in *IEEE Global Communications Conference Workshops*, Honolulu, Hawaii, Nov. 2009, pp. 1–6.

List of Publications

Journals

1. J. Coimbra, and N. Correia, “Repeated Game Theory as a Framework for Algorithm Development in Communication Networks,” to be published.
2. J. Coimbra, and N. Correia, “Survey on Fiber-Wireless Access Networks and Enabling Technologies,” to be published.
3. Alvaro L. Barradas, N. Correia, G. Schütz, and J. Coimbra “Energy Saving in Fibre Wireless Access Networks: A Load Adaptive and Fault-Tolerant Scheme,” to be published.
4. J. Coimbra, G. Schütz, and N. Correia, “Energy Efficient Routing Algorithm for Fiber-Wireless Access Networks: A Network Formation Game Approach,” submitted to *IEEE Transactions on Networking*.
5. J. Coimbra, G. Schütz, and N. Correia, “A game-based algorithm for fair bandwidth allocation in Fibre-Wireless access networks,” *Elsevier Optical Switching and Networking*, vol. 10, no. 2, pp. 149–162, Apr. 2013.
6. N. Correia, J. Coimbra, and G. Schütz, “Fault-tolerance planning in multiradio hybrid wireless-optical broadband access networks,” *IEEE/OSA Journal of Optical Communications and Networking*, vol. 1, no. 7, pp. 645–654, Dec. 2009.
7. N. S. C. Correia, J. Coimbra and M. C. R. Medeiros, “Sparse traffic grooming in WDM networks using coarse granularity OXCs,” *Springer Photonic Network Communications*, vol. 17, no. 1, pp. 49–62, Feb. 2009.

Conferences

1. J. Coimbra, G. Schütz, and N. Correia, “Network game based routing for energy efficient Fibre-Wireless access networks,” in *IEEE International Conference on Communications*, Ottawa, Ontario, Canada, 2012, pp. 1958–1963.

2. J. Coimbra, G. Schütz, N. Correia, “Forwarding repeated game for End-to-End QoS support in Fiber-Wireless access networks,” in *IEEE Global Communications Conference*, Miami, FL, USA, 2010.

3. J. Coimbra, G. Schütz, N. Correia, “Modeling Fiber-Wireless Access Networks using Repeated Game Theory,” in *IEEE European Conference on Networks and Optical Communications*, Faro, Portugal, 2010, pp. 359–366.

4. N. S. C. Correia, J. Coimbra, and G. Schütz, “Multi-Radio Hybrid Wireless-Optical Broadband Access Networks,” in *Conference on Telecommunications*, Stł Maria da Feira, Portugal, May 2009, pp. 311–314.

5. N. S. C. Correia, J. Coimbra, and M. C. R. Medeiros, “A minimization cost heuristic approach for traffic grooming in ip-over-wdm networks,” in *IARIA International Conference on Systems and Network Communications*, Sliema, Malta, Sep. 2008, pp. 90–97.

6. J. Coimbra, N. S. C. Correia and M. C. R. Medeiros, “Distributed Algorithm for Traffic Grooming in IP-over-WDM Network,” in *IEEE Eurocon*, Warsaw, Poland, Sep. 2007, pp. 2144–2149.

7. N. S. C. Correia, J. Coimbra and M. C. R. Medeiros, “A Manageable and Bandwidth Effective Solution for Traffic Grooming in IP-over-WDM Networks,” in *IARIA Third International Conference on Networking and Services*, Athens, Greece, Jun. 2007, pp. 79, 19–25.