Channel Switching-Triggered Charging for Pay-TV over IPTV

TECHNISCHE UNIVERSITÄT DARMSTADT

vom Fachbereich Informatik
der Technischen Universität Darmstadt
genehmigte

Dissertation

zur Erlangung des akademischen Grades eines
Doktor-Ingenieurs (Dr.-Ing.)
von

Dipl.-Inform. Tolga Arul

geboren in Frankfurt am Main, Deutschland

Referenten der Arbeit:	Prof. Dr. Sorin A. Huss Technische Universität Darmstadt
	Asst. Prof. Dr. Abdulhadi Shoufan Khalifa University Abu Dhabi
	Prof. Dr. Stefan Katzenbeisser Technische Universität Darmstadt
Tag der Einreichung:	18.08.2016
Tag der mündlichen Prüfung:	06.10.2016

Darmstädter Dissertation
D 17

Darmstadt 2017

EHRENWÖRTLICHE ERKLÄRUNG

Hiermit versichere ich, die vorliegende Arbeit ohne Hilfe Dritter und nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus den Quellen entnommen wurden, sind als solche kenntlich gemacht worden. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, 18. August 2016

Tolga Arul

CHANNEL SWITCHING-TRIGGERED CHARGING FOR PAY-TV OVER IPTV

To my family

CONTENTS

List of Figures vii
List of Tables xi
Acknowledgments xv
Acronyms xvii

1 Introduction 1
1.1 Context 2
1.1.1 Pricing for Information Goods 4
1.1.2 Charging Models for Pay-TV 7
1.2 Short-Interval Charging 10
1.2.1 Consumer Opportunities 10
1.2.2 Consumer Challenges 11
1.2.3 Network Operator Opportunities 12
1.2.4 Network Operator Challenges 14
1.3 Objectives and Organization 15

2 Prospects 19
2.1 Market Participants 20
2.2 Market Background 21
2.3 Consumer Perspective 22
2.3.1 Surveys Addressing Short-Interval Charging 22

2.3.2 Methodology 23
2.3.3 Questions, Options and Results 23
2.3.4 Evaluation 26
2.3.5 Subsequent Developments 29
2.4 Producer Perspective 31
2.4.1 Market Background: An Update 31
2.4.2 Billing Plans 32
2.5 Conclusion 35

3 Basic Methods and Procedures 37

3.1 Broadcast Architectures 37
3.1.1 Structure of Broadcast Data 37
3.1.2 Components of the IPTV Service Architecture 44
3.2 Multicast Encryption 47
3.2.1 IP Multicast 48
3.2.2 Classification 49
3.2.3 Schemes and Examples 51

4 Channel Switching-Triggered Charging 55

4.1 CSTC Model 56
4.1.1 Novelty 57
4.2 User-Friendliness 60
4.2.1 Requirements 61
4.2.2 Specification 61
4.3 Integration 62
4.3.1 Requirements 63
4.3.2 Specification 66
4.4 IPTV Service Architecture for CSTC 67
4.4.1 Components 67
4.4.2 Protocols 69
4.5 CSTC System Architecture 73
4.5.1 Headend System 73
4.5.2 Set-Top Box 77
4.6 Validation of CSTC 78
4.7 Conclusion 80

5 Service Quality 81

5.1 Quality of Service Factors for IPTV 83
5.1.1 STB Start-Up Time 83
5.1.2 Audio and Video Quality 84
5.1.3 Audio-Video Synchronicity 84
5.1.4 Channel Change Time 85

5.1.5 Transmission Delay 85
5.1.6 Quality of other IPTV-related Services 85
5.1.7 Higher-Order Service Characteristics 86
5.1.8 Factors affected by CSTC 86
5.2 Channel Switching Process and Average Times 87
5.2.1 Transmission Delay (DC-14) 89
5.2.2 Initial Buffer Delay (DC-14) 90
5.2.3 Reordering Delay (DC-13) 91
5.2.4 Decoding and Display (DC-15) 91
5.2.5 Relation of Delay Components 93
5.3 Impact of CTSC on the Channel Switching Process 94
5.3.1 Channel Change Request Transmission Delay (DC-16) 94
5.3.2 Channel Change Request Deadline Delay (DC-17) 95
5.3.3 Channel Change Request Processing Delay (DC-18) 95
5.3.4 ECM Alignment RAP Delay (DC-19) 95
5.3.5 ECM Alignment Transmission Delay (DC-20) 96
5.3.6 ECM Alignment STB Processing Delay (DC-21) 96
5.3.7 Media Propagation Delay (DC-22) 97
5.3.8 Relation of Delay Components 97
5.4 Design of a Channel Change Time Measurement System 99
5.4.1 Test System Extensions 100
5.4.2 Measurement Procedure and Evaluation 101
5.4.3 Case Study 104
5.5 Impact of CSTC on QoE 107
5.6 Conclusion 109

6 Conclusion and Future Work 111

References 115

A List of Publications 131

B List of Supervised Theses 133

LIST OF FIGURES

1.1	Classification of Tariff Designs	2
1.2	Different Types of Offers in the Context of Windowing	6
1.3	Structure of This Work	16
2.1	Simplified Value Chain of Broadcast Television Service	20
2.2	To Which Age Group Do You Belong?	23
2.3	Are You Aware of the Term IPTV?	24
2.4	What Exactly Does IPTV Mean for You?	24
2.5	How Do You Receive Your TV?	24
2.6	Do You Use Pay-TV Services Such as Arena or Sky?	24
2.7	Do You Pay for Video Content in One or More of the following Forms?	25
2.8	Under Which Conditions Would You Be Willing to Use Pay-TV?	25
2.9	Which Pricing Model for Pay-TV Would You Prefer?	26
2.10	Comparison of Age Distribution of Survey Participants and TV Households in Germany	27
2.11	Comparison of Transmission Paths of Survey Participants and TV Households in Germany	27

2.12	Comparison of Revenues for Video Content and Spending of Survey Participants	28
2.13	Simplified Billing Plan of a Major German Network Operator	33
3.1	Combing	38
3.2	Conversion to YCbCr Color Model and Chroma Subsampling	39
3.3	2D Discrete Cosine Transform using 8x8 Basis Functions	40
3.4	Open Group of Pictures of Length 12 in Presentation Order	41
3.5	Open Group of Pictures of Length 12 in Transmission Order	42
3.6	Closed Group of Pictures of Length 12 in Presentation Order	43
3.7	Structure of Broadcast Data for Transport	44
3.8	General IPTV Service Architecture	45
3.9	Block Diagram of Headend System	45
3.10	Block Diagram of Set-Top Box	47
3.11	Mapping of IP Multicast Addresses to Ethernet Physical Addresses	48
3.12	Key Star Scheme Example	52
3.13	LKH Example	54
4.1	Overview Chapter 4	55
4.2	User States in Free-TV	56
4.3	User States in CSTC	56
4.4	Overview of Actions Related to Postpaid CSTC	69
4.5	Overview of Actions Related to Prepaid CSTC	71
4.6	Block Diagram of Headend System Supporting CSTC	73
4.7	Key Update Message Format	75
4.8	Private Section Format	75
4.9	Block Diagram of STB Supporting CSTC	77
5.1	Relationship between QoE and QoS	82
5.2	Factors contributing to QoE	83
5.3	IPTV Architecture Components Involved in the Channel Switching Process	87
5.4	Input and Decoder Buffer States during Decoding and Display Process	89
5.5	Video Buffers for Encoder and Decoder	90

5.6 Channel Change Time in Conventional IPTV 93
5.7 Channel Change Time for CTSC 98
5.8 Channel Change Time Measurement System for CSTC 100
5.9 Sequence of Actions during the Measurement of Channel Change Times 102
5.10 Computation Process of Channel Change Times 103
5.11 Histogram of Worst-Case Measurement 105
5.12 GOP lengths and CCTs for 4 and 4000 CCR/s 105
5.13 MOS Values for Measured Channel Change Times 108

LIST OF TABLES

1.1	Comparison of Charging Models	8
1.2	Short-Interval Charging Model	10
2.1	Comparison of Related Consumer Surveys	29
3.1	Zero Message Scheme Example	53
4.1	Comparison Aspects for Related Work	58
4.2	Comparison of Properties of CTSC with Related Work	59
4.3	Message Types Used for Signaling between HES and STB	76
4.4	Comparison of Charging-Related User Actions	79
5.1	Delay Components Contributing to Channel Change Time	88
5.2	Delay Variables	92
5.3	Delay components added by CSTC	96

ABSTRACT

IPTV as an alternative transmission path for broadcast is gaining in importance increasingly. Promoted by the continuous expansion of broadband networks and IP convergence, IPTV is an enabler for several service-based developments such as time-, device-, and place-shifted viewing. In this regard, IPTV is attractive for multiple service operators as it can be used both as an instrument of customer retention and an additional source of revenue.

Despite these technical advantages we observe, that the technical potential of IPTV has not been fully reflected by any pay-TV charging model for broadcast content so far. In particular, a consumer-oriented charging model can act as an advantage for pioneering service operators who offer novel content and technologies in highly competitive markets.

In this work, we develop a novel short-interval charging model for linear pay-TV over IPTV called channel switching-triggered charging. For the design, implementation, and evaluation of this model we consider requirements of pay-TV consumers and service operators. In particular, a special emphasis is placed on the aspects of acceptance. This charging model is based on the conventional channel switching actions of users and is realized by employing multicast encryption schemes. After implementing the proposed model we present a case study. We prove that our contribution provides additional benefits for the consumer and the service provider while maintaining an equivalent level of service quality compared to Free-TV.

ABSTRACT (IN GERMAN)

IPTV als alternativer Übertragungsweg für Rundfunksendungen gewinnt zunehmend an Bedeutung. Begünstigt durch den kontinuierlichen Breitbandausbau und IP-Konvergenz, ermöglicht IPTV zahlreiche dienstbasierte Innovationen wie zeit-, geräte- und ortsungebundene Nutzung. In dieser Hinsicht ist IPTV eine attraktive Technologie für Netzbetreiber, da sie sowohl als ein Instrument der Kundenbindung als auch als zusätzliche Einnahmequelle genutzt werden kann.

Trotz dieser technischen Vorteile ist zu beobachten, dass das technische Potenzial von IPTV bisher noch von keinem Abrechnungsverfahren für Pay-TV berücksichtigt worden ist. Dabei könnte insbesondere ein kundenorientiertes Abrechnungsverfahren als Wettbewerbsvorteil für innovative Netzbetreiber dienen, die neuartige Dienste und Technologien auf hart umkämpften Märkten anbieten.

In der vorliegenden Arbeit wird ein neuartiges Abrechnungsverfahrens für lineares Pay-TV über IPTV entwickelt. Dieses Abrechnungsverfahren wird als *channel switching-triggered charging* bezeichnet. Für den Entwurf, Implementierung und Bewertung dieses Ansatzes werden Anforderungen von Verbrauchern und Dienstanbietern herangezogen. Insbesondere werden Aspekte der Akzeptanz berücksichtigt. Das Verfahren basiert auf dem von Nutzern ausgeführten üblichen Vorgang des Senderwechsels und wird mit Hilfe von Methoden der sicheren Gruppenkommunikation verwirklicht. Nach der Implementierung des vorgestellten Verfahrens wird eine Fallstudie vorgestellt. Hierbei wird gezeigt, dass zusätzlicher Nutzen für Verbraucher und Dienstanbieter bei gleichwertiger Dienstgüte im Vergleich zu frei empfangbarem Fernsehprogramm geschaffen wird.

ACKNOWLEDGMENTS

This work was carried out during my work as a research assistant in the cyber-physical systems working group at the Center for Advanced Security Research (CASED), a joint interdisciplinary center of research and technology of the Technische Universität Darmstadt, Fraunhofer Institute for Secure Information Technology and the University of Applied Sciences Darmstadt.

First of all, I wish to express my deep gratitude to my supervisor Prof. Dr. Sorin A. Huss. He gave me the possibility to develop and refine my ideas and excellently guided me through my time as a PhD student. I could always count on his counsel and patience, which more than once enabled me to find my way out when I was stuck on a dead-end road.

In the same way, I would like to thank my vice-supervisor Prof. Dr. Abdulhadi Shoufan, who not only gave the first push to start my PhD but also is an inspirational researcher with whom I had several fruitful discussions that substantially contributed to the quality of this thesis. Furthermore, I want to thank Dr. Michael Kreutzer, who heavily supported the continuation of my position.

I like to thank all my former colleagues, who supported me in different ways to complete my thesis, among them Tom Assmuth, Alexander Biedermann, Carsten Büttner, Thomas Feller, Marco Grimm, Annelie Heuser, Adeel Israr, Atilla Jäger, Zheng Lu, Felix Madlener, Sunil Malipatlolla, Hans-Gregor Molter, André Seffrin, Marc Stöttinger, Hagen Stübing, Qizhi Tian, Maria Tiedemann, and Michael Zohner.

Additional thanks go to all students I supervised in the one form or the other during my work: Evgeny Bubnov, Zuhaib Ahmed Chohan, Sarmed Javed, Patrick Neugebauer, Björn A. Flubacher, Stefan Pöschel, Leonardo Solis-Vasquez, Goutham Samala, and Konrad Stahlschmidt.

Finally, I am greatly indebted to my parents and my sister Elif. Without their unconditional love and their unlimited support, I would not have been able to write this thesis.

Tolga Arul

ACRONYMS

2-D	Two-dimensional
3-D	Three-dimensional
3DES	Triple Data Encryption Algorithm
AC	Alternating current
ACPI-PMT	Advanced Configuration and Power Interface Power Management Timer
ACR	Absolute Category Rating
AES	Advanced encryption standard
ANI	Automatic number identification
AOC	Advice of charge
ARP	Address resolution protocol
ATIS	Alliance for Telecommunications Industry Solutions
AVL-tree	Adelson-Velskii and Landis tree
B-frame	Bidirectional predicted frame
CAM	Conditional access module
CAS	Conditional access system
CAT	Conditional access table
CBR	Constant bit rate
CCDF	Complementary cumulative distribution function

CCR	Channel change request
CCT	Channel change time
CDF	Cumulative distribution function
CDN	Content Delivery Networks
CDR	Call detail records
CI	Common interface
CRT	Cathode-ray tube
CSA	Common scrambling algorithm
CSTC	Channel switching-triggered charging
CTR	Counter mode
CW	Control word
DASH	Dynamic Adaptive Streaming over HTTP
DC	Delay Component
DCT	Discrete cosine transform
DMB	Digital multimedia broadcasting
DRM	Digital rights management
DSL	Digital subscriber line
DSLAM	Digital Subscriber Line Access Multiplexer
DTS	Decoding Time Stamp
DVB	Digital Video Broadcasting
DVB-C	Digital Video Broadcasting- Cable
DVB-S	Digital Video Broadcasting - Satellite
DVB-T	Digital Video Broadcasting - Terrestrial
DVD	Digital versatile disc
ECC	Elliptic curve cryptography
ECM	Entitlement control message
ECMG	Entitlement control message generator
EMM	Entitlement management message
EMMG	Entitlement management message generator
EPG	Electronic program guide
ES	Elementary stream
FPPC	Flexible-pay-per-channel
FPPG	Flexible-pay-per-group
FSF	Freiwillige Selbstkontrolle Fernsehen e.V. - Organization for the Voluntary Self Regulation of Television in Germany
FSK	Freiwillige Selbstkontrolle der Filmwirtschaft - Voluntary Self Control of the Movie Industry

FTTH	Fiber-to-the-home
GC	Group controller
GOP	Group of pictures
GUI	Graphical user interface
HCT	High correlation transform
HD	High definition
HES	Headend system
HPET	High-Precision Event Timer
HTTP	Hypertext transfer protocol
HW	Hardware
IBPAYWS	Internet-based pay-as-you-watch system
ID	Identifier
I-frame	Intracoded frame
IGMP	Internet group management protocol
IP	Internet protocol
IPDV	IP packet delay variation
IPER	IP packet error ratio
IPLR	IP packet loss ratio
IPPV	Impulse-pay-per-view
IPTD	IP packet transfer delay
IPTV	Internet protocol television
ISDB	Integrated Services Digital Broadcasting
ISP	Internet service provider
ITU	International Telecommunication Union
JMStV	Jugendmedienschutz-Staatsvertrag - Interstate Treaty on the Protection of Minors in Media
JSS	Jugendschutzsatzung - Statute on the Protection of Minors
KJM	Kommission für Jugendmedienschutz - German Commission for the Protection of Minors in the Media
KMS	Key management system
LC	Liquid crystal
LKH	Logical key hierarchy
LTE	Long-Term Evolution
MOS	Mean opinion score
MP@ML	Main profile at main level
MPEG	Moving Picture Experts Group
MPK	Master personal key
MPTS	Multi-program transport stream

MSO	Multiple services operator
NC	Not considered
NGN	Next Generation Network
NIT	Network Information Table
NVoD	Near Video on Demand
OPPV	Ordered-pay-per-view
OSD	On-screen display
OTT	Over-the-top
PAT	Program association table
PCR	Program clock reference
PDF	Portable document format
PES	Packetized elementary stream
P-frame	Predicted frame
PID	Packet Identifier
PIM	Protocol Independent Multicast
PIN	Personal identification number
PIU	Percent IP service unavailability
PLL	Phase locked loop
PMT	Program management table
PPV	Pay-per-view
PRNG	Pseudorandom number generator
PSI	Program service information
PSNR	Peak-Signal-to-Noise-Ratio
PTS	Presentation Time Stamp
PVoD	Push Video on Demand
QoE	Quality of experience
QoS	Quality of Service
RAM	Random-access memory
RAP	random access point
REK	Rights encryption key
RGB	Red, green and blue
RSA	Rivest, Shamir, and Adleman
RTP	Real-time transport protocol
SAP	Session announcement protocol
SAS	Subscriber authorization system
SDT	Service Description Table
SI	Service information

SIC	Short-interval charging
SIP	Session Initiation Protocol
SK	Service key
SMS	Subscriber management system
SPTS	Single-program transport stream
STB	Set-top box
SVoD	Subscription Video on Demand
SW	Software
TDT	Time and Date Table
TS	Transport stream
TSC	Time Stamp Counter
T-STD	Transport Stream - System Target Decoder
TV	Television
UDP	User datagram protocol
UIK	User identity key
UMTS	Universal Mobile Telecommunications System
URK	User root key
VBR	Variable bit rate
VLAN	Virtual local access network
VoD	Video on Demand
VoIP	Voice-over-IP
WG	Workload Generator
WHT	Walsh-Hadamard transform
WTP	Willingness-to-pay

CHAPTER 1

INTRODUCTION

Our everyday life is affected by the assessment of values even though most of the time this task is performed unknowingly. Many of these assessments deal with the value of goods we intend to acquire. For the producers of goods, it is both challenging and vital to anticipate the value consumers attach to their products.

When I was in sixth grade a friend of our family gave me a toy, an electronic decision maker. Playing with it was so amusing that I brought it to school to show it to my classmates. Many of them enjoyed this toy so much that they asked me where I had bought it and whether I could sell it to them. Since it was a present, I did not want to sell mine but promised to ask for more. It turned out that these electronic decision makers were giveaways of the company our friend worked for and the next week I was supplied with eight new decision makers. The day I brought all my "products" to school I pondered how to fix a reasonable price. After all, I didn't pay anything to obtain the toys. But giving them away for free did not appear to be a smart decision since my classmates already expressed their buying interest. Putting little trust into the decision-making competence of the toy, I intuitively figured out that two Deutsche Mark was a good price and that fifty Pfennig should be the minimum price. Still indecisive, during the morning break I was approached by my first "customer" who asked how much the toy did cost. I countered how much he would be willing to pay. After a moment of reflection, he said that four Deutsche Mark would be appropriate. Barely able to conceal my delight, I agreed and handed him the first "unit". Asking the customer how much he is willing to pay seemed to be a profitable strategy and so I asked everyone who wanted to buy for his opinion. Interestingly, all of them valued the price of the toy at least at two and a half Deutsche Mark. The next day, I

was angrily confronted by my customers. Apparently, word had spread that I had charged different prices for the same toy. Customers who had paid more than others emphatically stated that they felt unjustly treated. In order to avoid unnecessary inconvenience, I decided to give back the difference to everyone who paid more than two and a half Deutsche Mark. Many years later I discovered that my initial approach was considered to be the theoretical optimal pricing strategy and that the ire of my classmates was a result of the market realities.

1.1 Context

Defining an appropriate pricing policy is a critical task in business as it influences the sales volume, the revenue, the market share, the competitive position, the company image and the profitability.

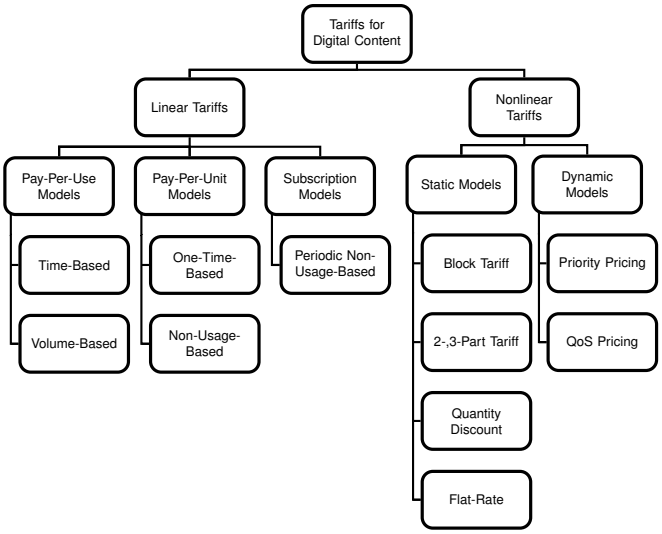


Figure 1.1: Classification of Tariff Designs

Generally, pricing schedules for goods and services can be classified into linear and nonlinear tariffs as shown in Figure 1.1 [1]. Linear tariffs depend solely on some sort of quantity or consumed rate of a good or a service. Examples for linear tariffs are pay-per-use models such as time or volume-based tariffs, for instance, used for dial-around telephone services, and non-usage-based models such as one-time-based tariffs and periodic subscriptions.

In contrast, nonlinear pricing refers to tariffs which are not strictly proportional to the quantity purchased [2]. When static nonlinear models are used consumers pay different prices for each article depending on prior usage, quantity, time or other factors. An instance for such pricing is the block (-declining) tariff. Here the price of subsequent units decreases in steps as a function of the number of already purchased units. Another static nonlinear tariff is the two-part tariff where consumers pay a fixed subscription fee in addition to fixed usage-based fees. Quantity discounts can be granted depending on the extent of the purchase by offering lower prices either for particular units or for all units. In this regard, the discount may apply to a single tariff, a part of a multipart tariff or to a menu of tariffs.

Finally, a tariff where only a fixed fee is charged irrespective of the number of purchased units is called a flat-rate tariff.

Costs incurred using dynamic nonlinear tariffs are even irrespective of quantity or consumption. When, for instance, priority pricing is used, the price is determined by the waiting time in a queue. This queue in the context of electronic commerce could be a priority queue of some networked computing system providing a service [3]. When quality of service (QoS) pricing is used, in contrast, the processing quality of the service request and delivery are specified as predefined classes. Here, the price is determined according to the incurred costs to ensure the processing quality of these classes.

From an economic view, pay-TV as an information product belongs to the broader family of information goods. In general, the construction of pricing schedules works to the advantage of certain parties. These parties are usually stakeholders in the value chain. For information goods, the work in [4] has identified three beneficiaries upon whom current pricing research focuses: consumers, suppliers, or government. In this work, we only investigate the effects of some pricing policy on suppliers in the form of the network operators. However, all market participants will be introduced in more detail in Section 2.1.

Pricing models for information goods in the context of communication have been addressed in the literature for a long time [5, 6]. Several proposals relate to pricing models for Internet sessions [7], for IP telephony [8], for software distribution [9], and for video on demand (VoD) services [10]. Information goods in contrast to other types of goods are characterized by several particular properties:

- The quality of information goods does not deteriorate in the course of time.
- Information goods can be copied with next to no cost without any loss in quality.
- Consequently, information goods feature high production costs for the first unit but almost no reproduction costs and time expenditure for all subsequent units.
- Thus, the value of and therefore the pricing strategies for information goods are often volatile.
- Information goods can be easily manipulated.
- Information goods are not bound to a medium, they can be stored on every medium that allocates the required capacity (disembodiment).
- Information goods can be experienced before purchase (sampling).
- Information goods, in particular, entertainment products, are subject to *network externality*. Network externality refers to the effect that the more consumers purchase a specific information good the more additional consumers will be inclined to purchase that good due to emerging trends, social prestige, and word-of-mouth effects.
- However, the effect of network externality is inhibited by *information asymmetry*. This means that due to its complex nature often it is not possible to assess the value of some information good unless one has experienced it. This leads to the situation that consumers who have consumed a commodity have more or better information than other consumers.

1.1.1 Pricing for Information Goods

As a result of the aforementioned unique characteristics of information goods, different approaches are necessary in order to specify successful pricing strategies for these goods. Particularly, the fact that subsequent units of information goods have very low production costs has inspired research to define optimal pricing strategies [11]. As a consequence, the common approach to establish prices is market-driven rather than cost-driven. The work of [12] has identified two major methods for this purpose, namely, price discrimination and bundling.

Theoretically, for a producer, the most profitable way to fix a price for a good would be to ask each potential customer how much money he would be (at most) willing to pay for how many units of some product. Thus, with price discrimination, the approach is pursued to charge different customers different prices for the same good. In this context, price discrimination methods have been classified in the work of [13] into three stages:

First-degree or perfect price discrimination is also called personal pricing and assumes the situation we have described above: A producer has perfect knowledge regarding the demand of each consumer and accurately charges the willingness-to-pay (WTP).

In contrast, second-degree price discrimination assumes that the factors driving the decision of the consumers to purchase some good, such as the WTP, are unknown to the producer. Thus, in order to overcome this situation of imperfect information, the demand of the users is approximated by modifying all kinds of aspects of the commodity. In the following, we will describe three different strategies: Bundling, versioning, and windowing.

Bundling

When bundling is used, two or more products are offered together as a bundle while the consumer is charged less than the sum of the individual prices of each commodity. As a result of a study performed in [14], the authors could explain why this is an effective approach. When several articles are bundled the average WTP of consumers are increased because a considerable fraction of consumers rates the combined value of these articles higher than the value of each individual article. In addition, bundling reduces the variety of WTP among consumers. Consequently, adding more products to the bundle increases the profit and reduces the effort to find the optimal price [15].

With pure bundling, consumers are allowed to purchase a commodity only within a bundle and not separately. However, this approach leads to profit loss when consumers assign no value to a large subset of the offered bundle [16]. In this case, it is more effective to pursue a mixed bundling strategy. Here, a consumer has the choice to purchase an individual article for a specific price or to purchase a bundle containing the desired article for another (higher) price [17].

Bundling can be applied to products of different types, such as additional features to a certain base product, as well as to products of the same kind. In the latter case, bundling is equal to nonlinear pricing [2]. In particular, bundling can be seen as a more general form of quantity discounts that are also offered in block tariffs [18].

Furthermore, creating mixed type bundles of physical goods with information goods are able to increase the total profit, because the costs to produce an additional unit of such mixed type bundles are lower than the costs for bundles of physical goods [15].

Altogether, bundling can overcome the problems caused by imperfect information regarding consumer preferences. However, finding the proper number of articles and devising an effective bundling strategy are challenging tasks when bundling is employed.

Versioning

In general, the objective of versioning is to produce different versions of a good with the least effort by omitting different features in order to match the WTP of a variety of consumers.

The simplest form of versioning is to charge different unit prices for different amounts of the good purchased [19]. Obvious examples for this approach are different cup sizes for soft drinks and coffee to which different names are assigned. As we can see, this approach corresponds to the concept of nonlinear pricing we have already discussed above.

Another form of versioning relates to functional and nonfunctional aspects of the good or service. Functional aspects involve characteristic functions of the product such as the set of features. For instance, a software for handling documents in the Portable Document Format (PDF), usually, has different versions, which can either only read or read and write files in this format. Nonfunctional aspects comprise versions

- which offer different quality in terms of resolution, sampling rate, streaming bandwidth, 3-D capability, frame rate, high dynamic range of luminosity, update rate, accuracy, error rate, latency, availability, etc.
- which offer updates and upgrades to the newest product version for different durations
- which offer a different level of service and support, reaction time, and time to repair in the event of failure
- which offer different rights of use regarding the form of publication, geographical distribution, duration of use, permission to record, playback, copy, and output to different interfaces
- which support different usage policies regarding the number of concurrent accesses, the number of requests per time unit, etc.
- which represent value to collectors, such as special packaging and additional exclusive or merchandising articles.

Theoretically, individual versions could be adjusted for each consumer at low costs. These versions would provide perfect price discrimination and optimal profit. However, the compilation of these versions would confuse the consumers since differences in product performance would not be easy to grasp while making the purchase decision. For this reason, in practice usually three versions are offered and consumers most often select the medium package for purchase [1].

Windowing

Windowing characterizes the offer of the same digital good at different time frames using different exploitation schemes. In the following, we will illustrate the concept of windowing with the help of Figure 1.2 from [20]. Usually, a motion picture is at first theatrically released and can be seen only in cinemas for the first six months. Subsequently, it is exclusively available for purchase on digital optical disc media (Digital Versatile Disc (DVD) and Blu-ray Disc). After three months, the motion picture is additionally made available via Video on Demand and Pay-Per-View offers. After another three months, it is also shown on regular pay-TV. Roughly after two years having its initial release the motion picture is shown on nationwide free-TV. After several reruns on nationwide free-TV, it can be seen on local free TV channels. Windowing is used in order to avoid the emergence

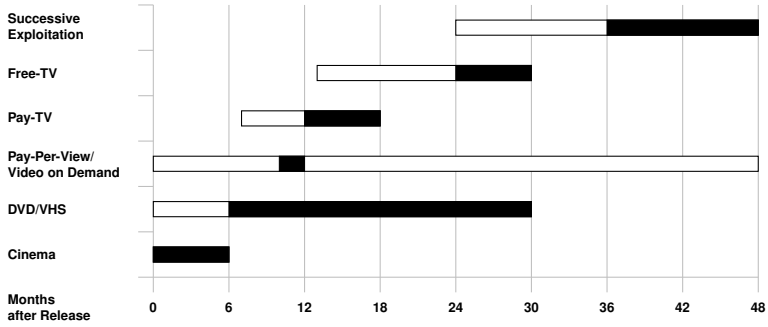


Figure 1.2: Different Types of Offers in the Context of Windowing

of cannibalization effects. In case the motion picture would be available on optical disc media immediately upon theatrical release, fewer consumers would go to the cinema. As the required WTP of the consumers is gradually decreased with successive exploitation scheme, in the course of time the motion picture becomes attractive for different groups of buyers. In order that network externalities take effect a considerable time frame is allotted for each exploitation scheme. However, recently the time frames are more relaxed. While exploitation times in previous years were mostly successive as indicated by the filled portions of the time frames shown in Figure 1.2, nowadays, these times are extended for almost each exploitation scheme. Consequently, the time frames overlap as illustrated by the blank portions of the time frames in Figure 1.2. However, motion pictures whose production has been subsidized, for instance by the German Federal Film Fund, have to adhere to specific holdback periods, in the given instance pursuant to §20 Act on Film Promotion [21].

When third-degree price discrimination or group pricing is employed, the producer uses auxiliary data on consumer properties such as gender, age, domestic or foreign address, affiliation to an occupational group, company, and loyalty programs, etc. in order to correlate the corresponding WTP. The idea is that consumers who share the same properties also have the same WTP. For instance, consumers who buy software for personal use have a lower WTP than business users who generate income using the same software. However, in many cases, it is difficult to derive a common WTP from the affiliation to some group because the WTP of group members toward a specific product differs is too much.

Now that we have become acquainted with price discrimination and bundling, we also want to introduce some of the conditions, which need to be satisfied in order that these methods can be applied (see [2]):

- The producer needs to have information about consumers and their demand. Otherwise, it is not possible for the producer to devise different prices for the corresponding consumers.
- The producer must be in the position to prevent resale. Otherwise, consumers can take advantage of the price differential.
- Price discrimination has to be socially and legally acceptable.

Coming back to my anecdote from the beginning of this chapter, we can see that I had perfect information about my customers since I directly asked them for their WTP. How-

ever, because of the social and legal convention, it is considered an unfair trade when the price or, in cases the price cannot be fixed in advance, the way the price is calculated is not disclosed to the consumer. In fact, it is deceptive trade practice and liable to prosecution.

Nevertheless, my approach could have been legitimated in several ways. From a certain perspective, the reduced price is a preorder offer. I sold the decision maker for two Deutsche Mark to my classmates who initially asked me to sell mine to them. Later I sold the toy for four Deutsche Mark to the classmates who approached me once brought the other units. In this case, I would have applied third-degree price discrimination to the group of classmates who ordered in advance and to the group of all others. As a side effect, classmates who owned a toy would help me to overcome information asymmetry by letting the other classmates play with it. This, in turn, would lead to network externality so that even more classmates would be inclined to buy the toy. Seen from a different perspective, I also could have applied second-degree price discrimination in the form of windowing. Classmates who initially wanted me to sell them my toy would be charged a higher price since they would enjoy the toy earlier than others. All other classmates would be charged less for getting the toy later.

Nevertheless, it is common practice to ask consumers for their opinions, their valuation, and thus WTP, for some product, and for their preference among different alternative products in the course of polls and surveys and therefore in situations outside of the buying process. As a consequence, we apply the methodology of opinion poll on several occasions in this work. In particular, this whole thesis deals with short-interval charging, a charging model introduced in the next Section 1.2. This charging model could be seen as the principal approach to shorten the feedback cycle of identifying the WTP of consumers, depending on the implementation solely for themselves or additionally for the network operator. Accordingly, in the course of this work, we apply this charging model to pay-TV, improve it to increase its usability, and propose a technical solution. Furthermore, we ask consumers for their opinion in order to assess the interest in our solution in Section 2.3. Finally, in Chapter 5 we use models derived from opinion polls to assess the quality users experience when they use our proposed technical solution.

1.1.2 Charging Models for Pay-TV

With the ever-expanding broadband network connectivity, television and the Internet are converging and the Internet Protocol Television (IPTV) is gaining in importance increasingly. IPTV is one of altogether four transmission paths for broadcast television alongside cable, satellite and terrestrial transmissions. It differs considerably from web or Internet-TV, which has different requirements on the network infrastructure and therefore also uses different protocols. Enabled by its return channel, IPTV is characterized by several developments such as time-, device- and place-shifted viewing. Similarly to conventional television, the IPTV standards support pay-TV. Pay-TV is a business model for funding broadcast transmission of media content, where the subscriber has to pay for the provided content. The market for pay-TV shares more than 40% of the total TV industry worldwide [22]. Free-(to-air) TV, in contrast, is a business model, where the subscriber does not pay for the provided content. In this case, the broadcast transmission of media content is either sponsored by advertisements, state-subsidized as a part of the public broadcast service, or entirely government-financed as state-run television.

Charging model	Usage-Based Cost Attribution	Cost Cap	Interactivity of Entitlement	Adaptability of Services
Subscription-Based Pay-TV	Low	High	Low	Low
Pay-Per-View	Medium	Medium	Medium	Medium
Video-On-Demand	Medium	Medium	Medium	High

Table 1.1: Comparison of Charging Models

Currently, there are three major charging models, which are used by pay television service providers:

- Subscription-Based Charging,
- Pay-Per-View, and
- Video On Demand.

As a result of a survey we conduct in Section 2.3, we will discover that each charging model has several shortcomings with regard to certain aspects consumers demand. These aspects comprise the attribution of usage costs and the availability of an upper limit for costs. In addition, some models require users to accept a subscription period, which restricts the interactivity of entitlement. Finally, certain models force users to specify which category of content they want to consume limiting the adaptability of services. In order to establish a better understanding, all charging models are compared in Table 1.1.

When subscription-based charging is used, consumers need to take out a monthly or an annual subscription for some channel or channel package, in which they are interested. This subscription-based pricing model offers two main advantages for users regarding convenience and insurance. Specifically, subscribed members, on the one hand, do not need to deliberate upon cost and benefit each time they want to view some content. On the other, the fixed-price subscription model protects consumers from surprisingly high bills. Nevertheless, subscription-based pay-TV has several drawbacks, which may deter many consumers from buying this service:

1. Consumers, who watch TV on occasion or infrequently, often regard long-term subscriptions as too cost-ineffective. This is due to the fact that subscription-based pay-TV by design offers low contract flexibility.
2. Households with a wide interest would wish to subscribe to several channels or channel packages. For instance, a household with many members of different ages would wish to subscribe to several channels or channel packages, for example, for sports, movies, cartoons, documentaries, etc. Such a solution, however, is associated with high expense.
3. The digital TV technology is experiencing a steady sophisticated evolution ranging from 3-D high-definition TV, through Free Viewpoint TV and Ultra Smart TV, to television based on the 3-D hologram technique. We can assume that production costs and correspondingly subscription prices for content using such novel techniques will be extremely high.

4. The convergent TV technology assumes viewing IPTV on mobile devices. It is however questionable, whether long-term subscriptions will be appropriate in this use case where many subscribers are used to paying for services in time- or volume-based billing units.

Pay-Per-View (PPV) is another business model for paid media content, where the user notifies the pay-TV operator in order to be entitled to a single event, for instance, a concert or a boxing match. However, PPV is intended for live events of short duration with many users watching the same event. Since the process of notifying the operator requires a back-channel, which is not available for previous transmission paths such as terrestrial, cable, and satellite transmissions, methods like automated telephone systems, live phone customer services, and analog modems are used to start the purchase. Also, these methods account for the drawbacks of this scheme. In any case, the user has to inform the operator about the purchase intention a certain period of time before the event starts (latency of the back-channel). In most cases, the entitlement is not possible after the start of some event. Although this constraint is weakened by Impulse-Pay-Per-View (IPPV) systems in contrast to Ordered-Pay-Per-View (OPPV), the operator still needs some time to compute and distribute the entitlement information to the users. Consequently, in most cases, the entitlement is not possible after the start of some event.

Video on demand (VoD) is a business model for IPTV, where users can choose among individual prerecorded movies. Users are able to consume the content at individual times allowing them even to pause and continue viewing within a certain period of time. Nevertheless, this model offers low after-sale flexibility: Users have to pay for the ordered content entirely, even if they do not consume it completely for any reason. Another shortcoming is that content is requested and provided through individual streams. A setup serving content to a large number of users requires the allocation of comparatively high bandwidths and computational resources for every single user during the entitlement and delivery process. In particular with the recent widespread use of bit rate adaptive streaming technologies such as the standardized dynamic adaptive streaming over the HTTP (MPEG-DASH) [23], a high number of request-response pairs to different peers are initiated by the receiver. Since connection-oriented protocols are used, these messages are not only required to enable adaptation to the available bandwidth but also to alleviate the effects connection timeouts and to increase the resilience against network congestion [24]. Consequently, in addition to the considered bandwidth requirements, VoD services make high computational demands on the network. Notably, these services put strain on network components that operate on individual packets and streams such as components enforcing policies regarding security and quality of service on the application level such as application-aware firewalls and traffic shapers.

The number of these request-response pairs can reach more than 800 per minute for a single user of a VoD service [25]. The aforementioned drawbacks of VoD become even more prominent when VoD services are provided using peer-to-peer technologies [26]. For these scalability reasons, VoD cannot be considered as a charging model for broadcast and thus has so far not been regarded as an alternative to subscription-based linear pay-TV.

A classification of the introduced charging models for pay-TV according to the scheme we discussed in previous Section 1.1 will be performed in the course of our analysis of the present billing plan of a major German network operator in Section 2.4.2.

1.2 Short-Interval Charging

The aforementioned shortcomings of established charging models can be addressed by a novel charging model called *short-interval charging* (SIC). In the style of pricing models for conventional telephony [27], the proposed model relies on time-based charging for pay-TV. According to the SIC scheme, users may register to the pay-TV service without a subscription. After the registration, users may view any of the provided channels and need only to pay for the viewed minutes or seconds. However, the lineup of channels could consist of a mix of free and paid channels and users may seamlessly switch between these channels. In order to provide better control for the consumer, the paid channels could be labeled accordingly and the actual balance could be displayed by inserting it to the on-screen display (OSD) by the receiver terminal. Ideally, usage costs would be conveniently deducted using a postpaid method.

According to the classification of tariff designs depicted in Figure 1.1, the SIC model on its own is a linear time-based pay-per-use model. However, it can also be used to implement nonlinear pricing. For instance, SIC could a part of a nonlinear static n-part model. Here, SIC could provide a usage-based component in addition to n-1 base cost components. In another use case, SIC could be used to implement a block tariff, where consumers would be charged declining unit prices the more they watch a specific channel or altogether. Moreover, discounts could be allowed if consumers remain on a channel during a commercial break. Altogether, completely novel and unconventional tariffs could be designed as we will see in the subsequent analysis. In the following, we discuss benefits and assumed reservations against the SIC model in the perspective of either considered party: The consumers and the network operators.

1.2.1 Consumer Opportunities

Charging Model	Usage-Based Cost Attribution	Cost Cap	Interactivity of Entitlement	Adaptability of Services
Short-Interval Charging	High	Medium	High	High

Table 1.2: Short-Interval Charging Model

The SIC scheme provides usage-based cost attribution as no subscription is needed and after-sale flexibility is provided. In this way, also the term of contract can be omitted resulting in a higher cost-efficiency for the user. Users can interactively get entitled to the content they want to consume and are able to adapt the service regarding all available content types (genres). As the users know their viewing time, they can easily estimate the amount they have to pay for each view and, consequently, have full cost control. The merits of SIC model are summarized in Table 1.2.

1.2.2 Consumer Challenges

Since the SIC model is usage-based, consumers could fear that they face a cost explosion once they use this charging model extensively. However, there are at least two remedies to overcome this reservation. First, once users realize that their costs increase, they can switch to a more advantageous charging model with respect to their amount of consumption, for instance, to a flat-rate model. Second, the software in receiver terminals can be programmed in such a way that a warning to the user is issued once a specific usage duration is reached. In this way, users can control their costs similarly to programmable data volume limits supported by operating systems of cell phones.

Another potential limitation of the SIC model is related to the selection freedom of content. As SIC is designed for broadcast transmissions, users are not able to choose from any kind of content, as it is possible with video on demand offers that are transmitted individually to each user by unicast. However, when linear broadcast content is consumed, in general, consumers compare pay-TV content to free content. This results in attraction to higher-quality content which is usually accessible over pay-TV. Although the same content potentially could be consumed using VoD, more steps would be needed to select and decide on the desired content. Depending on the connotation in literature this situation is referred to as the lean forward experience or the selection problem. However, decision making is a tedious task as it consumes time and is confusing when possibilities are vast. When SIC is used in contrast, the consumer just decides whether the broadcast content is appealing or not since the program decision is assumed by the respective Head of Programming for each channel. This situation is referred to as the lean backward experience.

We assume that for linear broadcast the lean backward experience is preferred by consumers. The first indicator for this assumption is that the total number of average viewing minutes per day is increasing on a yearly basis [28]. This shows that consumers seem to be satisfied by the programming choices of the channel operators. A more elaborate analysis with different models for explaining television program choices suggests that television viewing is in part affected by exogenous factors such as weather, daylight, the day of the week, etc. [29]. However, program choices are also controlled by certain habits. These habits result from individual preferences and become manifest in loyalty to some specific, mostly adjacent, group of channels (relevant set) [30] and accustomed search routines for finding pleasurable content [31].

Another important observation is that viewers remain on some specific channel after the chosen program has ended due to inactivity. This phenomenon is referred to as inheritance effect [32], passive audience [30], and audience flow. As a consequence, it is assumed that television viewing is a passive activity performed in remaining leisure time. Regarding content quality, consumers seem to be satisfied with the "least objectionable program" [33] that offers content quality appealing to the "common denominator" rather than generally refraining from watching TV [34]. The aforementioned knowledge has long been exploited by channel operators to develop strategies that serve various purposes.

When strip programming or stripping is used, the audience is made accustomed that a specific program starts at a certain time on a certain day of the week. By forming this habit, consumers do not need to search for their show in some program guides and align their daily routine according to the program schedule. Lead-in, lead-out and lead-off effects are used to gain higher audience ratings or promote new programs. Lead-in refers

to the fact that programs with high audience ratings inherit their audience to subsequent programs with lower ratings due to audience flow. Lead-off refers to a program with a strong lead-in that is introduced at the prime time and binds the audience to many consecutive programs and thus to the channel for the whole evening. Lead-out describes the same effect as lead-in but affecting the previous program due to the fact that consumers don't want to miss the start of their target program. Moreover, also advocates of the classic lean forward experience start to take advantage of the effect of audience flow. For instance, YouTube, the current leading service for hosting user-generated video content, recently introduced the autoplay feature [35] with the objective of increasing the number of views and, consequently, advertisement revenue. Once a video has ended, this feature alleviates the decision problem by automatically playing an additional related video based on the user's viewing history after a countdown of 10 seconds [36]. In summary, we are able to state that SIC combines the advantages of high-quality content with the habitual preselection of content by the pay-TV channel operator on behalf of the consumer.

Reservation against SIC could also emerge as a result of privacy concerns. Since the duration and channel selection of each user has to be recorded for charging purposes, the viewing behavior can be tracked and analyzed. In particular, each user in a household can be identified and their preferences can be determined and disclosed to third parties in order to provide target group adapted advertisements. We believe that this limitation is appropriate and can only be overcome by corresponding legislation. In the spirit of privacy measures for telephony applied to call detail records, network operators have to delete retained data used for charging and billing after a short period. In addition, technical measures have to be imposed so that user data are stored securely and an exposition to third parties is excluded or permitted only for aggregated data.

1.2.3 Network Operator Opportunities

Aside from benefits for the users, SIC also holds several interesting virtues for the network operator. In the following, we list different aspects we believe to be emerging future challenges for network operators and where SIC can be an advantageous approach.

Optimality

In the search for an optimal pricing strategy, the analysis of [11] emphasizes that profits can be increased by offering nonlinear usage-based pricing in addition to fixed-fee pricing. This result stems from the observation that digital goods exhibit no marginal costs but at least low transactions costs. Furthermore, according to the model used by the authors it is more appropriate to use low fixed-fee pricing in order to penetrate emerging markets. In contrast, for mature markets, it is advisable to employ a broad spectrum of usage-based pricing models.

New Content Types

According to research about emerging issues concerning digital goods markets in [37], one of the five challenging research questions is the transformation of the technology-enabled value chain. In particular, alternative business strategies are necessary in order to effectively handle content which is generated by consumers. In this context, SIC can be used to support charging for user generated content that attracts a high number of viewers.

Convergence

With broadband expansion over the last decade, the broadcast market experiences convergence with the Internet economy increasingly. On the one hand, content originally produced for the transmission over broadcast is accessible on the Internet. On the other hand, video content available on the Internet is delivered over-the-top (OTT) to the TV screen in the form of video on demand offers. In addition, smart TVs are able to access user-generated video content, for example YouTube, and other services using dedicated application software (Apps).

On a large scale, convergence leads to a higher competition, since not only companies of the same industry compete but also companies from the converging industry. The underlying reason is that, owing to convergence, products increasingly feature similar properties and, consequently, become substitutable. For companies belonging to a certain industry, in this situation, it is more profitable to enhance the functionality and specialization of their existing products rather than to extend the product range. According to the work presented in [38], only innovations in the core industry that lead to extended functionality increase profits. Therefore, SIC as an innovation for the broadcast industry can be used to ensure profitability in converging markets.

Piracy

In the capacity of a legal owner, only the author of intellectual creations has, among others, the exclusive right over the reproduction of his work. In this regard, a characteristic problem of information goods is that they are easily reproducible by making a copy. Most of the time the cost of making copies is negligible and the quality of the copy is identical to the original information good. The reproduction, use, and dissemination of unauthorized copies are referred to as digital piracy. This problem is exacerbated by the immaterial nature of information goods, which allows them to be transmitted, indexed, searched and distributed effortlessly over the Internet.

Currently at least two major strategies are used to counter digital piracy [39]:

1. Digital Rights Management (DRM) schemes provide technical means to prevent the production and use of unauthorized copies by employing cryptographic algorithms.

2. Legal actions are taken by passing bills for penalizing copyright infringement and taking legal proceedings against people who primarily distribute copyrighted material.

However, market developments in the last decade have shown that also appropriate pricing strategies provide effective means to manage or even prevent piracy. Please note that in the following we will only consider end-user piracy. In contrast, commercial piracy is motivated differently since it has the objective of generating revenue by counterfeiting [39].

In the work of [40], the authors recommend a two-part tariff in order to maximize profits in markets which experience piracy. In an example of their model, it is shown that a two-part tariff consisting of a fixed part plus a variable usage-based component is profit maximizing. For their analysis, the authors assume that the number of customers and their valuation for a specific product is modeled according to the shifted beta density function.

Considering markets which experience a high level of piracy, they assume a low fixed price and steeply rising usage-based costs. In contrast, with regard to markets with a low level of piracy the fixed component is marked up and the usage-based costs feature a flat increase.

Another observation suggests that piracy also serves as a mean to assess the value of a product. Since information goods have a complex nature and their value has to be learned through experience, piracy avoids the risk to buy a dislikable product consumers otherwise would take. In this regard, piracy is used as a substitute sampling method. This view is underpinned by a study where the absence of DRM for digital music increased sales [41]. In particular, less known niche albums experienced a higher demand than established hit albums. This effect can be explained by the higher uncertainty consumers face whether a niche product meets their taste or not [41], [42]. Moreover, the effects of sampling may be increased by network effects. As described earlier, the more consumers purchase a product the more additional consumers will be inclined to purchase that product due to recommendations. Furthermore, sampling also enables addiction effects [43] where the pleasurable consumption of a product increases the value. Consequently, the WTP for the successive purchase of products involving identical features such as franchise, artists, or series is also increased. Recently, these findings have been considered in order to devise new charging models. In [44] the authors analyze offers of streaming services for digital music referred to as freemium, a portmanteau of free and premium. In this model consumers who enjoy free access to music streams are tried to be convinced to purchase a paid premium offer, which enables additional features. These features can comprise access to a higher number of songs, the support of a higher number of playback devices, higher sound quality etc. The work of [45] surveys which strategy is optimal for information goods when consumer valuation can be altered by sampling and content may either be financed by customer purchase or by advertisements. Their results suggest that the optimal strategy depends on several factors such as price, sample size, actual and expected content quality as well as content demand.

Sampling and, consequently, the corresponding privacy-preventing effects can be implemented elegantly using SIC. By utilizing SIC, users could enjoy the first 10 to 15 minutes of a movie or series for free. Pirates, cord cutters, and pay-TV deniers who do not want to afford a flat-rate are able to assess and decide individually whether the offered content is valuable for them. In addition, sampling durations can be adjusted individually depending on the content in order to fully exploit network and addiction effects.

Innovative Tariffs

New types of linear and nonlinear tariffs can be designed and not only channels but also programs or even program segments can be priced individually and dynamically by using SIC. Due to the comprehensive information with regard to viewed channels and the exact viewing durations, SIC can be used for more effective price discrimination. For instance, movies and series can be priced content-based according to segments which show prior events of successive episodes or based on suspense. Consumption on mobile devices where the costs for data provision are comparatively high due to limited and shared bandwidth can be priced location-based. In this way, the additional location information can be used to specify different unit prices in areas with poor network coverage and, consequently, fund network expansion in these areas. Moreover, variants of more recent charging models enabled by electronic commerce such as demand collection, auctions and inverse auctions can be implemented by utilizing SIC.

1.2.4 Network Operator Challenges

By employing SIC, additional expenses in the form of recurring transaction costs incur for the network operator. The usage details of each customer have to be monitored and

recorded in order to issue an invoice and provide the consumer with an itemized statement of their usage. However, network operators who offer IPTV and are a target to SIC most often already possess the needed infrastructure for their telephony service and are able to share it for this purpose. In other cases, these costs have to be considered when fixing the price for the service.

Further financial burdens may result from the implementation of SIC. Aside from the acquisition of additional functional components, these components also have to be integrated into the existing transmission infrastructure. On the one hand, corresponding components in the playout center of the network operator have to work together with equipment in place. On the other hand, components at the consumer side have to be deployed in order to provide SIC functionality. This can be done either by replacing the operational devices or by initiating remote software updates. To minimize these financial burdens we can already devise requirements for the design of an SIC system. First, new components have to be compatible with existing infrastructures based on architectures described in corresponding standards or in line with the industry standards and best practices. Second, the scope and number of new components on the consumer side have to be laid out adequately based on the following premises. Generally, high costs for the network operator during the migration phase have to be avoided. Furthermore, parallel operation with existing conventional pay-TV systems has to be supported because we cannot assume that all customers of some network operator change their tariff to SIC-based tariffs. In Chapter 4, we will particularly discuss extent and location of necessary components for SIC and modifications on existing components.

Many works we mentioned in our analysis use theoretical models to derive the discussed properties of existing pricing strategies. Almost all of these models assume a monopoly producer who offers a single digital product. The reduction to a single product is rather unproblematic since pay-TV offers in fact usually consist of a single product. This product is usually extended by using the methods of price discrimination and bundling we have previously examined in order to increase the product range. We will verify this observation in detail when we inspect current offers in the German market in Section 2.4.2.

The restriction regarding the monopoly is justified in literature as a sufficient approximation for information markets where comparable products have similar prices and consumers are not sure of the quality of each product. It is further assumed that the decision to purchase a specific product from a specific producer is driven by the extent certain external factors meet the consumers taste such as brand, packaging, shipping costs, etc. In some cases, the aforementioned assumptions may be insufficient in order to assess whether SIC is applicable in the desired setting or not. Since a thorough investigation of all aspects would go well beyond the scope of this work, we rate the above analysis as an encouraging pointer to potential use cases rather than as an economic proof. Therefore, the in-depth examination of the subject is left for future work.

Nevertheless, in order to ascertain the demand of the consumer and the network operator for the SIC model, we perform further investigations in Chapter 2.

1.3 Objectives and Organization

The main objective of the thesis at hand is to address shortcomings of current charging models for linear pay-TV over IPTV. For this, it is required to consider usability and quality aspects as well as consumer and service provider interests.

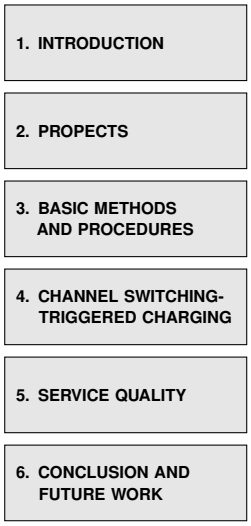


Figure 1.3: Structure of This Work

The structure of this work is illustrated in Figure 1.3 and follows mostly the course of research objectives, which are investigated in the corresponding chapter or section. As a result of our analysis in the motivating section of this chapter, so far, we could establish that the short-interval charging model has the potential for overcoming the barriers and limitations of the most common charging models for pay-TV. Taking this insight as a starting point, in the next chapter we want to get an idea about the relevance of the subject matter to consumers. For this purpose, we identify whether there is a potentially latent market demand for short-interval charging. Consequently, we phrase our first research question, which we investigate in Chapter 2:

Q1 What are the prospects of short-interval charging to become a relevant alternative pay-TV charging model?

As a technical foundation for our following investigations, in Chapter 3 we present which methods and procedures are used to perform broadcast over IPTV and how the connection to charging is established.

In the further course of this work, we propose a technical solution for the realization of short-interval charging starting in Chapter 4. We refer to the resulting technical approach as channel switching-triggered charging (CSTC) and anticipate its working principle in Section 4.1. For the development of CSTC we consider aspects that facilitate acceptance. We believe that by placing a special emphasis on acceptance, consumers and network operators harness the potential of this charging model and benefit most from the advantages we discussed in Section 1.2. In particular, we consider two important aspects that contribute to acceptance: usability and quality.

Usability from the perspective of the consumer pertains to user-friendliness and ease of use. Therefore, the next question we investigate for the design of CSTC in Section 4.2 is:

Q2 How should the functionality of short-interval charging be implemented technically in order to achieve user-friendliness?

Usability with regard to the service operator involves the applicability, adaptability, and ultimately the integration of the proposed solution into the existing infrastructure. Thus, we address the following question in Section 4.3:

Q3 How can CSTC be introduced to the operational environment of the network operator?

To answer this question, we first investigate in Section 4.3 what the general requirements of a pay-TV system are. The next aspect we address is quality. The quality of a technical solution from the perspective of the network operator comprises many features. In this work, we discuss scalability, which is in our view one of the most crucial preconditions for the acceptance of a solution in an operational deployment. Therefore, the next question we consider in Section 4.3.1.3 is:

Q4 What are the requirements regarding scalability for CSTC in an operational deployment?

In the following, we continue our consideration of quality but in this case, we assume the consumers' point of view. In this context, service quality relates to question how consumers perceive the solution. Consequently, we put the following question in Chapter 5:

Q5 To what extent does CSTC have an influence on the users' perception of IPTV service quality?

In the light of the results of the last question, we are able to assess the influence of our approach on the user experience under real-world conditions. Finally, Chapter 6 concludes this work and gives an outlook to future work.

CHAPTER 2

PROSPECTS

In this chapter, we focus on the prospects for short-interval charging to become an accepted charging model. In order to identify the market demand for this pricing scheme we take the perspectives of both involved parties. Hence, we perform an assessment for the demand side and the supply side. We obtain the opinions of consumers by conducting a survey. At first, we ask consumers whether they would consider using a pay-TV offer priced according to short-interval charging. Among other things we also identify barriers that deter consumers from using pay-TV in general. We then investigate market developments from the producer perspective and clarify whether present offers reflect an approach to short-interval charging. In a subsequent step, we analyze how producers deal with barriers we identified by means of our consumer survey. For a better understanding of our results, we first briefly introduce the market participants of the broadcast television market and identify the value chain among these participants. Since our consumer survey has been conducted in Germany and our market analysis considers the German market, we then give a brief introduction into the German IPTV and pay-TV market situation for the time the survey was conducted. We then proceed to our own consumer survey. To rate the results of the survey accordingly, we detail the market developments that have taken place after the survey has been conducted up to the time this thesis has been written in our market analysis.

2.1 Market Participants

The diagram in Figure 2.1 outlines the value chain among the market participants in the broadcast television market. For a simplified presentation, on the one hand, we considered only the content- and conditional access-related subsegments. On the other hand, only the purchase costs but not the goods and services which are provided in return are shown.

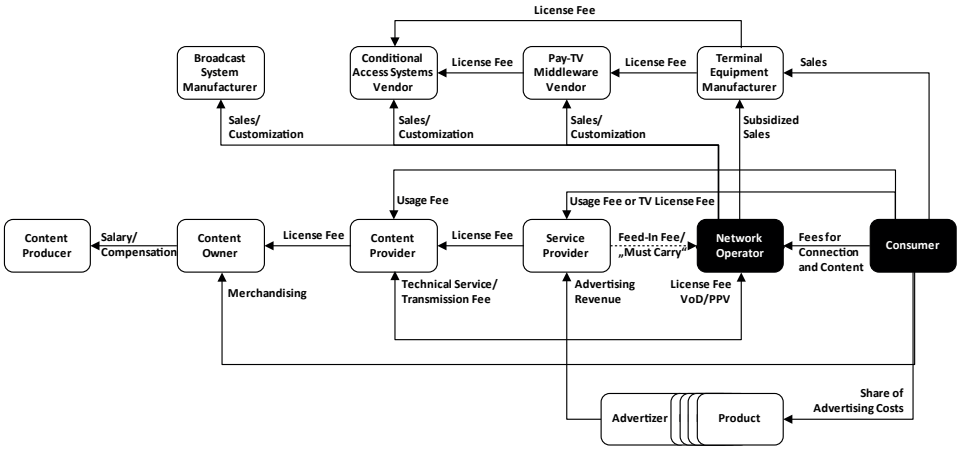


Figure 2.1: Simplified Value Chain of Broadcast Television Service

Content producers and owners bring their content into the market and are interested in protecting their value. Although content producers perform the artistic act of production, content owners market content as a product. Revenue is generated by selling content to content providers and through merchandising. Content providers bundle content into consumable program offers and bouquets. Depending on their field of business, revenue is generated either by direct customer payment or by remarketing program offers to service and network providers. Service providers create own programs or use programs from content providers and broadcast these with the aid of network operators. State-run broadcasters are fully financed by the government whereas public-service broadcasters are state-subsidized and receive their share of funding from TV license fees. In contrast, commercial broadcasters are either financed by advertisements or funded directly by consumers in the form of pay-TV. In principle, advertisements are effectively funded by consumers since advertisement costs are considered in the pricing of products consumers purchase. The advertisement subsegment consists of many more participants but here we only consider the last participant who places the order for the advertisement at the service provider for illustration purposes. Network operators provide the technical means to transmit broadcasting content to the consumers. Technical solutions for the signal transmission of linear broadcast comprise satellite, terrestrial, cable and IPTV transmissions. Depending on market and jurisdiction, network operators either charge feed-in fees for their service or are obligated to broadcast the supplied content from service and content providers in line with a “must carry” agreement. Furthermore, consumers are charged for network access and content.

Another related subsegment we consider engages in conditional access. Broadcast system manufacturers provide technical equipment for the acquisition, processing, and dissemination of broadcast signals in the form of hardware and software. Network operators

generate revenue with sales, rental, customization, integration, and from other market participants in the way of licensing fees for their software solutions. Conditional access vendors offer products for the entitlement of customers using content encryption techniques. Income is achieved by customization and licensing of products for network operators and terminal equipment manufacturers. Pay-TV middleware vendors deliver necessary components for the user interface, control, and other services carried out on terminal equipment. Revenue is generated in the way of sales and customization for content providers and network operators as well licensing for terminal equipment manufacturers and other market participants. Terminal equipment manufacturers deliver terminal devices to consumers or as a wholesale business to network operators. Income is achieved by sales to retail stores and to network operators, who buy high volumes of set-top boxes and resell them with a subsidy to consumers. Consumers play a primary role among all market participants since they fund terminal equipment, transmission networks, programs, and content by regularly dedicating a certain amount of their household income for media use.

Nowadays, service providers assume many tasks, which have been attributed to different market participants in the description above. For instance, advertising-financed commercial broadcasters not only purchase content from content providers but also produce content in-house. These productions are also licensed to other television stations. Moreover, additional revenue is generated by teleshopping, merchandising, as well as call-in, televoting and phone-in quiz shows [46]. In this regard, some state-subsidized TV channels also assume the role of a network operator and broadcast their content either directly or with the aid of subsidiary companies [47]. However, pay-TV broadcasters act as content and service providers at the same time when they produce sporting events such as football and soccer matches, whereas the content owner is the corresponding league or association. This trend is also observable for conditional access vendors, who not only offer the proper pay-TV middleware but also exert influence on the design of terminal equipment on the pretext of security to achieve vendor lock-in [48].

While we will investigate technical solutions for the implementation of short-interval charging from the perspective of the conditional access related market participants in Chapter 3, we also consider the requirements of consumers and the network operators in Chapter 4. The reason for this approach is that we regard consumers as the main drivers for the demand for short-interval charging and network operators as the first contact point to meet this demand as a result of our findings in this chapter.

2.2 Market Background

At the time of our survey in the year 2009, 35.5 [49] to 37.5 million TV [28] households received an average of 73 channels in Germany. The typical German watched TV for 212 minutes on average per day [49] and 53% of all TV households received TV signals over cable connections, 42.2% via satellite, 10.7% over terrestrial free-to-air transmission, and 3.5% over IPTV (multiple forms of reception are possible) [28]. In total, more than 5.3 million subscribers obtained pay-TV services [28], which equates to a market share of about 14%. Sky Deutschland having about 2.48 million subscribers was the then market leader [50]. The total number of broadband households in Germany was estimated around 26.5 million [51]. About 23.8 million thereof were supplied with digital subscriber lines (DSL). Providing a bandwidth of 6 Mbit/s and more, a portion of 52.4% of these DSL lines was capable of transmitting IPTV [52]. This corresponds to ca. 12.5 million potential IPTV subscribers. At that time two IPTV operators were active in Germany: T-Com (the German

Telecom) and Alice, an affiliated company of Telefonica. T-Com had approximately 13.87 million active DSL lines with 1.3 million subscribers using their triple-play service (voice, Internet, IPTV), called Entertain TV, [53]. Alice, in contrast, had around 2.09 million DSL customers with 0.06 million subscribers for IPTV [54]. Thus, 1.36 million IPTV customers were recorded in Germany at that time.

Compared to other countries, the IPTV market penetration in Germany could still be described as relatively low. One of the main reasons for this situation is the competition with many well-established transmission paths including terrestrial free-to-air transmission, cable lines, and satellite transmission. The digital terrestrial television signal is being made available by public broadcasters and provides a considerable number of TV channels for free. Digital cable TV is also very widespread in Germany and records high growth rates.

Additionally, Germany is located in a favorable geographical position concerning the coverage zones of several satellites. Thus, hundreds of unencrypted TV channels can be received with a low-cost receiver and a satellite dish with a small diameter.

Despite the fierce competition of transmission paths and the slow start of IPTV, the pay-TV over IPTV market in Germany undergoes growth correspondingly to the world market. One important driving factor for this growth is the high and increasing broadband penetration in Germany. Another reason is that IPTV, unlike the other transmission paths, increasingly attracts customers with its unique technical properties like time-, place-, and device-shifting. In the light of the above insights, we believe that Germany is a suitable place for the research of consumer opinions on short-interval charging for IPTV since it features a highly competitive market and a high and increasing broadband penetration.

2.3 Consumer Perspective

In this section, we present the results of our assessment about the acceptance of the short-interval charging model in an actual market. For this purpose, we conduct a survey we presented in [55] for determining the fraction of users willing to accept this model. For a better evaluation of our results, we first consider related work. In the next step, we introduce our methodology and the results of the survey. Due to our first insights, we are able to draw an initial conclusion.

2.3.1 Surveys Addressing Short-Interval Charging

Since IPTV is a comparatively new technology, related studies and surveys have focused more on the adoption of the IPTV service than on diverse charging models, that could be used in combination with the IPTV technology [56], [57]. In [58], for instance, the familiarity of consumers with the concept of IPTV and their willingness to purchase IPTV services is surveyed. In [59], the adoption of IPTV is investigated considering the role of a user gratification model. Further studies assess the interest of consumers in advanced features of IPTV [60] involving Tele-Commerce [61] and the vision of *connected home* [62]. Regarding charging models and especially the willingness to pay depending on different models, the work of [63] surveys consumer opinions for mobile TV services. As for the proposed short-interval charging model for pay-TV over IPTV, we are not aware of any relating study up to now.

In summary, to the best of our knowledge, there have been no other studies which specifically addressed consumer opinions on short-interval charging for pay-TV over IPTV

up to now. Pay-TV business models were addressed in several academic research work and patents.

2.3.2 Methodology

Our survey was conducted online using a dedicated website during a period of six weeks. For the creation and management of the web-based questionnaire, the LimeSurvey application [64] was used. The participants were asked by email to take part in and to recommend the survey. As an incentive, all participants, who completed the survey and submitted their email address, entered a prize draw for a voucher of an online store. Out of total 337 responses, incomplete responses were excluded leaving 315 complete responses for evaluation.

2.3.3 Questions, Options and Results

The online questionnaire was simple in design. At first, some demographic information regarding the gender, the age and the occupation of the participants were requested. The proportion of female attendees approached 33%. More than 83% of the attendees are between 18 and 39 years old, see Figure 2.2. The majority of the participants consists of persons with high payment ability or payment potential such as employees, self-employed, employers, and students. Only a minimal part of 3.17% and 0.95% is retired or unemployed, respectively.

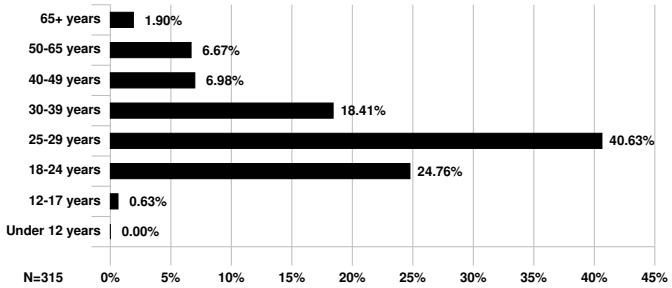


Figure 2.2: To Which Age Group Do You Belong?

Toward its main target in estimating the acceptance of the short-interval charging model by consumers, the survey tries to collect various information about the familiarity of the respondents with IPTV. Furthermore, the behavior of respondents with regard to their consumption of TV and pay-TV is surveyed. Depending on this information, some questions are skipped or considered. For instance, a participant, who does not watch any TV, is not asked about the type of TV reception in her or his household because the probability that this participant does not have a TV at home is high. By this means, we tried to increase the informative value of each answer. The fact that IPTV is still in its infancy in Germany has been confirmed by the answers to the basic question: Are you aware of the term IPTV? See Figure 2.3.

Note that the high percentage of respondents not aware of IPTV, does not have a negative impact on the final result of the survey. Remember that we aim at finding out how attendees

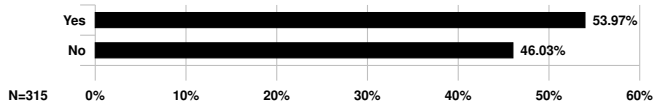


Figure 2.3: Are You Aware of the Term IPTV?

think about charging models for pay-TV in general. It is well-known that IPTV is often confused with other video content provided on the Internet. To be more specific, therefore, we asked the respondents, who regarded themselves as aware of IPTV, to specify what they understand under this concept, see Figure 2.4. Fortunately, most participants could assign IPTV as television over DSL, which is the correct definition of IPTV.

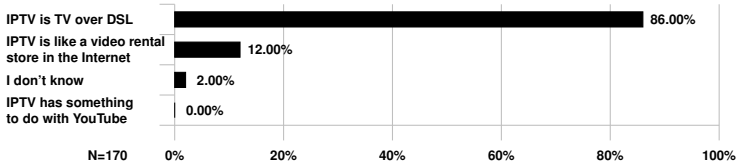


Figure 2.4: What Exactly Does IPTV Mean for You?

The next questions relate to the respondents' behavior regarding the consumption of TV, pay-TV, and video content in general. First, we questioned the attendees about their form of TV reception, see Figure 2.5. The answers to this question reflect the general situation of the current market situation for TV reception in Germany. The most common form of reception is cable TV (digital and analog) followed by satellite and terrestrial reception. About 9% of the participants do not watch any television.

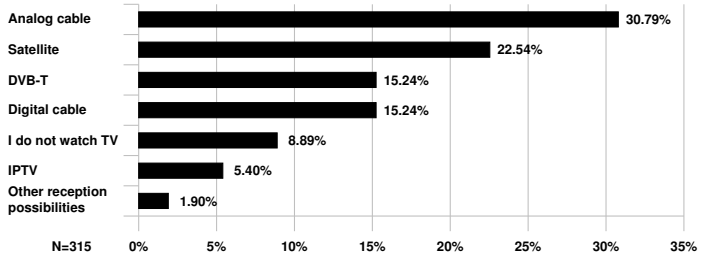


Figure 2.5: How Do You Receive Your TV?

Again, the lower IPTV reception in Germany does not worsen the main survey objective, as our purpose is to learn about the participants' behavior and attitude regarding pay-TV and other paid video data in general. In the next question, we found out that only 9% of the participants with TV reception watch pay-TV such as Arena or Sky see Figure 2.6.

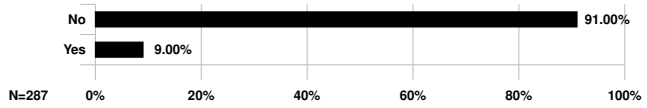


Figure 2.6: Do You Use Pay-TV Services Such as Arena or Sky?

However, more than 72% of all attendees pay for video content such as DVD purchase, video rental, or visits to the cinema, see Figure 2.7.

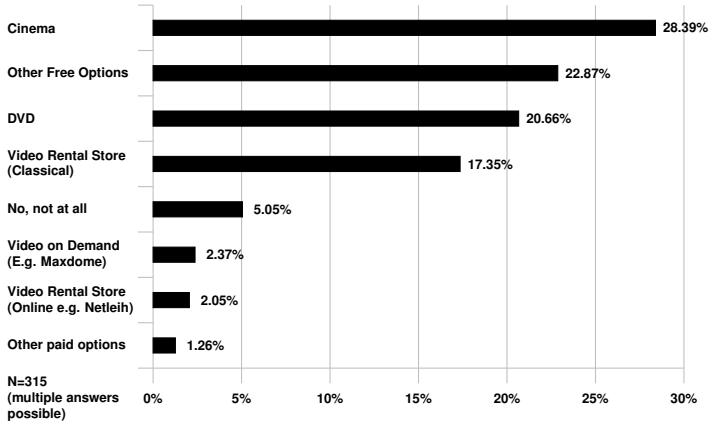


Figure 2.7: Do You Pay for Video Content in One or More of the following Forms?

Combining the answers to the last two questions it can be assumed that the lower interest in pay-TV is not attributed to a low willingness of the participants to pay for media content. Rather, there must be other reasons, which make pay-TV less attractive and deter people from buying this service. The next point, therefore, was to ask the respondents, who do not access pay-TV, what would attract them to buy pay-TV content, see Figure 2.8. Surprisingly, the answers to this question confirm our assumption, that it is the way of pay-TV offering, which hinders its wide acceptance. More than 83% of respondents would buy pay-TV under some conditions. Most of these conditions relate to the price and the contract, namely, the subscription. Obviously, more than 35% find that pay-TV prices are too high and a total of about 38% has difficulties with the subscription-based model itself or with long subscription periods.

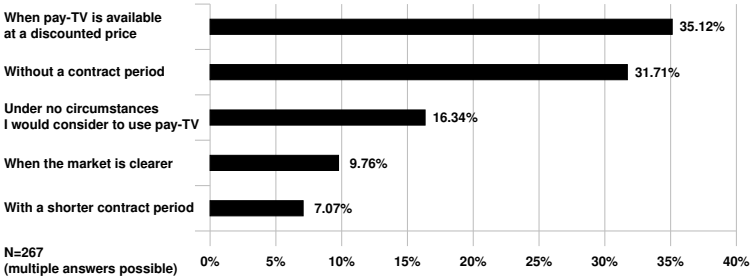


Figure 2.8: Under Which Conditions Would You Be Willing to Use Pay-TV?

The result of the previous question confirms the analysis given in Chapter 1 regarding the problems of current pay-TV pricing models and suggests that a new model is overdue. The last and most relevant question aims at the specific information on whether the proposed short-interval charging model would attract more customers, see Figure 2.9. The attendees are confronted with three pricing models and asked for the preferred one. To avoid any misunderstanding, each of these models was clarified shortly in the survey:

1. **PPV/VoD:** You pay for a selected film.
2. **Monthly Subscription:** You pay a monthly fee.
3. **Accurate Deduction:** You only pay for the seconds or minutes you watch.

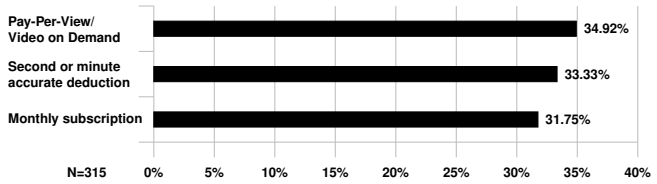


Figure 2.9: Which Pricing Model for Pay-TV Would You Prefer?

In summary, the survey provides the following main information:

1. More than 72% of the survey respondents already pay for video content in one way or another. Even the attendees, who do not watch any TV (ca. 9% according to Figure 2.6), seem to consume paid video in several ways. By analyzing the answers of this group to the question of Figure 2.7, we found out, for instance, that 71% of these attendees go to the cinema, 46% buy DVDs, and 32% utilize the services of video rental stores. In total, 90% of all the respondents pay for video content.

2. Although pay-TV is very well-known, it still lacks a wide attractiveness for most people. Only 9% of the respondents with TV reception make use of this service (Figure 2.6). Even if there may be other reasons for this situation, most respondents identify the price and the charging model (subscription-based charging) as the most important obstacles of today's pay-TV (Figure 2.8), which is comprehensible considering the market situation described in Section 2.2.

3. A short-interval charging model for pay-TV is preferred by 33% of the survey participants. Whereas 39% of this group were attendees, who are not aware of the term IPTV. Also, the respondents, who do not pay any money for video content (ca. 10% of all respondents), seem to be most attracted by the new model. Their voice for the model reaches 44%.

2.3.4 Evaluation

In the following, we assess the validity of survey outcome by setting its particular results into relation to market analyses and studies, which addressed similar questions.

In Figure 2.10 the age distribution of the TV households is compared to the age distribution of the survey participants. We can see that the age-group of 18-39 is disproportionally overemphasized in our sample [65]. Additionally, the gender ratio in our sample is 67% (male) to 33% (female) whereas the gender ratio of all TV households is 49% (male) to 51% (female) [66]. Relating to the IPTV awareness the ratio is 46% (aware) to 54% (unaware) in our sample. This result matches exactly with results of a representative study [67], where the participants have the same ratio of 46% (aware) to 54% (unaware).

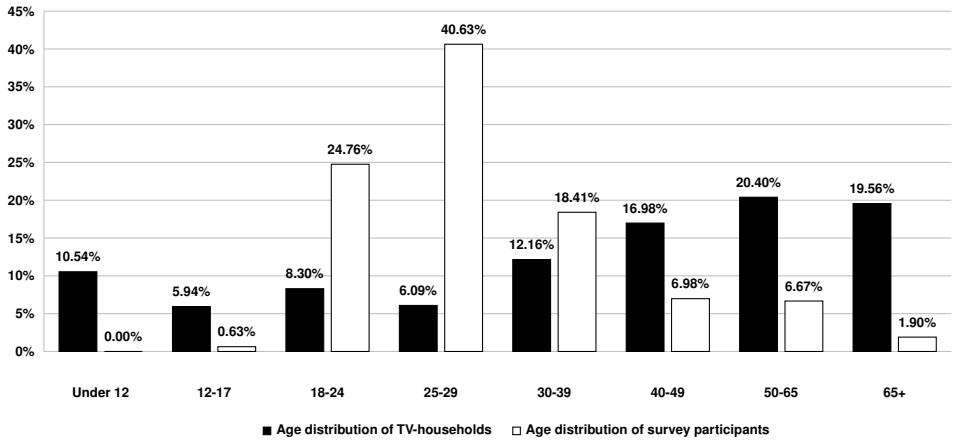


Figure 2.10: Comparison of Age Distribution of Survey Participants and TV Households in Germany

A comparison between the distribution of transmission paths of all TV households [68] and our sample is depicted in Figure 2.11. It shows that viewers receiving their TV broadcast over satellite are underrepresented whereas such receiving their TV broadcast over IPTV and terrestrial digital video broadcast (DVB-T) are overrepresented. Also, there is a minor shift in the ratio of pay-TV subscribers. The ratio is 9% subscribers to 91% nonsubscribers in our sample and 12% subscribers to 88% nonsubscribers in the German market [28].

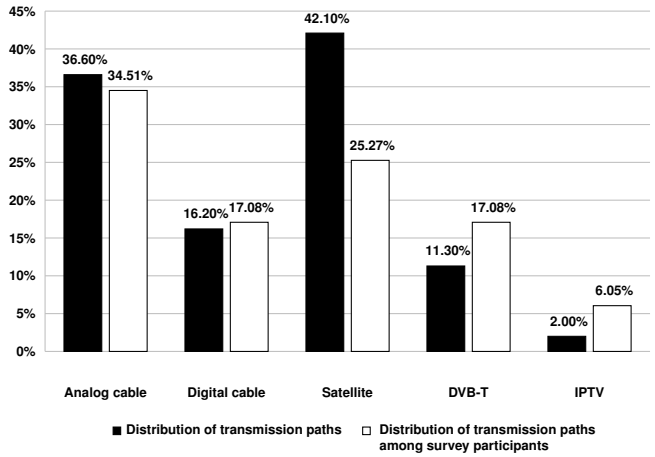


Figure 2.11: Comparison of Transmission Paths of Survey Participants and TV Households in Germany

Figure 2.12 shows the revenues for video content in Germany compared to the spending of the survey participants [69], [70]. The share of customers, who provide video content from video rental stores (classical and online) as well as video on demand customers are

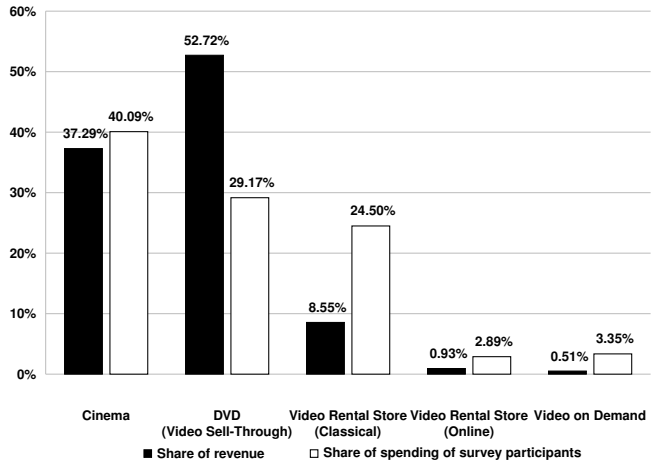


Figure 2.12: Comparison of Revenues for Video Content and Spending of Survey Participants

clearly overrepresented in our sample, whereas customers of home video products (video sell-through) are represented in smaller extent.

When asked for the conditions for taking pay-TV into consideration, the two highest rated options in our sample were relating to discounted price and the omission of a contract period. Interestingly, when participants of a similar study [67] have been asked about the reasons for their reservation against switching to IPTV, identically, the highest rated reasons were the prize and the deterrent effect of the subscription period. This reveals at least two insights. On the one hand, the price is a strong indicator for user acceptance of a new product or model in the context of IPTV and pay-TV. On the other hand, obviously, the subscription period, as well as the price, are the main factors discouraging customers from using IPTV and pay-TV.

In the last question, the respondents have been asked for an abstract tendency toward our short-interval model by stating a general preference. Since this model is new, it is clear, that no respondent has ever experienced it. In order to avoid any bias during the process of forming their opinion, we provide the respondents only with the main merit of our model: You only pay for the seconds or minutes you watch. Thus, we assume that the respondents associate the proposed model with the next related model in their everyday life, which is short-interval charging for (mobile) phone calls or Internet usage. As we expect that all respondents have experienced the short-interval charging model in such context, we regard their assessment of this model as valid. Based on this assumption, the perceived benefits of our model is independent of the knowledge of the term IPTV or the properties of the content (genre, duration, and so on). So, all participants of the survey have been asked the last question, since their opinions are of equal value for us.

We could see that participants most sensitive to price and subscription period chose our short-interval model most:

Almost 70% of the participants who chose our short-interval model stated that either price or subscription period are important factors for taking pay-TV into consideration. This shows that the reasons for respondents to choose our short-interval model are indeed price or subscription period since the participants most sensitive to these factors decided

in favor of it. In contrast, participants who opted for a monthly subscription were comparatively the least sensitive to price or subscription period. Only 45% of these participants deemed price or subscription period to be important when deciding on a pay-TV service purchase.

2.3.5 Subsequent Developments

In order to complete our picture of short-interval charging market relevance, we put our results in relation to subsequent studies and market developments that took place at the time after we conducted our survey.

Generally, we observe that the proceeding convergence leads to substitution effects. As a result, over-the-top (OTT) VoD offers increasingly gained popularity whereas pay-TV offers recorded a drop in demand. According to a study [71] with 2000 participants among 14-75-year-olds, 9% of all pay-TV subscribers in the U.S. canceled their pay-TV subscription in the year 2011. Furthermore, 11% of the participants are considering canceling their contract because they could watch almost all of their favorite shows online. In addition, 15% of all participants stated that they will most likely watch movies, television programs, and videos from online digital sources in the near future [71]. Next, we consider another online study conducted in June 2011 with 1,013 participants. Here, 10% of the customers who are subscribed to a major VoD provider and previously canceled their pay-TV subscription over cable or satellite indicated that they are willing to cancel their VoD subscription if a traditional pay-TV provider would start an offer with a similar service at a similar price [72].

Survey	**Our Survey** [55]	Amdocs [73], [74], [75]	Deloitte [76]
Time of Survey	**2009**	2014	2014
Origin of Respondents	**Germany**	11 Countries	U.S.
Mode of Survey Participation	**Online**	Online	Online
Total No. of Respondents	**315**	4070	2076
Base Population	**See Section 2.3.4**	Pay-TV and OTT Customers	Representative U.S. Population*
No. of Respondents Expressing Charging Preference	**315**	4070	Unknown
Population Expressing Charging Preference	**Identical to Base Population**	Pay-TV and OTT Customers	Consumers with Pay-TV service

Table 2.1: Comparison of Related Consumer Surveys

*Population calculated by weighting year 2014 projections of population division from 2010 U.S. Census Bureau.

In accordance with the insights we gained from our survey, participants specified high price and long contract terms as the motivating force for their decision to cancel the pay-TV

subscription. Consumers complain of rising subscription fees needed to cover increasingly expensive licenses for sports events even though they are not interested in such offers. In this context, consumers also criticize additional charges such as connection and installation fees. Moreover, video on demand providers aggressively advertise their short term of contract in contrast to the long subscription periods of pay-TV offers at a time of economic woes when the unemployment rate is at 9.1% and the economic growth is slowed to 1% in the U.S. [77]. Therefore, we can conclude that besides price increase and long term of contract, the superordinate reason for the discontent of the consumers arises from the perceived unfairness resulting from the cost-attribution that does not reflect usage.

In another representative online survey published in 2014 [75] with 4070 OTT and pay-TV subscribers in 11 countries including Germany participants are asked a similar question regarding their preference for a charging model we asked in our survey. However, in this survey the participants have the choice among the following three given options:

1. A set-fee for a basic package and then pay only for the extra items/channels I watch
2. A set-fee for all available channels
3. Only pay for the items/channels I watch

Interestingly, similar to the results of our survey 36% of all respondents selected the last option which offers a higher degree of usage-based cost attribution and interactivity of entitlement. In contrast, the first and second options were met with less approval amounting to 29% and 35% respectively [75].

In contrast, in a different related online survey with 2076 respondents conducted in 2014 in the U.S. [76] slightly other options lead to other results. In particular, pay-TV subscribers are asked which way of purchasing paid television they would prefer and are given the following options:

1. Subscribe only to the channels I watch regularly
2. Subscribe to a package of channels even if I do not regularly watch them all
3. Purchase only those individual shows and events I want to watch

Here, only 8% of the respondents chose the last option, whereas 52% chose the first and 40% chose the second option, respectively. Although there is a clear tendency toward usage-based cost attribution and interactive entitlement when compared to the results of the previously mentioned survey [75], the respondents in this study seem to be more reluctant to pay for individual content.

However, we believe that there are two reasons for this difference. The first reason is that the base population who is asked regarding its charging preference in the second survey is different: It entirely consists of pay-TV subscribers. In contrast, in our survey, this population is more general and all participants are asked regarding their charging model preference.

As we could see in our evaluation, respondents who are already pay-TV subscribers are least sensitive to the factors of price and subscription period and, consequently, value the advantages of charging models providing these features least. Similarly, also in our survey the share of pay-TV customers who prefer short-interval charging is comparatively low accounting for only 20%. The second reason is a subtle difference in the phrasing of the options. In the first survey, the formulation accentuates that participants "*only pay*" for

something, which evokes associations with a more passive action that is further trivialized. In the second survey, in contrast, the participants are requested to *purchase*. In our opinion, this wording describes a more active process and is further complicated by the selection problem emphasized by the addition of "*only those individual shows and events I want to watch*".

In both surveys, the options implying the highest usage-based cost attribution and interactivity of entitlement still do not correspond to the short-interval charging model we suggested in our survey. Nevertheless, we can see a general tendency of consumers toward charging models offering these properties. We compare the results of our survey to the most important properties of related surveys. A summary of this comparison is shown in Table 2.1.

Moreover, respondents also state that they are more satisfied with the content, customer service, and video quality in broadcast pay-TV than with over-the-top (OTT) and online video services (such as Netflix, Hulu, etc.) [74].

In general, we can observe that consumers perceive the cost-value ratio for pay-TV offers as unbalanced. Hence, 24% of the respondents in the U.S. and Canada, who are pay-TV subscribers and additionally own a subscription to an OTT service consider canceling or reducing the amount they spend on their pay-TV service [73]. However, more than the half of these respondents would maintain their expenses in case their pay-TV provider would give them a single source to search, discover, and watch all of their content, including the content available on OTT offers. Again 62% of these respondents would spend more on such a service than they currently spend on pay-TV [74].

Another reason for the shift to VoD offers is the freedom of choice regarding content selection. In contrast to pay-TV offers, which are categorized according to genres, VoD providers enable consumers to watch only the desired content and pay for it. Thus, the service offered to consumers becomes fully adaptable. With regard to the adaptability of services, respondents coming from the U.S. and Canada are willing to pay an average of 7.0% more to receive services tailored to their viewing. In this context, 86.3% of the respondents coming from the U.S. and Canada would approve that their usage information is collected and analyzed for this purpose [73].

2.4 Producer Perspective

In this section, we detail the measures taken by pay-TV providers in order to counter current market developments such as the copious cancellation of subscriptions we found out in the previous section. In order to rate these measures accordingly, we first update our data with regard to the German market. In a subsequent step, we analyze current innovations of pay-TV tariffs and show to what extend these tariffs accommodate recent developments.

2.4.1 Market Background: An Update

The business volume of the German television market was composed of 4.774 billion euro from TV license fees, 4.289 billion euro from net advertisement revenues and 2.098 billion euro from pay-TV revenues in the year 2014 [78]. In contrast the business volume of the video market which is about 15% of the television market. In the video market, substantial shifts from DVD sales, which amounted to 1.503 billion euro in 2009 and only

0.906 billion euro in 2015, to Blu-ray Disc and VoD sales can be observed between 2009 and 2015. In this time frame, Blu-ray Disc sales volume almost quadruplicated from 0.135 billion euro to 0.536 billion euro and VoD sales volume increased to more than tenfold from 0.021 billion euro to 0.236 billion euro [79]. While the typical German watched television for 212 minutes in 2009, this value increased up to 225 minutes in 2011 and declined to 216 minutes in 2015 [49].

Between 2009 and 2015 the number of TV households increased by approximately 1.5 million totaling to 38.9 million [79]. The distribution of transmission paths increased in favor of satellite (+4.4%) and particularly IPTV. While in 2009 IPTV accounted for only 1.0% of all distribution paths, in 2015 this value increased to 4.8%. In return, fewer (-6.7%) consumers received their television signals over cable and over terrestrial transmission (-1.6%) totaling to 46.1% and 9.7% respectively. Thus, in 2015 satellite and cable transmissions are almost equally prevalent in Germany respectively amounting to a share of 46.5% and 46.1% among the transmission paths.

The number of pay-TV subscriptions increased by 1.7 million to 7.0 million in total between 2009 and 2015 [80]. As a consequence, approximately 12 million viewers watch pay-TV in Germany in 2015. Sky as the largest pay-TV provider acquired 1.6 million additional customers from 2009 to 2015 and serves a total of 4.123 million subscribers at the end of 2014. This was achieved by means of a decreased subscriber churn rate of recently 8.2% and new products such as online and VoD offers [78].

In the meantime also broadband expansion succeeded in Germany. While the number of broadband households increased by 3.1 million to a total of 29.6 million, the number of DSL connections decreased by half a million totaling to 23.3 million between 2009 and 2015. Nevertheless, the capacity of the DSL connections substantially increased. While in 2009 only 52.4% of all DSL connections featured a bandwidth of 6 Mbit/s and more, in 2015 this value increased to 97.8%. Furthermore, 85.4% of all DSL connections feature a bandwidth of 16 Mbit/s and more and 68.7% are capable of transmitting 50 Mbit/s and more in 2015.

IPTV services are currently offered by T-Com (the German Telecom) and Vodafone. Alice, an affiliated company of Telefonica active as an operator in 2009, discontinued its IPTV offer at the end of 2013. T-Com could increase the number of IPTV subscribers from 0.8 million to 2.4 million in 2014 and further projects to serve 5 million subscribers in 2018. This success was partly achieved thanks to the VoD offers in cooperation with maxdome and Netflix, the two most popular VoD providers in the German market [78].

2.4.2 Billing Plans

As we could see in the previous section, pay-TV service providers and network operators experienced continuous growth during the period under consideration. We will see that this positive development is a result of offers, which meet the market demand we could determine in our prior survey. In the following, we will analyze the billing plan and innovations in the product range of a major network operator in Germany, the German Telekom. A simplified structure of the current billing plan is illustrated in Figure 2.13. Components with white background color indicate optional offers and components with gray background color show mandatory or bundled products. Moreover, components with black background color show discounts.

At first glance, we can see that four different services, usually referred to as quadruple play, are offered and compose a multipart tariff. These services consist of fixed line tele-

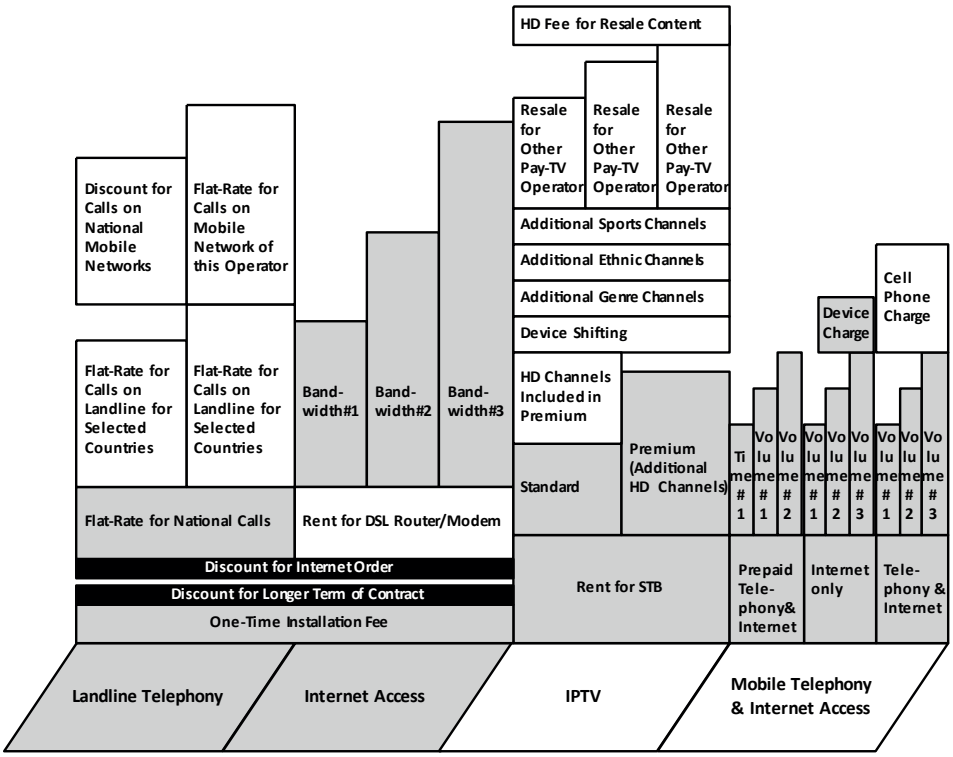


Figure 2.13: Simplified Billing Plan of a Major German Network Operator

phony, landline Internet access, IPTV, and combined mobile telephony and Internet access. Fixed line telephony and Internet access as the historical main business segments form the core services and are bundled to a mandatory base product. In addition, IPTV and mobile services are optional offers. However, various forms of price discrimination are applied. Flat-rates to fixed line destinations in different countries are bundled in two different pure bundles. The price for Internet access is fixed by using the versioning strategy depending on different up- and downlink bandwidths. Mixed bundling is applied for the channels of the IPTV offer. These channels may be obtained by ordering the premium product or by selecting the standard product and additionally ordering the residual channels as an optional product. Generally, channels are subject to versioning either by their number or by the availability of a higher resolution (HD). Furthermore, instances of the application of different types of group pricing can be found. Consumers preferring channels broadcasting in a specific language or channels of a certain genre can order special channel packets. Additionally, consumers ordering the products over the Internet receive discounts on the base fee. Usually, broadband access and, consequently, IPTV is provided over DSL using copper wires or over fiber optic cables using Fiber-to-the-home (FTTH). Another form of third-degree discrimination is applied for geographic locations where the network operator is not able to offer a broadband connection due to the lack of own cables. For these areas, the IPTV offer is replaced by a comparable service over satellite.

A further pricing strategy is the discount on the base fee for a certain period of time (12 months) if the consumer chooses a longer term of contract (24 months). This discount can

be seen as a block-rising tariff. Also, the installation fee is a one-time fee and the rent for the set-top box can be regarded as a periodical non-usage-based fee.

Generally, two trends regarding product innovation can be observed during the period under consideration. In addition to the regular offer of linear broadcast content, network operators provide access to a VoD service mostly free of charge. This service comprises a considerable number of free movies either provided by an in-house service or with the aid of an established VoD provider. This trend can also be observed for network operators and service providers who offer their services over IPTV, cable, and satellite. When consumers subscribe to a VoD service provider directly, in contrast, VoD access is referred to as over-the-top (OTT). In this case the network operator is not involved in the management and dissemination of the VoD content. Other cooperations result in the resale of pay-TV service provider content by IPTV and cable network operators. Here, the billing plan of the pay-TV service, which mostly consists of different channel bundles, is adapted to the billing plan of the network operator. This trend clearly confirms our assumptions we made regarding convergence in Chapter 1. We asserted that in the face of inter-industry substitution, it is more profitable for a company belonging to a certain industry to enhance the functionality and specialization of their existing products than to extend the product range. As a consequence, network operators collaborate with VoD and pay-TV service providers to meet the consumer demand for interactive entitlement and adaptable services and thus to decrease subscriber churn.

Another trend we could observe is the streaming of live broadcast content to other devices such as PC and mobile devices as an optional product extension. In case an additional cell phone contract with the network operator exists, the subscriber is also able to stream some of the channels over third- and fourth-generation cellular networks (Universal Mobile Telecommunications System (UMTS) and Long-Term Evolution (LTE)). This product category meets the consumer demand for the availability of content on multiple devices and is also referred to as device shifting. According to a representative survey [74], consumers equally attribute this property to pay-TV and VoD service providers and 29% of all consumers would pay 5-10% more for this feature.

In addition to the trends described above, also variants of the presented charging models exist on the market. One instance of such a variant is postpaid pay-per-view. Here, the consumer usually has a subscription to a pay-TV service provider and the ordered PPV content is not debited immediately but with the following invoice. Furthermore, we already described another variant applied to VoD as subscription VoD (SVoD). When staggered or near video on demand (NVoD) is used, identical programs are started at short time intervals such as 15 minutes. This concept is used as a remedy for the lack of a return channel which prevents users from consuming an ordered program at the desired time. However, NVoD consumes high bandwidth for every program since several channels are occupied depending on the duration and starting offset. For push video on demand (PVoD), a selection of popular programs is sent to the receiver and recorded to a hard disk drive. The transmission is usually carried out in times when free capacity is available, for instance, at night or during the day. In this way, the user can select, order, and consume a program with low latency although no return channel is available. This variant, however, requires that the STB is equipped with a hard disk drive.

2.5 Conclusion

In this chapter we address our question Q1 regarding the prospects of short interval charging to become a relevant alternative pay-TV charging model. In order to show that a significant share of consumers is attracted by short-interval charging, we conduct an online survey with the participation of 315 respondents in Germany. We are able to show that 33% of the survey participants prefer short-interval charging to traditional models. Our findings are mostly supported by two other surveys which have been conducted in the U.S. and in 11 countries including Germany, respectively. Thus, the proposed model seems to meet open demands and attract a relevant share of consumers on the IPTV market. Once implemented especially in segmented markets, this new charging model suggests accounting for a relevant share of the total pay-TV market besides VoD/PPV and subscription-based pay-TV. We observe that the demand for short-interval charging is driven by the criticism of high prices. In particular, consumers perceive cost-attribution that is independent of actual usage as unfair. This conclusion confirms our assumption that there is a high demand for usage-based cost attribution. In the following market analysis, we are able to see a shift in demand in favor of VoD service providers. From our findings of other surveys and analyses, we are able to deduce that this reorientation of consumers toward the charging model of VoD is the result of a higher interactivity of entitlement and a higher adaptability of services. In our subsequent analysis of current billing plans, we show that service providers and network operators take account of these recent developments and seek to adopt measures to meet the consumer demand and decrease churn.

CHAPTER 3

BASIC METHODS AND PROCEDURES

In this chapter, we investigate which technical concepts and architectures are involved for realizing IPTV broadcast and pay-TV. For this purpose, we initially analyze the structure of the data being transmitted. Subsequently, we briefly look into the components and interfaces which are generally used to provide a broadcast service. For the discussion of multicast encryption, we first inspect the concept of multicast in the context of the Internet protocol. Then, we examine methods for establishing confidentiality in group communication. Finally, we introduce group key management schemes and give examples for illustrating their working principle.

3.1 Broadcast Architectures

3.1.1 Structure of Broadcast Data

Pictures on a TV set usually are displayed on a rectangular grid of points. Individual points are called picture element, pel, or pixel and feature a color. This color is generated as a mix of the primary colors green, red and blue and produced by light-emitting elements on the display device. In order to specify a particular color, the intensity of each primary color is represented by a number. Thus, a particular color is described by three numbers. The number of bits used to represent the color intensity is referred to as color depth. Usually, eight bits are used to represent the intensity of each color, since the resulting color space is sufficient and the processing of numbers of this size is convenient for electronic devices.

Display resolutions, that is, the number of points on the grid, are defined in video system standards. Resolutions are specified by indicating the number of pixels for the width and the length of the display image. Typical resolutions are 768x576 [81], 1280x720 [82], and 1920x1080 pixels [83] [84].

In order to ensure a fluent visual perception, the images of a video have to be updated regularly. The number of updates per second is called frame rate. Frame rates are also defined in video system standards and common values are 25, 29.97, 30, 50, and 60. Depending on the values for color depth, resolution, and frame rate we can calculate the required bandwidth for transmission. As an example, the required bandwidth of a single video transmission having a color depth of 8 bit, a resolution of 720x576, and a frame rate of 25 frames per second amounts to 248.8 Mbit/s. In order to save bandwidth in particular for transmission over wireless connections such as satellite links, *data compression* has to be employed. Recent compression methods are able to reduce the bandwidth requirement for our example to about 1.5 – 3.0 Mbit/s. Since the structure of broadcast data are determined by the employed compression methods in the following we consider the most characteristic methods used in the common standards for video encoding such as [85], [86], and most recently [87].

Figure 3.1: Combing

3.1.1.1 Compression Methods

The earliest form of compression is *interlacing*. Here, only pixels of odd and even numbered rows (lines) of an image, which are called half-images or fields, are transmitted at a time. In early TV sets featuring cathode-ray tubes (CRT) the frequency of the AC power supply voltage of 50 Hz respectively 60 Hz was utilized in order to receive and alternately scan the resulting fields 50 or 60 times per second. Thus, by using interlacing it is possible to transmit the double number of frames by using the same amount of bandwidth. However, interlacing also introduces some problems especially on newer liquid crystal (LC) displays. Pixels of CRT-based displays consist of successive areas, which are excited by an electron beam and feature an afterglow.

In contrast, pixels of LC displays are controlled individually and permanently. This difference leads to undesirable effects such as combing and interline twitter. Combing occurs when fast objects move through the image or a ticker is displayed. Since in this case only a single field, namely every second line, covers the information of the movement, the edges of corresponding objects resemble combs. An example for combing is given in Figure 3.1 where a laser pointer beam moves rapidly across the image. Interline twitter is caused by horizontally aligned thin segments. These segments are beyond the resolution of the recording device and therefore sometimes added only to one field and sometimes to both fields. This causes a flickering of the lines covering these segments alternately in rapid succession.

Another early compression method that emerged with color television is *chroma subsampling*. This compression technique is based on the working principle of the human color perception. Human vision follows the concept of complementary colors where certain pairs of colors are never perceived simultaneously in a single color but are rather opposing endpoints of a continuous scale. These pairs are red-green and blue-yellow. This manner of perception has physiological reasons caused by the way visual stimuli are produced by cone cells and transmitted to the visual cortex over the optic nerve. In addition, the perceived spatial resolution of these color components is much lower as the human eye is not able to distinguish differences in color (chrominance) as well as differences in brightness (luminance). This is presumably the result of adaptation to the occurrence of color in nature where smooth transitions of color intensity are common but abrupt changes in color intensity are very rare. Hence, the color components of a picture can be stored with a lower resolution.

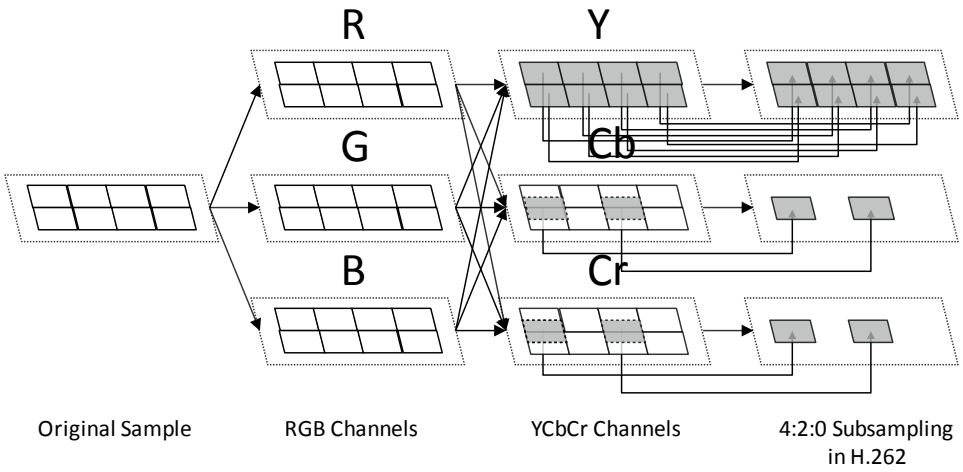


Figure 3.2: Conversion to YCbCr Color Model and Chroma Subsampling

This knowledge is applied in the YCbCr color model, which is generally used in all kinds of video equipment and also in media broadcast. Instead of storing intensity values for the primary colors red, green and blue (RGB), in this model, the luminance (Y) and the chrominance, that is the blue-yellow portion (Cb) and the red-green portion (Cr) of a pixel are stored. In order to specify the ratio of bits used to store these individual portions when an RGB image is converted to this color model, a notation in the form of x:y:z is used. Here, x indicates the number luminance (Y) samples taken from the sampling area of the RGB image which is 2 pixels high and x pixels wide. The y value indicates the number of blue-yellow (Cb) and red-green (Cr) samples successively taken from the first row of the sampling area. However, the z value represents the number of additional Cb and Cr samples in the second row of the sampling area. The color subsampling ratio used in broadcast transmissions is usually 4:2:0. The positions from where the chrominance samples are taken vary in different standards. In the case of H.262, chrominance samples are taken vertically on alternating lines and horizontally aligned to the luminance values correspondingly. As a result, four luminance (Y) values are stored with a single value for each chrominance component (Cb and Cr) as shown in Figure 3.2.

Another compression method makes use of the fact that the human eye is less sensitive to a high number of changes of intensity. These changes occur particularly near the edges of depicted objects and are described by the term spatial frequency. For this reason modern compression methods use *transform coding* in order to transfer the image from the spatial to the frequency domain using algorithms such as the discrete cosine transform (DCT) [88], Walsh-Hadamard Transform (WHT) [89], [90], and High Correlation Transform (HCT) [91], [92], [93]. As a result, instead of intensity values of color components, coefficients representing the magnitude of frequencies in a horizontal and vertical direction (2D) are stored.

Frequency in this context describes the amount of variation between neighboring pixels. Consequently, similar color intensities among neighboring pixels correspond to a low frequency whereas greatly differing color intensities among neighboring pixels correspond to a high frequency. In particular, the input image is sliced into blocks of 8x8 pixels and frequency coefficients are stored as weights for a predetermined linear combination of basis functions. This process is exemplified in Figure 3.3 where the working principle of the discrete cosine transform as it is used in H.262 is depicted.

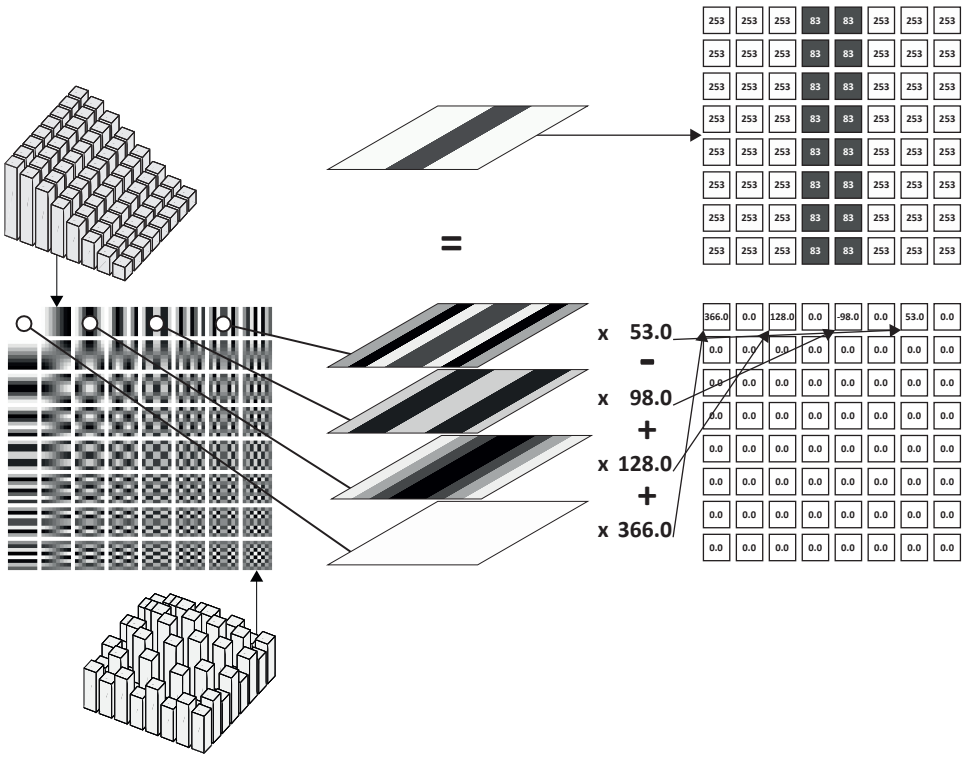


Figure 3.3: 2D Discrete Cosine Transform using 8x8 Basis Functions

However, no compression is achieved by taking these steps alone. Since the range of values for coefficients (11 bit) is greater than the range of values for color intensities (8 bit), on the contrary, the amount of required data are increased. In fact, compression is achieved by considering the following two observations. First, images from natural scenes feature a higher value for low-frequency coefficients and a lower value for high-frequency coefficients. Furthermore, coefficients whose values are close to each other, particularly

with increasing frequency, are far less distinguishable by human perception. As a consequence, the resulting coefficient values of the transform are further quantized [88]. This leads to lossy compression and allows to continuously control the quality of the resulting image. Consequently, only a limited number of different values for frequency coefficients are allowed. In addition, higher frequencies are stored with less fidelity and thus using a smaller amount of data. In order to achieve consistently high image quality by adapting the quantization factors to the corresponding scene, modern video encoding standards allow the update and transmission of quantization matrices on different levels of the resulting stream. In a subsequent step, the resulting values are serialized and arithmetically encoded for further compression [94], [95], [96], and [97].

In addition to spatial redundancy, image sequences also feature temporal redundancy. This type of redundancy is handled by another compression method. Here, only parts of an image sequence that have changed compared to one or more reference images are stored. Reference images are called intracoded (I-) frames and are self-contained, that is, their content does not depend on any other frame. I-frames achieve a moderate compression ratio of 10:1 by employing the compression methods described above. This type of frame is also required in order to start the playback of the video from arbitrary positions (random access) and to limit the propagation of errors coming from differential frames, which are sometimes referred to as intercoded frames.

The first representative of intercoded frames is the predicted (P-) frame. P-frames may contain new and differential image data with reference to previous I- and P-frames in the form of transform coefficients. In addition, P-frames may contain prediction data in the form of motion vectors that indicate the displacement of certain image segments with reference to previous I- and P-frames. Motion vectors are the result of the motion compensation process [98]. This process searches for the segment to be compressed in the vicinity of the segment in previously referenced frames during encoding. In cases motion vectors alone do not provide a satisfactory match with the original image data in process, the encoder can include additional transform coefficients to increase the visual match with the resulting compressed segment. Thus P-frames may contain transform data in addition to motion vectors in order to describe a single segment. As a result, P-frames achieve a better compression ratio of about 20:1.

Another representative of intercoded frames is the bidirectional predicted (B-) frame that also contains image data and motion vectors [99]. However, B-frames refer to temporally preceding and subsequent I- and P-frames. Depending on the compression standard, B-frames may refer to other B-frames and even establish a hierarchy among themselves. Consequently, B-frames achieve the highest compression ratio of 50:1 compared to uncompressed image data.

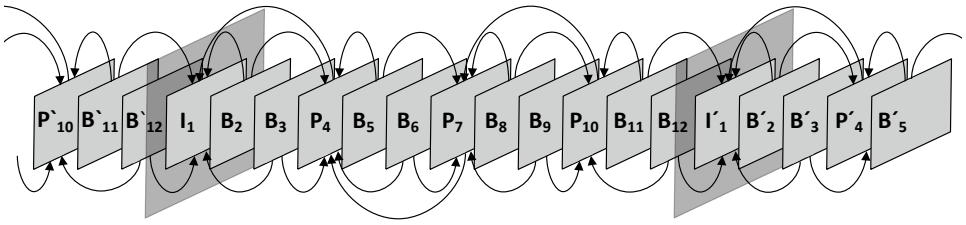


Figure 3.4: Open Group of Pictures of Length 12 in Presentation Order

A series of frames is assembled to a group of pictures (GOP). GOPs always start with an I-frame and may contain zero or more P- and B-frames. In order to exhaust a given target bit rate and to accommodate to scene changes and fade-in effects the encoder can adjust the ratio of used intercoded frame types and the total length of a GOP. A typical GOP sequence used for broadcasting has the form IBBPBBPBBPBB and is given in Figure 3.4. In this figure, the start of a GOP is indicated by a bigger transparent frame and references to other frames are marked by exiting arrows. The display order of sequence for the frames is indicated by numbers in the subscript. Frames of the preceding GOP are indicated by the grave accent (`) and frames of the subsequent GOP by the acute accent (´). The given sequence exemplifies the display/presentation order of the frames. Since B-frames can contain references to temporally successive image information, the sequence of frames is reordered for the transmission. In transmission/decoding order, referenced I- and P-frames are conveyed before the referencing B-frames appear as shown in Figure 3.5. However, since the last two B-frames in our example have forward references to the I-frame of the next GOP, these frames become enmeshed with the frames of the next GOP and, consequently, the sequence of frames is not altered. Without reordering, the decoder would have to wait for the corresponding referenced I- and P-frames to arrive before it could start to decode B-frames.

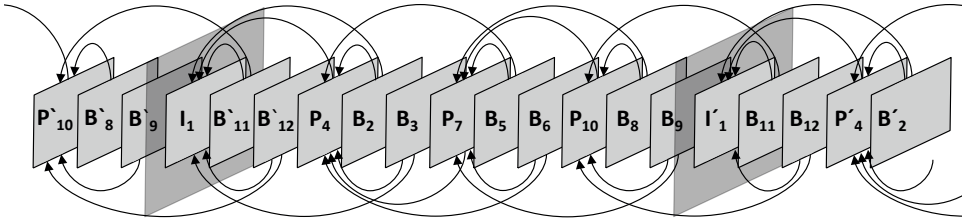


Figure 3.5: Open Group of Pictures of Length 12 in Transmission Order

Another distinction is made between open and closed GOPs. Frames in closed GOPs refer only to other frames within the same GOP. In contrast frames in open GOPs refer to other frames in adjacent GOPs. Closed GOPs are particularly useful for editing purposes and for videos supporting multiple angles. In both cases, it is desirable that the loss of a subsequent GOP does not affect the decoding of the current GOP. This behavior can be achieved by closed GOPs since they are self-contained in contrast to open GOPs. However, open GOPs require marginally less data for a specific visual quality compared to closed GOPs of equal length and structure because some frames refer to frames located in neighboring GOPs. For these reasons, most often open GOPs are used in broadcast. The example shown earlier in Figure 3.4 is an open GOP in presentation order. A closed GOP in presentation order is illustrated in Figure 3.6.

Generally, video coding standards are defined from the decoder perspective and the encoder perspective is left open for organization by the encoder manufacturers. In consequence, parts of certain standards are occasionally implemented only in a limited scope. An example for such a situation relates to closed GOPs. According to the standard [85] (7.6.6.3/7.6.6.4) B-frames may reference to temporally preceding, subsequent or preceding and subsequent frames. Nevertheless, most encoder manufacturers restrict the reference capabilities of B-frames to the last option so that B-frames are forced to exhibit two references. Consequently, an additional P-frame is required at the end of each closed GOP in

order to support arbitrary GOP lengths in these cases. As a result, the majority of observable closed GOPs have the structure shown in Figure 3.6.

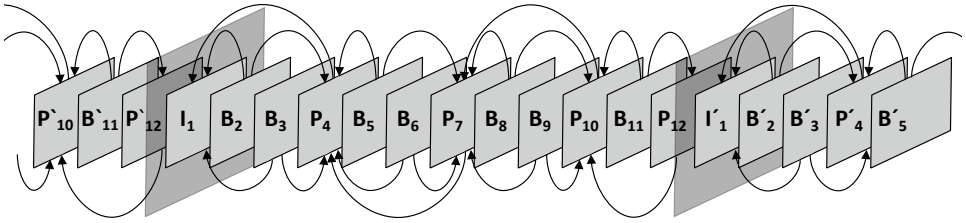


Figure 3.6: Closed Group of Pictures of Length 12 in Presentation Order

3.1.1.2 Transport

Next, we illustrate the structure of broadcast data up to the point where it is ready for transport over IP networks as shown in Figure 3.7. For this purpose, we consider the coding according to the H.262 standard [85] due to its sustained wide use and simplicity. More recent standards offer more possibilities and correspondingly are able to define more complex structures. As we could see in our discussion of compression methods, the fundamental layer of video consists of quantized coefficients resulting from the frequency transform. At this level, run-length coding is used as arithmetic coding for lossless compression. According to our considered coding, usually areas of 8x8 pixels called blocks are sampled for each color component from the original image. Macroblocks contain 2x2 luminance blocks as well as a number of chrominance blocks depending on the subsampling ratio. For 4:2:0, one block is added for each chrominance component.

In addition, descriptive information about the contained block content type such as coefficients, residual coefficients, motion vector data, and optional individual quantization tables are included to the macroblock. Macroblocks in turn form slices and slices form complete frames (pictures) or in case interlacing is used they form fields (half pictures). Frames of different types constitute GOPs and one or more GOPs form a sequence. At the level of sequences, the byte stream is referred to as video elementary stream (ES). Other types of ESs are audio ES and data ES used, for instance, for Teletext and conditional access. Each single ES forms a packetized elementary stream (PES) by adding a PES header. The PES header specifies the content type of the contained ES and includes other additional information. Although named with the prefix “packetized”, the PES on its own is not bounded in length. Only for transmission, the PES is split into packets of 184 bytes and forms the transport stream (TS) by adding a header of 4 bytes [100].

The TS either contains all PESs for a single program and is called single program transport stream (SPTS) or the PESs for several programs and is called multi program transport stream (MPTS). Program service information (PSI) [100], [101] is added to the TS in order to specify the structure of the TS and to convey auxiliary data and meta-information. PSI again features a specific section structure. A single section may span over multiple TS packets and the PSI may span over multiple sections. In addition to PSIs with a given structure, the TS can feature sections with user defined format, so-called private sections. Components responsible for implementing pay-TV services use private sections to transmit entitlement information. An additional optional TS header field is regularly included and contains a time reference called program clock reference (PCR). The PCR is a 27 MHz timestamp and used to enable buffer management and streaming. Particulary, by using

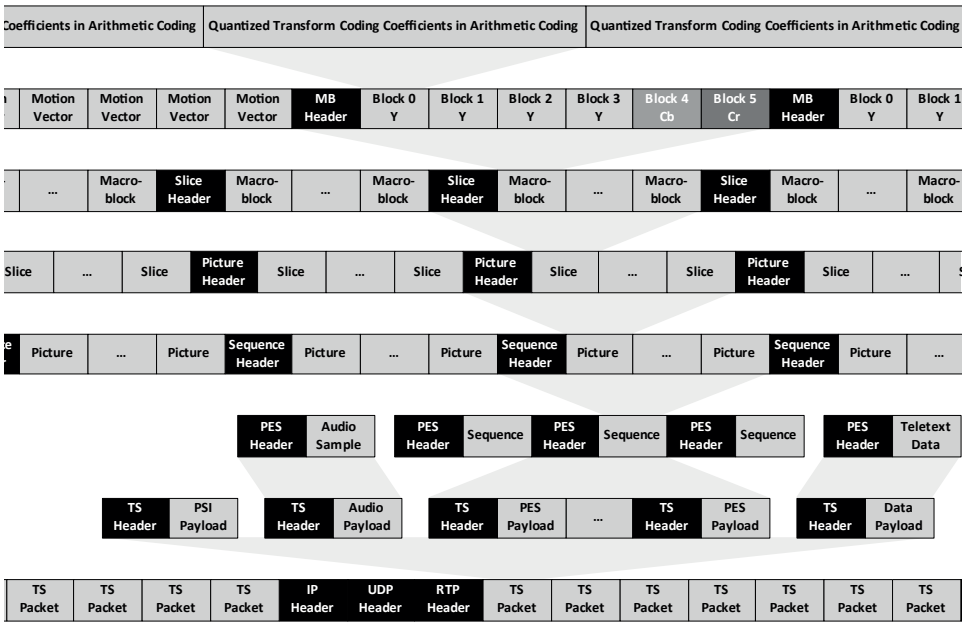


Figure 3.7: Structure of Broadcast Data for Transport

PCRs along with a phase locked loop (PLL) at the receiver, a continuous adaptation of the transmission rate for the synchronous reception and decoding of the bitstream is achieved.

In order to achieve efficient transmission and to avoid IP packet fragmentation, usually 7 TS packets are grouped to form an IP packet (recommended in [102]). The IP packets are transmitted using the User Datagram Protocol (UDP) [103], a connectionless and unreliable transport protocol that specifies only the source and destination services and the length of the packet. In addition, the UDP packets are encapsulated in Real-Time Transport Protocol (RTP) [104] packets. Packet reordering and detection of missing packets is carried out by using sequence numbers contained in the RTP packet headers. The header also features a timestamp field for synchronizing different media streams. In addition, a unique synchronization source identifier in the header provides information regarding the source of a stream when a service sends multiple streams. Furthermore, extensions and profiles for different use cases are specified for RTP. Usually, IPTV services are organized as multicast groups. Each channel is streamed as an SPTS using RTP to a particular multicast group.

3.1.2 Components of the IPTV Service Architecture

The general architecture of an IPTV service consists of a headend system (HES), several networks and the home network containing the terminal equipment as shown in Figure 3.8. The HES is used to gather, process, and emit broadcast content. Regional HESs include tailored content for target audiences from specific geographic regions whereas so-called Super HESs provide broadcast content at the national level for the general audience. The network operator uses network segments such as the core, distribution, and access network to transport data and provide services such as Internet access, Voice over IP, and IPTV.

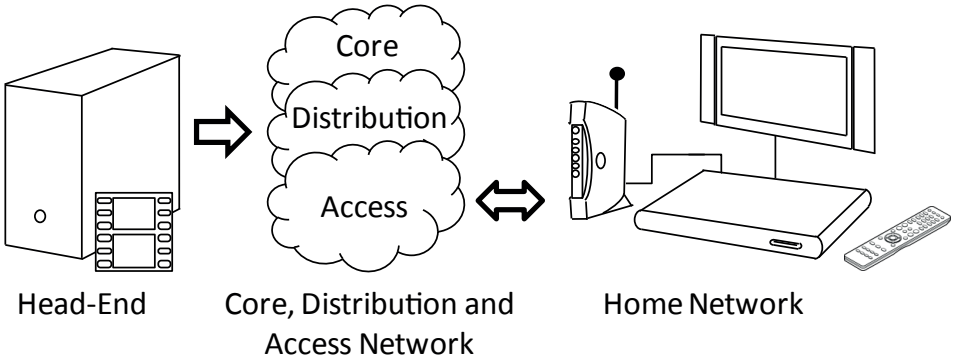


Figure 3.8: General IPTV Service Architecture

Usually, these network segments are also supervised by the network operator. The home network comprises components at the subscriber premises. Usually, besides a TV set, the home network consists of a home network gateway, namely a wireless radio-enabled network router with an internal DSL-modem, and a home network end device often referred to as set-top box (STB).

In the following, we further investigate the structure of HESs. In particular, we look into the working principle of components responsible for implementing pay-TV services. These components constitute the conditional access system (CAS). In the next step, we consider the architecture of the STB and analyze how the entitlement process is carried out.

3.1.2.1 Headend System

For a better overview, we illustrate the simplified structure of the relevant functional components of an HES in Figure 3.9. In this overview, components that are related to the CAS and implement pay-TV are indicated by dotted frames.

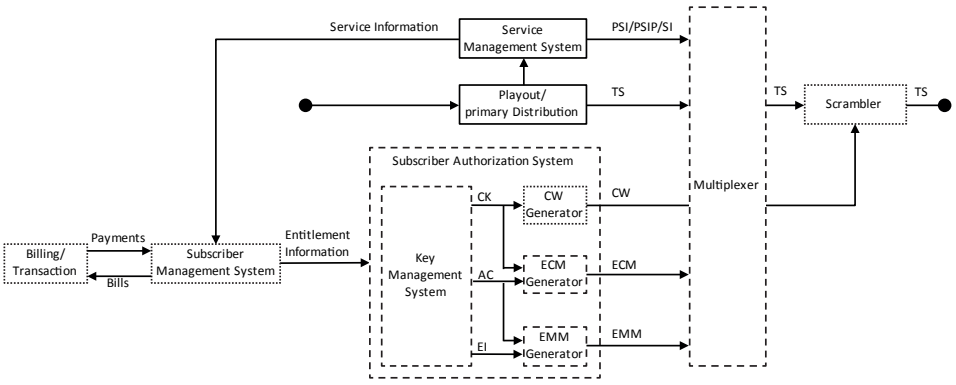


Figure 3.9: Block Diagram of Headend System

As suggested previously, the main tasks of an HES are the acquisition, processing, and dissemination of broadcast data. The acquisition is performed using special connections to preceding HESs or using established means for transmission such as over terrestrial, cable, and satellite links. Subsequently, the incoming streams are edited according to the objec-

tives of the operator. Incoming streams can be transcoded with more effective compression algorithms in order to preserve bandwidth. Later, advertisements and local programs can be inserted into the transmission. Furthermore, to fully utilize the bandwidth of a single carrier frequency of a wireless link, different individual channels can be multiplexed into a single multi-program stream. For this purpose, a multiplexer is used. In the following we examine the processing step related to the implementation of pay-TV.

After a contract with the corresponding service provider is concluded, the pay-TV subscription is initiated. In this context, the subscriber management system (SMS) is used to store and manage all subscriber-related information. In addition to customer data, such as address, banking information, and subscription details, the SMS also stores technical data, for instance, the serial numbers of delivered STBs. Furthermore, entitlement information indicating the channels a subscriber is allowed to watch is stored in the SMS. An important function of the SMS is to issue and update the user identity key, a unique key shared only between the HES and the subscriber.

More specifically, this key is not disclosed to the subscriber but resides in a secure storage in the STB or is stored on a smart card. In order to share this key with the subscriber, it is either sent via mail or delivered included in the bundled STB. In corresponding literature many names for the user identity key such as master personal key (MPK), rights encryption key (REK) or user root key (URK) are mentioned. However, in the following, we continue to refer to this key as user identity key (UIK). Some of the entitlement information present at the SMS is forwarded to the subscriber authorization system (SAS) to include the new subscriber to the group of viewers of the entitled channels. The SAS converts the entitlement information for accessing a specific channel or channel package into a set of cryptographic keys. These keys are stored along with the UIK in the key management system (KMS) and enable the subscribers to decrypt broadcast data in accordance with their entitlement. As it is the most critical component of a CAS, the internal details of the key management are not standardized and kept secret.

In order to entitle the new user, a new service key (SK) is issued and encrypted with the UIKs of all newly added subscribers. The resulting key is embedded as an entitlement management message (EMM) into the broadcast data. The control word (CW) is used as a seed for a pseudorandom number generator (PRNG). The resulting pseudorandom number is used as the symmetric encryption key for the scrambler. Additionally, the CW is encrypted using the SK to form the entitlement control message (ECM) and fed into the broadcast data. Usually, the CW is updated every 2 – 10 s, whereas the SK is updated at particular times, for instance, when new subscribers are activated in batch. In contrast, the UIK is usually not updated or only in exceptional cases. Newer CASs use an additional key between the SK and the UIK in the key hierarchy outlined above in order to support more flexible subscriber management.

The scrambler encrypts the broadcast data of each channel in order to ensure that the service is only accessible to authorized subscribers. Depending on the selected approach, media data can be scrambled at PES level before or at TS level after it has been multiplexed into a TS. Usually, encryption is performed at the TS level. For encryption, the scrambler utilizes cryptographic encryption algorithms such as the common scrambling algorithm (CSA) or AES [105]. The billing system forwards payment information to the SMS and receives billing information from the SMS concerning individual subscribers.

3.1.2.2 Set-Top Box

Figure 3.10 details relevant functional components of the set-top box. Components related to conditional access are indicated by dotted frames. The depacketizer connected to

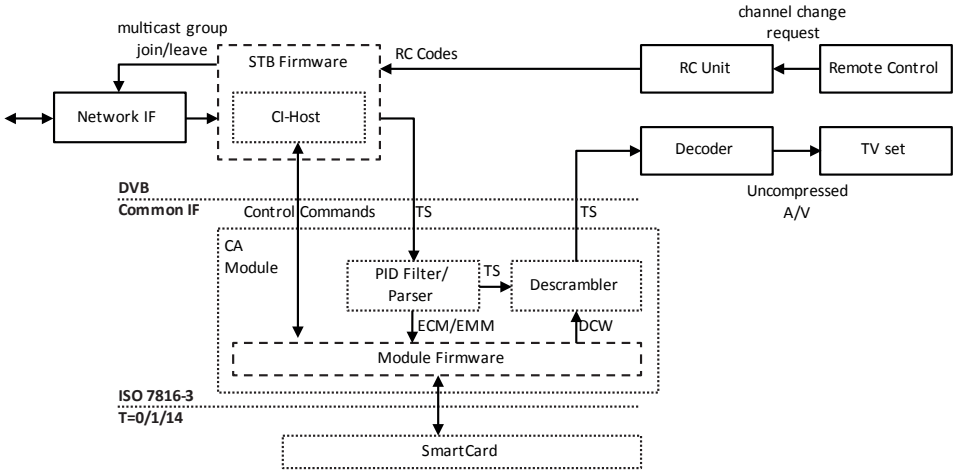


Figure 3.10: Block Diagram of Set-Top Box

the network interface forwards the TS packets and directs them to the common interface (CI) host. The CI-Host is a software module that implements a protocol for supporting removable security modules, so-called conditional access modules (CAMs). The CAM implements the counterpart of the SAS. For supporting multiple different CAS implementations, these modules are designed to be detachable. A demultiplexer in the CAM separates media data from the data relevant for conditional access. Particularly, ECMs and EMMs are sent to decryption units either implemented on a smart card or on the CAM itself. Thus, ECMs and EMMs are decrypted accordingly by using the UIK that is stored either on the tamper-resistant memory of the smart card or on a secure storage on the STB. Additionally, new SKs are stored in the secure memory of the STB. After the CW has been obtained, it is processed by a corresponding pseudorandom number generator in order to compute the content key. Finally, the content key is used to decrypt the media data that is passed on to the corresponding STB components for decoding and display.

3.2 Multicast Encryption

For the implementation of CSTC, we employ the concept of multicast encryption, a scheme that provides means for access control by key update and delivery in a multicast environment. In the course of this section, we first present the concept of multicast before we discuss multicast encryption. Generally, multicast is a method for the communication of peers in a group. In contrast, unicast is a communication method enabling two peers to directly exchange messages with each other. Moreover, broadcast is a communication method allowing one peer to communicate to all other existing peers in a network. In the following, we will detail how the multicast communication method is implemented in computer networks using the Internet protocol (IP) [106].

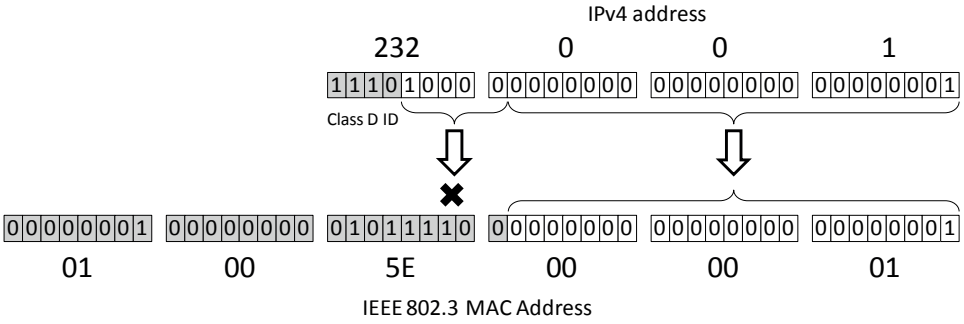


Figure 3.11: Mapping of IP Multicast Addresses to Ethernet Physical Addresses

3.2.1 IP Multicast

When the Internet Protocol is employed as a network protocol in a communication network, hosts identify each other by using an IP address. The IP address is a 32-bit number and usually represented in the form of four decimal numbers. These numbers are separated by dots and each of them ranges from 0 to 255, for instance, 127.0.0.1. All members of a single multicast group are addressed by a shared IP address. By convention, this multicast group address has to be in the designated range of 224.0.0.0 to 239.255.255.255.

In wired computer networks, data packets of the Internet Protocol are typically transmitted using an underlying link layer protocol called Ethernet [107]. In direct communication (unicast), the device driver of the sending host encapsulates an IP packet within an Ethernet frame. The Ethernet frame contains the source Ethernet address and an appropriate destination Ethernet address. The Ethernet address is a 48-bit number uniquely assigned to the network interface controller of a host. It is used for communication among hosts on a shared physical network segment. In Ethernet networks this segment is usually limited by adjacent network components such as switches and routers, which do not require the physical network segment to be shared.

Generally, hosts accept only Ethernet frames containing the matching destination address. All other frames received by the host are ignored. In order to determine the Ethernet address of the destination host, the address resolution protocol (ARP) [108] is used. To support multicast however, a different approach for constructing the Ethernet destination addresses is necessary. In multicast, packets are directed to multiple hosts at once and it is required to distinguish among multiple multicast groups. For this purpose, Ethernet frames containing multicast traffic use a destination address derived from the multicast [109] address of the contained IP packet. Technically, the lower 23 bits of the IP multicast destination address are mapped to the corresponding portion of the Ethernet destination address. The upper 24 bit of the Ethernet destination address is statically set to 01:00:5E. The residual bit is zeroed. As a result of this mapping, 5 bits of the complete IP multicast destination address range are dropped since the mapping is not bijective (Figure 3.11 according to [109]).

When a host wants to receive traffic from a specific multicast group, the network device driver is configured to receive frames directed to a given Ethernet multicast address. Since the detailed IP-to-Ethernet address mapping does not provide a one-to-one correspondence, additional filtering by the device driver is required. This is accomplished by checking the

destination IP address in addition to the destination Ethernet address before passing the packet to the IP layer. This approach ensures that the application requesting multicast traffic does not receive unneeded datagrams. In contrast, hosts who are not members of a specific multicast group do not monitor incoming traffic for Ethernet frames and IP packets directed to multicast addresses. Consequently, these frames are filtered out by lower layer hardware-based mechanisms of the network interface.

For the registration to or the deregistration from a certain multicast group, the host has to send particular messages conforming to IGMP (Internet Group Management Protocol) [110]. As a result, adjacent routers are For forwarding and delivering multicast traffic beyond network segments, multicast-capable routers are used. These routers process IGMP messages and employ distribution trees in order to deliver multicast data to interested hosts. Many multicast algorithms have been proposed to establish and maintain these distribution trees, for instance, source-based and shared-tree algorithms.

Multicast as a communication method is particularly useful for the transmission of IPTV traffic. By using multicast, a single copy of a message is sufficient in order to send the message to all group members. This is accomplished by underlying network components that automatically deliver the message to all interested members of a multicast group. In this context, television channels can be considered as groups and group members can be seen as users watching a particular channel. However, IP multicast does not provide any security mechanisms. Any peer is able to join a multicast group and subsequently receive data addressed to the group. Even without joining a group, data exchanged in a multicast group can be intercepted by peers who are not members of this group. Since IP multicast is a method for group communication it does not provide any form of data confidentiality. In order to achieve data confidentiality, multicast encryption schemes are used. In the following, we introduce different properties of such schemes. Subsequently, two trivial constructions are discussed to illustrate some of the properties. Finally, a scheme called logical key hierarchy, which we use for the implementation of CSTC, is introduced.

3.2.2 Classification

A common problem related to access control for pay-TV is to exclude certain users from the group of entitled users. The entitlement for users has to be revoked either because they voluntarily canceled their subscription or because pirates managed to extract and copy access information of legitimate users. In general, access control is achieved by encrypting all group communication with a single key, the group key. In this way, the problem of managing the access to the whole group communication is reduced to the problem of managing the access to the group key. As new members join and existing members leave, the group key is updated in order to grant access for the current set of legitimate members and to deny access to former members. For this purpose, each member owns an individual user key, which is not disclosed to the user and is supplied using out-of-band communication means such as by mail. Consequently, the user key is stored on a secure storage, for instance, a smart card.

In order to achieve the exclusion of formerly entitled subscribers, one or more of the following different approaches are used. The easiest approach is to force the former member to return the user key stored on a smart card. This can be accomplished by using different incentives. For instance, the cancellation of the subscription could only take effect when the smart card is returned to the pay-TV service provider. Alternatively, the subscriber could deposit an amount when the contract is concluded and would only be able to get it

back when the smart card is returned. Further schemes use the terminal equipment in order to enforce the deactivation of the former member. For this purpose, the user key is provided with a preconfigured expiration date which particularly coincidences with the expiration of the long-term pay-TV contract. Moreover, a deactivation command encrypted with the user key of the former member can be sent to the terminal equipment. This command permanently deletes the user key and prevents any further access.

In contrast, group key management schemes provide algorithmic solutions to the access control problem. As the name suggests, the idea is to alter or renew the group key in such a way that existing members and users who joined the group of entitled users are able to compute the new group key. Most often this computation is enabled by additional key update information. In contrast, former members, users who just left the group of entitled users, and uninvolved parties should be unable to gain any information regarding the new group key from the key update information. Since the group key is mostly managed by renewing it, group key management schemes are also often referred to as (group) rekeying schemes. Rekeying schemes can be classified according to various properties. In the following, we will introduce the most important attributes.

When centralized rekeying schemes are used, a central entity called group controller (GC) is in charge of managing the group. Join and leave request are directed to the GC and changes in the group composition result in the update of the shared group key. The update as well as the corresponding distribution of the key update information is performed by the GC. In decentralized schemes, the task of the GC is divided among several subgroup controllers. However, this approach requires additional entities for group management and additional communication among subgroup controllers. When distributed schemes are employed, no GC exists. Instead, either the members promote one of the members to a GC or all members together agree on, or even contribute, to a new group key. This approach is suitable for settings where many-to-many communication is required and fault tolerance regarding network and node errors is important. However, these schemes are not scalable since they feature high costs for computation and communication.

Stateless rekeying algorithms do not require previous versions of the group key or the key update information in order to compute the current version of the group key. This property is particularly useful in environments where no return channel to the GC is available. For this reason, these schemes are used in traditional pay-TV systems that assume a one-way communication between the pay-TV service provider and the receiving users. With regard to the corresponding communication method, these schemes are also often referred to as broadcast encryption schemes. In case only leaving members are considered in this context, corresponding schemes are referred to as revocation schemes.

As a consequence, service providers are not readily able to identify illegitimate users when broadcast encryption schemes are used. In this context, legitimate users who have shared their user keys with illegitimate users are called traitors. Thus, methods for locating illegitimate users are called traitor tracing schemes and represent an own field of research. Usually, stateless rekeying schemes suffer from several shortcomings such as the support of limited group dynamics.

In contrast, stateful rekeying algorithms require all previous versions of the group key in order to compute the current version. Here, the member has to request synchronization information from the GC to compute the current group key in case a member leaves the group or the previous key update information has been missed for any other reason. Accordingly, it is assumed that a return channel is available. Correspondingly, these algorithms are referred to as multicast encryption schemes.

A mixture of stateless and stateful rekeying algorithms is the group of self-healing schemes. Here, a member is able to reconstruct the current group key after receiving a certain number of key update information and without contacting the GC. However, these schemes have high costs for computation and communication, don't support the immediate revocation of members, and offer limited user dynamics. In contrast, stateful rekeying algorithms are suitable for large and dynamic groups. As a return channel is also available in the context of IPTV, stateful rekeying algorithms are appropriate for our considered solution.

Static rekeying schemes support a fixed number of members that has to be determined in the setup stage of the algorithm. In contrast, dynamic schemes support an arbitrary number of members. Dynamic schemes are more flexible and seem to be more desirable in practical implementations. As we will see however, the implementation of SIC makes high demands on performance, particularly on computation times. These demands are met better by employing static schemes as they don't require time for the allocation and freeing of dynamic data structures to adjust to group dynamics.

When periodic batch rekeying [111] is used, the GC collects join and leave requests of users for a specific period of time, the rekeying interval. Then, the GC processes them in batch and multicasts the corresponding key update information. In contrast, individual rekeying refers to the immediate processing of each single request. Periodic batch rekeying is particularly effective for tree-based rekeying schemes. In a d-ary tree data structure the group key is represented by the root, the user keys are represented by the leaves, and intermediary keys are called help-keys. During rekeying of tree-based schemes, all keys on the path from the leaf containing the user key to the root containing the group key have to be renewed, encrypted and transmitted. When periodic batch rekeying is used, the number of required key renewals and encryptions is substantially decreased compared to individual rekeying. Consequently, the key update information is also smaller. Since help-keys on the way from the leaves (user keys) to the root (group key) are shared among several leaves, they need only be traversed, renewed, and encrypted once during the rekeying interval.

Backward secrecy is a property of rekeying schemes, which ensures that users who newly joined a group are not able to decrypt previous group communication which took place before they joined the group. Similarly, forward secrecy implies that a user is not able to decrypt later group communication once she or he has left the group. Nongroup confidentiality and key indistinguishability are properties, which ensure that users who have never been a member of a group neither are able to decrypt any data sent to the group nor are able to compute or learn any information regarding the group key. Collusion freedom guarantees that users who left a group are not able to decrypt any subsequent multicast communication although they jointly use keys which they have obtained during their membership in that group.

3.2.3 Schemes and Examples

In the following, we will review two simple schemes, namely the key star and the zero message scheme. Then, we discuss the logical key hierarchy scheme we use for the later implementation of a SIC solution.

3.2.3.1 Key Star Scheme

The key star scheme is often called naive scheme in literature and implements a simple idea. The GC stores the group key and the keys of every user. The following the steps

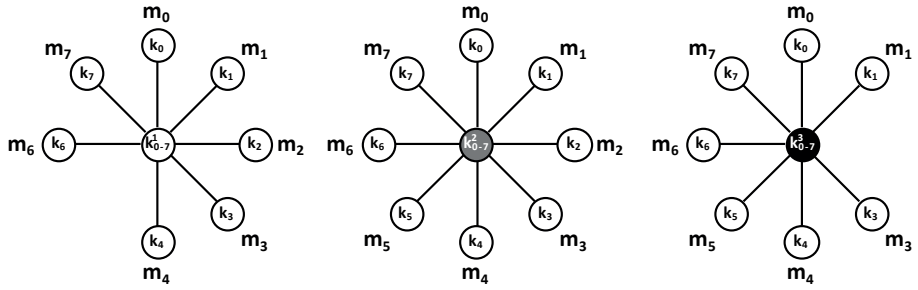


Figure 3.12: Key Star Scheme Example

for including and excluding a user can be followed with the help of Figure 3.12. When a new user requests to be added to the group, the GC creates a new node in the key graph containing the user key of the requesting user and connects it to the group key. In our example, member m_5 requests to join the group and the corresponding key k_5 is added to the group key. Subsequently, the server renews the group key k^1_{0-7} in state 1 and generates the new group key k^2_{0-7} in state 2. The group key state is indicated in superscript and incremented in each step. The set of member keys the group key is valid for is shown in subscript. In our example, the group key is valid for all 8 members. In the next step, the GC encrypts the group key in the current state with the group key of the previous state and with the user key of member m_5 and sends both key update information

$$E_{k^1_{0-7}}(k^2_{0-7}), E_{k_5}(k^2_{0-7})$$

in concatenated form to all group members via multicast.

Here, the notation $E_{k_a}(k_b)$ indicates the encryption of the key k_b with the key k_a. All former members use the preceding version of the group key to recover the new version whereas member m_5 uses his own user key to decrypt the new group key.

When a user requests to leave the group, as shown in the example in Figure 3.12, the GC deletes the node of the member in the key graph containing the user key of the requesting user. In our example, member m_2 requests to leave the group and the corresponding key k_2 is deleted. In order to exclude member m_2 from the group, the GC renews the group key again and generates the new group key k^3_{0-7}. Subsequently, the GC encrypts the new group key with the user keys of each remaining member and sends the following key update information to the group via multicast.

$$E_{k_0}(k^3_{0-7}), E_{k_1}(k^3_{0-7}), E_{k_3}(k^3_{0-7}), E_{k_4}(k^3_{0-7}), E_{k_5}(k^3_{0-7}), E_{k_6}(k^3_{0-7}), E_{k_7}(k^3_{0-7})$$

Finally, each remaining member uses his own user key in order to decrypt the new group key. Apparently, this rekeying scheme is not scalable since its complexity regarding computation and communication increases linearly with the group size. Still, a minimal number of two keys need to be saved by each user when this scheme is used.

3.2.3.2 Zero Message Scheme

A simple scheme featuring performance properties at the other extreme is the zero message scheme. Here, the GC stores one key for each possible composition of the group. An example of a possible memory layout for a group of eight members is given in Table 3.1. The group composition is represented by a binary sequence where 1 indicates

that the member at the corresponding position has joined the group and 0 indicates that the member at the corresponding position has left the group. If the maximum number of group members is given by G, the GC has to store $\mathcal{P}(G) = 2^G$ keys. Since users possess only keys for all group compositions they are part of, the required storage for each user is 2^{G-1}. When a user requests to join the group, the GC needs to send only the corresponding number of the key representing the group composition. In case the user requests to leave the group, the GC multicasts the number of the key representing the current group composition excluding the requesting user. The communication overhead of this scheme is a minimal constant and amounts to $\log_2(G)$ bits. Unfortunately, the requirement to store an exponential amount of keys renders this scheme unusable. In addition, the zero message scheme is prone to collusion attacks.

3.2.3.3 Logical Key Hierarchy

Logical Key Hierarchy (LKH) is a tree-based rekeying scheme independently proposed by [112] and [113]. The basic idea behind LKH is to divide the group into hierarchical subgroups and to provide the members of each subgroup with a *help-key*. Consider the example illustrated in Figure 3.13 (left tree) for an eight-member group. In this model, members m_0 and m_1, for instance, build a subgroup with the help-key k_{0-1}. All members compose the largest subgroup with the help-key k_{0-7}. This key represents the group key used to encrypt payload data. Consequently, a member holds several keys, namely, the user identity key k_d known only to this member and to the GC, the group key k_g known to all group members, and some help-keys k_{x-y} corresponding to the subgroups the member belongs to. Member m_6, for example, holds $k_d = k_6$, $k_g = k_{0-7}$, and two help-keys, namely k_{6-7} and k_{4-7}.

When, for instance, member m_2 requests to leave, the keys k_{0-3}^{new} and k_{0-7}^{new} are generated, encrypted, and sent to the remaining members needing them. The right side of Figure 3.13 shows the key tree after this processing. Consequently, the GC has to generate the following rekeying submessages in order to exclude member m_2 from the group:

$$E_{k_3}(k_{0-3}^{new}), E_{k_{0-1}}(k_{0-3}^{new}), E_{k_{0-3}^{new}}(k_{0-7}^{new}), E_{k_{4-7}}(k_{0-7}^{new})$$

A similar analysis can be performed for the case of joining member. LKH enables efficient rekeying due to the logarithmic relation of rekeying cost to the group size. LKH is based on the management of a key tree on the GC. As an effect of multiple disjoins, the key tree may get out of balance. Several solutions have been proposed to rebalance

Group Composition	Key
00000000	k_1
00000001	k_2
00000010	k_3
00000011	k_4
00000100	k_5
00000101	k_6
⋮	⋮
11111111	k_{256}

Table 3.1: Zero Message Scheme Example

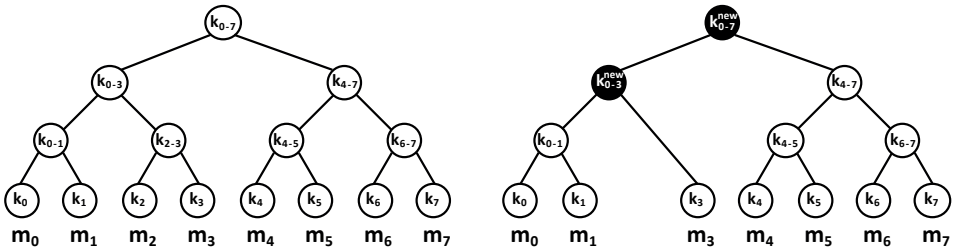


Figure 3.13: LKH Example

the tree in this case. The first contribution is made by Moyer [114] who introduced two methods to rebalance the key tree, namely immediate and periodic rebalancing. A cost analysis is given only after one disjoin request for the first method. The periodic rebalancing is not analyzed. Moharrum [115] presented a method for rebalancing based on subtrees. A comparison with the solution of Moyer is drawn, but not with the original LKH. Rodeh [116] applied AVL-tree (Adelson-Velskii and Landis tree) rebalancing methods to key trees. However, no backward access control is guaranteed in this solution. Goshi [117] proposed three algorithms for tree rebalancing. Simulation results provided assume equally likely join and disjoin behavior. However, this condition alone ensures tree balancing, since a new member can be joined at the leaf of the most recently removed member. The same applies to the simulation results of Lu [118]. We use LKH for the implementation of SIC because it offers a good performance in particular with periodic batch rekeying. In this case, communication and processing overhead is substantially reduced and the scalability of the resulting solution is improved. In addition, LKH features required security properties, such as backward and forward security, collusion freedom and nongroup confidentiality.

CHAPTER 4

CHANNEL SWITCHING-TRIGGERED CHARGING

In this chapter, we introduce a novel charging model we call channel switching-triggered charging (CSTC). This model gives a solution to our research objective how the functionality of short interval charging can be implemented technically. An overview of the structure of this chapter is given in Figure 4.1.

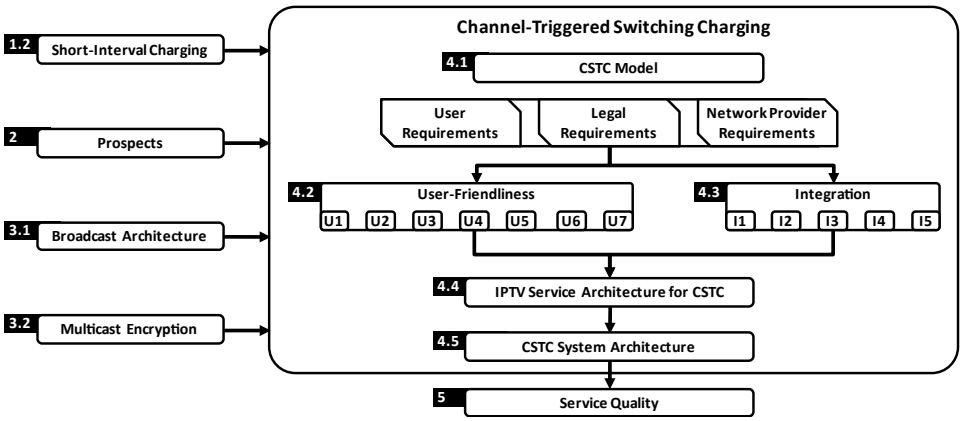


Figure 4.1: Overview Chapter 4

Based on the insights gained from previous chapters, we first describe the working principle of CSTC in Section 4.1 and compare its properties to related charging propos-

als. Afterward, we analyze requirements of relevant stakeholders (users, network operators) as well as legal requirements for CSTC. By considering requirements regarding user-friendliness (Section 4.2) and integration (Section 4.3), we develop specifications **U1** - **U7** and **I1** - **I5** correspondingly.

In Section 4.4 we then examine which additional protocols and components are neccessary in order to incorporate CSTC to a common IPTV service architecture. We describe a prototype IPTV system architecture implementing the CSTC model in Section 4.5. Here, we design both the network operator infrastructure in the form of a headend system and the set-top box residing at the consumer premises. Then, we validate in Section 4.6 how far required specifications have been covered by the proposed IPTV service and system architectures. Finally, we give a summary and conclude the scientific questions addressed in this chapter in Section 4.7.

4.1 CSTC Model

For enabling seamless short-interval charging without altering established user habits, we introduce the method of channel switch-triggered charging (CSTC) presented in [119]. This concept enables us to implement short-interval charging while meeting several requirements regarding user-friendliness. For the technical realization of CSTC, we make use of multicast encryption introduced in Section 3.2. This concept provides us with the fundamental functionality to grant and deny access to media data for viewers in a group environment. In addition, multicast encryption is able to resolve some of the privacy concerns expressed by users.

An overview of the related user actions performed according to this scheme is given by the diagram in Figure 4.3. For comparison, additionally actions according to free-TV are given in Figure 4.2. As we detailed previously in conventional pay-TV usage schemes the user is entitled to watch a certain channel, program, or movie. According to these schemes, the processing of the entitlement request is especially time-consuming

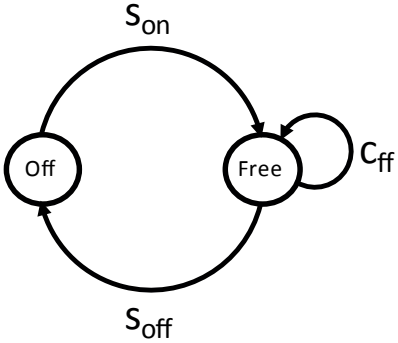


Figure 4.2: User States in Free-TV

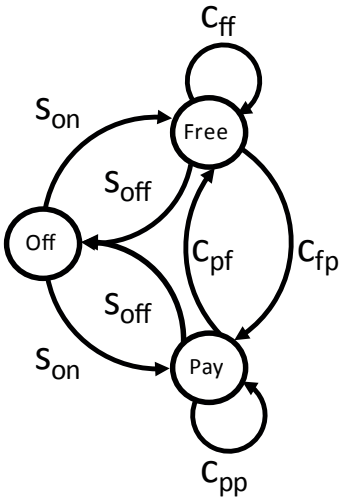


Figure 4.3: User States in CSTC

as it is associated with concluding a contract or at least with placing an order triggering further management actions including registration and authentication. The comparison to these schemes is difficult as many steps with different and partly extensive durations are involved. For this reason, we compare CSTC to free-TV which features a higher similarity.

To support short-interval charging, the user model must be modified, so that users can start and stop viewing paid content with high flexibility and without having to repeat any registration actions. For this purpose, we propose a three-state user model as depicted in Figure 4.3.

The state Off is the same as in the free-TV user model. In contrast, the state Free is now split into two states:

1. Free, in which the user has already completed all necessary registration and authentication actions but has decided not to watch paid content and
2. Paid, in which the user has the obtained necessary entitlement to access the media stream.

The transitions between the states Free and Off are similar to the free-TV user model of Figure 4.2. In contrast, the transitions between the states Free and Pay can be activated just by pressing any button on the remote control that performs channel change, namely, by zapping.

4.1.1 Novelty

Before we move on to the merits of CSTC, we first examine the novelty of this concept. For this purpose, we first define comparison aspects according to which we perform a literature review in a subsequent step. Finally, we analyze how CSTC contributes to our desired solution by meeting the targeted requirements.

4.1.1.1 Comparison Aspects

For defining comparison aspects in order to perform a literature review, we further refine and concretize the concept of CSTC. In addition, we emphasize properties that we regard as distinct for CSTC. Clearly, we envisage CSTC as a charging concept for IPTV. As we will elaborate in the next section, we, consequently, assume that CSTC will be employed in a single source IP multicast environment. This environment is operated on a fixed line network and is centrally managed by a single operator such as an Internet service provider (ISP) or a multiple services operator (MSO).

For our comparison with other concepts in literature, we contrast them with the benefits of short-interval charging. In the next section we are going to show that these benefits are particularly realized by CSTC. Therefore, we investigate whether the respective concept supports the access to different types of content immediately and interactively. In particular, we are interested in the minimum unit of serviceable content a user can be charged for. Moreover, we check whether the compared method supports interactive entitlement in the sense that the service request and entitlement response messages are signaled in-band. In this context in-band means that users do not need to perform additional actions in order to request or activate a service such as the following.

- Use of any additional communication means such as postcard, call center, telephone or the Internet

- Pushing of any additional buttons on the remote control
- Selection of desired content in printed or electronic menus, the electronic program guide (EPG), reservation systems, landing pages or in the Internet
- Communication of identity, authentication, and payment data

We also examine whether the compared concept provides usage-based cost attribution. In particular, we are interested in how the usage is measured and at which location the duration of usage is calculated and monitored. In a final inspection, we study whether the compared concept considers different payment methods such as prepaid and postpaid charging. A summary of considered comparison aspects is given in Table 4.1.

Broadcast Technology		A
Adaptability of Services	Minimum Service Unit	B
Interactivity of Entitlement	Service Request Mode	C.1
	Entitlement Response Mode	C.2
Usage-Based Cost Attribution	Usage Measuring Method	D.1
	Usage Detection Location	D.2
Payment Method		E

Table 4.1: Comparison Aspects for Related Work

4.1.1.2 Comparison to Related Charging Proposals

In the following, we compare CTSC to other related work from several academic research work and patents according to the aspects we discussed previously. For a better overview, the results of this comparison are summarized in Table 4.2. Please note that aspects not considered in respective work are indicated by the abbreviation NC.

In [120] the authors present a CAS called Eurocrypt, which operates over analog satellite television and supports pay-per-view. Users can purchase services grouped into a set of channels called bouquets. For requesting a service, an out-of-band method using an analog modem is employed. In contrast, the entitlement response is delivered in-band. The usage data are collected centrally by a subscriber authorization system in the central office of the service provider. However, usage measuring methods, a method for the calculation of the usage duration as well as payment methods are not considered. Also, the technical realization of the system is not described in detail.

In another work [121] an Internet-based pay-as-you-watch system (IBPAYWS) is introduced. It allows on-demand streaming for stationary and mobile broadband-enabled devices such as cell phones and PDAs. The system offers pay-per-view charging for prerecorded videos and live streams where users dont pay for the downloaded data volume of the media but for the consumption time. The service request and the entitlement are performed using a public web portal. The extent of usage is calculated by a central online system that also transmits the video content. Payment is triggered by the central online system, which contacts a micropayment broker. The broker, in turn, retrieves micropayment coins from an electronic wallet software. This software works together with the player software and a smart card on the user device. Consequently, payment arrangements are not considered and outsourced to the micropayment broker.

	CSTC	Eurocrypt [120]	IBPAYWS [121]	FPPC [122]
A	**IPTV**	D2MAC	Internet	unidir. DVB
B	**Program Segments**	Bouquets	Streams/Videos	Channels
C.1	**In-Band**	Out-of-Band	Web Portal	Out-of-Band
C.2	**In-Band**	In-Band	Web Portal	In-Band
D.1	**Time-Based**	NC	Volume-Based	Request-Based
D.2	**Sender-Based**	NC	Sender-Based	NC
E	**Pre-, Postpaid**	NC	Micropayment Broker	NC

	FPPG [123]	IPPV [124]	PPV-EPG [125]	DVB-SI [126]
A	unidir. DVB	CATV	IPTV	unidir. DVB
B	Channels	Programs	Programs	Program Segments
C.1	Out-of-Band	Out-of-Band	In-Band	Out-of-Band
C.2	In-Band	In-Band	In-Band	In-Band
D.1	NC	Program-Based	Program-Based	Time-Based
D.2	NC	Sender-Based	Receiver-Based	Receiver-Based
E	NC	NC	NC	Pre-, Postpaid

Table 4.2: Comparison of Properties of CTSC with Related Work

A CAS called Flexible-Pay-Per-Channel (FPPC) is described in the work of [122]. This system works in a unidirectional broadcasting environment such as a terrestrial, cable, and satellite network. According to the authors, the system has been drafted especially in the framework of the Digital Video Broadcasting (DVB) Standards. The specified CAS enables users to subscribe to an arbitrary combination of channels and to change their subscription at any time during the subscription period. However, the request to add or remove channels to the particular set has to be communicated using out-of-band methods such as telephone, cable or Internet. Therefore, it can be assumed that users will change the composition of their channels at rare intervals. For charging, the subscription request history of every subscriber is recorded. Still, the calculation of usage amount and components collecting usage data are not considered.

A charging model called Flexible-Pay-Per-Group (FPPG) and the design of a supporting CAS are introduced in [123]. The authors refer to the previous work of [122] and point out that their work is an enhancement regarding security and scalability. However, the model seems to support limited user dynamics since the authors consider an additional PPV functionality. Also, no additional aspects with regard to the referenced work have been considered.

An impulse pay-per-view (IPPV) system for one-way analog cable networks is proposed in [124]. For this purpose, it assumed that the cable operator is able to address each of the cable TV terminal devices directly. By using the introduced system, subscribers are able to purchase single programs (events). In order to send a service request, the system makes use of a service called Automatic Number Identification (ANI). This service is a feature of telephone networks and enables that the phone number of the caller and additional network-specific information is submitted automatically to the telephone operator. In particular, for requesting entitlement to some event the user places a phone call to a designated number

and adds the id of the desired program to this phone number. However, the telephone central office does not establish a connection to the desired number but rather forwards the contained information as a service request to the cable operators central control station. In this way, expensive autodial systems, labor-intensive call-in systems, and the overloading of the telephone system due to an excessive number of requests is avoided. Subsequently, the entitlement information is directed to the address of the terminal device and delivered in-band during the vertical blanking interval of the television signal.

An IPTV system supporting live broadcast of pay-per-view events is introduced in [125] (PPV-EPG). In this system, users are able to obtain information about available programs by using the electronic program guide (EPG), a call center, or a subscriber management center. The service request is sent in-band by using the return channel capability of IPTV. Upon authorization, a page confirming the actual request and necessary entitlement information is generated by the service operators central control station and displayed to the user. Accordingly, users are not able to get entitled directly for some program since the selection and confirmation steps are compulsory. Subsequently, the channel list of the user is updated according to the purchase. Once the terminal device has obtained the authorization information over in-band communication, the validity of entitlement is checked on every channel change. At the time the purchased program begins, a timer is started that instructs the terminal device to exit the channel after the purchased program has ended. Consequently, the user is charged for the whole duration of the program even if it is not viewed completely.

Another scheme for accurate billing using unidirectional broadcasting networks in the context of DVB is briefly presented in [126] (DVB-SI). In the proposed system, information required for charging and the request of the service are derived from service information (DVB SI) defined according to the DVB standard. This information is broadcasted with the media data. In particular, information regarding the channel a user watches, the starting and stopping times of a user for watching a particular channel as well as the pricing information are derived from the incoming broadcast data. Depending on the considered payment method the viewing time is either charged by using a prepaid account deployed on a smart card in the terminal device or by contacting the payment gateway of the service provider over the Internet for postpaid charging.

As a result of our investigation, we come to the conclusion that to the best of our knowledge no charging model comparable to CSTC has been proposed so far. In particular, CSTC stands out from the closest related solutions inasmuch as they require an intervention of the user during the service request or entitlement phase and users are charged for complete programs rather than short intervals.

4.2 User-Friendliness

We could already identify several consumer requirements related to pay-TV charging models in the course of our market survey in Chapter 2. In this section, we examine general expectations of consumers toward corresponding systems that implement these charging models. For this purpose, we investigate consumer requirements regarding the conditional access system (CAS) which is the particular component of the broadcast system that is responsible for the implementation of the charging model [48]. The CAS fulfills this function by granting and denying entitlement for customers using content encryption techniques. In this respect, the CAS is the key point where users make contact with the charging model. Consequently, the CAS determines the user-friendliness of the overall system and heavily

contributes to the acceptance of the service. In the course of our discussion, we provide technical interpretations for the requirements and propose a specification.

4.2.1 Requirements

In the general context of conditional access systems, consumers express privacy concerns particularly related to the disclosure of their identity and behavior to uninvolved parties. In particular, consumers require that usage data are not retained on the terminal equipment. In addition, consumers require that user data gathered by the network operator for charging and billing are used only for these purposes and are deleted after the settlement period. Access to content should be easy and include all available offers of a network operator. In particular, different types of content should be accessible using unified procedures and technologies.

In such cases when access is denied, consumers want to be able to precisely understand the reason and the responsible component for this situation, for instance, by means of a detailed notification. Also, consumers want to be informed regarding information that is sent over the return channel. In particular, operators should provide a notification which data are forwarded and whether they are stored, processed, and used or exploited in any other form.

Terminal equipment for the reception and descrambling of pay-TV services should guarantee a minimum set of features independent of the vendor. Underlying technical platforms for the processing of broadcast content should be harmonized in such a way that access to paid as well as free offers is possible using unified solutions. In this way, the diversity of the functional range and a long useful life of respective devices can be achieved and, consequently, costs for the purchase of terminal equipment can be saved.

Generally, for consumers, the use of pay-TV should always convey the distinct impression of additional benefit. After all, consumers have to experience a difference compared to free TV. At no time there should be a disadvantage compared to the earlier experience of watching TV. In addition, content featuring higher quality in terms of novelty, value, resolution, and so forth should be available. Despite the complex technologies in use, mechanisms and procedures for access and entitlement should be easy to use and flexible. Consequently, components in the terminal equipment responsible for entitlement should ensure and maintain the high quality of service customary in broadcasting and must not be error prone or outdated.

4.2.2 Specification

In the following, we draft a specification by considering requirements regarding user-friendliness we encountered so far. In order to refer to the corresponding requirement appropriately in the following sections, we use rectangles containing labels starting with the letter “U” for *user-friendliness* and the corresponding number.

Our subsequent market study reveals that consumers cancel their subscriptions and shift from pay-TV providers to VoD providers due to the interactivity of entitlement (**U1**) in two respects. First, consumers are offered short terms of contract and thus are able to opt-out anytime. Second, subscribers are able to consume the selected content immediately. Furthermore, our study shows that consumers appreciate the adaptability of services (**U2**) provided by VoD providers. In particular, consumers are no more trapped within genre boundaries but rather enjoy the freedom of choice among all available program offers. With the aid of our survey, we could show that consumers demand that costs for pay-TV

subscriptions should be calculated based on usage (U3). In Chapter 1 we could show that SIC addresses all of the aforementioned consumer demands. In the following, we show that further requirements have to be met.

Consumers require that the interaction for entitlement should be seamless (U4). Moreover, all available content should be accessible easily and flexibly within the framework of a unified procedure, technology, and system (U5). Technical solutions for providing paid content should on no account decrease the customary quality of service (U6).

Concerns and requirements regarding privacy are put forward by consumers since the discussed asset in the form of usage data are owned by this party. Consumers require that usage data should be accumulated and stored neither on the terminal equipment nor on modules for the support of different CASs located in terminal equipment (U7). Also, usage data should not be used for any other purpose than billing and must be deleted by the network operator after the settlement period. The latter requirement, however, is not related to the design of the CAS but is rather dependent on the policy of the particular network operator.

When access to content is denied, consumers wish to be informed with clear, understandable, and well-founded notifications what the underlying reasons are. Consumers want to be notified exactly at what time and what kind of information is forwarded to the network operator. Moreover, network operators should indicate whether and how these information are stored, processed and used otherwise. Similarly to the privacy requirements we discussed, due to the lack of legal requirements the fulfillment of transparency requirements are left to the discretion of the particular network operator. As a consequence, these requirements are not considered in the course of our work.

In addition, consumers also require that terminal equipment features a higher diversity of the functional range and a minimum set of functionality irrespective of the particular manufacturer. However, these requirements are out of scope for the specification of a solution supporting SIC since we do not consider the functional range of end devices beyond the support of SIC. In the following we list the requirements we will consider for the design of our solution:

U1 Interactivity of Entitlement

U2 Adaptability of Services

U3 Usage-Based Cost Attribution

U4 Seamless Interaction for Entitlement

U5 Single Procedure for Access to All Available Content

U6 No Disadvantage Compared to Free TV or Earlier Experience

U7 No Retention of Usage Data in Terminal Equipment

4.3 Integration

For our next consideration, we assume the perspective of the network operator and focus on his requirements regarding the properties of the conditional access system. As we know, the CAS is the particular component of the broadcast system that is responsible for the

implementation of the charging model. In addition, this time we also investigate legal requirements the network operator has to adhere to. Since scalability is a crucial property for the acceptance by consumers and service operators, we particularly address this topic in Section 4.3.1.3. In the next step, we devise a specification to bring requirements into a summarized form.

4.3.1 Requirements

4.3.1.1 Legal Requirements

Although legislation differs in each country, in the following, we identify inherent and predominant topics related to CASs. These topics are independent from national laws and commonly significant from this point of view.

Pursuant to §50 Article 1 Telecommunications Act CAS producers are required to lay out their systems in such a way, that it allows unrestricted control of services and cost-efficient transfer of control functions to network operators. This requirement ensures that network operators as licensees of CASs retain full control over the processing and dissemination of broadcast content.

Another requirement is that CAS manufacturers should not make their decision to grant a license to interested parties dependent on the existence of a common interface or other specific components for competing CASs in their design. In particular, the permission should not be denied for the reason that the common interface or other components would impair the transactional security of the respective content. This requirement pursuant to §50 Article 2 Telecommunications Act guarantees that terminal equipment manufacturers can support multiple CASs. Since a single CAS producer cannot weaken his competitors by enforcing his proprietary solutions on terminal equipment manufacturers his dominance is restricted.

Another legal requirement considers the set of features of reception terminals. According to Annex VI of the Directive 2009/136/EC of the European parliament and of the council, all consumer equipment intended for the (fixed) reception of conventional digital television signals has to process signals transmitted in the clear and according to a common European scrambling algorithm. However, in an amended version of this directive the constraint to use the common European scrambling algorithm also known as common scrambling algorithm (CSA) has been derestricted for all transmission paths except for terrestrial, cable and satellite exemplified by DVB-T/-C/-S. Consequently, CAS producers are legally free to choose any scrambling algorithm for IPTV.

Furthermore, there are several legal requirements dealing with the protection of minors. Generally, the protection of minors is implemented by employing two mechanisms. First, the dissemination by means of broadcasting times for programs relevant to the protection of minors is restricted. This restriction is referred to as *watershed* in British broadcasting, *safe harbor* in the U.S., and *Sendezeitbeschränkung* in Germany. The idea is that children are not allowed to watch television after a certain time of the day. Thus, programs with film ratings indicating that they are unsuitable for minors can only be broadcasted after a particular time of the day. Generally, film ratings are assigned by institutions either formed by a union of members of the movie industry or by nonprofit organizations. Examples for the former are the Motion Picture Association of America and the British Board of Film Classification. In Germany, ratings are assigned by a nonprofit organization called Organization for the Voluntary Self Regulation of Television in Germany (Freiwillige Selbstkontrolle Fernsehen e.V. - FSF). As a result, programs with a rating of FSK16 in Germany (comparable to R or 15) can only be shown from 10 p.m. to 6 a.m. in television. Programs

with a rating of FSK18 (comparable to NC-17 or 18) in turn are broadcasted only between 11 p.m. an 6 a.m.

The second mechanism is related to the handling of access to media harmful to minors pursuant to §3 Section 1 Statute on the Protection of Minors (Jugendschutzsatzung - JSS).Technical provision has to be made that the content is scrambled and blocked in case programs with film ratings indicating that they are unsuitable for minors are broadcasted at other times. Moreover, unblocking either for display or recording must only be possible for the duration of the selected program. In order to enforce this requirement in practice the service provider delivers a four-digit PIN code to the customers of age, which allows descrambling the blocked programs. In case the terminal equipment is not supplied by the provider, consumers are usually able to set up a four-digit PIN code by programming commercially available terminal equipment in order to protect minors in a household. In this context, higher restrictions apply to pornographic content. This type of content must not be made available over broadcast but over different telemedia (Internet services, Teletext, etc.) pursuant to §4 Section 2 page 2 Interstate Treaty on the Protection of Minors in Media (Jugendmedienschutz-Staatsvertrag - JMStV). In addition, the dissemination must not be public but rather within the scope of a closed user group. For forming such a user group, age and identity verification, as well as authentication mechanisms, are required. These mechanisms have to be approved by the German Commission for the Protection of Minors in the Media (Kommission für Jugendmedienschutz - KJM) by issuing a certificate of nonobjection.

4.3.1.2 Network Operator Requirements

Requirements of network operators regarding CASs are usually related to the reduction and avoidance of costs. Naturally, network operators strive for terminal equipment whose costs for purchase and operation is as low as possible. In addition, costs for logistics either for installation or for necessary upgrades should be minimized. In order to achieve low prices and freedom of choice among terminal equipment manufacturers, a standardized base system that supports free as well as scrambled services should be designed.

Such standardized solutions for IPTV STBs could be defined by harmonized specifications supporting various hardware platforms, middleware, and CASs. These specifications would provide standardized interfaces and processes according to which exchangeable software components could be implemented. Depending on the respective solution provider these components could be provisioned during the initial installation of the terminal equipment at the customer premises. The secure transmission of the components would be guaranteed by virtual local access networks (VLANs) under the supervision of network operators. In this way, the operating system, auxiliary service software and CAS could be adapted with little effort for the respective network operator.

Furthermore, the current operation of independent systems for the protection of linear (broadcast) and nonlinear (VoD) content is economically ineffective and should be avoided in future. However, requirements for each use case lie far apart. For instance, it is required that the encryption of broadcast content is realized by using the common scrambling algorithm (CSA) whereas for VoD the advanced encryption standard (AES) is used. Similarly, the mechanisms for the end-to-end signaling of use of rights for linear and nonlinear content are incompatible. This current practice is economically ineffective as well and should be avoided in future.

In the context of short-interval charging, the investment for the support and migration should be minimized by maintaining interoperability with existing equipment supporting conventional pay-TV. This interoperability could be achieved by making as little modi-

fications on standardized architectures as possible while providing necessary services to support short-interval charging. Since it can be assumed that consumers gradually adopt short-interval charging, in this way also methods for a concurrent operation can be facilitated. In addition, transactional and periodic infrastructure costs for the support of short-interval charging should be minimized. This could be achieved by utilizing existing infrastructure conforming to standardized architectures and best practices.

4.3.1.3 Scalability

In order to avoid undesired effects such as high channel changing times or even interrupts while receiving broadcast content, high-performance demands are made on CSTC and in particular on the employed key management system and the multicast encryption scheme. In the following analysis, we investigate which requirements with regard to communication and computation exist in operational deployment.

Communication Requirements

In order to devise upper bounds for our system design, it is essential to specify how much bandwidth is available for key update messages when broadcast content is transmitted using a DVB compliant transport stream. According to the standard decoder model (TSTD) in [100] the bandwidth for all system data, that is, for all data except the data for audio and video streams, should at most amount to 1 Mbit/s.

Furthermore, in a DVB compliant transport stream, the following mandatory service information (SI) must be present and updated regularly according to [101]: Program Association Table (PAT), Program Management Table (PMT), Conditional Access Table (CAT), Network Information Table (NIT), Service Description Table (SDT), and Time and Date Table (TDT).

Thus, the available bandwidth for key update messages results from the overall bandwidth for system data less the bandwidth consumed by the listed mandatory SI. According to our own calculations and considering calculations from literature such as [127], we have come to the conclusion that more than 104 kB/s are available for key update messages in a DVB compliant TS.

In our design of CSTC, the length of the key update message is dependent on the user dynamics of the managed channel. In order to estimate expectable user dynamics, we refer to empirical data from the literature. In [128] the authors evaluate a dataset retrieved from a nationwide IPTV provider in Spain (Telefonica) broadcasting 150 channels during a time period of 6 months. As a result of their analysis, at most 30% of all users watch TV concurrently whereas 8% of all users watch the most popular channel. Most interestingly, the authors are able to specify that at peak times a maximum of 1% of all users watching the most popular channel performs a channel change per second. In another study [129] the authors analyze the traffic of a nationwide IPTV provider from Belgium for a duration of 4 days. Here, only a maximum 0.5% of all users watching the most popular channel perform a channel change per second. We will refer back to these values for the evaluation of our implementation in Section 5.4.3.

Computational Requirements

The STB is a security-sensitive system since it performs critical tasks for conditional access and is permanently exposed to potential physical attacks as it resides at the customer premises. Consequently, nowadays STBes provide means for remote configuration and update of security-critical components [130]. Confidential keys in modern STBs are physically stored either on smart cards or on secure (memory) modules on the STB cir-

cuit board. Both approaches have similar specifications and circuitry for resistance against various attacks. Aside from storage, some variants of these components provide crypto-processors for the execution of encryption and digital signature algorithms on-chip. By using these processors, confidential keys do not have to leave the chip.

In this connection, execution times of implemented algorithms can be reduced significantly compared to software implementations. For instance, the execution time for a single key decryption using a software implementation of the AES-128 algorithm is 10 ms on a common smart card. This value can be decreased to values between 100 and 150 μs by utilizing smart cards featuring a cryptoprocessor [131], [132]. Current products are able to process cryptographic schemes such as 3DES, AES, the RSA cryptosystem, and ECC (Elliptic curve cryptography) [133], [134].

For the implementation of the key management system supporting CSTC at the head-end, we propose the logical key hierarchy (LKH) [112], [113] as the multicast encryption scheme. We find that this scheme is particularly suitable since it causes only logarithmic communication and computational overhead. At same time LKH maintains forward and backward secrecy. Nevertheless, in future work also other multicast encryption schemes could be employed. These schemes could be evaluated in load situations regarding channel change requests we described above. These evaluations could be performed by using simulations [135], [136] or by using a measurement system such as the one we describe in Section 5.4.

However, for the employment of the LKH scheme in the key management system, we suggest several adjustments. Each channel should be managed using a dedicated LKH tree in order to reduce management costs for user addressing. In addition, the position of each user in the tree data structure should be allocated statically for each channel in order to save allocation costs.

Finally, communication and computational overhead is dramatically reduced by using LKH in batched mode [111]. When batch processing is used, the group key is updated at regular time intervals (batch intervals) rather than every time the composition of the group changes, namely, when a single user leaves or joins the channel. As we have seen in previous Section 4.4.2.2, this approach is particularly reasonable. Specifically, in video streams, data are decodable only at certain points in time. Consequently, too frequent updates of the group key triggered by changes in the group composition would result in the protection of undecodable data.

4.3.2 Specification

In the following, we draft a specification by considering requirements regarding integration we get to know in the previous section. In order to refer to the corresponding requirement accordingly in the following sections, we use rectangles containing labels starting with the letter “I” for integration and the corresponding number.

Consumers and network operators require interoperability of terminal equipment with different CASs. This requirement has also been propagated to legislation. As a legal requirement, terminal equipment should feature a common interface for this purpose (**I1**). Furthermore, terminal equipment should support content transmitted in clear and scrambled (**I2**). For achieving these goals, specifications need to be harmonized so that solutions for terminal equipment and CASs can be standardized. However, the purpose of this interoperability is the saving of costs. For consumers, interoperable devices guarantee a long useful life and thus the protection of investment. Similarly, network operators

do not need to deliver all components of subsidized terminal equipment when they need to be upgraded and thus also save costs. Interoperability is also a key factor for integration in the broadcasting transmission infrastructure. Currently, network operators need to maintain independent systems for linear broadcast and VoD. One step toward integration would be the operation of unified systems for IPTV and VoD. In particular, the use of the same encryption algorithm preferably AES could save multiple spending (I3). Moreover, the service architecture implementing CSTC should allow for the integration into existing employments. Equipment related to CSTC should maintain interoperability with existing components supporting conventional pay-TV in order to minimize investment for support (I4). In addition, the existing infrastructure conforming to standardized architectures should be utilized by components used for the support of CSTC in order to minimize transactional and periodic infrastructure costs (I5).

In order to restrict access to media harmful to minors at times which are broadcasted outside of the designated times, terminal equipment should provide support for PIN code request and processing. However, this requirement is a feature of the terminal equipment rather than a feature of the CAS in use. Consequently, it will be omitted in further consideration. In the following, we list the considered requirements regarding integration.

I1 Support for Different CASs in End Devices by Means of a Common Interface

I2 Support for Clear and Scrambled Transmission

I3 Resource Sharing for Support of Different Charging Models

I4 Interoperability with Existing Operator Equipment

I5 Utilization of Existing Operator Infrastructure

4.4 IPTV Service Architecture for CSTC

In the following, we investigate how a CAS implementing CSTC can be included in a typical IPTV architecture. In particular, we identify functions and interfaces that have to be enhanced or completed for the support of CSTC in order to achieve the desired functionality while maintaining interoperability. For our discussion, we assume an IPTV architecture in compliance with the widely adopted suite of standards developed by the digital video broadcasting (DVB) project. However, the discussed concepts are applicable to other relevant standards such as ATIS, ISDB, and DMB since all utilize MPEG-2 transport streams conforming to [100].

4.4.1 Components

The required modifications of affected functional components for the support of CSTC in broadcast architectures generally consist of different processing. This different processing is required for two originally existing components located in the HES and for two originally existing components located in the Home network, in particular in the STB. In the following, we will discuss the required modifications for each component.

For introducing CSTC to the broadcasting architecture, the subscriber authorization system has to be modified. In particular, a different key management algorithm for generating entitlement messages has to be implemented. This algorithm has to be able to consider channel change requests from users transmitted over the return channel. In addition, synchronization with the multiplexer has to be taken into account. Moreover, the key management has to feature high-performance with the aid of methods such as batch processing in order to avoid higher channel change times. In the context of IPTV, the Subscriber Authorization System itself and its internal sequence of processing including the key management algorithm and the message formats are proprietary and, consequently, not specified. Standardization bodies argue that in this way conditional access systems are harder to circumvent. The only specification we are aware of can be found in [137]. Here the authors recommend a hierarchical key management scheme and the use of at least a 4-level key hierarchy for achieving scalability. In addition, it is suggested that the update frequency for the content key should be high enough so that it is not worthwhile to extract and publish it before the next update occurs. As an example, an update frequency of one second is given. However, these recommendations are not useful for the design of our system. Since our proposed approach is novel, the key management algorithm we need to employ has to process user requests. In conclusion, the modifications of the Subscriber Authorization System are in compliance with current respective standards.

For the integration of CSTC, furthermore, the multiplexer has to synchronize the generation of entitlement messages by the SAS and their inclusion into the transport stream. In general, multiplexers allocate different data flows in order to efficiently share a single resource among multiple services. For this purpose, a multiplexer operates on different MPEG-2 transport streams conforming to [100] and seeks to improve bandwidth and minimize buffering delays. Therefore, standards for the specification of multiplexers usually deal with the message format it operates on. As we don't change the MPEG-2 transport stream format, the multiplexer is, in this respect, in compliance with current standards. However, for the alignment of broadcast and entitlement data (discussed in Section 4.4.2.2) in order to support channel-switch triggered charging two additional arrangements are required. At first, the multiplexer has to signal the occurrence of a random access point to the key management component of the corresponding channel. Still, this modification is not serious since advanced multiplexers that apply statistical multiplexing already analyze the incoming stream in greater detail. Even more, sophisticated multiplexer implementations transcode the incoming streams in order to adapt them to bandwidth constraints. Furthermore, the multiplexer has to buffer and include the incoming ECMs from the SAS in a timely manner according to the discussed alignment. These two functions do not interfere with existing standards and are assumed by the injector component described in our system architecture proposal in Sectionr 4.5.

When CSTC is introduced to the broadcasting architecture, the key management algorithm used in the SAS also has to be the supported by the conditional access module. In addition, corresponding optimizations for the key management algorithm used in the SAS such as batch processing have to be implemented correspondingly. As already discussed for the modification required for the SAS, correspondingly the key management algorithm used in the CAM is proprietary. Thus, the modifications of the conditional access module are in compliance with current respective standards.

For integrating CSTC, furthermore, the firmware running on the set-top box has to be modified. In particular the business logic responsible for power on/off module/routine has to be adapted in order to integrate the log in/out to service. Also, the existing channel change module/routine has to be adapted in order to integrate the use of the return channel

for the service request. To the best of our knowledge, there are no standards giving specifications how a set-top box firmware should be programmed. Consequently, this modification does not represent any deviation from the broadcast architectures we investigated.

4.4.2 Protocols

In general, the modification of protocols is caused by the different principle of operation of the functional components and is related to the executed protocol steps, the included data, and, consequently, to the message format. For the implementation of channel-switching triggered charging an existing protocol, namely, the Entitlement Management and Control, has to be modified and a new protocol, namely, the Channel Change Signaling, has to be added to the architecture.

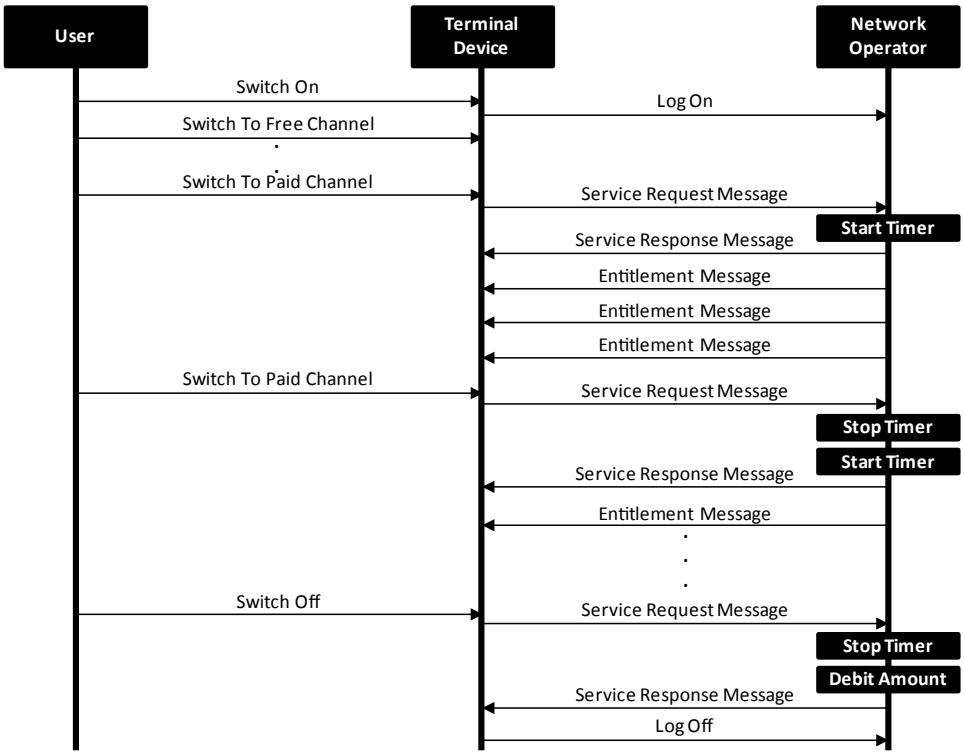


Figure 4.4: Overview of Actions Related to Postpaid CSTC

However, before we list the required changes, in the following, we examine the use of these protocols in the context of postpaid and prepaid charging since both charging models are supported by CTSC. In Figure 4.4 actions and messages necessary for the handling of the postpaid charging method with reference to all involved parties, namely, the user, the STB, and the SAS, are shown. When a user switches on the terminal device a log-in is performed automatically by the terminal equipment. Subsequently, the user may access the complete program offer by switching to free and paid channels.

In case the user decides to switch to a free channel, no further actions are taken. In contrast, in case the user decides to switch to a paid channel the charging process is started.

For this purpose, the terminal device signals an in-band service request to the network operator on behalf of the user. In this context in-band means that messages are exchanged between the terminal device and the network operator without the need for intervention by and notification to the user.

In the next step, the network operator sends an in-band entitlement response to the user. Subsequently, the network operator starts a timer to measure the usage duration for the channel the user has recently switched to. Furthermore, the network operator starts to send entitlement messages to the terminal device at regular intervals. When the user decides to leave the paid channel or switches off the terminal device a corresponding in-band service message is sent to the network operator. Subsequently, the network operator stops the timer and debits the complete amount from the user's account. When the user has switched off the terminal device additionally a log-out is performed.

In Figure 4.5 actions and messages necessary for the handling of the prepaid charging method are depicted. Here, in contrast to the postpaid scheme, the user has a prepaid account with the network operator. In regular time intervals and before each service request, that is, a channel change, the credit balance of the user is checked. Additionally, on this occasion, the corresponding amount up to the time of the next credit balance check is debited from the user's account. Only after these steps the network operator starts or continues the timer and correspondingly the transmission of entitlement messages to the terminal device. However, if the account of the user has no positive balance as a result of the credit balance check further access to the channel is denied.

4.4.2.1 Entitlement Management and Control

Entitlement Management and Control in the context of DVB is realized using two types of messages. Entitlement Management Messages (EMM) are used to reflect changes in the composition of the group of entitled users. In case a new subscriber has to be entitled or the entitlement of a user who canceled his subscription has to be revoked, EMMs are used to communicate corresponding information.

An Entitlement Control Message (ECM) usually contains two control words (CW) called odd and even. These control words do not indicate a change in the composition of the group of entitled users but rather prevent users who are not entitled from illegitimate access. The key derived from one CW is used for the current cryptoperiod and is in force. The key derived from the other CW is the key for the next cryptoperiod. In order to signal the change of the applied key, transport stream packets feature a 2-bit indicator in their header, called transport_scrambling_control. When the transport_scrambling_control in one of the incoming TS packets changes, the receiver learns that the key in force has changed and can apply the key derived from the other CW.

In contrast to the usual semantics of the DVB standards, we use ECMs instead of EMMs to indicate changes in the composition of the group of entitled users. We pursue this approach since we want to convey key update messages for every single channel. However, EMMs have a global scope in the transport stream, whereas ECMs apply to a specific program.

4.4.2.2 Alignment with Broadcast Data

For the discussion of aligning key update with broadcast data, we first refresh our knowledge we gained from Section 3.1. Generally, video streams consist of a series of still images. Most of the adjacent images share a fair amount of redundant information resulting from panning cameras during recording. Video compression algorithms, among other

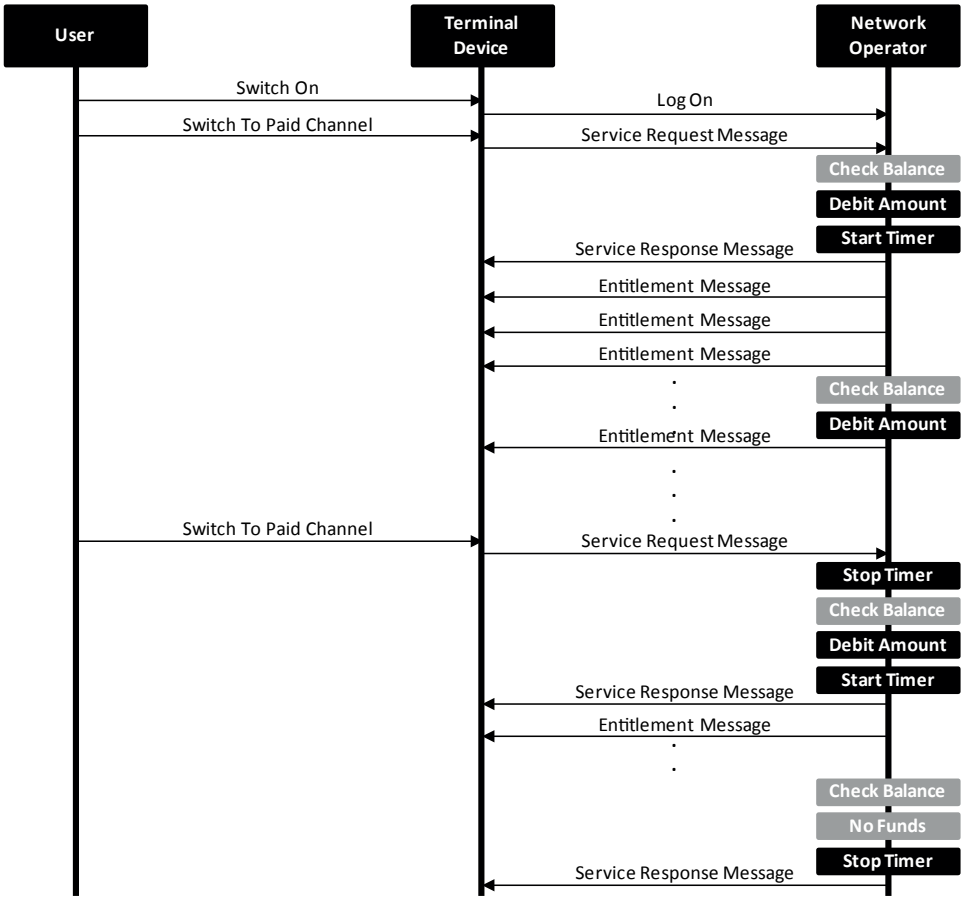


Figure 4.5: Overview of Actions Related to Prepaid CSTC

things, take advantage of this fact by storing only differing parts of successive images after a reference image has been saved. In literature, reference images are called intracoded frames since the way they are stored is self-contained. In contrast, images that contain differential data are called intercoded frames.

Since errors occur and multiply with an increasing number of intercoded frames, video compression algorithms regularly add one intracoded frame at appropriate positions during compression. Consequently, intercoded frames lie in between successive intracoded frames, which explains the naming. But intracoded frames are added in certain intervals not only to resolve errors but also to enable channel change in acceptable times. The first uncompressed image after a channel change is only recoverable when an intracoded frame has been processed. Previous data are not decodable due to the lack of relevant reference information. The presence of an intracoded frame is indicated as a random access point (RAP) on lower layers of the stream so that decoders do not need to parse and process unnecessary data.

Moreover, we also recapitulate our knowledge regarding multicast encryption from Section 3.2. Generally, we employ the method of batch processing for the key management of CSTC in order to increase performance. When batch processing is used, the requests of

users leading to changes in the group composition do not take immediate effect. Instead, the group controller marks the changes in the underlying internal data structure. In regular intervals, that is, batch intervals, these marked changes are processed in batch. As a result, a key update message and a new group key are computed.

We propose that data between consecutive RAPs should be encrypted with the same key. The time it takes to stream these data is the ideal duration for the validity of each key, namely, the batch interval. The interval between consecutive RAPs is reasonable because smaller portions of video data are not decodable and therefore charging for them is pointless. However, it is also not advisable to increase the duration of the batch interval, for instance, to two RAP periods since in this case, every user who wants to switch channels has to wait for two RAP periods.

However, the creation of the key update message consumes considerable computation time which is not constant since it depends on the user dynamics reflected in the current batch. Accordingly, we must consider a lead time for starting the batch processing of marked changes. Additional time is required for the inclusion and transmission of the key update message. Since this process is executed subsequent to the creation of key update, it increases the lead time. Finally, we have to consider a lead-time at the STB so that key update message can be processed and the content key can be recovered in time. Otherwise, the STB would be not able to decode the scrambled broadcast. However, this lead-time has also to be taken into account at the headend since the key update message is added into to the transport stream here. Again, this time has to be considered subsequent to the transmission of the key update message and, consequently, increases the lead time further.

As a result, the total lead-time consists of the time required for the creation of the key update message, the inclusion and transmission of the key update message, and the processing time of the key update message in the STB. In our further discussion in Chapter 5 we refer to this lead-time as channel change request (CCR) deadline since after this point in time the processing of all incoming channel change requests is deferred to the next batch interval.

4.4.2.3 Channel Change Signaling

Channel change signaling for the purpose of charging is not considered for digital video broadcast since previously only one-way transmission was assumed. However, channel change signaling for the purpose of multicast group management is necessary for IPTV in order to join and leave multicast groups which are used for broadcast data provision. For this purpose, the related protocols Internet Group Management Protocol [110] and Protocol Independent Multicast [138] are used. The processing of channel change signaling for conditional access on the group management layer would create associations on the wrong architectural level. Charging can be regarded as a higher-level application. Group management, in contrast, is a transport function and is considered on a lower level from an architectural point of view. Aside from the fact that implementing charging functions on the group management layer would require serious modifications in fundamental protocols of already deployed devices throughout the network hierarchy, it is also counterintuitive. Since multicast-enabled routers are used to manage the distribution of data according to the membership of downstream components, the addition of upstream functionality to signal service requests to the headend diverts these routers from their intended use.

Alternatively, channel change signaling for charging could be implemented by using SIP (Session Initiation Protocol) [139], which is used as a communication protocol for signaling and controlling Voice-over-IP (VoIP) telephony applications. The use of SIP would follow the current trend of IP convergence aiming to carry out all communication using the

Internet Protocol. In particular, this is reflected by the Next Generation Network (NGN) standards, which would be a reasonable context to implement channel change signaling for charging over SIP. In particular, most network operators provide IPTV in the framework of their triple play offers, which includes Internet access and VoIP telephony services. Consequently, this approach would allow the use of other related components and mechanisms so far used for VoIP such as fraud detection and admission control for handling overload situations. In addition, the reuse of existing infrastructure would decrease recurring expenses.

A quick survey showed that in contrast to multicast group management protocols, SIP has already arrangements for this kind of signaling purposes in the form of protocols dealing with call detail records (CDR). These records contain usage information and are used for the charging and billing of phone calls. In addition, so-called advice of charge (AOC) messages could be used to convey charging rates on channel change and balance information during viewing. As we could ascertain, the SIP standard is easily extensible by profiles for new use cases.

4.5 CSTC System Architecture

In this section, we provide the details for an implementation of a system supporting CSTC. For this purpose, we consider architectural components and protocols, which have been elaborated in previous Section 4.4. The main components of the system are the Head-End System and the Set-Top-Box.

4.5.1 Headend System

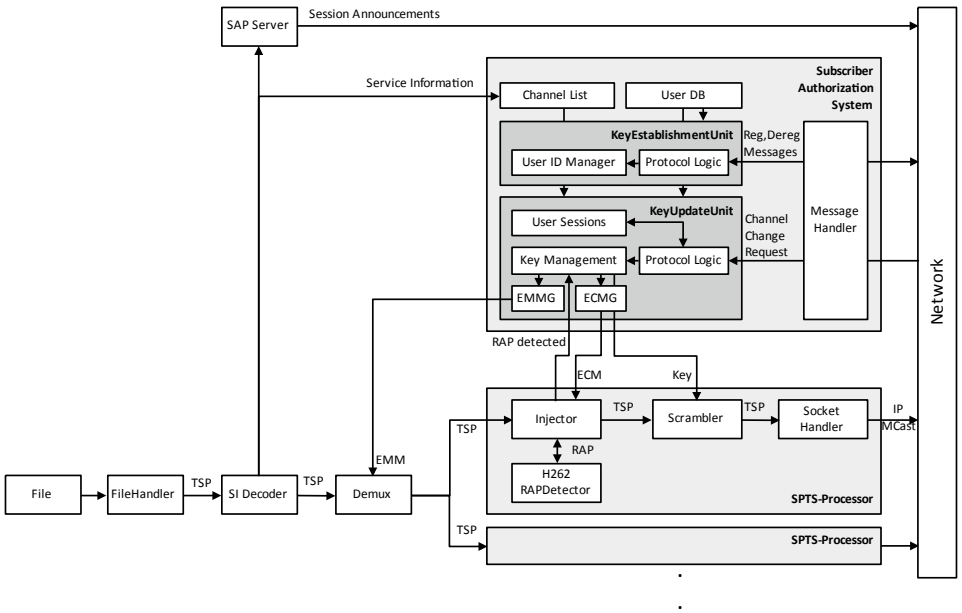


Figure 4.6: Block Diagram of Headend System Supporting CSTC

The architecture of our headend system (HES) is given in Figure 4.6. In order to broadcast scrambled content, the HES utilizes recordings of a prior broadcast stored in a file that contains a DVB-compliant transport stream (TS) [100], [101]. In particular, we used different recordings of DVB-S and DVB-T broadcasts for system test.

Transport streams can contain either the content of a single program (single-program transport stream - SPTS) or the content of multiple programs (multi-program transport stream - MPTS). Satellite, cable, and terrestrial transmissions use MPTS in order to utilize the available bandwidth efficiently. In contrast, IPTV uses SPTS so that every channel is addressable individually by using a different IP multicast address and port combination.

Service Information (SI) is added to the TS in order to specify the number and structure of contained channels. After reading the input file, the SI Decoder is used to extract this information that is required by Demux to generate multiple SPTSs from one incoming MPTS. Each single program transport stream is then processed in a dedicated SPTS-Processor that is described below.

The service information is also used by a session announcement protocol (SAP) server to notify potential receivers regarding available streams and required parameters for access [140]. Additionally, the service information is used in the Subscriber Authorization System (SAS) to instantiate one corresponding Key Management component for each channel.

4.5.1.1 SPTS-Processor

The SPTS-Processor contains an Injector, a Scrambler, an H262 RapDetector, and a SocketHandler.

The Injector has two functions. The first function is to inform the corresponding Key Management component in the SAS about the occurrence of a random access point (RAP). For detecting the RAP in the H262-compliant video stream, the Injector uses the H262RapDetector. We encapsulated the RAP detection functionality into a separate component to provide extensibility. Thus, other transport streams featuring H264- or H265-compliant video streams can be used in the Head-End System. The second function of the Injector is to add the resulting ECMs from the key update into the corresponding SPTS. The format of the ECMs will be detailed in Section 4.5.1.3

The scrambler encrypts the TS on TS level [141] using the AES-128 encrypting algorithm in counter mode (CTR) without padding [142], [143]. We chose this mode of operation in order to account for the TS packet size, which is not a multiple of the usual AES-128 block size of 16 bytes. In this regard, the AES algorithm is utilized as a stream cipher.

For the transmission, as usual, seven TS packets are packetized to form an IP packet in the SocketHandler. Each channel is streamed to a different multicast address using the real-time transport protocol (RTP) [104].

4.5.1.2 Subscriber Authorization System

The message handler sends registration and deregistration requests to the key establishment unit and channel change requests to the key update unit. The protocol logic component in each unit performs sanity checks on the incoming messages and implements a simple business logic. The used message formats are detailed in Section 4.5.1.4.

As mentioned, the key establishment unit is used to handle registration and deregistration messages. Once the registration of a user is completed, the user is able to direct channel change requests to the key update unit.

The key management component in the key update unit issues EMMs embedded by the Demux into each SPTS to identify the conditional access system (CAS) in use.

Also, channel change requests are processed by the key management component. As mentioned in the previous section, a logical key hierarchy scheme (LKH) in batch mode is used for this purpose. This approach requires that channel change requests are processed in a marking phase without computing of new keys. Only when an RAP is indicated by the Injector the batch processing phase is initiated to determine the new keys including the new group key and to build the key update message. The format of the key update message is explained in Section 4.5.1.3. The key update message is processed further by the ECM generator (ECMG) so that it can be added to the transport stream. The group key is forwarded to the scrambler for encrypting the transport stream.

4.5.1.3 Entitlement Management and Control

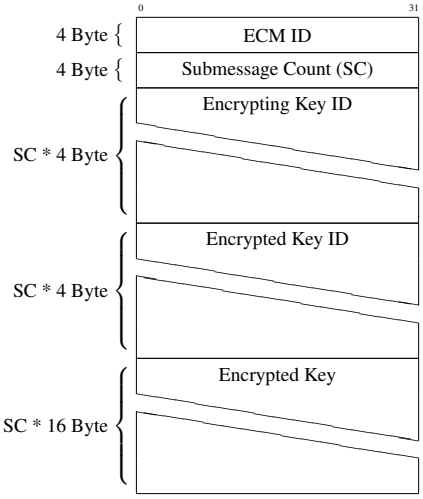


Figure 4.7: Key Update Message Format

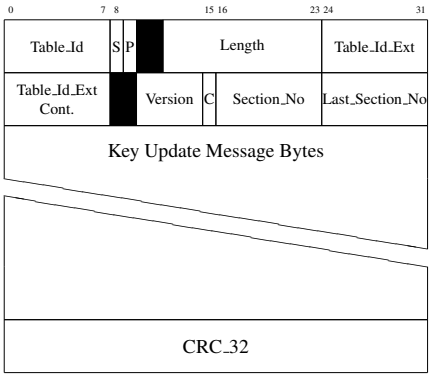


Figure 4.8: Private Section Format

Key update messages are generated in the key management component of the SAS. As depicted in Figure 4.7, the key update message contains a monotonically increasing ECM ID and three arrays. According to LKH, a couple of keys in tree nodes must be updated, as a rule. Each of these keys must be encrypted by the keys of the descendant nodes. Each submessage in the key update message consists of an encrypted key (assigned to the lower array), the ID of this key (assigned to the medium array), and the ID of the encrypting descendant key (assigned to the upper array). We preferred using three arrays in this format instead of one mixed-type array in order to improve the performance of serialization and deserialization of key update messages.

Key update messages are processed in the ECM generator (ECMG) that translates these messages into the entitlement control message format. The ECMG uses the private section format defined in [100] as illustrated in Figure 4.8. Similarly to all private tables in a transport stream, the ECM can be segmented into up to 256 private sections with 4096 bytes each [100]. In our system, the ECMs are added to the stream of each channel by the Injector component as can be seen in Figure 4.6.

Similarly, entitlement management messages (EMMs) are created in the EMM generator (EMMG). EMMs also use the private section format and contain meta-information about the active conditional access system. In our implementation, EMMs are added to the stream of each channel by the Demux.

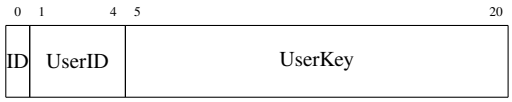
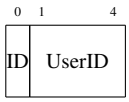
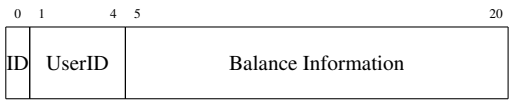
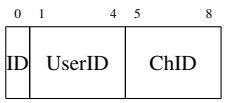
Message Type	Direction	Message Format
RegRequest	STB → HES	
RegResponse	HES → STB	
DeRegRequest	STB → HES	
DeRegResponse	HES → STB	
ChannelChange Request	STB → HES	

Table 4.3: Message Types Used for Signaling between HES and STB

4.5.1.4 Channel Change Signaling

Message types used for registration, deregistration and channel change signaling as well as the corresponding message formats are shown in Table 4.3. The RegRequest and RegResponse messages are used during the registration phase of the set-to-box (STB). In addition, DeRegRequest and DeRegResponse messages are used during the deregistration of the STB. ChannelChangeRequest messages are used to indicate a channel change event by the user. The ID field indicates the message type and consists of a single byte.

UserID is a 4-byte integer and is used for user identification. UserIDs are managed by the user ID manager in the SAS (see Figure 4.6). The UserKey is a 16-byte AES key assigned to a specific UserID. Both UserID and UserKey are stored in the UserDB component of the SAS (see Figure 4.6).

Here, including the UserKey in the RegResponse message only serves test purposes. In particular, the user key, or master private key as it is referred to in literature, is a pre-shared secret between the headend and CAS-related components of the STB. This key is never disclosed as it could be copied and used for service theft. Therefore, the user key is stored on secure and tamper proof hardware, for instance, on a smart card.

The Balance Information field is a 16-byte String used to present the balance information to a user once the deregistration is completed. The ChID field contained in the ChannelChangeRequest message specifies the ID of the destination channel a user has switched to. Channel IDs are used to uniquely identify the broadcast channels and are stored in the Channel List component in the SAS. In addition, Channel IDs are part of the session announcements sent to the STBs by the SAP server in the headend (see Figure 4.6). Since the ID of the current channel is not sent during channel change, state information of the users are stored in the User Sessions component in the headend (see Figure 4.6).

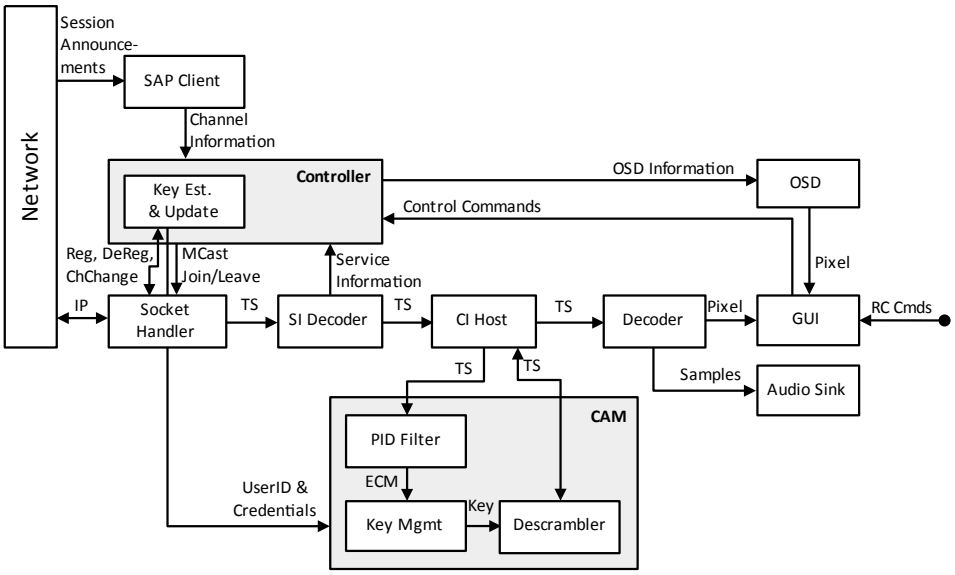


Figure 4.9: Block Diagram of STB Supporting CSTC

4.5.2 Set-Top Box

The architecture of the STB is shown in Figure 4.9. Available channels are discovered by session announcements received by the SAP client. These announcements are gathered and form a channel list. The controller represents the control logic of the STB and uses IP multicast join and leave messages according to Internet Group Management Protocol (IGMP) to access channel groups from the channel list. These multicast messages and all other IP traffic are processed in the SocketHandler.

The key establishment component in the controller performs registration and deregistration at the headend. The received UserID and UserKey are forwarded to the key management component of the CAM to process key update messages. The key update component is used to send channel change messages to the headend.

During channel change, a channel change message is issued by the key update component and the SocketHandler is instructed to join the multicast group of the desired channel simultaneously.

Once transport stream packets of the new channel arrive at the SocketHandler, they are passed to the SI Decoder to decode the service information contained in the transport stream. Relevant service information such as channel name, program schedule and electronic program guide are forwarded to the on-screen-display component (OSD) for display. The latter renders an image containing the delivered information for overlay on the video.

In the next step, the transport stream packets are sent to the common interface host (CI Host). This component passes the TS packets to the descrambler in the conditional access module (CAM). At the same time, the CI Host processes the control protocol specified in the common interface standard [144].

Containing the counterpart of the control protocol specified by the common interface, the CAM is provided with relevant information to filter ECMs and EMMs from the TS. The filtering is performed in the packet ID filter (PID Filter) inside the CAM. ECMs and EMMs are passed to the key management component. Afterward, the key management

component assembles and processes the key update messages. By using the client-side implementation of the LKH scheme, the content key is computed and forwarded to the descrambler.

The descrambler uses this key to decrypt the transport stream sent by the CI Host. The key update signaling is performed as described in Section 4.3. In the next step, the descrambled transport stream is forwarded to the decoder. The decoder, in turn, decompresses the audio/video data contained in the transport stream.

For our implementation, we use the decoder of the GStreamer multimedia framework because it allows access to the decoder buffer [145]. By controlling the access to the decoder buffer, we perform the time measurements presented in Section 5.4.

The decompressed video data are displayed with the on-screen-display (OSD) to the user. In this context, the OSD is part of the graphical user interface (GUI) used to operate the STB. The decompressed audio samples are output by the audio sink component. An image of a remote control presented on the GUI of our prototype enables the user to submit control commands, which, in turn, are sent to the controller.

4.6 Validation of CSTC

In the following, we briefly recall the requirements met by short-interval charging in order to show how CSTC conforms to them. Clearly, when CSTC is employed technically no term of contract is necessary as the service can be charged completely based on usage (**U3**). In an actual offer, however, a term of contract could be required for legal reasons. Nevertheless, in this case, no additional costs would incur when the service is not used. Furthermore, users are able to get entitled and consume the selected content immediately by switching to the desired channel. As a result, CSTC inherently achieves the required interactivity of entitlement (**U1**) and the adaptability of services (**U2**). In addition, CSTC meets additional requirements specified by consumers. Since the measuring of consumption is performed by the network operator, no usage related data are retained in the terminal equipment (**U7**). By employing CSTC network operators are also able to variably price content depending on the channel, context, time slot, etc. Consequently, access to all types of content can be made available using a single procedure, namely, the switching of channels (**U5**). For the discussion of necessary transitions and discontinuities of the used entitlement process, we refer to Table 4.4. Here, the charging-related user actions for all considered models including CSTC, are compared. In general, fewer user actions are preferred.

As a result of the review of related work, we could ascertain that CSTC is associated with a new user model compared to other methods such as subscription-based pay-TV, PPV, and VoD. Here, the user model of CTSC is essentially distinct from the other user models concerning the actions relating to usage and charging. The usage-related difference of this new user model has already been discussed in Section 1.2 in the context of our comparison with short-interval charging. In Section 4.1, we already investigated the charging-related actions and proved that CSTC achieves seamless interaction for entitlement (**U4**).

For a VoD service, in addition to the registration also an explicit log-in is often needed in order to provide necessary credentials. When VoD or PPV is used, the user has to make an explicit and possibly out-of-band request to get entitled. Once the request for entitlement

User action	VoD	PPV	Subscription	CTSC
Conclude Contract/Register to Service	X		X	X
Explicit Log-In to Service	X			
Explicit Service Request	X	X		
Provide Payment Information		X		
Out-Of-Band Delivery of Entitlement Credentials		X		
Input of Out-Of-Band Entitlement Credentials		X		
Termination of Contract (Otherwise Costs Incur)			X	

Table 4.4: Comparison of Charging-Related User Actions

is approved by the service provider, payment information has to be provided for PPV since no registration has been completed earlier. Also, the entitlement credentials are usually provided out-of-band for PPV and have to be keyed in the remote control to gain access to the desired content. All the mentioned charging models with exception of PPV require a registration or the conclusion of a contract. But only for subscription-based charging, additional costs incur if the contract is not terminated.

As we can see, CSTC requires only a single explicit user action in order to obtain the entitlement credentials and to provide payment information. All other necessary actions are performed implicitly by the STB. The log-in and log-out actions happen during the switch-on and switch-off of the STB. Similarly, service requests are made and entitlement information is delivered and processed in-band without user intervention.

Since during a channel change we cannot assume that a user knows which content will be delivered on the destination channel and whether this content will draw his interest, the presented approach of CSTC could be further enhanced regarding fairness. Usually, users continuously change channels for some time once they have lost interest in the content of some channel. This behavior is referred to as zapping or channel surfing. To address this user behavior, a sampling period during which a user can decide whether the shown content suits him could be introduced. In this way, the starting time for the charging of the destination channel would be postponed. Several studies suggest that users remain in the state of channel surfing for 30 seconds [146], [147], 60 seconds [128], [148] or even 4 minutes [31]. During this time, users perform 4 [128] channel changes on average and require about 4 [128] to 10 [148] seconds on average in order to decide whether the currently viewed content is appealing for them. In order to prevent the misuse of the sampling mechanism, the sampling action and times could be logged according to a certain sliding time window. Users who sampled the same channel several times during this time window would be charged for viewing the channel since they show a more than average interest in the content.

Apparently, so far we did not prove whether CSTC causes a degradation of service quality compared to free-TV or earlier experience (**U6**). This requirement has not been considered yet since we devote whole Chapter 5 for the discussion of this subject.

According to **I1**, it is required that different CASs in end devices have to be supported by means of a common interface. By reusing the standardized CI-Host and CAM architecture, this requirement is met. In addition, clear and scrambled transmission should be supported according to **I2**. This requirement is met by the inherent properties of CSTC allowing a mixture of scrambled and unscrambled channels. Network operators require

that resources should be shared in order to support different charging models I3. New CASs should be interoperable with existing equipment I4 and the existing operator infrastructure should be utilized I5. As described above, no new components have been added. Thus, all components have been reused in order to support CSTC.

4.7 Conclusion

In this chapter, we introduce a novel short-interval charging model called channel switching-triggered charging (CSTC). We prove that this charging model achieves user-friendliness as targeted by our research question Q2. For this purpose, we first examine the requirements consumer state regarding conditional access systems. We choose this way to identify consumer requirements since the CAS is the particular component of the broadcast system that is responsible for the implementation of the charging model and, consequently, to a great extent determines its user-friendliness. As a result, we show that all consumer requirements, except one, are covered. However, the remaining requirement will be considered separately in Chapter 5, since it is related to our research question Q5. After considering consumer requirements, we express them by drafting a specification. Then, we analyze how CSTC can be introduced to the operational environment of the network operator as specified in our objective Q3. We determine that CSTC is able to meet network operator and legal requirements related to conditional access systems. In a further analysis, we investigate communication and computational constraints imposed by the DVB suite of standards. Here, we determine the scalability of CSTC in an operational deployment as intended by Q4. We conclude that bandwidth of approximately 100 kB/s is allocatable for CSTC-related downstream communication toward the STB. In the opposite direction related work suggests that a maximum of 0.5 – 1.0% of the users watching the most popular channel in an IPTV deployment perform channel changes per second. Based on the logarithmic properties of the employed multicast encryption scheme, we assume that computational requirements are satisfiable Moreover, we identify options for further optimization of the multicast encryption scheme we use. We then examine which additional protocols and components are neccessary in order to incorporate CSTC to a common IPTV service architecture. We show that only the channel change signaling protocol and two additional requirements for multiplexers are necessary in order to support CSTC. Existing structures of the current DVB architecture require only four functional components and two protocols to be modified. This is a result of the intentional omission of specifications related to conditional access in the set of DVB standards for security reasons. Finally, we present a prototype IPTV system architecture comprising a headend system and a set-top box component implementing the CSTC model.

CHAPTER 5

SERVICE QUALITY

The subjective user perception of a service directly contributes to the user satisfaction and, consequently, to the acceptability of the service. For this reason, we pursue the question to what extent our approach of CSTC has an influence on the overall TV watching experience of a user in this chapter. At first, we identify technical factors related to IPTV service quality, which generally contribute to the service perception of users. In the next step, we decide whether these factors are affected by CSTC. We then analyze and estimate the potential impact of CSTC on each factor by assuming properties of a common IPTV service architecture. By using and improving our prototype implementation, we devise a system for measuring the actual effect of CSTC on respective IPTV service quality factors. With the aid of our measurement system, we conduct a case study and verify our previous assumptions. In the final step, we analyze the results of our case study and conclude the impact on the user experience.

In general, a user's quality of experience (QoE) regarding the use of a service, on the one hand, consists of factors that are objectively quantifiable. These factors are called quality of service (QoS) factors and relate to general properties of the service, such as responsiveness and reliability, as well as characteristic properties, such as video quality and the responsiveness of the electronic program guide. On the other hand, a user's QoE depends also on factors that are related to human perception referred to as human components [149]. Some of these factors are context, previous experience, expectation, emotional state, attention, motivation etc. For instance, users rate the visual quality of a sequence differently depending on whether it is presented on a high definition TV in a living room or as a

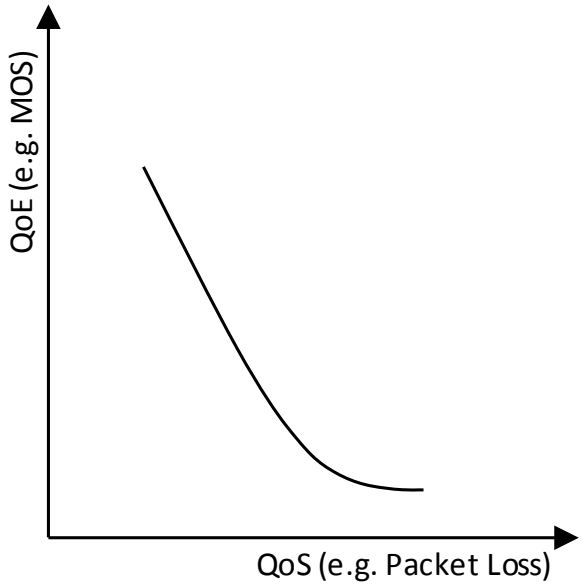


Figure 5.1: Relationship between QoE and QoS

web video on a commodity computer. Nevertheless, QoS and QoE are not independent. In fact, the QoE for some service factor has a nonlinear relationship with the corresponding QoS. This relationship is controlled by the human components. The connection between QoE and QoS is briefly sketched in Figure 5.1 based on [150].

In most standards, QoS factors are attributed to one or more layers of the architecture the standard is concerned with. Here, particular requirements and recommendations are defined for the respective layer in order to achieve a specific service quality. Typically these layers are the transport layer, the service layer, and the application layer. For instance, the QoS factor of video quality has implications for the transport layer since the video data are broadcasted from the headend to the user's set-top box. Consequently, requirements regarding the amount of packet loss have to be defined at this layer. However, the resulting acceptable impairment of the visual quality is considered on the service layer. Furthermore, the impact of the resolution and compression algorithm on the visual quality are considered on the application layer. Factors contributing to QoE are summarized and illustrated in Figure 5.2 based on [149].

As a result of factors related to human components, the overall assessment of the QoE with regard to specific service aspects is a nontrivial task. Many of the human aspects, such as expectation, experience, context, and emotions are difficult to measure and subject to ongoing research. For empirically obtaining quantitative values, sometimes, a test panel consisting of technical experts is consulted in addition to a user survey. Here, participants express their satisfaction with a certain service aspect by rating the quality on a 5-point scale called mean opinion score (MOS). This score originally has been developed for the assessment of telephone transmission quality. According to the MOS, 1 corresponds to bad and 5 corresponds to excellent quality [151]. In this context, an MOS rating of 3.5 is considered as acceptable quality [151]. However, also other scales such as a 9-point, an 11-point, a quasicontinuous scale [152], or a 100-point [153] scale are in use for this purpose. MOS values of different aspects are not necessarily comparable, since they can be

used to describe absolute ratings, comparative ratings or the degree of degradation [151]. Moreover, factors related to human components, such as resembling the experience of watching TV at home, have to be controlled carefully during tests to achieve reproducible results, validity, and, consequently, general statements.

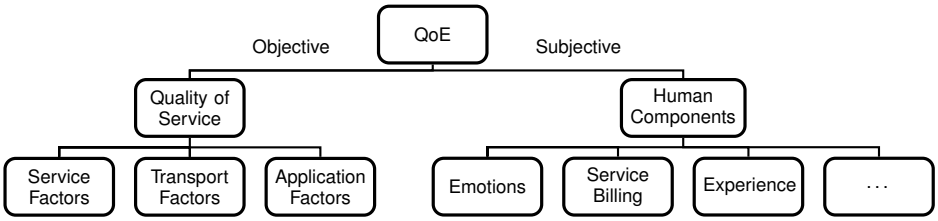


Figure 5.2: Factors contributing to QoE

Accordingly, the assessment of the QoE of some service aspect entails great effort since it is time-consuming and expensive. There is considerable interest in identifying the relationship between one or more QoS metrics and the QoE of some service aspect. This relationship can be used to arithmetically predict the QoE from one or more given QoS metrics. However, the resulting QoE is only valid for the specific assumptions regarding the human components (context, motivation, etc.) that were considered when the QoE was initially determined. When human components are not considered or fully understood, QoE values obtained in this way are not suitable to devise general statements regarding higher order objectives such as acceptability. Nevertheless, a relationship between QoS and QoE can be employed to determine the minimal end-to-end QoS of a system for a given QoE.

In the context of IPTV broadcast services, requirements for QoE are defined by different standardization bodies such as the Alliance for Telecommunications Industry Solutions (ATIS) [154], the International Telecommunication Union (ITU) [149], and the Broadband Forum (DSL Forum) [150]. Respective standards provide recommendations for derived metrics related to QoS factors in order to achieve certain levels or classes of experienced quality. In the following, we will introduce the most common QoS factors and identify the corresponding impact CSTC has on them.

5.1 Quality of Service Factors for IPTV

Generally, QoS factors are grouped regarding some independent high-level aspects such as control, data, usability, etc. [150], according to activities associated with the stages of use of the IPTV Service [154], [155], or according to aspects related to the properties of the IPTV service [149]. Most of the QoS factors that we introduce in the following can be encountered in every standard.

5.1.1 STB Start-Up Time

Boot-up as well as system and service initialization processes contribute to the set-top box start-up time. Service initialization includes the eventual download of firmware and other service-related software updates, such as the update of the VoD offering catalog. Moreover, the initialization and authentication of middleware components, service discovery and selection, parsing and decoding of the electronic program guide (EPG), and other processes

are performed. The STB start-up time starts with pushing the respective button to turn on the STB and ends with the STB being in operational and responsive state presenting the first picture of broadcast data of some tuned channel [156], [157]. In practice, there is additionally a distinction between the start-up from standby and a full start-up when the STB is completely turned off. As a guideline, the STB start-up time from standby has to be in the order of 10 seconds [150].

5.1.2 Audio and Video Quality

The perceived audio and video quality depends on many different aspects. The quality of the display device with regard to display size, resolution, sharpness, contrast, brightness and color fidelity is as important as the viewing environment. Correspondingly, the speaker quality and arrangement is crucial for the perceived audio quality. Moreover, the quality of the footage, the employment of preprocessing and also properties and parameters of the used compression algorithms are essential. Since lossy compression algorithms using psychoacoustic and psychovisual models are employed to reduce the required bandwidth, the baseline quality of the used codec standard as well as corresponding parameter settings are decisive. In particular, the GOP structure, motion vector search range, quantization settings and many other codec settings have to be adjusted for achieving high compression and to accommodate various content types. Furthermore, the target bit rate and subsequent rate control mechanisms for combining different streams have a considerable influence on the target quality. In this connection, a constant bit rate (CBR) leads to a variable quality and a variable bit rate (VBR) leads to constant quality. Audio and video quality is also affected by dependent mechanisms such as the underlying network transport. Packet loss, varying packet latencies (jitter), packet bursts and late packets due to insufficient bandwidth as well as duplicate and out of sequence packets lead to image errors, audible cracks, frozen pictures and in the worst case to black screens.

As a consequence of the aforementioned factors contributing to audio and video quality, corresponding metrics and recommendations are diverse. Aside from MOS values for the perceptual quality of the decoded audio and video data, metrics such as the Peak-Signal-to-Noise-Ratio (PSNR) are used. For assessing the amount of visual impairment using PSNR, the spectral energy of the original uncompressed footage data is compared to the spectral energy of the decompressed data emitted by the user receivers. With regard to effects of the network transport on the audio and video quality, respective metrics, such as IP packet transfer delay (IPTD), IP packet delay variation (IPDV), IP packet error ratio (IPER), IP packet loss ratio (IPLR), Percent IP service unavailability (PIU), and others as well as corresponding recommendations are in use [158].

5.1.3 Audio-Video Synchronicity

Audio-Video synchronicity describes how well the video stream is consistent with the audio stream. In general, human perception is more tolerant of audio that appears after video than audio preceding video due to different propagation velocities of each signal type. For instance, according to standard in [159] that considers audio-video synchronicity in the context of videoconferencing, it is required that the audio stream should not precede the video stream by more than 90 ms and shall not succeed it by 185 ms. For IPTV, even more restrictive constraints are recommended in [150]. Here, a maximum audio lead video time of 15 ms and a maximum audio lag video time of 45 ms is defined.

5.1.4 Channel Change Time

The time period that starts with pressing the button on the remote controller to initiate a channel switch and ends with the first frame of the new channel appearing on the display of the TV is called channel change time. However, this quantity refers only to channel changes to the next higher or lower channel since a direct channel change to a specific channel number involves a certain period of inactivity. This pause is used to allow the user to type in the channel number one digit at a time using the remote controller. As explained previously, IPTV data are generally delivered using IP multicast. But the line on the last mile toward the customer premises features bandwidth only sufficient for the transmission of one channel at a time. Consequently, several network components on the signaling path are involved in addition to processes in the STB during channel switch, Channel change times on other transmission paths for digital broadcast typically range from 2 to 4 seconds for satellite and 1 to 2.5 seconds for cable [150].

Recommendations related to channel change time are mostly aligned with the human perception of time. In this regard, users prefer interactive systems that offer response times less than 1 second [160]. During this time, users have the feeling that they are controlling the interaction with the system and are able to maintain their focus on the current train of thought [161], [162]. When response times exceed 2 seconds users are not able to proceed at their own pace and, consequently, become aware of waiting. This fact causes dissatisfaction since users feel held back by the system. Their short-term memory starts to fade and the chain of thought is interrupted [163]. Finally, the number of transactions decreases considerably when system response times exceed 4 seconds and even more abruptly beyond 12 seconds [164]. As a consequence, it is recommended that channel change times should be targeted in the order of 1 second [165] [150] and should amount to a maximum of 2 seconds [150].

5.1.5 Transmission Delay

The delay between the time an event happens on live broadcast or is observable at the headend and the time this event is displayed on the TV screen is called transmission delay. Varying transmission delay is called peer lag or playout difference and can be observed when users receive broadcast content at different times due to the use of different transmission paths, for instance, DVB-S and IPTV. This usually becomes evident on sports events when some users celebrate a goal while other users watch footage preceding the goal. Generally, playout difference is the result of a varying number of different involved components and links used for each transmission path. Usually, corresponding standards are concerned with a constant transmission delay in order to necessitate small buffers. Consequently, instead of playout difference, rather transmission delay is considered as a QoE factor in some standards. Since in some situations such as in the referred sports event, playout difference is annoying for users, there is an ongoing discussion of the feasibility and technical aspects of solutions for synchronizing different transmission paths [156].

5.1.6 Quality of other IPTV-related Services

Other QoE factors consider accompanying services such as the provision of metadata, operating menus and user interface, browsers, and content navigation. Here, usability and responsiveness aspects are examined. In addition, metadata such as subtitles, Teletext, and

the electronic program guide (EPG) are taken into account. Here, font support, availability of character sets, and initialization and response time [150], [149] are checked.

5.1.7 Higher-Order Service Characteristics

Some QoE factors are related to technical properties of the IPTV system but also feature properties of higher order service objectives. For instance, generally, the distortion of a picture is associated with video quality. However, in case the distortion is so severe that the picture becomes unintelligible or completely disappears, the impairment becomes more related to service reliability and, consequently, to availability and dependability. In this context, picture freezes and blank screens up to a duration of 10 seconds are considered as quality impairment. The impairment is considered as service outage when this time frame is exceeded. Recommendations for the reliability of an IPTV service are based on respective experiences with satellite and cable networks, which feature a reliability of more than 99.99%. This rate corresponds to a service loss of 53 minutes per year [150]. Other higher-order service factors are functional correctness and usability but also impairments related to charging and billing. Here, respective metrics are used, for instance, to identify the overcharging probability or the billing integrity. The latter describes whether the presented bill correctly reflects the type and duration of service use [155]. In addition, nontechnical factors affect the users' QoE of a service such as the manner of the service provider during the conclusion and cessation of the contract or in cases the service requires repair.

5.1.8 Factors affected by CSTC

Considering the previous discussion of QoE factors, we are able to identify two QoE factors that are affected by CSTC:

1. Channel Change Time and

2. Transmission Delay

CSTC affects channel change time since additional operations are performed during the channel switching process. Other than in conventional IPTV, the channel change request has to be signaled up to the headend system. Subsequently, the request has to be processed and corresponding entitlement information is included in the broadcast stream. Similarly, CSTC affects transmission delay due to the processing of requests and the involved delay in the headend. Nevertheless, we don't examine the effects on transmission delay since current solutions involving playout synchronization suggest that remedies are not a matter of design decisions concerning a single system but rather an effort involving several heterogeneous systems.

Hence, for further discussion and current approaches, we refer to [166] and [167]. In the following, we investigate the impact of CSTC on the channel change time. For this purpose, we first analyze the channel switching process of conventional IPTV systems and estimate the average channel change time for an IPTV system supporting CSTC. In the next step, we verify this channel change time by performing a measurement on our prototype implementation. Finally, we analyze our results and project consequences on the users' QoE.

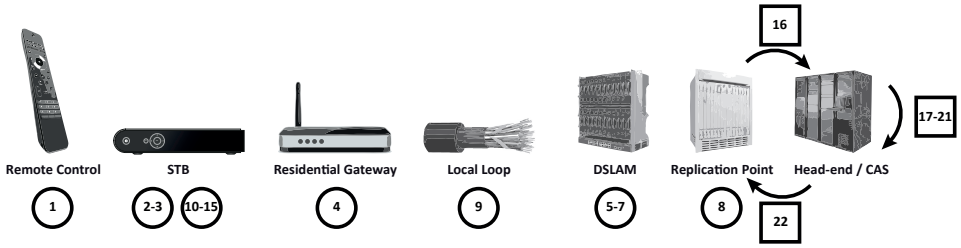


Figure 5.3: IPTV Architecture Components Involved in the Channel Switching Process

5.2 Channel Switching Process and Average Times

Channel switching starts by pressing the corresponding button on the remote control and ends when the picture of the new channel is displayed. According to [168], a TV viewer switches channels 25 times a day on average. In conventional analog cable TV, in off-the-air broadcast as well as in digital broadcast transmissions such as DVB-C or DVB-T, all transmitted channels are available on the TV set or on the STB simultaneously. Channel switching, therefore, is accomplished just by tuning to the desired frequency.

In contrast, channel change time in IPTV is relatively long and often regarded as a disturbing factor. This is attributed to the limited bandwidth of subscriber lines, which inhibits a simultaneous reception of several channels. For this reason, IPTV providers transmit their channels only up to certain points in their network known as replication points, see Figure 5.3. A further transmission of any channel depends on the desire of some user to watch this channel. Consequently, channel change time includes several delay components caused by actions in different components of the IPTV system as illustrated in Figure 5.3.

Related work on IPTV channel change time lists up to 15 delay components; see [169] and [170]. Table 5.1 summarizes all these components according to the findings in [169], [170]. For illustration, delay component numbers are given in Figure 5.3 to refer to the system component causing each delay component. The numbers 16 – 22 refer to delay components caused by CSTC and will be treated in Section 5.3. In the following, a brief description of the channel switching process with reference to the delay components is given. A delay component is abbreviated as DC followed by its number. For instance, DC-1 refers to the remote control to STB delay.

Whenever a user switches a channel utilizing the remote control, the STB receives an infrared signal and decodes it, which is the first source for the delay (DC-1). Depending on the user command, the STB then generates one message containing the command for leaving the multicast group of the currently viewed channel (DC-2) and another message for joining the multicast group of the desired channel (DC-3). These messages are processed by an IPTV-enabled residential gateway, for instance, a home router, which features an IGMP-Proxy. This proxy manages and passes group management messages to the next adjacent component in the operator's access network (DC-4). In case DSL is employed as the access technology, this component is the Digital Subscriber Line Access Multiplexer (DSLAM). The DSLAM aggregates network traffic from multiple lines and processes the group management messages (DC-5 and DC-6). If the media data of the desired channel is available at this point, the DSLAM performs the channel switch and starts to deliver these media data (DC-7). Otherwise, the DSLAM sends a request to the replication point, which replies supplying the media data of the desired channel (DC-8). On its way to the user,

No.	Delay Component	[169]		[170]		Source
		Avg. (ms)	Max. (ms)	Avg. (ms)	Max. (ms)	
1	Remote Control to STB IR Delay (IR Decode)	-	-	5	10	STB
2	STB Sends IGMP Leave		10	2.5	5	STB
3	STB Sends IGMP Join		10	2.5	5	STB
4	IGMP-Proxy in DSL Router	-	-	5	10	Residential Gateway
5	DSLAM Gets IGMP Leave		10	2.5	5	DSLAM
6	DSLAM Gets IGMP Join		10	2.5	5	DSLAM
7	DSLAM Switches Streams Ch1-Ch2	30-50	50	5	10	DSLAM
8	Multicast PIM-SSM Join at Replication Point	20-60	200	-	-	Core/Aggregation Network
9	FEC/Interleave Latency of DSL	10	10	20	20	DSLAM
10	Network Dejitter Buffer	50-200	300	60	100	STB Network Unit
11	Wait for and Parse PAT/PMT	125	100-500	-	-	STB MPEG Decoder Buffer
12	Wait for ECMs and Parse	125	100-500	-	-	STB MPEG Decoder Buffer
13	Wait for Next Occurrence of I-Frame (RAP)	250	500	250	500	STB MPEG Decoder Buffer
14	Receive I-Frame into MPEG Buffer	750	2000	100	300	STB Network Unit
15	Decode I-Frame	50	50	10	10	STB MPEG Decoder
	Total Average (ms)			**1255**		

Table 5.1: Delay Components Contributing to Channel Change Time

media data underlie delays in the subscriber line, namely, in the local loop due to forward error correction and interleaving (DC-9). After changing the channel, the STB buffers media data in order to compensate the network jitter, that is, the varying delay of the incoming packets. This buffering adds further latency (DC-10). As soon as enough packets arrive in the buffer, the STB starts processing. First, reference data referred to as program allocation table (PAT) and program map table (PMT) must be captured. As this data are only sent in designed time intervals, some waiting time may be necessary (DC-11). When the media data are encrypted using a CAS in the HES (see Figure 5.3), the STB must extract the entitlement control messages (ECMs), which contain information for computing the content decryption key (DC-12).

As discussed previously in Chapter 3, media data are encoded into frames and transmitted in compressed form to save bandwidth. Only some frames, denoted as I-Frames, include full pictures. Other frames only include partial data, which must be extended using I-Frames. To start decoding, therefore, the STB must wait for an I-Frame to arrive (DC-13). According to [170], I-Frames contain 20-60% of image information within the media stream. Hence, the transmission of these frames additionally takes considerable time (DC-14). Having all required data, the STB initiates the decoders to process the media data and to generate the image and audio signals for the TV set (DC-15). From this analysis and based on averaging the data given in [169] and [170], we estimate a total average of 1255 ms for the channel change time.

In the following, we will take a closer look at the intricacies of delay components DC-10, DC-13, DC-14, and DC-15 by using the illustration presented in Figure 5.4. For our following examination, we assume an exemplary media stream that is compressed according to the H.262 [85] standard in the main profile at main level (MP@ML). The resulting stream has a maximum bit rate of 15 Mb/s, in which the video has a resolution of 720×576 pixels, a frame rate of 25 Hz, and a color subsampling ratio of 4:2:0. Since at a frame rate of 25 Hz each frame is presented for 40 ms and the media stream features a GOP length of 12, the resulting inter-RAP duration is 480 ms. Moreover, we assume that the data volume ratio of B, P, and I frames is $1 : 1.5 : 3.75$, respectively. Although the given ratio is sufficient to specify corresponding transmission times, for the purpose of illustration and referring

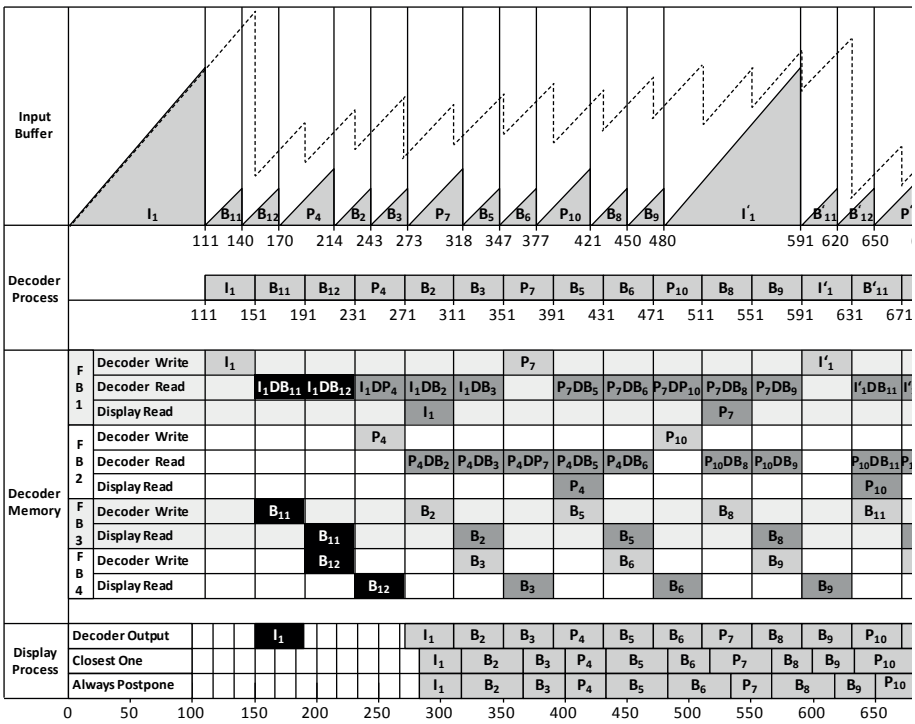


Figure 5.4: Input and Decoder Buffer States during Decoding and Display Process

to minimum bit rates given in [149], we assume an actual bit rate of 1.25 Mb/GOP. Consequently, I-Frames have a constant size of 36 kB, P-Frames have a size of 14.4 kB, and B-Frames have a size of 9.6 kB. Consequently, the media stream requires a line having a capacity of more than 2.6 Mb/s since additional data such as audio, service information and other metadata has to be transmitted too. Regarding the computational performance, we assume a worst-case decoder. This means that the decoder has to process frame data at least at a speed that corresponds to the duration each frame is presented on the display. As we assume that our media stream features 25 frames per second, the decoder is granted a processing time of 40 ms per frame. Finally, we assume a display refresh rate of 60 Hz for the connected TV set, so that a new frame is presented every 16.6 ms. The aforementioned assumptions roughly correspond to properties, which can be encountered in a typical IPTV deployment. Certainly, our example is heavily idealized since usual media streams feature not only a variable GOP length in order to accommodate to scene changes but also a varying bit rate leading to a different amount of data for each frame. In addition, broadband connections feature varying bandwidth and delay (jitter) to a certain extent. Nevertheless, we abstract from these variabilities in order to facilitate understanding.

5.2.1 Transmission Delay (DC-14)

In the upper section of Figure 5.4, the state of the input buffer of the STB is presented. Gray triangles indicate levels of incoming frame data that arrive at the input buffer. The labels in the triangles indicate the frame type (I-, B-, or P-frame). Since the frames arrive in transmission order, the display order is indicated by the frame label index n, for instance, I_n.

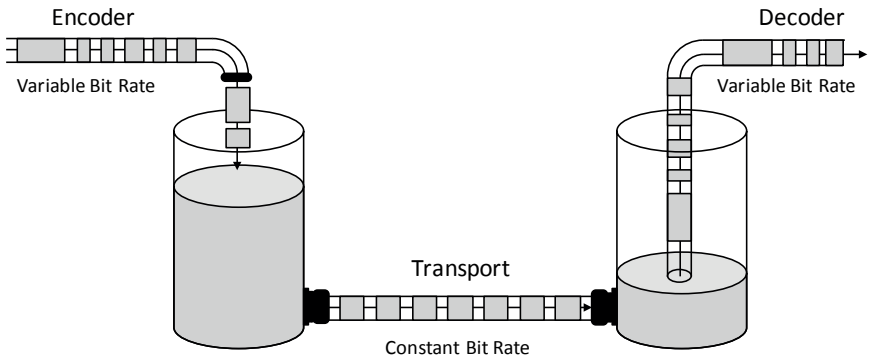


Figure 5.5: Video Buffers for Encoder and Decoder

Moreover, the dashed line shows the overall level of the input buffer. As we can observe, a considerable time is spent on the transmission of the initial data to start the decoding process, although we assumed an optimistic ratio for the data amount consumed by I-Frames (ca. 20% of total GOP). This characteristic is due to the linear nature of broadcast where data are transmitted in near real-time. As a consequence, it is not possible to shorten this delay, for instance, by sending out the initial data in a burst, without further measures. Not shown in Figure 5.4 but mentioned in Table 5.1 is another usual delay caused by buffering in order to remove jitter (DC-10). To compensate variations in the arrival time of packets and to avoid a later shortage of data, the decoding process is suspended until the input buffer reaches a certain level. This step usually delays decoding for 100 to 500 ms [150].

5.2.2 Initial Buffer Delay (DC-14)

The initial buffer delay is a further cause for a delayed start of the decoding process and is implied in DC-14. This delay is related to synchronization and rate control. As we learned, the encoding process results in data featuring a variable bit rate (VBR) due to the use of different frame types and the dynamic nature of the content. However, the burstiness of this data has to be controlled and smoothed in order to save resources on the transmission network and to avoid packet arrival intervals that are too diverse.

For this purpose, a buffer depicted in Figure 5.5 ([171]), a so-called leaky bucket, is placed at the output of the encoder in order to create output that features constant bit rate. In order to recover the bursts and to ensure that the decoder reads corresponding sections of the stream at the same rate at which the encoder wrote them, a second corresponding buffer is required in front of the decoder. Consequently, during operation, these two buffers feature complementary levels and the sum of both levels is constant. In general, the constant sum of buffer sizes represents the maximum time contributed to the channel change delay by this mechanism. The encoder has to foresee the corresponding buffer levels at the decoder to anticipate potential buffer underflow and overflow. For instance, in cases where it becomes apparent that the remaining decoder buffer is exceeded by the encoder output due to burstiness, the encoder adjusts corresponding parameters in order to balance buffer levels using a feedback loop. Therefore, the operator has to trade off buffer size and, consequently, channel change time against picture quality when fixing the aggregate buffer size at the encoder.

Furthermore, the notion regarding the extent and duration of the smoothed bursts has to be conveyed. Without this information, the decoder would run the risk of buffer underflows by taking data too early from the buffer leading to a situation where subsequent frames would arrive later than their time of presentation. In particular, when a channel switch occurs an initial buffer delay prevents the decoder from reading from the buffer and starting the decoding process until the amount of data reaches a certain limit. This procedure is followed regardless of the presence of a random access point (RAP) in the input buffer. As we learned in Chapter 3, a common time is established between the headend and the STB by using a phase locked loop (PLL) and time stamps in the transport stream called program clock reference (PCR). After the internal clock of the STB has been set, additional time stamps called decoding time stamp (DTS) and presentation time stamp (PTS) are used to determine the start time for the decoding process. In particular, the STB regularly compares the DTS/PTS times of the frames in the buffer with its internal clock in order to determine the time to start decoding. In this connection, PTSs and DTSs share the same time base as PCRs and are embedded into the packetized elementary stream (PES). Naturally, the initial buffer delay depends on the designated buffer settings in the encoder and, furthermore, on the current buffer level at the decoder. Following an analysis in [171], it can take up to 2 s until a frame in the decoder buffer becomes ready to be processed.

5.2.3 Reordering Delay (DC-13)

In Chapter 3 we learned that frames are ordered differently depending on the purpose of their processing. In particular, in encoding and display order B-Frames contain references to temporally preceding as well as successive frames. Consequently, for transmission, the GOP is reordered in such a way that all frames that the B-Frames depend on appear prior to the B-Frames themselves. In this way, a delay that occurs due to the subsequent arrival of required referenced frames is avoided. Unfortunately, this foresighted approach is undone by another approach we became acquainted with Chapter 3, namely, open GOPs. In contrast to closed GOPs, open GOPs allow frames at the edges of a GOP to make references to neighboring GOPs in order to preserve bandwidth. In this way, B-Frames of the previous GOP are interleaved with the I-Frame and the P-Frame of the subsequent GOP as shown in Figure 5.4. Consequently, on channel change, the STB still experiences a delay that is associated with the transmission of 1 P-Frame and 2 B-Frames. Furthermore, the data contained in the 2 B-Frames cannot be used since they temporally precede the I-Frame and ultimately require data from the previous I-Frame in order to become decodable. In order to illustrate the situation in case no channel change would have occurred, the corresponding frames are shown as black boxes with white caption in the decoder memory and the display process. Confusingly, this delay is often referred to as reordering delay although the frames don't require reordering but rather wait. In general, the bandwidth saving justifies the higher channel change time so that most operators use open GOPs.

5.2.4 Decoding and Display (DC-15)

In our analysis, we assume the worst-case decoder that is able to process incoming data just as fast as it is displayed. Since the GOP we consider contains 2 consecutive B-Frames, the decoder requires at least 4 different frame buffers. These frame buffers and their allocation over time is depicted in Figure 5.4. Letters in the captions indicate frame type. Numbers in the subtext indicate display order. Light-gray boxes indicate currently decoded frames that are processed by the decoder and subsequently will be written to the corresponding

Delay Variable	Delay Component
$t_{network\_STB\_RP}$	1 + 2 + 3 + 4 + 9 + 5 + 6 + 7 + 8
$t_{network\_RP\_STB}$	9 + 14
$t_{processing\_STB}$	10 + 11 + 12 + 15
t_{RAP}	13
$t_{network\_RP\_HE}$	16, 22
$t_{processing\_HE}$	17 + 18 + 19 + 20 + 21

Table 5.2: Delay Variables

frame buffer. Dark-gray boxes indicate read operations of a frame either for display or for use as reference data from another already decoded frame. The decoded frame type and display order in subtext is preceded by the used frame type and display order in subtext and separated by the letter D. As described previously, black boxes show the processing of frames in case no channel change would have taken place. However, due to channel change, the processing of frames arriving after the first I-Frame is delayed, so that the display of the I-Frame is also deferred in order to avoid the impression of a stuck video.

Since the refresh rate of the display device differs from the frame rate of the incoming video, the display process has to make adjustments. In our example in Figure 5.4, we assume prevalent values of 25 frames per second for the video frame rate and 60 Hz for the display refresh rate. Usually, producers of TV sets and display manufacturers employ proprietary algorithms featuring different complexity in order to extrapolate and display pixels that have not been received for achieving deinterlacing and seamless rate adaptation. This processing adds further delay to the channel change time. In our example, we illustrate two simple methods for rate adaptation, namely “closest one” and “always postpone”. “Closest one” adjusts the display duration for the corresponding frame to the closest time boundary of the output refresh rate. In contrast, “always postpone” displays the corresponding frame in the next time interval once it has exceeded the subsequent time boundary of the output refresh rate.

In our example in Figure 5.4, the first frame can be displayed after 271 ms even if the user changes at the best possible point in time for receiving the first I-Frame of the destination channel. This delay is caused by waiting for required data and is referred to as transmission delay. In the worst case, this duration is increased by the full GOP duration, which in our example in Figure 5.4 is 480 ms. Thus, in case the user has just missed the random access point of the destination channel the delay totals to 751 ms. Further delays are contributed by the decoding and display processes. The decoding process can only take 40 ms in the worst case whereas the display process adds an unknown amount. In the best case, however, the display delay is the inverse of the refresh rate. Substantial additional delays not considered in our example relate to the characteristics of the underlying network. Some of them are the delay of group membership communication, dejitter delay and initial buffer delay. These delays are based on the extent and quality of the network infrastructure and require corresponding decisions of the operator. In this regard, these delays can dynamically add up to additional 2.5 s to channel change time.

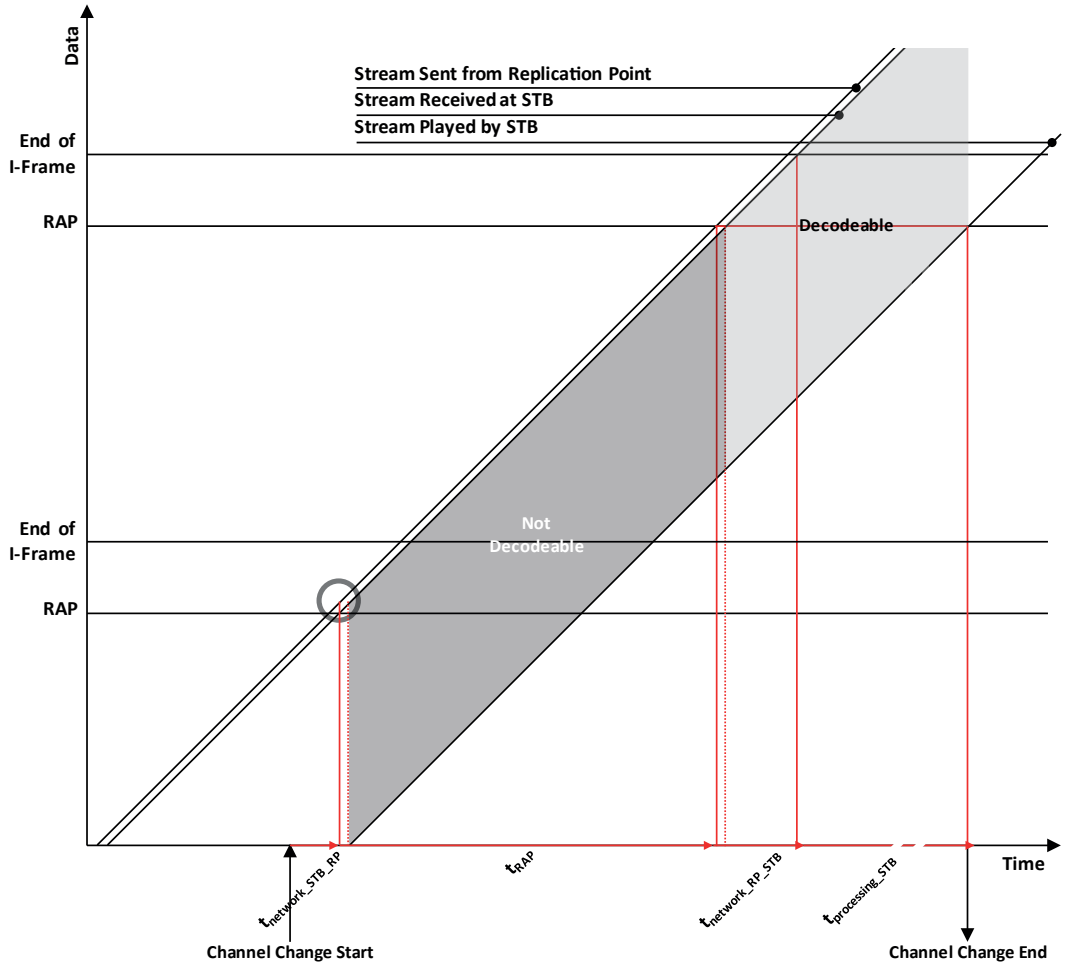


Figure 5.6: Channel Change Time in Conventional IPTV

5.2.5 Relation of Delay Components

For our further consideration of the channel changing process, we will analyze the relations between introduced delay components and their contributors. Since the high number of delay components makes traceability and comprehension difficult, we first merge related delay components to delay variables in Table 5.2. Here, $t_{network\_STB\_RP}$ represents all delay components that are directed toward the operator network. These delay components include all actions starting from the button press to indicate channel change up to the IP multicast group join for the delivery of data from the destination channel at the replication point. Conversely, $t_{network\_RP\_STB}$ specifies delays from the replication point to STB. Please note that $t_{network\_STB\_RP}$ and $t_{network\_RP\_STB}$ involve different delay components since $t_{network\_STB\_RP}$ triggers the channel switching whereas $t_{network\_RP\_STB}$ relates to network and interleaving latency as well as transmission delay. All delays related to the processing in the STB are included in $t_{processing\_STB}$. These delays comprise dejitter and initial buffer delay as well as delays associated with the decoding and display process.

However, the delay associated with the occurrence of the subsequent random access point is assigned to an additional variable t_{RAP} since it is not constant and requires differentiated consideration.

In the next step, we use delay variables in order to illustrate the worst-case channel change time by considering related parties in Figure 5.6. In this connection, we use delay values assessed so far in order to create a simplified presentation with corresponding dimensions. Essentially, the sent media data, which extends across the replication point, as well as the input and the output of the STB, is assigned to the elapsed time. Additionally, the random access points and the end of the I-Frames are indicated. The channel switch starts by sending corresponding group management requests toward the replication point taking time $t_{network\_STB\_RP}$. The illustrated situation and in particular the gray circle suggest that the specific time of the channel change start resulted in the fact that the STB has just missed the next RAP. Consequently, the STB starts to receive data from the replication point beginning with the time marked by the first dashed line. However, since only referenced data are received, no frame is decodable. A whole GOP duration (t_{RAP}) later the RAP passes the replication point and arrives at the STB as indicated by the second dashed line. Accordingly, the STB starts to receive decodable data. However, considerable time ($t_{network\_RP\_STB}$) passes until the first frame is transmitted completely. Thereafter, the STB is able to proceed with further processing steps taking time $t_{processing\_STB}$. Subsequently, the channel switching process is completed by displaying the first frame. As a result of our analysis we are able to express the channel change time more formally in Equation 5.1:

$$t_{CCT} = t_{network\_STB\_RP} + t_{network\_RP\_STB} + \mu \times t_{RAP} + t_{processing\_STB}, \quad \text{where } \mu \text{ is the expected value of the distribution of GOP lengths.} \tag{5.1}$$

5.3 Impact of CTSC on the Channel Switching Process

In this section, we discuss 7 additional delay components introduced by CSTC. These contribute to increased channel change time and are given in Table 5.3. Please note that for the purpose of simplified presentation, the delay components DC-17 – DC-21 denoted in Table 5.2 are combined in delay variable $t_{processing\_HE}$.

5.3.1 Channel Change Request Transmission Delay (DC-16)

In contrast to conventional pay-TV systems, CSTC requires that channel change requests are end-to-end. This means that requests are sent from the user changing the channel to the CAS at the headend. The CAS, in particular the key management system (KMS), is responsible for granting this request by performing the rekeying process described in Section 4.3. Recall, however, that channel switching itself also generates group management messages such as join and leave requests, which are processed at the replication point, as shown in Figure 5.3 and Table 5.1. Due to embedding the rekeying process into the channel changing process, our approach makes arrangements for additional requests that are processed by the CAS at the headend. As a consequence, the first additional delay component is related to further forwarding these requests from the replication point to the headend. The latency for sending such a message highly depends on the infrastructure of the network operator and is rather difficult to assess.

For our estimation, we assume that the headend is affiliated to the core network and the replication point is the connecting link between the aggregation and the distribution network in the infrastructure of the operator. We further suppose that the delay of the router representing the replication point is already considered by DC-8. Thus, the resulting channel change request transmission delay is the sum of the delays induced by the routers in the distribution and core network in addition to the propagation delay of the network signal. For the purpose of identifying router latencies, we refer to [172]. Here, the latency for routers in the distribution network is estimated to be 3 ms and for routers in the core network to be 2 ms. The discussion of propagation delay is particularly important for large networks that extend to great distances. Since the replication point is situated at the edge of the aggregation network, we assume that still a substantial portion of the line distance remains on the way to the core network and accordingly to the headend. For estimating the propagation delay, we assume that the core network of a national service operator is located in the geographical center of a country. Moreover, we use the calculation scheme given in [173]. Exemplary results suggest that the propagation delay for Germany takes 1.7 ms and for the U.S. 9.7 ms. For further considerations, we therefore rate the total channel change request transmission delay to be between 7 and 15 ms.

5.3.2 Channel Change Request Deadline Delay (DC-17)

Clearly, setting up a rekeying message is one of the most critical operations in group rekeying because of the scalability problem mentioned previously. Consequently, we investigate the delay associated with this process soon. The impact of this delay component, however, becomes noticable earlier. As we learned previously in Chapter 3, one way to counter the scalability problem is to use batch processing. As a result, at certain points in time, denoted channel change request (CCR) deadlines, incoming requests are not processed in the current batch but deferred to the next batch interval. In our previous consideration of channel change times for conventional IPTV the arrival time of a group management request at the replication point determined whether a GOP duration was added to channel change time. When CSTC is used, however, a GOP duration is added to channel change time depending on the point in time when a request arrives at the headend. Consequently, DC-17 supersedes DC-13, which previously considered the discussed delay. The CCR deadline delay is explained graphically in more detail in Figure 5.7 at the end of this section.

5.3.3 Channel Change Request Processing Delay (DC-18)

After receiving the channel change request, the key management system (KMS), as a component of the subscriber authorization system (SAS) in the CAS, performs rekeying starting with the generation of the rekeying message, see Section 4.3. A complete rekeying solution with and without hardware support for a group of 2^{17} members is presented in [174]. The hardware-supported solution, denoted as rekeying processor, takes about 4 ms to construct the rekeying message. In contrast, the software-based solution takes approximately 55 ms.

5.3.4 ECM Alignment RAP Delay (DC-19)

In the next step, the rekeying message is formatted according to [100] for transmission. An entitlement control message (ECM) is created and subsequently included at a particular position in the stream. We described this approach referred to as alignment in Section 4.4.2.2.

No.	Delay Component	Value
16	Channel change request transmission from replication point to headend	7 – 15 ms [172],[173]
17	Delay associated with the channel change request deadline (KMS batch interval)	0 – t_{GOP} (480 ms), supersedes DC-13.
18	Processing of channel change request by KMS in the CAS	55 ms (software solution) or 4 ms (rekeying processor) [174]
19	Alignment of ECM with RAP	0 ms, when buffering is used
20	Transmission delay of ECM	0 – 100 ms
21	Processing of ECM at STB	0 – 5 ms, estimation
22	Media transmission from headend to replication point	7 – 15 ms [172],[173]
	Estimated total average	**143 ms**

Table 5.3: Delay components added by CSTC

In particular, the multiplexer component in the headend inserts an ECM at such a point in the stream that receiving STBes are able to receive (DC-20) as well as parse and process (DC-21) it before the next RAP appears. This alignment is necessary since the stream is encrypted with the content key starting from the position of the RAP. The content key in turn is conveyed by using the corresponding ECM. Consequently, ECMs have to be placed prior to the subsequent RAP, which usually incurs delay when processed in real-time since the multiplexer has to wait for it to appear. By creating a buffer and delaying the output of the stream, however, this delay can be reduced. Aside from increased implementation complexity, the only disadvantage of this approach is that it is implemented at the expense of playout delay. Considering the QoE factor related to playout difference we introduced in Section 5.1 this approach could increase playout difference and degrade the QoE. Accordingly, we assume that the ECM alignment delay is removed by employing buffering.

5.3.5 ECM Alignment Transmission Delay (DC-20)

As suggested in the discussion of the ECM alignment RAP delay (DC-19), the insertion of the ECM takes a considerable time. However, this delay depends on the size of the ECM and on the total bit rate of the stream. Since we determined an upper bound for the data volume of key update information that is conveyed over the transport stream in Section 4.3.1.3, we are able to calculate the worst-case transmission delay. Assuming a worst-case transport stream bitrate of 3.2 Mb/s and key update information to the amount of 100 kB/s a maximum delay of 100 ms incurs.

5.3.6 ECM Alignment STB Processing Delay (DC-21)

Another delay component hinted during the discussion of the ECM alignment RAP delay (DC-19) is the delay due to processing of the ECMs in the STB. Since this delay is taken into account during the alignment process in the headend, it does not interfere with the timing requirements at the STB. In this respect, this delay component is different from

DC-12, where waiting time incurs at the STB. When CSTC is used, the delay associated with content key acquisition from the ECM is considered when the channel change request (CCR) deadline is fixed at the headend. Even though this delay depends on the ECM size and the employed algorithms for key management, according to the approach discussed in Section 4.3.1.3 a small number of simple operations are performed. Considering the limited computational performance of STBes we estimate that the STB processing delay is in the order of 5 ms.

5.3.7 Media Propagation Delay (DC-22)

The final additional processing step introduced by CSTC is related to the propagation of the fully processed media data toward the replication point. This delay can be taken as the same for transmitting the rekeying request from the replication point to the headend (DC-16). Thus, an average value of 7 to 15 ms will be assumed.

5.3.8 Relation of Delay Components

In the following we analyze the relations between the newly introduced delay components related to CSTC and their contributors. For this purpose, we merge related delay components to delay variables presented in Table 5.2. The delay associated with forwarding of channel change requests from the replication point to the headend and vice versa amounts to the same value and thus is mapped to delay variable $t_{network\_RP\_HE}$. Moreover, the offset between CCR deadline and RAP represents the complete delay of processing in the headend and contains DC-17 – DC-21. Consequently, these delay components are merged to delay variable $t_{processing\_HE}$.

Next, we illustrate the worst-case channel change time by considering related parties in Figure 5.6. For this purpose, we use delay values discussed in Table 5.3 in order to create a presentation with corresponding dimensions. Compared to our previous analysis of channel change times in conventional IPTV in Figure 5.6, we see that an additional party, namely, the headend, is involved in the channel changing process.

Upon initiating channel change, a request related to group management is forwarded to the replication point and incurs delay to the amount of $t_{network\_STB\_RP}$. An additional request is further forwarded to the headend, which takes time $t_{network\_RP\_HE}$. By the time the channel change request reaches the headend, first data of the newly switched channel becomes available at the STB since we assume that $t_{network\_RP\_HE}$ is equal to $t_{network\_RP\_STB}$. However, due to the lack of the corresponding content key the stream cannot be decrypted by the STB.

As highlighted by the gray circle, the request arrives at the headend just when the channel change request deadline has passed. As a consequence, the processing of the request is delayed by the amount of one GOP duration t_{GOP} as a part of the overall headend processing time $t_{processing\_HE}$. Subsequently, the request is processed by the KMS and an ECM is created. The ECM is inserted into the transport stream according the considerations regarding alignment we discussed previously. Next, the media stream is transmitted to the replication point taking time $t_{network\_RP\_HE}$ and further forwarded to the STB taking time $t_{network\_RP\_STB}$.

Since the ECM has been embedded into the transport stream prior to the RAP, at this point the STB has already obtained the corresponding content key and starts to decrypt the stream. Nevertheless, data of the first frame is still being received by the STB. In the following, the STB performs necessary steps associated with delay variable $t_{processing\_STB}$

completing the channel switching process. Concluding our analysis we are able to express the channel change time for CSTC with respect to regular channel change time in Equation 5.2

$$t_{CCT\_CSTC} = t_{CCT} + 2 \times t_{network\_RP\_HE} + t_{processing\_HE}. \quad (5.2)$$

Referring to the results of our analysis the following important conclusions can be drawn:

1. The CTSC approach potentially worsens the channel changing time by approximately 10%, depending on various aspects discussed in this section.

   Although the additional delays are to some extent of dynamic nature, they don't depend on the underlying media data and its related dynamics.

2. Considerable contribution to the channel change time comes from the size of the ECM, which in turn depends on group variations of the managed channel.

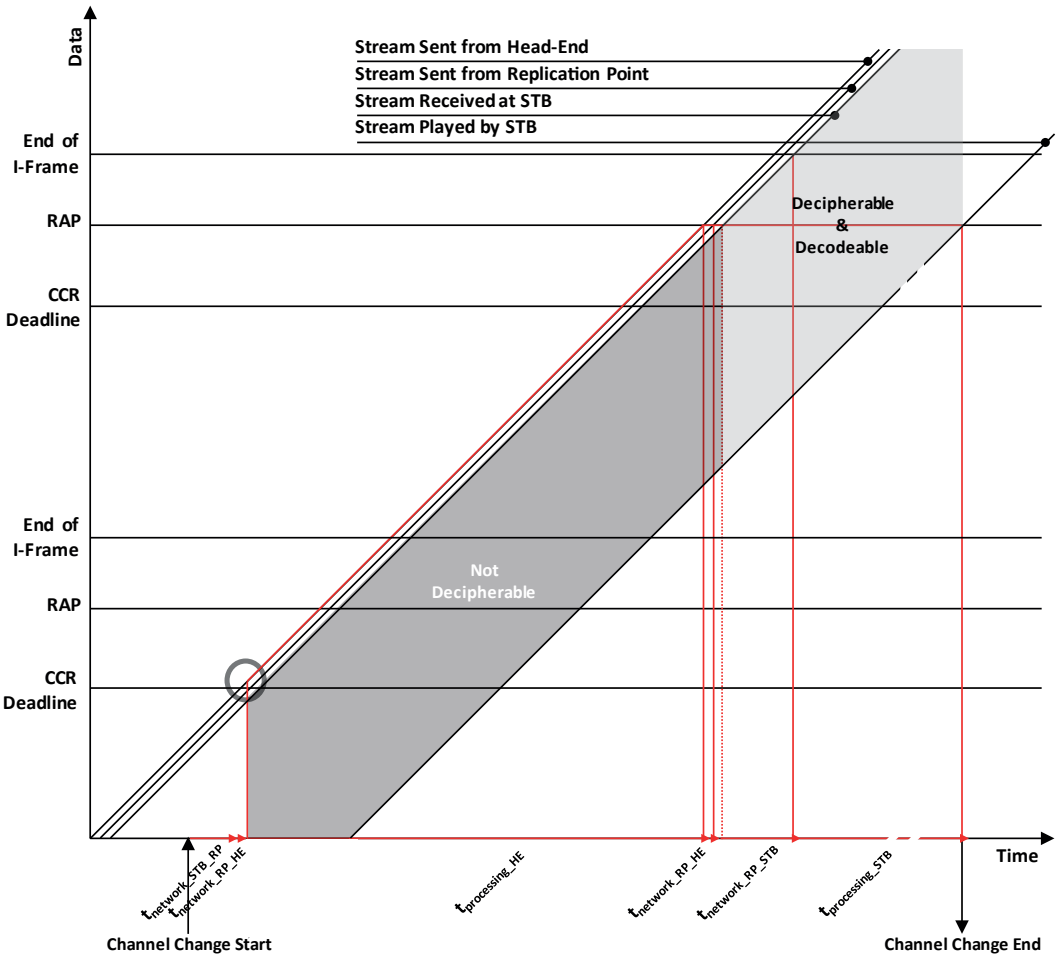


Figure 5.7: Channel Change Time for CTSC

3. The role of channel change processing delay (DC-18) so far is unclear since the acquired values from [174] relate to a worst-case consideration of a single leaving user.

   In addition, measurements involve operations, such as hashing and digital signing, which are unnecessary for our purpose.

For pay-TV channels with a large number of viewers, who feature highly dynamic behavior, it should be assumed that many users may switch to or from the same channel simultaneously. This results in multiple rekeying overhead for the CAS. To resolve this problem batch rekeying can be deployed as suggested in Section 4.3.1.3. In this rekeying mode, join and leave requests of users for some channel are collected for a fixed period of time triggering some computationally cheap operations. Only at the end of every batch period the computationally expensive rekeying process is performed once. Thus, batch rekeying can reduce the computing overhead on the CAS and minimize the number of rekeying messages delivered over the network considerably. In order to assess the channel change processing delay in the context of batch rekeying and, furthermore, verify our assumptions regarding channel change times in the next section, we specify a measurement system.

5.4 Design of a Channel Change Time Measurement System

As we detailed in the previous sections, additional actions are performed during the channel switching process when CSTC is used. We defined the channel change time as the period that starts when the user presses the up/down button on the remote control and ends when the first frame of the corresponding paid channel appears on the screen. However, when the user moves to a paid channel by editing its number using the remote control, the channel change time starts when the built-in editing pause has elapsed. Note that the differentiation of these two cases (that is, pressing up/down button and editing the channel number) is irrelevant for the performance estimation because the editing pause is usually not considered.

For a reliable evaluation of the system behavior and an accurate estimation of the channel change times, we incorporate the proposed CSTC system into an appropriate test environment. This test environment simulates the behavior of real users and allows for an accurate acquisition and evaluation of timing data. Our test environment for broadcasting n channels is illustrated in Figure 5.8.

Usual deployments of IPTV services provided by Tier-1 service providers feature a wide network, multimillion STBs, and several regional headends. Since we are not able to instantiate such a high number of set-top boxes, we have to source the functionality of components responsible for sending channel change requests out to a dedicated component. In our test environment we call this component the Workload Generator (WG). The WG simulates the users' behavior by sending the combined number of channel change requests to the headend system. The functionality of components responsible for receiving data remains in the STB. That means the STB decrypts, decodes, and displays the incoming stream. Consequently, each STB represents all users watching a particular channel. Therefore, we instantiate the set-top-box component n times in order to simulate a broadcast with n channels. This configuration is appropriate for streaming with the use of IP multicast since every member of a group receives the same data.

In our measurement setup, we run the WG and the STB components on the same system, in order to avoid clock offsets and synchronization issues among different systems, see

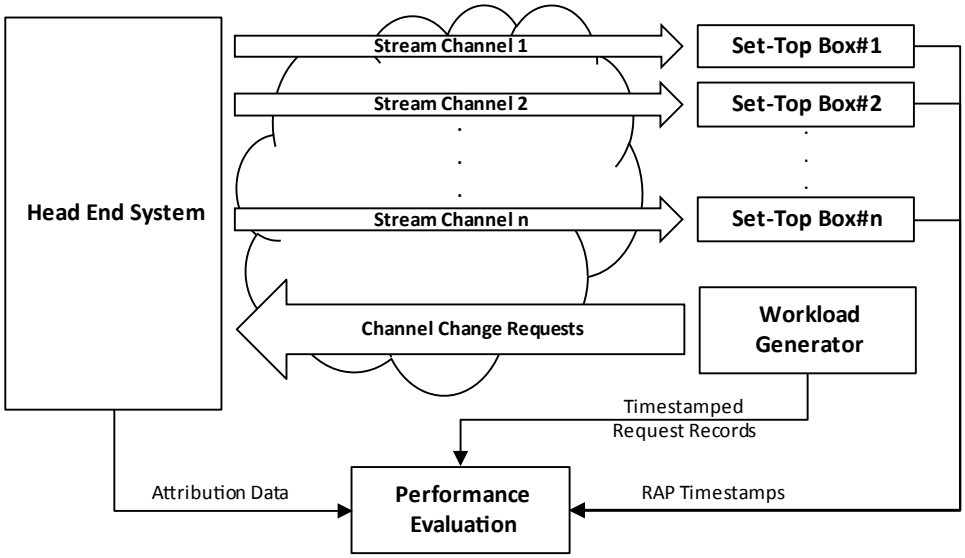


Figure 5.8: Channel Change Time Measurement System for CSTC

discussion in Section 5.4.2.1. By this means, we are able to directly subtract the time stamps delivered by the STB from the time stamps delivered by the WG in the course of determining the channel changing times.

5.4.1 Test System Extensions

5.4.1.1 Workload Generator

The WG creates channel change requests and sends them to the HES over the network interface. These requests simulate users we refer to as active users. In addition, the WG creates passive users that are registered at the HES and are evenly distributed on the broadcasted channels before the actual measurement is started. We introduce passive users to examine the overall performance of the key management system when already a high number of users are watching a particular channel, for instance, during the broadcast of live sport events.

The WG always creates channel change requests for the next second all at once. For generating a constant number of channel change requests, the identification numbers (IDs) of the involved users and the destination channels are chosen randomly. All requests are evenly distributed in the 1-second time frame and written to a text file for later analysis.

A single request entry consists of:

- the time stamp when the network packet containing the channel change request was sent over the network interface,
- the user ID the channel change request is attributed to,
- the channel ID of the channel the requesting user is watching currently, and
- the channel ID of the channel the user wishes to switch to.

With the aid of the time stamp, we are able to relate the user ID to the corresponding starting time of the channel switching action.

5.4.1.2 Headend Server

During the measurement, the HES writes a text file for each streamed channel. Each of these files contains IDs of users who have joined the respective channel along with the ID of the ECM that was created to entitle them. In this way, an association between the user, who requests a channel change and the corresponding entitlement information, which grants the access to the requested channel is established. This association is required to determine the channel change time for each user.

5.4.1.3 Set-Top Box

The STB is used to process the incoming stream from the HES on behalf of all users who sent channel change requests through the workload generator. Initially, available channels are discovered using an SAP client. Then, each STB registers itself at the HES as an independent user that is not managed by the WG. The STBes are registered at the HES after all active and passive users have been registered. As a result of the registration, necessary identity and security information are delivered. The STB is then tuned to the multicast address of the corresponding channel, and the related user requests a channel change to the corresponding channel. During the measurement the users related to the STB components remain at their corresponding channel and the STB is able to decrypt, decode and display the stream.

During its execution, the STB writes out a text file containing an ECM ID and a time stamp. The stream data between consecutive RAPs are decrypted using the key update information contained in the ECM of the corresponding ECM ID. The time stamp indicates at which time the first byte of the preceding RAP has been copied into the decoder buffer.

The additional time which elapses until the first image of the new channel appears on the screen depends on the MPEG decoder, the GOP structure, and TV set implementation, as we have seen in our analysis in Section 5.2. This delay consists of either three or four frame durations plus some offset caused by the post-processing algorithms, such as deinterlacing, up-scaling, and pull-down and is caused by efforts to minimize errors and to enhance the resulting visual experience.

In order to obtain comparable values for our evaluation, in our measurement we consider the time when incoming stream data are passed to the decoding buffer as the end time point of the channel switching process.

5.4.2 Measurement Procedure and Evaluation

The sequence of actions during the channel change time measurement is shown in Figure 5.9. Initially, the headend system and the workload generator components are started on the corresponding commodity computers. Then the workload generator is configured to support a maximum number of users, which corresponds to the maximum number of users that can be handled by the subscriber authorization system (SAS).

Another important configuration relates to the number of channel change requests per second (CCR/s), which represents the user dynamics. Accordingly, this value is configured at the workload generator.

Upon measurement start, the workload generator automatically registers all users at the HES in order to provide the users with user IDs and private keys. After that, the users are distributed evenly over the available number of channels. Subsequently, the STBs are started and registered. Then the STBs request a channel change to channel 1 by default. Consequently, in our exemplary test setup in Figure 5.8 three STBs have to switch to the corresponding channel in order to measure the right time stamps. After this, the

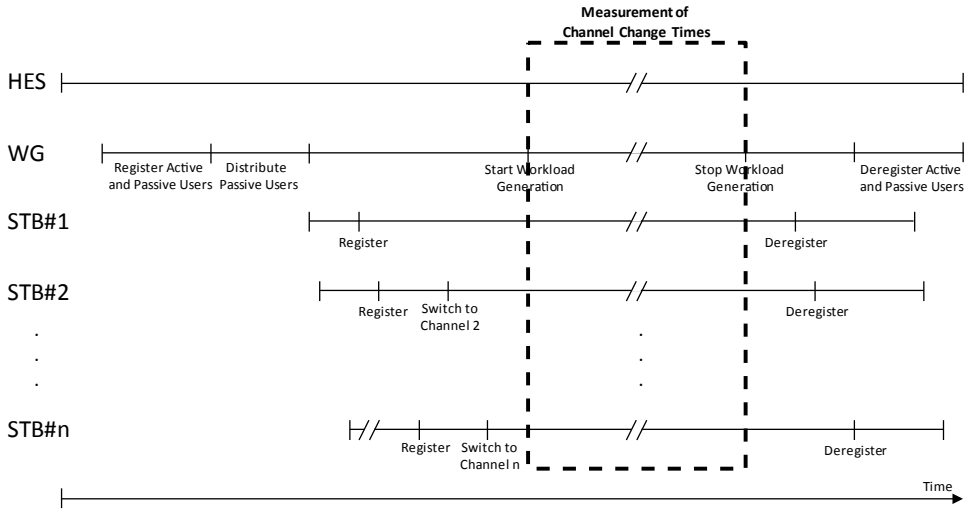


Figure 5.9: Sequence of Actions during the Measurement of Channel Change Times

actual channel change time measurement can be performed. At the end of the measurement period, each STB is deregistered and subsequently all users emulated by the WG are deregistered from the HES in order to return to a well-defined state.

For the evaluation of the measurement results, a Matlab script is used. The steps performed by the script are shown with the help of an example illustrated in Figure 5.10.

1. The script starts with processing the entries of the WG output. The first entry shows that the user with ID 12 switched from the Channel 4 to Channel 1 at the point in time given in the corresponding time stamp. As a result, the corresponding files indicated by the DstCh field are selected for further processing (step 1 in Figure 5.10).

2. The ID of the ECM that contained the key update message as a result of the channel change request of user 12 is looked up in the HES Output file (step 2 in Figure 5.10). In this example, the key update message for the channel change of user 12 was embedded in ECM 1.

3. In the third step, the time at which a certain video chunk has been forwarded to the decoder buffer in the STB is determined. This video chunk started with an RAP and was decrypted using the key derived from ECM 1.

4. In the fourth and final step, the channel change time is computed. For this, the time stamp indicating the end of the channel switching process is subtracted from the time stamp indicating the start of the process. In this example the channel change takes approximately 1.493 s.

5.4.2.1 Sources of Error

Like for any other measurement procedure, the results of the presented channel change time measurement method contain errors. Since we perform time measurement using time stamps on commodity computers, in the following we briefly assess the accuracy of the obtained time stamps. For this purpose, we initially identify affecting sources of error and subsequently discuss their impact on our setup.

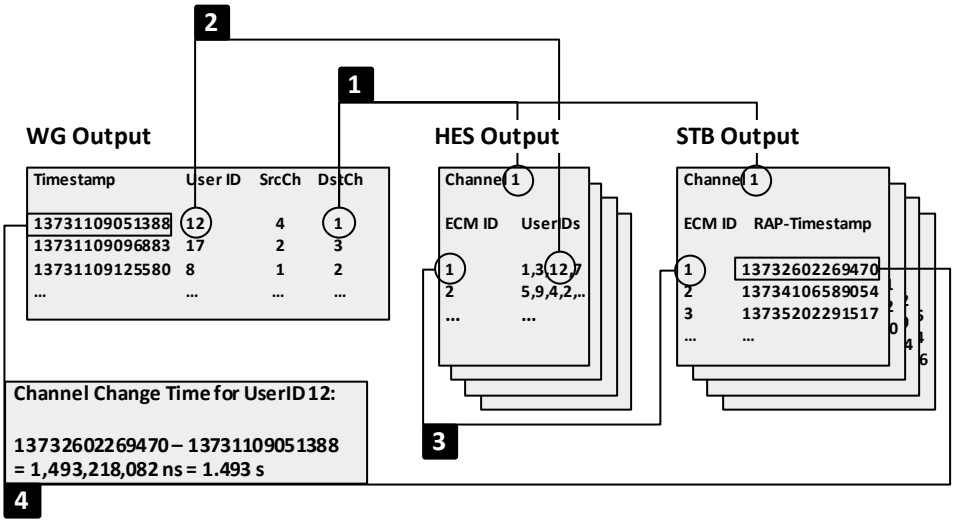


Figure 5.10: Computation Process of Channel Change Times

Commodity computers feature a number of hardware clocks which are polled in order to get a time stamp. The first source of error is related to the accuracy of these hardware clocks which contain physical oscillators. Caused by varying temperature in the operational environment, oscillators inherently feature drift. Depending on the accessed hardware clock variations of 30 – 100 parts per million (ppm) can be observed in commodity computers [175], [176].

The next source of time stamp inaccuracy is related to the access to the selected hardware clock. Dynamic system properties such as operating system interrupts defer the access to as well as results coming from the clock. Furthermore, power saving measures cause changes in clock reference rate and processor core input voltage. Also, in overheat situations the processor core clock frequencies are throttled in order to avoid permanent system damage. Moreover, time stamps regularly consist of large numbers that are prone to rounding errors.

Usually, the only options for remedy of the presented error sources are to use the most accurate clock available in the system or to synchronize the clock with a more accurate source. For the latter case, various types of synchronization protocols can be used in order to adjust clocks of one or more different systems that run asynchronously. These protocols, however, introduce new types of inaccuracies.

For the implementation of the presented channel change time measurement system, the Java programming language is used. On the Windows operating system the Java Runtime Environment obtains time stamps by accessing the so-called QueryPerformanceCounter, an interface provided by the operating system [177]. The QueryPerformanceCounter in turn relies on one of the following hardware clocks available in x86 architectures:

1. the Advanced Configuration and Power Interface Power Management Timer (ACPI PMT),
2. the High Precision Event Timer (HPET), and
3. the Time Stamp Counter (TSC) of one or more processor

Depending on the system configuration the operating system selects the most suitable hardware clock for retrieving time stamps during system start-up.

Since we measure short durations in our measurement, the impact of the presented sources of error on the setup, paticularly effects caused by hardware clock deviations are insignificant. Assuming a pessimistic clock drift of 100 ppm and channel change times in the range of 1 to 2 s as discussed in Section 5.1, the resulting error would be less than 1 µs The accuracy of a time stamp obtained using the QueryPerformanceCounter is specified to be in the vicinity of 1 µs [175]. The timer resolution, however, that is, the number of distinct possibilities to retrieve a time stamp value, is limited to 1000 in our implementation using the Windows operating system. Finally, the asynchrony problem among different systems does not arise since we take care that all durations are measured on the identical hardware system. In order to achieve this, the WG and the STB components are executed on the same system. As a result of our analysis, we estimate that our measurements have an overall accuracy of 1 ms.

5.4.3 Case Study

In order to assess the channel change processing delay in the context of batch rekeying, and furthermore, verify our assumptions regarding channel change times, in the following we perform a case study. For this purpose, we assume the same group size as mentioned in [174].

Consequently, we configure the workload generator to support $N_{max} = 2^{17}$ users, which corresponds to the maximum number of users that can be handled by the subscriber authorization system (SAS). Furthermore, we use a transport stream (TS) previously recorded from German DVB-T broadcast featuring 4 channels and a total bandwidth of 13.2 Mb/s. We run tests with 3 group sizes, which refer to the total number of users concurrently watching any of the 4 channels. These group sizes are 1000, 60 000, and 120 000. Note that the last value of 120 000 is chosen close to N_{max} in order to test the system closely to a worst-case scenario. Another important configuration of the WG relates to the number of channel change requests per second (CCR/s), which represents the user dynamics. In order to cover a wide dynamic range, we conduct measurements with 4, 1000, 2000, 3000, and 4000 CCR/s. Since video in broadcast usually features a variable GOP length, we use the measurement with 4 CCR/s particularly to determine the best possible channel change time for each channel. The WG creates channel change requests for the emulated users for a duration of approximately five minutes.

The workload generator and the STBes run on a commodity computer featuring an Intel Core i3 processor with 2 GiB of random access memory (RAM) and a gigabit Ethernet network interface. The HES is executed on a separate commodity computer equipped with an Intel Core i5 processor with 4 GiB RAM and a gigabit Ethernet network interface. Both computers are interconnected using an unmanaged 8-port gigabit Ethernet network switch.

The results of the worst-case measurement involving 120 000 passive users and 4000 channel change requests per second are depicted in Figure 5.11. In the histogram we can see that most users need 1.35 s to 2.5 s in order to complete a channel change when the system is under heavy load.

Since information is hard to grasp in this form of presentation, we first consider the cumulative distribution function (CDF). This function is used in notable literature dealing with channel change acceleration methods such as in [178], [179] or [180] and assigns a certain channel change time to a portion of users of the sample population. However, we consider this form of presentation still unsuitable for our purpose. Our aim is to illustrate

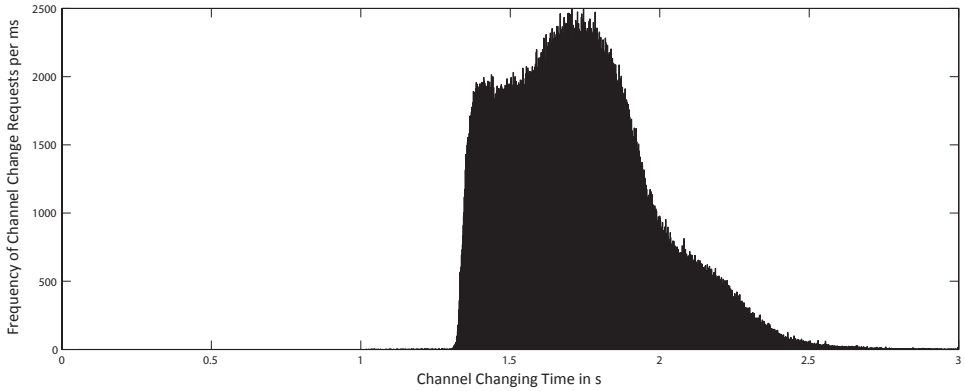


Figure 5.11: Histogram of Worst-Case Measurement

the worst case, namely, the shares of users that have to wait *at most* to perform a channel change. The CDF, however, assigns the shares of users to a specific channel change time they have to wait for *at least* For this reason, we present our results using the complementary cumulative distribution function (CCDF) which exactly fulfills our requirements.

In Figure 5.12 we depict the results of our measurement. The functions annotated with 1 show the GOP lengths, that is, the time intervals of random access points for each channel. Here, we assume that the channel requests are uniformly distributed since we directed the WG to create channel change requests in this manner. Since the predominant portion of GOPs in our transport stream has a duration of 0.6 s, half of all users wait for 0.3 s or less for an RAP to appear in the stream. We show the functions of GOP lengths in this context since they are one of the highest single contributors to the channel change time.

The functions annotated with 2 show the channel change times of our measurement involving no passive users and 4 CCR/s. We performed this measurement in order to provide a baseline for further measurements. In particular, the impact of the channel change processing delay at the HES is the least for this setting. As we can see, channel change times in this measurement extend from about 1.1 s up to 1.9 s.

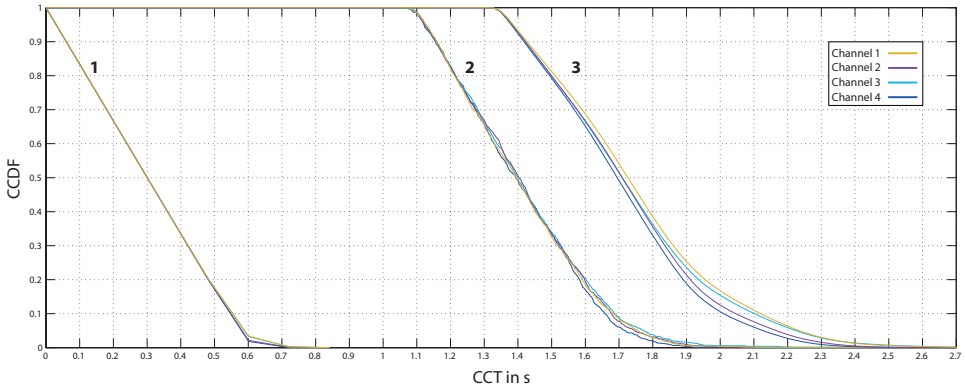


Figure 5.12: GOP lengths and CCTs for 4 and 4000 CCR/s

Series marked with 3 in the figure illustrate the measurement involving 120 000 passive users and 4000 CCR/s. Here, channel change times range from about 1.3 s up to 2.3 s and users wait around 1.7 s on average when a channel is switched.

For the performance assessment of the obtained values we recall our analysis from Section 4.3.1.3, where we found out that the maximum combined channel change rate is 4.77% of all users per minute at peak times on the most popular channel. Considering the dimensioning of our case study this would correspond to approximately 104 CCR/s. If we liberally assume that all the 4 channels we broadcast are most popular, we need to process only 417 CCR/s. This means that our prototype implementation without further optimization has reserve capacities to handle 10 times more requests per second without affecting the channel change time considerably. Such high request rates can occur during singular events, for instance, season finals, blockbuster movies, charity concerts as well as nationwide and worldwide sports events.

While differences regarding the channel change times are little for the baseline measurement and mostly negligible for GOP lengths, they become more prominent when the system is working under load. This effect could be attributed to buffering used to overcome DC-19. Particularly, our implementation doesn't employ an encoder using a master clock. Neither does the implementation scan the whole used transport stream file to determine the stream transmission rate of each file segment. In fact, the recorded stream is rebroadcasted similar to the situation in a headend where streams are gathered from many contribution links and are broadcasted further after some processing. Consequently, the internal clock and the processing speed is adjusted by using a PLL and PCR time stamps included into the incoming transport stream (see Chapter 3). However, 2 successive PCR time stamps are required in order to determine the elapsed time in the corresponding stream and to adjust the transmission rate. As a result, buffering causes at least a delay of these 2 successive PCR time stamps that appear roughly every 40 ms in the transport stream we use. Furthermore, buffering and identifying the position to insert the ECM incurs overhead. Since a small fraction of GOPs is longer than the average, the channel change time is further increased by these GOPs due to the effects described above.

Additionally, we can see that channel change times increase generally from 200 ms to 300 ms for the portion of users who already experience a high channel change times under heavy load. This effect could be caused by the fact that the key renewal under load for some users is deferred to the subsequent batch interval. With regard to scalability, we observe that the number of passive users has no significant impact on the channel change times.

As a general result of our case study, we see that channel change times take 50 ms to 150 ms longer as the average sum of the delay components we estimated and summarized in Table 5.3. Aside from delays related to DC-19, this is also a result of our prototype implementation. By profiling the HES during operation, we identified that a certain amount of delay is caused by thread contention. This means that our analysis in large part is accurate and there is certain room for improvement regarding our implementation.

In conclusion, we remember related literature [150] and [165] stating that channel change times below 2 s or sometimes below 1 s are considered as satisfactory and lead to a positive user perception. Regarding this statement, however, we want to obtain a more detailed view. Consequently, in the following we investigate how users would specifically experience the channel change times we achieved.

5.5 Impact of CSTC on QoE

In order to conclude the QoE of the users regarding channel change times from the correspondent QoS values we gained using our case study, we use the mapping developed in [181].

In this work, the authors develop a general zapping model from subjective channel change experiments with 25 users in a lean backward environment. This means that the experiments are carried out in an environment, which resembles a typical living room and where people are able to position themselves in a comfortable and relaxed way in front of a TV set. Correspondingly, channel switching is performed using a cell phone simulating a common TV remote control. After a training session during which the test subjects can get used to the MOS rating scale we introduced earlier, the actual experiment begins. Here, 10 different and randomly ordered channel change times, namely, 0, 0.1, 0.2 (2x), 0.5 (2x), 1, and 2 s, are applied to the performed channel switches. For each channel change time, the test subject is allowed to switch between different channels as often as desired. Then, the test subject is asked to rate the perceived quality of the channel change time according to the 5 point MOS ACR scale. The resulting mapping function of this experiment is given in Equation 5.3.

$$\mathrm{MOS}_{\mathrm{CCT\_fixed}} = \begin{cases} -2.10 \times x + 4.92, & \text{if} \quad 0 \leq \quad x \quad < 1.04, \\ -1.11 \times ln(x) + 2.78, & \text{if} \quad 1.04 \leq \quad x \quad < 4.97, \\ 1, & \text{if} \quad 4.97 \leq \quad x \end{cases} \tag{5.3}$$

,where x is CCT in s.

In subsequent experiments, the authors determine the impact of variations in channel change time. For this purpose, 3 different mean channel change delay times (0.5, 1, and 2 s) are investigated, whereas for each delay time has 3 – 4 variance times. Consequently, 15 randomly ordered sequences of a combination of channel change delay time and variance time are offered to the test subjects for evaluation.

The combinations are namely

- for the mean channel change delay time of 0.5 s, variations of 0, 0.2, and 0.5 s,
- for the mean channel change delay time of 1 s, variations of 0 (2x), 0.2, 0.5, and 1 s (2x),
- for the mean channel change delay time of 2 s, variations of 0, 0.2, 0.5, 1, and 2 s (2x).

According to the authors, applying particular channel change times twice serves the purpose of testing the consistency of delivered ratings. As a result of the presented experiments, the authors are able to determine that the rating decreases when users experience variance in channel change times. Correspondingly, the additions given in Equation 5.4 and 5.5 were made to estimate the MOS for channel change times in a lean back environment:

$$\text{Decrease of } \mathrm{MOS}_{\mathrm{CCT\_fixed}} = \begin{cases} \mathrm{Var(CCT)}, & \text{if } \overline{CCT} < 0.42, \\ 0.42 \times \frac{\mathrm{Var(CCT)}}{\overline{CCT}}, & \text{if } \overline{CCT} \geq 0.42. \end{cases} \tag{5.4}$$

$$\mathrm{MOS}_{\mathrm{CCT}} = max(\mathrm{MOS}_{\mathrm{CCT\_fixed}} - \text{Decrease of } \mathrm{MOS}_{\mathrm{CCT\_fixed}}, 1). \tag{5.5}$$

After obtaining a mapping of numerical channel change times to the subjectively perceived quality of these times, we are now able to estimate the quality of experience for our CTSC approach.

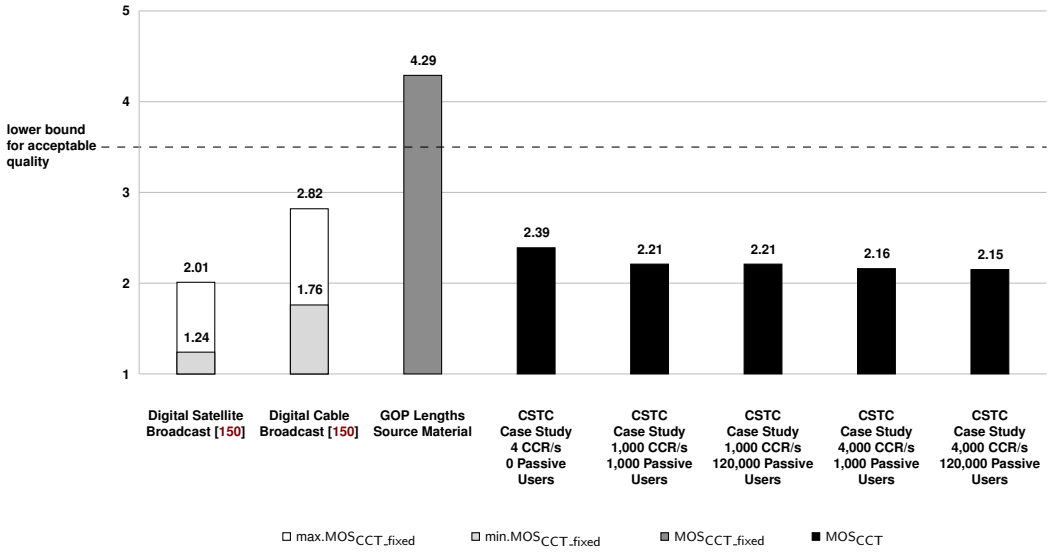


Figure 5.13: MOS Values for Measured Channel Change Times

For this purpose, we use the results obtained from our case study in Section 5.4.3 and present them in Figure 5.13. Furthermore, we add MOS ratings calculated from channel change times for digital satellite broadcast and digital cable broadcast given in [150]. Here, the channel change times are reported to be 2 to 4 s for digital satellite broadcast and 1 to 2.5 s for digital cable broadcast. For the calculation of the MOS value, we used Equation 5.3 that is formed for fixed channel change times, because we don't have any knowledge regarding the minumum, maximum, and variance of values taken from the literature. We take a similar approach in order to compute the corresponding hypothetical MOS for the GOP durations of the transport stream we used for our measurements. In this case, we use the expected value of the mean GOP duration, namely, 300 ms, as input for the function. Since in both cases the available data extends over a large range of values, the application of Equation 5.5 would reduce the MOS value to 1, that is, the worst possible value. For this reason, we don't consider the decrease of the MOS due to variance but rather apply the MOS for fixed delays given in Equation 5.3.

At first glance we can see that the MOS rating for IPTV using CSTC is comparable and pertaining to digital satellite broadcast, at any rate, better than the MOS values for conventional broadcast. In particular, the MOS value in the most challenging situation for our prototype only decreases by 0.24 compared to the idle state.

Considering Figure 5.13 we can also observe that none of the transmission paths is able to achieve the lower bound for subjectively acceptable channel change times. This bound is fixed to an MOS value of 3.5 and corresponds to a channel change time of 0.67 s according to Equation 5.3. The reason for this is that GOP lengths used in conventional broadcast video are a trade-off between channel change time and bandwidth. In particular, shorter GOP durations than 0.5 s entail an exponential increase of video bit rate, see [182] and [171]. Thus, even if the channel change time of a broadcast would solely consist of the

GOP access time, the resulting MOS rating would be indeed acceptable but still not perfect. Consequently, among other things, broadcasts employing current compression algorithms are not able to accomplish channel change times that are satisfactory to consumers without taking further actions. In this context, channel change acceleration methods are used to improve channel change time.

Therefore, we note that context is of prime importance for subjective perception and, consequently, for the MOS rating. In the lean backward context an MOS of 3.5 is achievable with a channel change time of 0.67 s [181].

However, the same MOS rating requires a channel change time of 0.43 s [183] in a lean forward context.

Furthermore, also the presented content is important. In experiments where an advertisement instead of a black screen is shown during the channel change, the authors could determine an increased MOS value. This means that users perceive the situation as satisfactory, although the channel change time is further increased by the advertisements [184]. In this way an MOS rating of 3 can be maintained for channel change times lasting almost 1.5 s. The function for calculating the MOS rating in this context is given according to [184] in Equation 5.6.

$$\begin{aligned} \mathrm{MOS}_{\mathrm{CCT\_Ads}} = \quad & max(\quad -15.8 \times x + 4.58, \\ & \quad min(0.10 \times ln(x) + 3.27, -0.93 \times ln(x) + 3.27)). \\ & \text{,where } x \text{ is CCT in s.} \end{aligned} \tag{5.6}$$

5.6 Conclusion

In this chapter we investigated to what extent CTSC has influence on the users' quality of TV watching experience (Q5). We identified 2 factors related to quality of service which are affected by CSTC, namely, channel change time and playout difference. Since the factor of playout difference is out of scope for our subject matter, we pursued the analysis of channel change time. For this purpose, we identified delay components contributing to channel change time and examined underlying causes. In the following, we specified delay components introduced by CSTC and highlighted their impact on the channel switching process. In order to verify our findings, we devised a system for measuring channel change times. As a result of a subsequent case study, we could ascertain our previous assumptions regarding the impact of CSTC on the channel switching process. In order to infer the impression of CTSC perceived by consumers, we applied an empirically verified mapping function on the compiled measurement data. As a result, we could confirm that CSTC does not cause any impairment on the quality of experience of users.

CHAPTER 6

CONCLUSION AND FUTURE WORK

In this work, we investigate the demand for and acceptance of the short-interval charging model for linear pay-TV over IPTV. For this, we consider interests from the consumer and the network operator perspective. To assess the demand, we conduct an online survey with the participation of 315 respondents in Germany. Our results show that 33% of the survey participants prefer short-interval charging to traditional pay-TV models. Further analyses of market developments suggest that the reasons for the attraction to short-interval charging are caused by latent requirements of consumers fulfilled by this model. We observe that the considered model meets open demands and attracts a relevant share of consumers on the IPTV market.

In the further course, we propose a technical approach for the realization of short-interval charging. This charging model is based on channel switching actions of users and is implemented by employing multicast encryption schemes. We call the resulting technical approach channel switching-triggered charging (CSTC).

All aspects we consider for the development of this approach are centered on the attainment of acceptance. We are convinced that acceptance is a prerequisite for consumers and network operators to benefit from the advantages of this charging model. Consequently, we consider usability and service quality as factors for increasing acceptance.

For designing our technical approach, we take the usability aspects of user-friendliness and integration into account. We survey network operator requirements with regard to integration and assert that most of the requirements relate to operating resources. In particular, we specify what effort it takes to integrate CSTC with a common IPTV architecture conforming to the DVB suite of standards. For this purpose, we indicate expenses by re-

ferring to additions and modifications to the assumed system. We conclude that only four functional components and two protocols require changes.

Moreover, we consider scalability and service quality aspects. We examine communication and computation requirements for prospective implementations of scalable CSTC systems that comply with the DVB suite of standards. Furthermore, we describe details of a prototype system architecture of an IPTV system supporting CTSC. We continue our consideration of service quality assuming the consumers' point of view. In this context, service quality gives rise to the question how much CSTC alters the users' quality of experience. In the course of our analysis, we identify channel change time as the particular critical factor affected by CSTC. Consequently, we analyze the channel change process and the impact of CSTC on this process. In order to validate our analysis, we devise a measurement system and conduct a case study. Our measurements indicate that the software-based prototype system supporting 2^{17} users and processing 4,000 channel change requests per second adds only approximately 300 ms on average to the individual channel change time of entitled users. We infer the users' perception of CSTC by applying an empirically verified mapping function on the results of our case study. As a result, we can ascertain that CSTC for IPTV does not deteriorate the experience of users.

Future Work

In the context of economic theories related to pricing strategies, we notice in Chapter 1 that further considerations regarding the demand and optimality of CSTC are required. Particularly, CSTC has to be assessed in a model of a competitive and converging market and considering piracy and other present challenges. Furthermore, the results of a broader consumer panel can verify our assumptions about the reasons for the attraction of consumers to short-interval charging. However, this consumer panel requires a higher number of respondents who feature representative demographic properties (age, gender, occupation).

In Chapter 5 we learned about QoS factors and their relation to QoE. Here, we noticed, that there is no order or weighting for QoS and QoE factors. Naturally, the audio and video quality are prime factors related to TV consumption. However, the degree of influence and rank of subordinate aspects such as channel change time or playout delay difference are not considered by respective standards yet. Thus, it is not possible to identify the importance of each factor and whether a system that performs poorly concerning a particular factor can compensate this drawback by performing better regarding one or more other factors. Moreover, the existence of such rank is a question for further research. In continuative work the MOS value for channel changes using CSTC could be verified experimentally. For this purpose, the prototype system developed in this work could be used and resulting MOS values could be compared with other systems. Furthermore, the effects of additional factors such as the duration of an initial cost-free period or the display of the current credit balance could be investigated.

Future work also includes technical aspects such as the elaboration on security properties and new attack vectors. In addition, appropriate authentication methods against remote channel switch attacks and for providing nonrepudiability for billing purposes have to be selected. Higher scalability could be achieved by investigating more efficient key management schemes. Components for IP telephony signaling usually present in IPTV operator networks could be used to decrease costs and to profit from existing schemes for channel change signaling and error handling. Particularly, components and protocols related to charging and transfer of call data records (CDRs) have to reviewed and adapted. The CTSC

approach could possibly be extended beyond the transmission path of IPTV toward one-way broadcast transmission schemes based on DVB-S/-C/-T. As a starting point, existing mechanisms for low-latency processing employed by content delivery networks (CDN) could be reviewed to perform composite signaling transport. In addition, the impact of CSTC on current and future trends such as channel change acceleration techniques and methods for countering transmission impairment, for instance, forward error correction methods, could be analyzed to rate the sustainability. Finally, the produced improvements and changes could be carried out on embedded systems typically used for STBes in order to conduct the previously mentioned user experiments conforming to the context.

REFERENCES

[1] F. Stahl, Paid Content: Pricing Strategies for E-Commerce of Digital Content, Deutscher Universitätsverlag, 2006, (In German). (see pp. 2, 5).

[2] R. Wilson, Nonlinear Pricing, Oxford University Press, 1993. (see pp. 2, 4, 6).

[3] A. Gupta, D. O. Stahl, A. B. Whinston, An economic approach to networked computing with priority classes, Journal of Organizational Computing and Electronic Commerce 6 (1) (1996) 71–95. doi:10.1080/10919399609540269. (see p. 3).

[4] W.-L. Chang, S.-T. Yuan, An overview of information goods pricing, International Journal of Electronic Business 5 (3) (2007) 294–314. doi:10.1504/IJEB.2007.014513. (see p. 3).

[5] R. Cocchi, S. Shenker, D. Estrin, L. Zhang, Pricing in computer networks: Motivation, formulation, and example, IEEE/ACM Transactions on Networking (TON) 1 (6) (1993) 627. doi:10.1109/90.266050. (see p. 3).

[6] C. Courcoubetis, R. Weber, Pricing Communication Networks: Economics, Technology and Modelling, John Wiley & Sons, Ltd, 2003. doi:10.1002/0470867175. (see p. 3).

[7] N. Kausar, B. Briscoe, J. Crowcroft, A charging model for sessions on the internet, in: Computers and Communications, 1999. Proceedings. IEEE International Symposium on, 1999, pp. 32–38. doi:10.1109/ISCC.1999.780758. (see p. 3).

[8] M. Caesar, S. Balaraman, D. Ghosal, A comparative study of pricing strategies for ip telephony, in: Global Telecommunications Conference, 2000. GLOBECOM '00. IEEE, Vol. 1, 2000, pp. 344 –349 vol.1. doi:10.1109/GLOCOM.2000.892027. (see p. 3).

[9] P. C. Fishburn, A. M. Odlyzko, R. C. Siders, Fixed fee versus unit pricing for information goods: competition, equilibria, and price wars, Internet Publishing and Beyond: The Economics of Digital Information and Intellectual Property 2 (7) (1997) 167–189. doi:10.5210/fm.v2i7.535. (see p. 3).

[10] K. Casier, B. Lannoo, J. Ooteghem, S. Verbrugge, D. Colle, M. Pickavet, P. Demeester, Adoption and pricing: The underestimated elements of a realistic IPTV business case, IEEE Communications Magazine 46 (8) (2008) 112–118. doi:10.1109/MCOM.2008.4597113. (see p. 3).

[11] A. Sundararajan, Nonlinear pricing of information goods, Management Science 50 (12) (2004) 1660–1673. doi:10.1287/mnsc.1040.0291. (see pp. 4, 12).

[12] H. R. Varian, Pricing information goods, in: Proceedings of Scholarship in the New Information Environment Symposium, Harvard Law School, 1995.
URL http://www.sims.berkeley.edu/~hal/Papers/price-info-goods.pdf (see p. 4).

[13] A. C. Pigou, The Economics of Welfare, 4th Edition, Macmillan, London, UK, 1920.
URL http://oll.libertyfund.org/titles/1410 (see p. 4).

[14] Y. Bakos, E. Brynjolfsson, Bundling and Competition on the Internet, Marketing Science 19 (1) (2000) 63–82. doi:10.1287/mksc.19.1.63.15182. (see p. 4).

[15] K. Altinkemer, J. Jaisingh, Pricing bundled information goods, in: Advanced Issues of E-Commerce and Web-Based Information Systems, 2002. (WECWIS 2002). Proceedings. Fourth IEEE International Workshop on, IEEE, 2002, pp. 89–96. doi:10.1109/WECWIS.2002.1021245. (see p. 4, 4).

[16] C. H. Brooks, S. Fay, R. Das, J. K. MacKie-Mason, J. O. Kephart, E. H. Durfee, Automated strategy searches in an electronic goods market: Learning and complex price schedules, in: Proceedings of the 1st ACM Conference on Electronic Commerce, EC '99, ACM, New York, NY, USA, 1999, pp. 31–40. doi:10.1145/336992.337000. (see p. 4).

[17] J. C.-I. Chuang, M. A. Sirbu, Optimal bundling strategy for digital information goods: Network delivery of articles and subscriptions, Information Economics and Policy 11 (2) (1999) 147–176. doi:10.1016/S0167-6245(99)00008-6. (see p. 4).

[18] S. Klein, C. Löbbecke, Signaling and Segmentation on Electronic Markets: Innovative Pricing Strategies for Improved Resource Allocation, in: Negotiations and interactions in electronic markets — Proceedings of the Sixth Research Symposium on Emerging Electronic Markets, , Münster, 1999, pp. 127–142.
URL http://www.wi.uni-muenster.de/inst/arbber/ab72.pdf (see p. 4).

[19] T. Andersson, Essays on nonlinear pricing and welfare, Ph.D. thesis, Lund University (2004). (see p. 5).

[20] W. Popp, L. Parke, R. Kaumanns, Rechtemanagement in der digitalen Medienwelt Rights Management in the Digital Media World, Media Perspektiven 9 (2008) 453 – 466.
URL http://www.ard-werbung.de/fileadmin/user_upload/media-perspektiven/pdf/2008/09-2008_Popp.pdf (see p. 5).

[21] No Author, Filmförderungsgesetz in der Fassung der Bekanntmachung vom 24. August 2004 (BGBl. I S. 2277), das zuletzt durch Artikel 1 des Gesetzes vom 7. August 2013 (BGBl. I S. 3082) geändert worden ist [Act on Film Promotion as amended and promulgated on August 24, 2004 (Federal Law Gazette part I page 2277), last amended by Article 1 of the Law on August 7, 2013 (Federal Law Gazette part I page 3082)] , Federal Law Gazette, (In German). Last accessed on October 30th, 2015. (Aug 2013).
URL http://www.gesetze-im-internet.de/ffg_1979/__20.html (see p. 6).

[22] IDATE Consulting & Research, Pay tv is even seeing sustained growth sales of 130 billion eur up to 2013, Last accessed on June 24th, 2015. (Sep. 2009).
URL http://www.idate.org/en/News/Pay-TV_602.html (see p. 7).

[23] International organization for standardization. Geneve (CH) and IEC, ISO/IEC 23009-1: Information technology : Dynamic adaptive streaming over HTTP (DASH) – Part 1: Media

presentation description and segment formats, International Standard (May 2014).
URL http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=040&ics3=&csnumber=65274 (see p. 9).

[24] R. Kuschnig, I. Kofler, H. Hellwagner, Evaluation of http-based request-response streams for internet video streaming, in: Proceedings of the Second Annual ACM Conference on Multimedia Systems, MMSys '11, ACM, New York, NY, USA, 2011, pp. 245–256. doi:10.1145/1943552.1943585. (see p. 9).

[25] Spirent Communications, Mommy, Netflix is eating my firewall!, Last accessed on February 29th, 2016. (Apr. 2011).
URL http://www.spirent.com/Blogs/Networks/2011/April/2011_04-07_Netflix_Eating_my_Firewall-m (see p. 9).

[26] T. Hossfeld, K. Leibnitz, A qualitative measurement survey of popular internet-based iptv systems, in: Communications and Electronics, 2008. ICCE 2008. Second International Conference on, 2008, pp. 156–161. doi:10.1109/CCE.2008.4578950. (see p. 9).

[27] G. Cepciansky, L. Schwartz, A note on tariffication strategy cases in telecommunications, Netnomics 9 (2) (2008) 95–103. doi:10.1007/s11066-009-9035-4. (see p. 10).

[28] ALM, ALM Jahrbuch 2009/2010 - Landesmedienanstalten und privater Rundfunk in Deutschland [ALM yearbook 2009/2010 - State media authorities and commercial broadcasters in Germany], Annual Report, (In German). Last accessed on August 23rd, 2015. (June 2010).
URL http://www.die-medienanstalten.de/fileadmin/Download/Publikationen/ALM-Jahrbuch/Jahrbuch_2010/ALM_Jahrbuch_2010_Druckversion.pdf (see pp. 11, 21, 21, 21, 27).

[29] A. Rott, S. Schmitt, Wochenend und Sonnenschein ... Determinanten der Zuschauernachfrage auf dem deutschen Fernsehmarkt ["Wochenend und Sonnenschein"... Determinants of Audience Demand on the German Television Market], M&K Medien & Kommunikationswissenschaft 48 (48) (2000) 537–553, (In German). doi:10.5771/1615-634x-2000-4-537. (see p. 11).

[30] J. G. Webster, J. J. Wakshlag, A theory of television program choice, Communication Research 10 (4) (1983) 430–446. doi:10.1177/009365083010004002. (see p. 11, 11).

[31] C. Heeter, The choice process model, in: C. Heeter, B. S. Greenberg (Eds.), Cableviewing, Communication, Culture, and Information Studies, Ablex, 1988, p. 1132. (see pp. 11, 79).

[32] G. J. Goodhardt, A. S. C. Ehrenberg, M. A. Collins, The Television Audience: Patterns of Viewing, Saxon House studies, Saxon House, 1975. (see p. 11).

[33] P. Klein, The men who run TV arent that stupid... they know us better than you think, New York Magazine 4 (6) (1971) 20–29. (see p. 11).

[34] B. M. Owen, J. H. Beebe, W. G. Manning, Television Economics, Lexington Books, 1974. (see p. 11).

[35] R. Gmez, YouTube tests automatically play suggested videos, Blog Entry, Last accessed on March 7th, 2016. (Aug. 2014).
URL http://allgoogletesting.blogspot.de/2014/08/youtube-tests-automatically-play-suggested-videos.html (see p. 12).

[36] Google Inc., Autoplay videos, YouTube Help Article, Last accessed on March 7th, 2016.
URL https://support.google.com/youtube/answer/6172631?hl=en (see p. 12).

[37] S. Bhattacharjee, R. D. Gopal, J. R. Marsden, R. Sankaranarayanan, Digital goods and markets: Emerging issues and challenges, ACM Trans. Manage. Inf. Syst. 2 (2) (2011) 8:1–8:14. doi:10.1145/1985347.1985349. (see p. 12).

[38] R. Mantena, A. Sundararajan, Competing in markets with digital convergence, Tech. rep., Stern School of Business (Jun 2004). (see p. 13).

[39] P. Belleflamme, M. Peitz, Digital Piracy: Theory, CESifo Working Paper Series 3222, CESifo Group Munich, Last accessed on October 20th, 2015. (2010).
URL http://ssrn.com/abstract=1698618 (see p. 13, 13).

[40] A. Sundararajan, Managing digital piracy: Pricing and protection, Information Systems Research 15 (3) (2004) 287–308. doi:10.1287/isre.1040.0030. (see p. 13).

[41] L. Zhang, Intellectual Property Strategy and the Long Tail: Evidence from the Recorded Music Industry, Tech. rep., Western University - Ivey Business School (dec 2013). doi:10.2139/ssrn.2515581.
URL http://inside.rotman.utoronto.ca/laurinazhang/files/2013/12/jmp_nov25.pdf (see p. 14, 14).

[42] R. D. Gopal, S. Bhattacharjee, G. L. Sanders, Do artists benefit from online music sharing?, The Journal of Business 79 (3) (2006) 1503–1533. doi:10.1086/500683. (see p. 14).

[43] T. Regner, J. A. Barria, J. V. Pitt, B. Neville, An artist life cycle model for digital media content: Strategies for the light web and the dark web, Electronic Commerce Research and Applications 8 (6) (2009) 334 – 342. doi:10.1016/j.elerap.2009.05.002. (see p. 14).

[44] P. Waelbroeck, Digital music: Economic perspectives, in: R. Towse, C. Handke (Eds.), Handbook of the Digital Creative Economy, Edward Elgar, Cheltenham, UK, 2013, Ch. 34, p. 389398. doi:10.4337/9781781004876.00047.
URL http://ssrn.com/abstract=2249690 (see p. 14).

[45] D. Halbheer, F. Stahl, O. Koenigsberg, D. R. Lehmann, Sampling strategies for information goods, Columbia Business School WP Series 118, University of Zurich, Last accessed on October 27th, 2015. (apr 2012).
URL https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/4609/SamplingStrategiesforInformationGoods.pdf (see p. 14).

[46] B. W. Wirtz, Media and Internet Management, Gabler, 2011, page 279. (see p. 21).

[47] T. J. Gerpott, P. Winzer, Verhältnismäßigkeit von Einspeiseentgelten für die Verbreitung öffentlich-rechtlicher Rundfunkprogramme über Kabelnetze aus ökonomischer Sicht [Commensurability of feed-in fees for the dissemination of public service broadcasting over cable networks from an economic point of view], in: Must Carry: Einspeisepflichten für öffentlich-rechtliche Rundfunkprogramme: Drei Gutachten im Auftrag der ARD-Landesrundfunkanstalten [Must Carry: Feed-in obligation for public service broadcasting programs: Three reports commissioned by the regional public broadcasting agencies of the consortium of public broadcasters in Germany], Nomos Verlagsgesellschaft mbH & Co. KG, 2013, pp. 9–88, (In German). Last accessed on November 2nd, 2015. doi:10.5771/9783845255347_9. (see p. 21).

[48] Ausschuss für technische Regulierung in der Telekommunikation (ATRT) [Committee for Technical Regulation in Telecommunications (ATRT], Abschlussbericht der Projektgruppe CA/DRM [Final report of the CA/DRM project group], Final report, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen [German Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway], (In German). Last accessed on November 2nd, 2015. (Nov 2009).
URL https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Technik/RundfunkuebertragungTeil4/ATRT-PG-CADRM/Abschlussbericht.pdf?__blob=publicationFile&v=1 (see pp. 21, 60).

[49] AGF/GfK Fernsehforschung, TV Scope - TV panel Germany + EU, Report, (In German). Last accessed on August 23rd, 2010.https://www.agf.de/daten/tvdaten/

digitalisierungsgrad/ and https://www.agf.de/daten/tvdaten/sehdauer/ (January 2010). (see pp. 21, 21, 32).

[50] Sky Deutschland AG, Sky deutschland announces financing measures to raise a minimum of 340 million euro and drive growth initiatives, Press Release, Last accessed on August 23rd, 2010. (August 2010).
URL http://info.sky.de/inhalt/common/stockaccess/boundary/AuthStockAccessRH.do (see p. 21).

[51] BITKOM e.V., Zwei drittel aller Haushalte nutzen ende 2010 Breitband [Two-thirds of all households use broadband by the end of 2010], Press Release, (In German). Last accessed on August 23rd, 2010. (March 2010).
URL http://www.bitkom.org/de/presse/8477_62900.aspx (see p. 21).

[52] VATM e.V., 11th Joint Analysis of the telecommunications market 2009, Dialog Consult / VATM, Study, Last accessed on August 23rd, 2010. (November 2009).
URL http://www.vatm.de/studien.html (see p. 21).

[53] Deutsche Telekom AG, Deutsche Telekom bestätigt mit starkem zweiten Quartal die Jahresziele 2010 [Deutsche Telekom confirms full year target for 2010 with strong second quarter], Press Release, (In German) Last accessed on August 23rd, 2010. (August 2010).
URL http://www.telekom.com/dtag/cms/content/dt/de/595714?archivArticleID=897750 (see p. 22).

[54] o2 Germany GmbH & Co. OHG, O2 als integrierter Anbieter auf Wachstumskurs [O2 on a growth curve as integrated provider], Press Release, (In German) Last accessed on August 23rd, 2010. (July 2010).
URL http://www.de.o2.com/ext/o2/wizard/index?page_id=16555;tree_id=1576;message_id=2899;category_id=1;style=portal;state=online (see p. 22).

[55] T. Arul, A. Shoufan, Consumer Opinions on Short-Interval Charging for Pay-TV over IPTV, in: Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on, 2012, pp. 147–153. doi:10.1109/WAINA.2012.95. (see pp. 22, 29).

[56] I. Ha, J. Yoo, J. Choi, S. Jong, S. Kim, Y. Chin, Adoption of iptv under the convergence of broadcasting and telecommunications, in: Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on, Vol. 02, 2009, pp. 1123 –1127.
URL http://ieeexplore.ieee.org/search/searchresult.jsp?newsearch=true&queryText=4809611 (see p. 22).

[57] D. Lee, I. Son, M. Yoo, J.-H. Lee, Understanding the adoption of convergent services: The case of iptv, in: System Sciences (HICSS), 2011 44th Hawaii International Conference on, 2011, pp. 1 –10. doi:10.1109/HICSS.2011.464. (see p. 22).

[58] Accenture plc, International iptv consumer readiness study, Study, Last accessed on September 27th, 2011. (April 2006).
URL https://newsroom.accenture.com/news/iptv-mystery-to-masses-accenture-survey-finds.htm (see p. 22).

[59] I. Ha, S. Yook, The effects of media characteristics on iptv adoption, in: Management of Engineering Technology, 2009. PICMET 2009. Portland International Conference on, 2009, pp. 2660 –2665. doi:10.1109/PICMET.2009.5261821. (see p. 22).

[60] M. Motoi, K. Kenichi, Public broadcasting and digitization of television: Survey of iptv subscribers, Report, Last accessed on September 27th, 2011. (March 2007).
URL http://www.nhk.or.jp/bunken/english/reports/pdf/06-07_no5_09.pdf. (see p. 22).

[61] E. Kim, S. Ko, Investigating user adoption of t-commerce, in: Computers, Networks, Systems and Industrial Engineering (CNSI), 2011 First ACIS/JNU International Conference on, 2011, pp. 95 –99. doi:10.1109/CNSI.2011.90. (see p. 22).

[62] Ericsson ConsumerLab, IPTV and the Connected Home - What consumers want from advanced TV services and the Connected Home, Research Study, Last accessed on September 27th, 2011. (2009).
URL http://blogit.realwire.com/media/Ericsson%20UK%20Connected%20Home%20Overview%202009.pdf (see p. 22).

[63] J. Trefzger, Mobile TV launch in Germany: challenges and implications, Working Papers of the Institute for Broadcasting Economics, Cologne University, Institute for Broadcasting Economics, 2005, Last accessed on September 27th, 2011.
URL http://www.rundfunk-institut.uni-koeln.de/institut/publikationen/arbeitspapiere/ap209.php (see p. 22).

[64] C. Schmitz, J. Cleeland, et al., LimeSurvey.org - THE survey software - free and open source!, Online, Last accessed on September 27th, 2011.
URL http://www.limesurvey.org (see p. 23).

[65] German Federal Statistical Office, Haushalte und Familien - Ergebnisse des Mikrozensus 2009 - Fachserie 1 Reihe 3 - 2009 [Households and families - Results of the micro census 2009 - Subject-matter series 1 Series 3 - 2009], Subject-matter series, (In German). Last accessed on February 28th, 2011. (01 2011).
URL https://www-ec.destatis.de/csp/shop/sfg/bpm.html.cms.cBroker.cls?cmspath=struktur,vollanzeige.csp&ID=1025954 (see p. 26).

[66] German Federal Statistical Office, Bevölkerung und Erwerbstätigkeit - Bevölkerungsfortschreibung - Fachserie 1 Reihe 1.3 - 2009 [Population and employment - Population update - Subject-matter series 1 Series 1.3 - 2009], Subject-matter series, (In German). Last accessed on February 28th, 2011. (07 2010).
URL http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Publikationen/Fachveroeffentlichungen/Bevoelkerung/Bevoelkerungsstand/Bevoelkerungsfortschreibung2010130097004,property=file.pdf (see p. 26).

[67] PriceWaterhouseCoopers, IPTV - Das neue Fernsehen? [IPTV - The new TV?], Report, (In German). Last accessed on August 23rd, 2010. (March 2008).
URL http://pic.tv1.de/media/tv1/easyonair/files/IPTV-Das-neue-Fernsehen.pdf (see pp. 26, 28).

[68] The State Media Authorities of Germany Regulatory Affairs Commission (ZAK), Digitisation 2009, Report, Last accessed on February 28th, 2011. (09 2009).
URL http://www.alm.de/309.html (see p. 27).

[69] German Federal Film Board, Der Kinobesucher 2009, Strukturen und Entwicklungen auf Basis des GfK Panels [Cinemagoer 2009, structures and developments based on the GfK panel], Study, (In German). Last accessed on February 28th, 2011. (04 2010).
URL http://www.ffa.de/downloads/publikationen/kinobesucher_2009.pdf (see p. 27).

[70] Federal association of audio-visual media (BVV), Video market 2009, BVV Business Report, Last accessed on February 28th, 2011. (02 2010).
URL http://www.bvv-medien.de/jwb_pdfs/JWB2009.pdf. (see p. 27).

[71] Deloitte LLP, Digital Democracy Survey, Sixth Edition, Tech. Rep. 6, Deloitte LLP (2011).
URL http://www2.deloitte.com/us/en/pages/technology-media-

and-telecommunications/articles/digital-democracy-survey-generational-media-consumption-trends.html (see p. 29, 29).

[72] GfK SE, More Than a Third of Americans Use Netflix at Least Once a Month New Knowledge Networks Report, Press Release (September 2011).
URL http://www.knowledgenetworks.com/news/releases/2011/092911_netflix.html (see p. 29).

[73] U. Gurevitz, The Digital Consumer: Global Views on the Pay TV Experience, Cable Analytics and Cable Wi-Fi, Presentation at The Internet and Television Expo (INTX) 2015 (May 2015).
URL http://www.amdocs.com/Solutions/cable-satellite/Documents/Amdocs-IEMR-Consumer-Pay-TV-Survey-2015-Highlights.pdf (see pp. 29, 31, 31).

[74] J. Pransky, Pay TV Global Survey: Your Customer's View of the Pay TV Experience, Company Presentation (May 2014).
URL http://www.amdocs.com/vision/market-insight/documents/paytv-global-survey.pdf (see pp. 29, 31, 31, 34).

[75] J. Pransky, Pay-TV: Breaking Out Before it Starts Breaking Bad, Company Presentation (May 2014).
URL http://www.amdocs.com/vision/market-insight/documents/paytv-retention-growth.pdf (see pp. 29, 30, 30, 30).

[76] Deloitte LLP, Digital Democracy Survey, Ninth Edition, Tech. Rep. 9, Deloitte LLP (2015).
URL http://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-DDS_Executive_Summary_Report_Final_2015-04-20.pdf (see pp. 29, 30).

[77] M. Snider, More consumers spurn cable TV bills, News website article, Last accessed on March 9th, 2016. (Nov. 2011).
URL http://usatoday30.usatoday.com/MONEY/usaedition/2011-09-12-Cutcord-0830_CV_U.htm (see p. 30).

[78] ALM, ALM Jahrbuch 2014/2015 - Landesmedienanstalten und privater Rundfunk in Deutschland [ALM yearbook 2014/2015 - State media authorities and commercial broadcasters in Germany], Annual Report, (In German). Last accessed on August 23rd, 2010. (May 2015).
URL http://www.die-medienanstalten.de/fileadmin/Download/Publikationen/ALM-Jahrbuch/Jahrbuch_2015/ALM_Jahrbuch_2014_2015_finale_Fassung.pdf (see pp. 31, 32, 32).

[79] G. Bauer, M. Deitenbeck, T. Fuchs, U. Hasebrink, S. Hölig, J. Kors, K. Kunow, S. Meyer-Tippach, A. Ünal, Digitisation 2015, Annual Report, last accessed on November 23rd, 2015. (August 2015).
URL http://www.die-medienanstalten.de/fileadmin/Download/Publikationen/Digitalisierungsbericht/2015/Digitisation_2015_english.pdf (see p. 32, 32).

[80] F. Giersberg, Pay-TV in Deutschland 2015 [Pay-TV in Germany 2015], Aktualisierter marktüberblick zum pressegespräch des vprt arbeitskreises pay-tv am 15. juli 2015 [updated market overview for the press interview of the vprt pay-tv working group on july 15, 2015], Verband Privater Rundfunk und Telemedien e. V. (VPRT) [Association for Private Broadcast and Telemedia], Berlin, (In German). Last accessed on November 23rd, 2015. (Jul. 2015). (see p. 32).

[81] ITU-R Recommendation BT.601-7 : Studio encoding parameters of digital television for standard 4:3 and wide-screen 16:9 aspect ratios, International Standard (Mar. 2011).
URL https://www.itu.int/rec/R-REC-BT.601-7-201103-I/en (see p. 38).

[82] Society of Motion Picture and Television Engineers (SMPTE), Smpte st 296:2012: 1280 x 720 progressive image 4:2:2 and 4:4:4 sample structure - analog and digital representation and analog interface, SMPTE ST 296:2012 (2012) 1–24doi:10.5594/SMPTE.ST296.2012. (see p. 38).

[83] ITU-R Recommendation BT.709-6: Parameter values for the HDTV standards for production and international programme exchange, International Standard (Jun. 2015).
URL https://www.itu.int/rec/R-REC-BT.709/en (see p. 38).

[84] Society of Motion Picture and Television Engineers (SMPTE), Smpte st 274:2008: For television - 1920 x 1080 image sample structure, digital representation and digital timing reference sequences for multiple picture rates, SMPTE ST 274:2008 (2008) 1–35doi:10.5594/SMPTE.ST274.2008. (see p. 38).

[85] Generic coding of moving pictures and associated audio information : ITU-T Recommendation H.262 and ISO/IEC 13818 Part 2, International Standard (Feb. 2012).
URL https://www.itu.int/rec/T-REC-H.262-201202-I/en (see pp. 38, 42, 43, 88).

[86] Advanced video coding for generic audiovisual services: ITU-T Recommendation H.264 and ISO/IEC 14496 Part 10, International Standard (Feb. 2014).
URL https://www.itu.int/rec/T-REC-H.264-201402-I/en (see p. 38).

[87] High efficiency video coding: ITU-T Recommendation H.265 and ISO/IEC 23008 Part 2, International Standard (Apr. 2015).
URL https://www.itu.int/rec/T-REC-H.265-201504-I/en (see p. 38).

[88] N. Ahmed, T. Natarajan, K. Rao, Discrete cosine transform, Computers, IEEE Transactions on C-23 (1) (1974) 90–93. doi:10.1109/T-C.1974.223784. (see pp. 40, 41).

[89] B. Fino, V. Algazi, Unified matrix treatment of the fast walsh-hadamard transform, Computers, IEEE Transactions on C-25 (11) (1976) 1142–1146. doi:10.1109/TC.1976.1674569. (see p. 40).

[90] W. Cham, R. Clarke, Dyadic symmetry and walsh matrices, Communications, Radar and Signal Processing, IEE Proceedings F 134 (2) (1987) 141–145. doi:10.1049/ip-f-1:19870028. (see p. 40).

[91] W. Cham, Family of order-4 four-level orthogonal transforms, Electronics Letters 19 (21) (1983) 869–871. doi:10.1049/el:19830592. (see p. 40).

[92] W. Cham, R. Clarke, Application of the principle of dyadic symmetry to the generation of orthogonal transforms, Communications, Radar and Signal Processing, IEE Proceedings F 133 (3) (1986) 264–270. doi:10.1049/ip-f-1.1986.0043. (see p. 40).

[93] H. Malvar, A. Hallapuro, M. Karczewicz, L. Kerofsky, Low-complexity transform and quantization in h.264/avc, Circuits and Systems for Video Technology, IEEE Transactions on 13 (7) (2003) 598–603. doi:10.1109/TCSVT.2003.814964. (see p. 40).

[94] D. Huffman, A method for the construction of minimum-redundancy codes, Proceedings of the IRE 40 (9) (1952) 1098–1101. doi:10.1109/JRPROC.1952.273898. (see p. 41).

[95] J. J. Rissanen, Generalized kraft inequality and arithmetic coding, IBM J. Res. Dev. 20 (3) (1976) 198–203. doi:10.1147/rd.203.0198. (see p. 41).

[96] R. C. Pasco, Source coding algorithms for fast data compression., Ph.D. thesis, Stanford, CA, USA, aAI7626055 (1976). (see p. 41).

[97] D. Marpe, H. Schwarz, T. Wiegand, Context-based adaptive binary arithmetic coding in the h.264/avc video compression standard, Circuits and Systems for Video Technology, IEEE Transactions on 13 (7) (2003) 620–636. doi:10.1109/TCSVT.2003.815173. (see p. 41).

[98] J. Jain, A. Jain, Displacement measurement and its application in interframe image coding, Communications, IEEE Transactions on 29 (12) (1981) 1799–1808. doi:10.1109/TCOM.1981.1094950. (see p. 41).

[99] D. Le Gall, Mpeg: A video compression standard for multimedia applications, Commun. ACM 34 (4) (1991) 46–58. doi:10.1145/103085.103090. (see p. 41).

[100] International organization for standardization. Geneve (CH) and IEC, ISO/IEC 13818-1: Information technology : Generic coding of moving pictures and associated audio information – Part 1: Systems, International Standard (1993).
URL http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=67331 (see pp. 43, 43, 65, 67, 68, 74, 75, 75, 95).

[101] European Telecommunications Standards Institute, Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems, European Standard (May 2014).
URL http://www.etsi.org/deliver/etsi_en/300400_300499/300468/ (see pp. 43, 65, 74).

[102] Pro-MPEG Forum, Transmission of Professional MPEG-2 Transport Streams over IP Networks, Pro-MPEG Code of Practice 3 Release 2 (Jul. 2004). (see p. 44).

[103] J. Postel, User Datagram Protocol, RFC 768 (Standard) (August 1980).
URL http://www.ietf.org/rfc/rfc768.txt (see p. 44).

[104] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, Rtp: A transport protocol for real-time applications, RFC 3550 (INTERNET STANDARD), updated by RFCs 5506, 5761, 6051, 6222, 7022, 7160, 7164 (Jul. 2003).
URL http://www.ietf.org/rfc/rfc3550.txt (see pp. 44, 74).

[105] J. Daemen, V. Rijmen, The block cipher rijndael, in: J.-J. Quisquater, B. Schneier (Eds.), Smart Card Research and Applications, Vol. 1820 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2000, pp. 277–284. doi:10.1007/10721064_26. (see p. 46).

[106] J. Postel, Internet protocol, RFC 791 (1981) 45. (see p. 47).

[107] Ieee standard for ethernet - section 1, IEEE Std 802.3-2012 (Revision to IEEE Std 802.3-2008) (2012) 1–0. (see p. 48).

[108] D. Plummer, Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware, RFC 826 (Internet Standard), updated by RFCs 5227, 5494 (Nov. 1982).
URL http://www.ietf.org/rfc/rfc826.txt (see p. 48).

[109] S. Deering, Host extensions for ip multicasting, RFC1112. (see p. 48, 48).

[110] B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan, Internet Group Management Protocol, Version 3, RFC 3376 (Proposed Standard), updated by RFC 4604 (October 2002).
URL http://www.ietf.org/rfc/rfc3376.txt (see pp. 49, 72).

[111] X. S. Li, Y. R. Yang, M. G. Gouda, S. S. Lam, Batch rekeying for secure group communications, in: Proceedings of the 10th International Conference on World Wide Web, WWW '01, ACM, New York, NY, USA, 2001, pp. 525–534. doi:10.1145/371920.372153. (see pp. 51, 66).

[112] C. K. Wong, M. Gouda, S. S. Lam, Secure group communications using key graphs, Networking, IEEE/ACM Transactions on 8 (1) (2000) 16–30. doi:10.1109/90.836475. (see pp. 53, 66).

[113] D. M. Wallner, E. J. Harder, R. C. Agee, Key Management for Multicast: Issues and Architectures, RFC 2627 (Informational) (Jun. 1999).
URL http://www.ietf.org/rfc/rfc2627.txt (see pp. 53, 66).

[114] M. Moyer, G. Tech, J. Rao, P. Rohatgi, Maintaining Balanced Key Trees for Secure Multicast, Internet draft, IRTF (June 1999).
URL http://www.securemulticast.org/draft-irtf-smug-key-tree-balance-00.txt (see p. 54).

[115] M. Moharrum, R. Mukkamala, M. Eltoweissy, Efficient secure multicast with well-populated multicast key trees, in: Parallel and Distributed Systems, 2004. ICPADS 2004. Proceedings. Tenth International Conference on, 2004, pp. 215–222. doi:10.1109/ICPADS.2004.1316098. (see p. 54).

[116] O. Rodeh, K. P. Birman, D. Dolev, Using avl trees for fault-tolerant group key management, International Journal of Information Security 1 (2) (2002) 84–99. doi:10.1007/s102070100008. (see p. 54).

[117] J. Goshi, R. E. Ladner, Algorithms for dynamic multicast key distribution, J. Exp. Algorithmics 11. doi:10.1145/1187436.1210587. (see p. 54).

[118] H. Lu, A novel high-order tree for secure multicast key management, Computers, IEEE Transactions on 54 (2) (2005) 214–224. doi:10.1109/TC.2005.15. (see p. 54).

[119] T. Arul, A. Shoufan, Subscription-free Pay-TV over IPTV, Journal of Systems Architecture (2015) –doi:10.1016/j.sysarc.2015.12.001. (see p. 56).

[120] J. Coustel, D2-MAC/Packet and Eurocrypt. Advanced solutions for innovative pay-TV and pay-per-view services, in: Broadcasting Convention, 1992. IBC., International, 358, 1992, pp. 414 –417, Last accessed on June 24th, 2015.
URL http://ieeexplore.ieee.org/search/searchresult.jsp?newsearch=true&queryText=160481 (see pp. 58, 59).

[121] A. Martinez-Balleste, J. Domingo-Ferrer, F. Sebe, Minpay: a multi-device internet pay-as-you-watch system, in: Information Technology: Coding and Computing [Computers and Communications], 2003. Proceedings. ITCC 2003. International Conference on, 2003, pp. 258 – 262. doi:10.1109/ITCC.2003.1197537. (see pp. 58, 59).

[122] H.-M. Sun, C.-M. Chen, C.-Z. Shieh, Flexible-pay-per-channel: A new model for content access control in pay-tv broadcasting systems, Multimedia, IEEE Transactions on 10 (6) (2008) 1109 –1120. doi:10.1109/TMM.2008.2001381. (see p. 59, 59, 59).

[123] C.-M. Chen, H.-T. Chiao, S.-T. Chen, H.-M. Sun, A new business model in pay-tv broadcasting systems and its conditional access system, in: TENCON 2010 - 2010 IEEE Region 10 Conference, 2010, pp. 797 –802. doi:10.1109/TENCON.2010.5686585. (see p. 59, 59).

[124] C. B. Bestler, G. E. Reichard Jr., T. J. Rossen, S. Sirazi, Impulse pay per view system and method, Last accessed on June 24th, 2015. (July 1988).
URL http://www.freepatentsonline.com/4755872.html (see p. 59, 59).

[125] Y. Chen, Method, system and apparatus for managing iptv live broadcast service, Last accessed on June 24th, 2015. (October 2008).
URL http://www.freepatentsonline.com/y2008/0244658.html (see pp. 59, 60).

[126] C. Bhaumik, A. Ghose, A novel scheme for accurate billing based on actual view-time in broadcast tv, in: Consumer Electronics (ICCE), 2011 IEEE International Conference on, 2011, pp. 43–44. doi:10.1109/ICCE.2011.5722672. (see pp. 59, 60).

[127] A. Lugmayr, S. Kalli, Transmission of dvb service information via internet, in: S. Rao, K. Sletta (Eds.), Next Generation Networks. Networks and Services for the Information Society, Vol. 1938 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2000, pp. 96–109. doi:10.1007/3-540-40019-2_9. (see p. 65).

[128] M. Cha, P. Rodriguez, J. Crowcroft, S. Moon, X. Amatriain, Watching television over an ip network, in: Proceedings of the 8th ACM SIGCOMM conference on Internet measurement, IMC '08, ACM, New York, NY, USA, 2008, pp. 71–84. doi:10.1145/1452520.1452529. (see pp. 65, 79, 79, 79).

[129] M. Mignon, K. Bouckhout, J. Gahm, A. C. Begen, Scaling server-based channel-change acceleration to millions of iptv subscribers, in: Packet Video Workshop (PV), 2012 19th International, 2012, pp. 107–112. doi:10.1109/PV.2012.6229721. (see p. 65).

[130] S. Malipatlolla, T. Feller, A. Shoufan, T. Arul, S. A. Huss, A novel architecture for a secure update of cryptographic engines on trusted platform module, in: Field-Programmable Technology (FPT), 2011 International Conference on, 2011, pp. 1–6. doi:10.1109/FPT.2011.6132705. (see p. 65).

[131] W. Rankl, W. Effing, Smart Card Handbook, 4th Edition, John Wiley & Sons, 2010. (see p. 66).

[132] Y. Eslami, A. Sheikholeslami, P. Gulak, S. Masui, K. Mukaida, An area-efficient universal cryptography processor for smart cards, Very Large Scale Integration (VLSI) Systems, IEEE Transactions on 14 (1) (2006) 43–56. doi:10.1109/TVLSI.2005.863188. (see p. 66).

[133] W. Rankl, Smart Card Applications: Design models for using and programming smart cards, John Wiley & Sons, 2007. (see p. 66).

[134] Infineon Technologies AG, Infineon Chip Card & Security ICs Portfolio, Product Selection Guide, Last accessed on July 7th, 2015. (Oct. 2014).
URL http://www.infineon.com/dgdl/Infineon-Infineon+Chip+Card+%26+Security+ICs+Portfolio_10.2014-SG-v01_00-EN.pdf?fileId=5546d4624933b875014999016c6e2bde (see p. 66).

[135] A. Shoufan, T. Arul, A benchmarking environment for performance evaluation of tree-based rekeying algorithms, Journal of Systems and Software 84 (7) (2011) 1130 – 1143. doi:http://dx.doi.org/10.1016/j.jss.2011.02.006. (see p. 66).

[136] A. Shoufan, T. Arul, Design Methodologies for Secure Embedded Systems: Festschrift in Honor of Prof. Dr.-Ing. Sorin A. Huss, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011. doi:10.1007/978-3-642-16767-6_5. (see p. 66).

[137] ITU-T Recommendation X.1193 : Secure applications and services - IPTV security: Key management framework for secure Internet protocol television (IPTV) services, International Standard (Oct. 2011).
URL http://www.itu.int/rec/T-REC-X.1193-201110-I (see p. 68).

[138] B. Fenner, M. Handley, H. Holbrook, I. Kouvelas, Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised), RFC 4601 (Proposed Standard), updated by RFC 5059 (August 2006).
URL http://www.ietf.org/rfc/rfc4601.txt (see p. 72).

[139] J. Loughney, G. Camarillo, Authentication, authorization, and accounting requirements for the session initiation protocol (sip), RFC 3702 (Informational) (February 2004).
URL http://www.ietf.org/rfc/rfc3702.txt (see p. 72).

[140] M. Handley, C. Perkins, E. Whelan, Session Announcement Protocol, RFC 2974 (Experimental) (Oct. 2000).
URL http://www.ietf.org/rfc/rfc2974.txt (see p. 74).

[141] Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems, European Standard (Oct. 1996).
URL http://www.etsi.org/deliver/etsi_etr/200_299/289/ (see p. 74).

[142] National Institute of Standards and Technology, FIPS PUB 197: Specification for the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication

(FIPS PUB) 197, U.S.Department of Commerce/National Institute of Standards & Technology, Gaithersburg, MD, United States (Nov. 2001).
URL http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (see p. 74).

[143] M. J. Dworkin, SP 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques, Special Publications 800-38A, National Institute of Standards & Technology, Gaithersburg, MD, United States (2001).
URL http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf (see p. 74).

[144] CENELEC, EN-50221: Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications, European Standard (Feb. 1997).
URL https://www.dvb.org/resources/public/standards/En50221.V1.pdf (see p. 77).

[145] GStreamer Open Source Multimedia Framework.
URL http://gstreamer.freedesktop.org/ (see p. 78).

[146] T. Qiu, Z. Ge, S. Lee, J. Wang, J. Xu, Q. Zhao, Modeling user activities in a large iptv system, in: Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement Conference, IMC '09, ACM, New York, NY, USA, 2009, pp. 430–441. doi:10.1145/1644893.1644945. (see p. 79).

[147] N. Liu, H. Cui, S.-H. G. Chan, Z. Chen, Y. Zhuang, Dissecting user behaviors for a simultaneous live and vod iptv system, ACM Trans. Multimedia Comput. Commun. Appl. 10 (3) (2014) 23:1–23:16. doi:10.1145/2568194. (see p. 79).

[148] A. Abdollahpouri, B. E. Wolfinger, J. Lai, C. Vinti, Elaboration and Formal Description of IPTV User Models and Their Application to IPTV, in: B. Wolfinger, K. Heidtmann (Eds.), MMBnet 2011, 6th GI/ITG-Workshop, Hamburg, 2011. (see p. 79, 79).

[149] ITU-T Recommendation G.1080 : Quality of experience requirements for IPTV services, International Standard (Dec. 2008).
URL https://www.itu.int/rec/T-REC-G.1080/en (see pp. 81, 82, 83, 83, 86, 89).

[150] Architecture & Transport Working Group, Triple-play Services Quality of Experience (QoE) Requirements, TR- 126, DSL Forum, Fremont, CA, USA (Dec. 2006).
URL https://www.broadband-forum.org/technical/download/TR-126.pdf (see pp. 82, 83, 83, 84, 84, 85, 85, 85, 86, 86, 90, 106, 108, 108, 108).

[151] ITU-T Recommendation P.800: Methods for subjective determination of transmission quality, International Standard (Aug. 1996).
URL https://www.itu.int/rec/T-REC-P.800-199608-I/en (see pp. 82, 82, 83).

[152] ITU-T Recommendation P.910 : Subjective video quality assessment methods for multimedia applications, International Standard (Apr. 2008).
URL https://www.itu.int/rec/T-REC-P.910-200804-I/en (see p. 82).

[153] ITU-T Recommendation G.107 : The E-model: a computational model for use in transmission planning, International Standard (Jun. 2015).
URL https://www.itu.int/rec/T-REC-G.107/en (see p. 82).

[154] ATIS Standard 0800008: QoS metrics for linear broadcast IPTV (Feb. 2007).
URL https://www.atis.org/docstore/product.aspx?id=25549 (see p. 83, 83).

[155] ITU-T Recommendation E.800: Definitions of terms related to quality of service, International Standard (Sep. 2008).
URL https://www.itu.int/rec/T-REC-E.800-200809-I/en (see pp. 83, 86).

[156] Speech and multimedia Transmission Quality (STQ); QoS and network performance metrics and measurement methods;Part 4: Indicators for supervision of Multiplay services, European Standard (Oct. 2010).
URL http://www.etsi.org/deliver/etsi_es/202700_202799/20276504/ (see pp. 84, 85).

[157] Operations & Network Management Working Group, IPTV Performance Monitoring, TR-160, Broadband Forum, Fremont, CA, USA (Nov. 2010).
URL https://www.broadband-forum.org/technical/download/TR-160.pdf (see p. 84).

[158] ITU-T Recommendation Y.1540 : Internet protocol data communication service - IP packet transfer and availability performance parameters, International Standard (Mar. 2011).
URL https://www.itu.int/rec/T-REC-Y.1540-201103-I/en (see p. 84).

[159] ITU-R Recommendation BT.1359-1: Relative timing of sound and vision for broadcasting, International Standard (Nov. 1998).
URL https://www.itu.int/rec/R-REC-BT.1359/en (see p. 84).

[160] B. Shneiderman, C. Plaisant, M. Cohen, S. Jacobs, Designing the User Interface: Strategies for Effective Human-Computer Interaction (5th Edition), 5th Edition, Pearson, 2009. (see p. 85).

[161] J. Nielsen, Response Times: The 3 Important Limits, Web Article, last accessed on March 16th, 2016. (Jan. 1993).
URL https://www.nngroup.com/articles/response-times-3-important-limits/ (see p. 85).

[162] J. Nielsen, Powers of 10: Time Scales in User Experience, Web Article, last accessed on March 16th, 2016. (Oct. 2009).
URL https://www.nngroup.com/articles/powers-of-10-time-scales-in-ux/ (see p. 85).

[163] G. R. Gallaway, Response times to user activities in interactive man/machine computer systems, Proceedings of the Human Factors and Ergonomics Society Annual Meeting 25 (1) (1981) 754–758. doi:10.1177/107118138102500196. (see p. 85).

[164] R. E. Barber, H. C. Lucas, Jr., System response time operator productivity, and job satisfaction, Commun. ACM 26 (11) (1983) 972–986. doi:10.1145/182.358464. (see p. 85).

[165] F. Kozamernik, L. Vermaele, Will Broadband TV shape the future of broadcasting?, Tech Review 302, European Broadcasting Union (Apr. 2005).
URL https://tech.ebu.ch/files/live/sites/tech/files/shared/techreview/trev_302-kozamernik.pdf (see pp. 85, 106).

[166] R. Mekuria, P. Cesar, D. Bulterman, Digital tv: The effect of delay when watching football, in: Proceedings of the 10th European Conference on Interactive TV and Video, EuroiTV '12, ACM, New York, NY, USA, 2012, pp. 71–74. doi:10.1145/2325616.2325632. (see p. 86).

[167] W. J. Kooij, H. M. Stokking, R. van Brandenburg, P.-T. de Boer, Playout delay of tv signals: Measurement system design, validation and results, in: Proceedings of the 2014 ACM International Conference on Interactive Experiences for TV and Online Video, TVX '14, ACM, New York, NY, USA, 2014, pp. 23–30. doi:10.1145/2602299.2602310. (see p. 86).

[168] A. Begen, N. Glazebrook, W. Ver Steeg, Reducing channel-change times with the real-time transport protocol, Internet Computing, IEEE 13 (3) (2009) 40 –47. doi:10.1109/MIC.2009.67. (see p. 87).

[169] R. Rajah, Iptv: Optimizing channel change times, Presentation given at Telecom 2008 Conference, available at http://www.teamlightbulb.com/telecom2008_technology_papers.htm. Last

accessed on August 2nd, 2010. (04 2008).
URL http://www.teamlightbulb.com (see pp. 87, 87, 88, 88).

[170] H. Uzunalioglu, Channel change delay in iptv systems, in: Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE, 2009, pp. 1 –6. doi:10.1109/CCNC.2009.4784832. (see pp. 87, 87, 88, 88, 88).

[171] P. Siebert, T. Van Caenegem, M. Wagner, Analysis and improvements of zapping times in iptv systems, Broadcasting, IEEE Transactions on 55 (2) (2009) 407 –418. doi:10.1109/TBC.2008.2012019. (see pp. 90, 91, 108).

[172] ITU-T Recommendation Y.1541 : Internet protocol aspects - Quality of service and network performance: Network performance objectives for IP-based services, International Standard (Dec. 2011).
URL https://www.itu.int/rec/T-REC-Y.1541/en (see pp. 95, 96, 96).

[173] ITU-T Recommendation Y.1542 : Internet protocol aspects - Quality of service and network performance: Framework for achieving end-to-end IP performance objectives, International Standard (Jun. 2010).
URL https://www.itu.int/rec/T-REC-Y.1542-201006-I/en (see pp. 95, 96, 96).

[174] A. Shoufan, S. Huss, High-performance rekeying processor architecture for group key management, Computers, IEEE Transactions on 58 (10) (2009) 1421 –1434. doi:10.1109/TC.2009.88. (see pp. 95, 96, 99, 104).

[175] Microsoft Corporation, Acquiring high-resolution time stamps, Web Article, last accessed on March 16th, 2016.
URL https://blogs.oracle.com/dholmes/entry/inside_the_hotspot_vm_clocks (see pp. 103, 104).

[176] VMware Inc., Timekeeping in VMware Virtual Machines, Information Guide, last accessed on March 16th, 2016. (Nov. 2011).
URL https://www.vmware.com/files/pdf/Timekeeping-In-VirtualMachines.pdf (see p. 103).

[177] D. Holmes, Inside the Hotspot VM: Clocks, Timers and Scheduling Events - Part I - Windows, Web Article, last accessed on March 16th, 2016. (Oct. 2006).
URL https://blogs.oracle.com/dholmes/entry/inside_the_hotspot_vm_clocks (see p. 103).

[178] C. Sasaki, A. Tagami, T. Hasegawa, S. Ano, Rapid channel zapping for iptv broadcasting with additional multicast stream, in: Communications, 2008. ICC '08. IEEE International Conference on, 2008, pp. 1760–1766. doi:10.1109/ICC.2008.338. (see p. 104).

[179] A. C. Begen, N. Glazebrook, W. V. Steeg, A unified approach for repairing packet loss and accelerating channel changes in multicast iptv, in: Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE, 2009, pp. 1–6. doi:10.1109/CCNC.2009.4784878. (see p. 104).

[180] Z. Li, A. C. Begen, X. Zhu, B. Girod, Accelerated iptv channel change with transcoded unicast bursting, in: Proceedings of the 18th ACM International Conference on Multimedia, MM '10, ACM, New York, NY, USA, 2010, pp. 779–782. doi:10.1145/1873951.1874076.
URL http://doi.acm.org/10.1145/1873951.1874076 (see p. 104).

[181] Model validation of channel zapping quality, Vol. 7240. doi:10.1117/12.808114. (see pp. 107, 109).

[182] I. Kopilovic, M. Wagner, A benchmark for fast channel change in iptv, in: Broadband Multimedia Systems and Broadcasting, 2008 IEEE International Symposium on, 2008, pp. 1–7. doi:10.1109/ISBMSB.2008.4536622. (see p. 108).

[183] R. Kooij, K. Ahmed, K. Brunnström, Perceived quality of channel zapping, in: Fifth IAESTED Intern Conf on Communication Systems and Networks (CSN 2006), Aug 28-30, 2006, Palma de Mallorca, Spain; Proc. Pp, 2006, pp. 155–158. (see p. 109).

[184] F. Kuipers, R. Kooij, D. De Vleeschauwer, K. Brunnström, Techniques for measuring quality of experience, in: Proceedings of the 8th International Conference on Wired/Wireless Internet Communications, WWIC'10, Springer-Verlag, Berlin, Heidelberg, 2010, pp. 216–227. doi:10.1007/978-3-642-13315-2_18. (see p. 109, 109).

APPENDIX A

LIST OF PUBLICATIONS

[1] Tolga Arul and Abdulhadi Shoufan. *Subscription-free Pay-TV over IPTV* Journal of Systems Architecture, Volume 64, pp. 37–49, March 2016.

[2] Tolga Arul and Abdulhadi Shoufan. *Consumer Opinions on Short-Interval Charging for Pay-TV over IPTV* 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 147-153, Fukuoka, Japan, March 2012.

[3] Sunil Malipatlolla, Thomas Feller, Abdulhadi Shoufan, Tolga Arul, Sorin A. Huss. *A novel architecture for a secure update of cryptographic engines on trusted platform module* 2011 International Conference on Field-Programmable Technology (FPT), pp. 1-6, New Delhi, India, December 2011.

[4] Abdulhadi Shoufan, Tolga Arul. *A benchmarking environment for performance evaluation of tree-based rekeying algorithms* Journal of Systems and Software, Volume 84, Issue 7, pp. 1130-1143, July 2011.

[5] Abdulhadi Shoufan, Tolga Arul. *Multicast Rekeying: Performance Evaluation* Lecture Notes in Electrical Engineering: Design Methodologies for Secure Embedded Systems, Volume 78, pp. 85-104, November 2010.

APPENDIX B

LIST OF SUPERVISED THESES

[1] Stefan Pöschel. *Design und Implementierung einer plattformunabhängigen softwarebasierten IPTV Set-Top-Box.* Master Thesis, TU Darmstadt, August 2014

[2] Konrad Stahlschmidt. *Hardware-based Measures against Packet Loss in Streaming Applications.* Diploma Thesis, TU Darmstadt, November 2013

[3] Goutham Samala. *Extensions on an FGPA-based Multiplexer Design.* Practical Course, TU Darmstadt, September 2013

[4] Leonardo Solis Vasquez. *A Novel Set-Top-Box Architecture Providing Dynamically Reconfigurable Security Components.* Master Thesis co-supervised with Thomas Feller, ERASMUS - Politecnico di Torino, October 2012

[5] Björn Alexander Flubacher. *Implementierung einer IPTV Set-Top-Box mit Hilfe eines FPGA-Entwicklungsboards.* Bachelor-Thesis, TU Darmstadt, March 2012

[6] Patrick Neugebauer. *MPEG2-TS MUX / DEMUX mit Sicherheitsfunktionen für DVB-IPTV.* Bachelor-Thesis, TU Darmstadt, January 2012

[7] Sarmad Javed. *Dynamic routing setup for multicast traffic.* Practical Course, TU Darmstadt, November 2011

[8] Zuhaib Ahmed Chohan. *System on a chip set-top box for IPTV.* Practical Course, TU Darmstadt, August 2011

[9] Evgeny Bubnov. *Traffic shaping, quality of service and resilience for IPTV traffic transport in multicast networks.* Practical Course, TU Darmstadt, May 2011

CURRICULUM VITAE

Tolga Arul

PERSONAL INFORMATION

	Born in Frankfurt am Main, May 6th, 1980
email	tolga@arul.de

EDUCATION

1999	University-level Entrance Qualification
1999 – 2000	Alternative Civilian Service
2000 – 2009	Technische Universität Darmstadt
	Studies in Computer Science Minor Subjects: Psychology, Business Administration, Bionics
2009 – 2015	Center for Advanced Security Research Darmstadt (CASED)
	Scholarship Holder at the Cyber-physical Systems Security Laboratory
2009 – 2016	Technische Universität Darmstadt
	Research Associate at the Integrated Circuits and Systems Laboratory

TEACHING

Winter Semester 2009/2010	Reconfigurable Processors
	Supervision and Coordination of Tutorials, Co-supervised with Thomas Feller
Summer Semester 2012	Modelling of Heterogenous Systems
	Supervision and Coordination of Tutorials, Co-supervised with Marc Stöttinger