A Unified Mobile Payment Transaction Exchange Service (UMTES) for Next-Generation Mobile Networks

ABDULKAREEM ALJOHANI

A submission presented in partial fulfilment of the requirements of the University of South Wales/Prifysgol De Cymru for the degree of Doctor of Philosophy

September 2014

University of South Wales
Prifysgol De Cymru

CERTIFICATE OF RESEARCH

This is to certify that, except where specific reference is made, the work described in this thesis is the result of the candidate's research. Neither this thesis, nor any part of it, has been presented, or is currently submitted, in candidature for any degree at any other University.

Signed ……..

Candidate

Date ……..

Signed ……..

Director of Studies

Date ……..

Abstract

Mobile Payments (MP) have been evolving over a decade and proliferation is largely for contactless wallet services. Most such services are closed loop payment services provided by specific service providers. Even after a decade of trials, proliferation is limited to closed loop systems (Eg: Starbucks) and card based wallet services for contactless payments. Independent Payment Service Providers (IPSPs) providing managed wallet services are becoming popular and have the potential for MP based services. Providers like PayPal have begun to provide such services and are capturing the market.

Various studies have been conducted to investigate the lack of proliferation of MP. Three major causes are the heterogeneous nature of the m-payment landscape, lack of co-operation, interoperability amongst the various m-payment players and a lack of standardization. Towards this, the study proposes a classification model that is transaction-centric rather than the current models that are m-payment player-centric.

Services such as PayPal have the advantage of instant settlements for their subscribers. Wallet services serve a niche need for retail payments and specifically low value payments. The intention of providing interoperability between such providers is to fulfill the need for instant settlements for low value payments. This could, potentially target cash payments which require instant settlements.

This study details a service architecture and a service description. Based on this, the Unified Mobile payment Transaction Exchange Service (UMTES) protocol is designed for low value payments with instant settlements. The payment protocol intends to be Simple, Speedy and Secure. The UMTES design implementation performs comparably with the time taken for a cash payment process at a PoS when performance measurements are made in a simulated environment. The implementation has its limitations, a predominant one being that the existing regulations do not explicitly permit interoperability between IPSPs, although they are recognized as non-bank financial institutions.

Acknowledgements

All praise and glory to Almighty Allah (Subhanahu Wa Taalaa), the Creator, the Holy One, who gave me courage and patience to carry out this work. His many blessings have made me what I am today.

I would like express my unrestrained appreciation to my thesis advisor Prof. Khalid Al-Begain, for his constant interaction and guidance. Thanks are also due to faculty of Computing, Engineering and Science for their interaction, cooperation, comments and constructive criticism. Acknowledgement is due to the University of South Wales for supporting this research and providing me with necessary infrastructure and excellent research environment.

I am grateful for the financial support of the Saudi Ministry of Higher Education. Special thanks are also extended to the Saudi Arabian Cultural Bureau in London.

The entire research effort would not have been possible without the support and understanding of my immediate and extended family. My deepest gratitude and appreciation to my wife Areej Attiyah Aljohani who was there at every step to encourage me, my children Daliya, Khalid, Abdulaziz and Abdulmalik who showed patience and understanding towards my involvement in my work. My Late father's encouragement and blessings, my mother's continued prayers and blessings have given me the courage to persist and finish the research work. I extend my acknowledgement and heartfelt love to my brothers and sisters, who have been with me all the time to spur my spirits and encourage me.

Finally, a big thank you to all my friends and well wishers who made this research effort possible and approach fruitful completion.

Table of Contents

CERTIFICATE OF RESEARCH ..... **ii**
Abstract ..... **iii**
Acknowledgements ..... **iv**
Table of Contents ..... **v**
List of Tables ..... **xi**
List of Figures ..... **xiii**
List of Abbreviations ..... **xv**
Chapter 1 ..... **1**
1.1 Introduction 1
1.2 Research Problem and Motivation 2
1.2.1 Assumptions 7
1.3 Research Goal – A Summary 8
1.4 Thesis Contribution 10
1.4.1 Conceptual Contribution 10
1.4.2 Developmental Contribution 11
1.5 Thesis Outline 12
Chapter 2 Mobile Payments **14**
2.1 Background 14
2.1.1 Payments and Mobile Payments 16
2.1.1.1 Payments 17
2.1.1.2 Payment Costs 20
2.1.2 Mobile Payments 20
2.1.3 Mobile Payment Models 24
2.1.4 Mobile Payment Service Adoption 28
2.2 Motivation 30
2.3 Research Problem 33
Chapter 3 Literature Review **35**
3.1 Background 35
3.1.1 Mobile Payment Literature Review Methodology 36
3.2 Definition and Classification of Mobile Payments 38
3.2.1. Mobile Payment Definition and Mis-Conceptions 38
3.2.2 Mobile Payment Classification 39

3.2.2.1 Hierarchical Classification 41
3.2.2.1.1 Tier 1 – Proximity and Remote 42
3.2.2.1.2 Tier 2 – Medium, Mode, Value and Terms 44
3.2.2.1.2.1 Based on Value 44
3.2.2.1.2.2 Based on Technology 45
3.2.2.1.2.3 Based on Payment Relationship 45
3.2.2.2 Mobile Payment as Value Network 46
3.3 The Eco-system and Technology Enablers 48
3.3.1 Mobile Payment Eco-system 48
3.3.2 M-Payment Stake Holders 48
3.3.3 Technology Enablers 49
3.3.3.1 Mobile Devices Evolution 50
3.3.3.2 Mobile Infrastructure Technology 51
3.3.3.3 Categories of items purchased 53
3.3.3.4 Mobile Payment Protocols 54
3.4 Standards 59
3.4.1 MP Standards and Consortiums 59
3.4.2 Regulation and Standardization Challenges 61
3.5 The Gap 61
3.5.1 Payment Industry standardization Problems 61
3.5.2 Large-Scale Adoption Problems – From the Provider Perspective 62
3.5.3 Large Scale Adoption Problems – Consumer Perspective 63
3.5.4 Requirements and Expectations of the Mobile-Payment Players 64
3.5.4.1 Simplicity and Usability 65
3.5.4.2 Interoperability and Universality 65
3.5.4.3 Cost and Speed of Transaction 66
3.5.4.4 Security, Integrity, Privacy and Trust 67
3.6 Scope of Current Study 68
Chapter 4 Unified Mobile Payment Transaction Exchange Service (UMTES) 69
4.1 MP Service Architecture 69
4.1.1 Actors in the MP Service 69
4.1.2 A Layered Model for MP Services 71
4.1.3 The MP Service Architecture 72

4.1.4 Service Elements 74
4.1.4.1 Service Elements of the PSA 74
4.1.4.2 Service Elements of the PSC 75
4.1.4.3 Service Elements of the PSS 77
4.1.5 Ownership of the Service Elements 77
4.2 MP Service Definition 77
4.2.1 The Core Service 77
4.2.2 The Security Support 79
4.2.3 The Application 80
4.3 The UMTES Service Context 80
4.3.1 What does the service provide? 80
4.3.2 The Target Audience 81
4.3.3 Type of Payments 81
4.3.4 The Application 82
4.3.5 Security 82
4.3.6 Standards and Compliance 82
4.4 The UMTES Protocol 83
4.4.1 The UMTES Model 83
4.4.2 Design of the UMTES Model 85
4.4.2.1 The Payment Process 85
4.4.2.2 The actors in the process 85
4.4.2.3 Real time, end-to-end 85
4.4.2.4 Transport connections between the actors 86
4.4.2.5 Security components 86
4.5 UMTES Terminology 87
4.5.1 Addressing the Actors 87
4.5.2 Account 88
4.5.3 Identification of actors 88
4.5.3.1 User Identity 88
4.5.3.2 The PSP ID 89
4.5.4 Making a payment 90
4.5.5 Transaction 91
4.5.6 Commands and Responses 91
4.5.7 Message 92
4.5.8 Clients and Servers 92

4.6 Design objectives for the payment protocol 92
4.6.1 Simple 92
4.6.2 Speedy 93
4.6.3 Secure 93
4.7 Conclusion 95
Chapter 5 Implementation of the Unified Mobile Transaction Exchange Service (UMTES) 96
5.1 The UMTES Protocol 96
5.1.1 Objectives of the UMTES Protocol 97
5.1.2 Payment Scenarios Supported by UMTES 98
5.1.3 Operational Overview of UMTES 99
5.2 UMTES Protocol Description 100
5.2.1 UMTES Procedures – An Overview 100
5.2.1.1 User Registration 100
5.2.1.2 Payment Transactions 101
5.2.2 UMTES Commands 102
5.2.3 UMTES Command Responses 103
5.2.4 UMTES Command Response Information Exchange 104
5.2.4.1 REGISTER and ACK 105
5.2.4.2 REFRESH and ACK 106
5.2.4.3 SWIPE 107
5.2.4.4 INITIALISE (Payment Request) and ACK 107
5.2.4.5 AUTHORISE and ACK 110
5.2.4.6 CONFIRM 111
5.2.4.7 TRANSFER and ACK 111
5.2.4.8 CLOSE 113
5.2.4.9 CANCEL 114
5.2.4.10 ABORT 114
5.3 Payment Scenarios using UMTES 114
5.3.1 Payment at a Point of Sale (PoS) Terminal at a Store 116
5.3.2 Payment at a Point of Sale (PoS) on a vending machine 120
5.4 Extended Payment Scenarios using UMTES 122
5.4.1 Topping up the user account on the PSP 122
5.4.2 Person to Person (P2P) payments 123
5.5 Evaluation 123

Chapter 6 Evaluation of the UMTES Implementation 124
6.1 Evaluation of the Mobile Payment Solution 124
6.2 Estimating the Performance of the UMTES Implementation 124
6.2.1 Scenario for Estimation 124
6.2.2 Assumptions 126
6.2.2.1 The smart phone and the smart phone user 126
6.2.2.2 The Mobile Network 126
6.2.2.3 Other Assumptions 127
6.2.3 The Total Time of the Payment Transaction – T_{trans} 128
6.2.3.1 Time spent by the user, $\boldsymbol{Tuser}$ 128
6.2.3.2 Time spent on computing, $\boldsymbol{Tcompute}$ 128
6.2.3.3 The time spent on the network, $\boldsymbol{Tnetwork}$ 129
6.3 Estimating the transaction time 131
6.3.1 Estimating $\boldsymbol{Tcompute}$ 131
6.3.1.1 Estimating $\boldsymbol{Tapp\_s}$ and $\boldsymbol{Tapp\_c}$ 132
6.3.1.2 Estimating $\boldsymbol{TUMTES}$ 132
6.3.1.3 Estimating $\boldsymbol{TSSL}$ 136
6.3.2 Estimating $\boldsymbol{Tnetwork}$ 138
6.3.2.1 Estimating $\boldsymbol{TPQR}$ 138
6.3.2.2 Estimating $\boldsymbol{Tconnection}$ 141
6.3.2.3 The $\boldsymbol{Tnetwork}$ estimate 142
6.3.3 Estimating $\boldsymbol{Tuser}$ 142
6.3.3.1 Estimating $\boldsymbol{Tmobile\_user}$ 143
6.3.3.2 Estimating $\boldsymbol{Tmobile\_PoS}$ 143
6.3.3.3 The $\boldsymbol{Tuser}$ estimate 144
6.3.4 The Transaction Time Estimate 144
6.3.5 Discussion 144
6.4 Transaction delay estimates on a simulated network 146
6.4.1 Simulation Platform 146
6.4.2 Simulating UMTES and its verification 147
6.4.3 The Network Infrastructure and Topology 149
6.4.4 Simulation Scenarios 150
6.4.5 Calibration of the Network 151
6.4.5 Configuration for a simulation run 154
6.5 Comparison with other mobile payment protocols 159

6.4 Comparison with Cash Payments 161
6.5 Conclusion 161
Chapter 7 Conclusion 163
7.1 Achievements 165
7.2 Contributions 166
7.3 Limitations 167
7.4 Future Work 169
References 171
Appendix A Network simulation to measure the protocol performance 184
A.1 Simulation Package 184
A.2 Simulation Details 184
A.3 Application Configuration in OPNET 184
A.4 Results 188
A.5 Network Design 194
A.5.1 4G micro cell configuration 197
Appendix B Delay measurement plots from the network simulation runs ... 200
B.1 RTT Plots 200

List of Tables

Table 1: Additional actors in the MP context (Crowe M (2012)) 22

Table 2: Actors vs Models - Potential Revenues from an MP service 27

Table 3: Key Distinguishing features: Proximity vs Remote Mobile Payment (Source: Dewan and Chen (2005)) 43

Table 4: Value based classification 44

Table 5: Technology based classification 45

Table 6: Classification based on Payment Processing Value Chain (FirstPartner (2013)) 47

Table 7: A functional comparison of mobile payment schemes. A * indicates that the particular attribute is implied and not specifically mentioned in the proposal 56

Table 8: Operational comparison of mobile payment schemes. A * indicates that the particular attribute is implied and not specifically mentioned in the proposal 57

Table 9: Interoperability features of mobile payment schemes. A * indicates that the particular attribute is implied and not specifically mentioned in the proposal 57

Table 10: Stakeholder perspectives on MP services 65

Table 11: Categories of status codes in UMTES 103

Table 12: Notations used to illustrate the information exchange in UMTES 104

Table 13: Indicative message parameters 116

Table 14: The information exchange for the registration process in UMTES 117

Table 15: The information exchange for a payment transaction 120

Table 16: The information exchange for the initialisation and close in proxy mode 122

Table 17: UMTES - Command and Argument sizes in Bytes 132

Table 18: Data size after encoding in XML 133

Table 19: Encoding, Encryption and Hash for the application data 135

Table 20: The application data size at the network layer 135

Table 21: Total delay for encryption and hashes at the application and SSL layers 136

Table 22: Compute time elements on the client and server. UMTES and SSL processing are similar. The server compute times are estimated on the client platform itself. 137

Table 23: Uplink and Downlink bandwidth for wireless mobile access networks 139

Table 24: Network transit delays on 3G, 3.5G and 4G wireless networks 140
Table 25: TCP connection time (Three way hand shake)..... 141
Table 26: Network delay component of SSL Handshake 141
Table 27:The time spent on establishing a secure connection to the PSP servers..... 142
Table 28: List of user interactions with the smart phone to make a payment..... 143
Table 29: Transaction time components, estimated 145
Table 30: The sequence of actions for making a payment and the time taken 145

List of Figures

Figure 1: The Purchase Process - functional components, simplified 16
Figure 2: Payment Order and Payment Transaction Semantics 18
Figure 3: Clearing House, Settlement and PSPs 19
Figure 4: Evolution of MP from Mobile Banking (Crowe M (2012)) 21
Figure 5: Mobile Payments Eco-system (Crowe M (2012)) 22
Figure 6: Bank-centric model - the bank owns and provides the entire service 25
Figure 7: Operator-centric model - the operator owns and provides the entire service 25
Figure 8: Collaborative Model - Banks and MNOs own and provide the service 26
Figure 9: Independent PSP (IPSP) model - The IPSP owns and operates the service an provides a single access point to the user 27
Figure 10: Literature Review Methodology 37
Figure 11: Hierarchical Classification of Mobile Payments 42
Figure 12: Proximity payments vs Remote payments 43
Figure 13: An example value network (Allee V (2011)) 47
Figure 16: Global mobile phone subscription, * = estimates (ITU (2013)) 51
Figure 17: Framework of factors impacting MP services 61
Figure 18: Model attributes of system acceptability (Nielsen 1993) 66
Figure 19: The Independent PSP model overlaid with the TSM interactions for Mobile Contactless Payments 70
Figure 20: The Three Layer Model for Payment Services 71
Figure 21: The IPSP model with the three payment service layers 72
Figure 22: The Generalised Three layer model for Payment Services 73
Figure 23: Payment Service Architecture showing the interfaces between layers. The PSU is part of the PSA layer 74
Figure 24: The generic UMTES service model 83
Figure 25: UMTES Protocol Stack on the Client and the Server 96
Figure 26: An overview of the UMTES protocol operation 99
Figure 27: Functional interaction of UMTES in Direct mode 115
Figure 28: Functional interaction of UMTES in Proxy mode 121
Figure 29: The Payment scenario considered for estimating the total time for a transaction 125
Figure 30: Time Components of the User Interaction 128

Figure 31: Time Components for Computing at the Clients and Servers 129
Figure 32: Time components of the Network Component 130
Figure 33: Wired and Wireless network segments in the path from the client to the server 139
Figure 34: Command and Data Transfer logic in the application modeller..... 147
Figure 35: Network topology for the transaction delay measurements on 3G..... 148
Figure 36: Simulation testbed for functional verification of the application protocol 148
Figure 37: Delay measurements of REG (green), TRAN (red) and REG+TRAN (blue) 149
Figure 38: Network topology for the transaction delay measurements on 4G..... 150
Figure 39: LTE - Macro Cell and Micro Cell configurations..... 150
Figure 40: Http traffic generated by 20 active users in a 4G Macro Cell 151
Figure 41: Http background traffic generated by ten active users on 3G 151
Figure 42: Video stream traffic received by one user 152
Figure 43: No Load transaction delay on the 3G network segment 153
Figure 44: No Load transaction delay on the 4G Network Segments 155
Figure 45: Transaction delay when 300 payer/payees were randomly initiated ... 155
Figure 46: Transaction delay in 4G Micro cells when randomly initiated..... 156
Figure 47: Packet drops on the uplink, under load 157
Figure 48: Packet drop rate on the downlink, under load 158

List of Abbreviations

3G	Third Generation Cellular Network
4G	Fourth Generation Cellular Network
ACM	Association for Computing Machinery
AES-256	Advanced Encryption Standard - 256
APDU	Application Protocol Data Unit
API	Application Programming Interface
ARPU	Average Revenue Per User
B2B	Business-To-Business
B2C	Business to Consumer
BRC	British Retail Consortium
CPU	Central Processing Unit
DoS	Denial of Service
EDI	Electronic Data Interchange
EFT	Electronic Funds Transaction
EMV	Europay MasterCard and Visa
EPC	European Payment Council
EPS	E-Payment System
ETSI	European Telecommunications Standards Institute
EUPC	European Payments Council
EVDO	Enhanced Voice-Data Optimized or Enhanced Voice-Data Only
F2F	Face to Face
FQDN	Fully Qualified Domain Name
GP	Global Platform
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GSMA	GSM Association

HSPA	High Speed Packet Access
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBAN	International Banking Account Number
IEEE	Institute of Electrical and Electronics Engineers
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPSEC	Internet Protocol Security
IPSP	Independent Payment Service Provider
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IR	Infrared
ISO	International Standards Organisation
ITU	International Telecommunications Union
IVR	Interactive Voice Response
J2ME	Java 2 Platform, Micro Edition
JSON	JavaScript Object Notation
LAN	Local Area Network
LE	Low Energy
LTE	Long-Term Evolution
MIME	Multi-Purpose Internet Mail Extensions
MITM	Man In The Middle
MMOGs	Massive Multiplayer Online Games
MNO	Mobile Network Operator
MP	Mobile Payment
MSET	Mobile Secure Electronic Transaction
MSISDN	Mobile Station International Subscriber Directory Number
MSP	Mobile Network Service

MTM	Mobile Trusted Module
MTU	Maximum Transmission Unit
MVAS	Mobile Value Added Services
NFC	Near Field Communications
NMG	Networld Media Group
OEM	Original Equipment Manufacturer
OTA	Over The Air
P2P	Business to Consumer
PCI	Payment Card Industry
PDA	Personal Digital Assistant
PI	Payment Instruments
PIN	Personal Identification Number
PIU	Physical Interface Unit
PO	Payment Order
PoS	Point of Sale
PS	Payment Service
P-SMS	Premium SMS
PSP	Payment Service Provider
PSU	Payment Service User
PT	Payment Transaction
PTD	Personal Trusted Device
RFID	Radio Frequency Identification
ROI	Return On Investment
RTGS	Real Time Gross Settlement
S/MIME	Secure/Multipurpose Internet Mail Extensions
SD	Secure Digital
SE	Secure Element
SEPA	Single European Payments Area
SET	Secure Electronic Transaction

SHA-256	Secure Hash Algorithm-256
SIM	Subscriber Identity Module
SIU	Service Interface Unit
SMPP	Short Message Peer-to-Peer
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAN	Transaction Authentication Number
TCG	Trusted Computing Group
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPC	Transaction Processing Council
TPC-E	Transaction Processing Council - OLTP workload
TSM	Trusted Service Manager
UDP	User Datagram Protocol
UICC	Universal Integrated Circuit Card
UMTES	Unified Mobile Payment Transaction Exchange Protocol
UMTS	Universal Mobile Telecommunications System
USSD	Unstructured Supplementary Service Data
UWB	Ultra-wideband
VAS	Value Added Service
VASP	Value Added Service Provider
WAN	Wide Area Network
WAP	Wireless Application Protocol
WiFi	Synonymously used with Wireless Local Area Networks
WiMAX	Worldwide Interoperability for Microwave Access
WPA2	Wi-Fi Protected Access II

WSDL	Web Services Description Language
WWW	World Wide Web
XBRL	eXtensible Business Reporting Language
XML	Extended Markup Language

Chapter 1

1.1 Introduction

The proliferation of the Internet and its ubiquity in the current context has led to the access of several automated services, online. The success of the Internet has been the continuous evolution of its technologies and services. Its two flagship services, the electronic mail (e-mail) and the World Wide Web (WWW) that enable a user, access to and transfer of information from/to sources connected to the Internet, was the primary reason for its vast proliferation. Information content has grown from text-only to multimedia. The Internet continues to evolve in various technical directions, and remains ubiquitous in the present day context.

The Internet which started off as a network of academic and research institutions has seen the growth of the use of the Internet for commercial purposes. While online shopping sites were the frontrunners, the services of the financial markets such as stock and share trading, online banking and similar services were provided access from the Internet. In short, any online service that is available, extends its access via the Internet as well. Security concerns such as secure access and information privacy are handled by the use of authentication and encryption mechanisms. In fact, the impact of the Internet on commerce, as an enabler, is so immense that growth rates of various economies are linked with the proliferation of the Internet.

Over the last decade, mobile telecommunications have dominated voice services and have has an unprecedented growth rate and proliferation (ITU 2013). This is especially so in growing economies. These telecommunications networks have evolved to provide access to the Internet from the mobile phones. Similarly, mobile phones have evolved from providing access to specific services (typically hosted by the mobile telecommunications provider) via Internet access to providing access via the Internet to all services. Such a wide spread access is primarily due to the change in the software system on the mobile device that has changed from a proprietary implementation to a open standards compliant system. Therefore, customised applications for

specific services are available. Typical examples are applications provided by super stores and super markets, newspaper companies, transport ticketing (bus/train/air/cruise) providers, etc. These applications, executing on the mobile phone, access the services via the Internet, using the mobile telecommunications network.

An important component of using these services successfully is being able to make payments for services. It is in this context that Mobile Payments (MP) began evolving more than a decade ago. As a service, MP have evolved along with the rest of the eco-system which consists of the Mobile phone manufacturers, the mobile telecommunications providers, the financial institutions that provide payment services and the end user requirements. However, despite the immense potential of the service, it has not proliferated as much as was expected.

1.2 Research Problem and Motivation

There are several reasons mentioned for the lack of proliferation of MP services. They are discussed in Chapter 2. One clear reason is that the entire eco-system (both the business and technology elements) has been in a state of evolution. The only constant has been the payment process. The technology elements such as the mobile devices (phones, tablets, etc.), the software development and availability of applications software for the mobile devices, the telecommunication network infrastructure (bandwidth availability), high speed wireless access from the mobile device to the mobile telecommunications network (3G/4G/WiFi/WiMAX) are all enablers of the MP service that are in a fairly evolved and stable state. Evolution is still evident in the business side of MP (Chaix, L; Torre, D (2012). The details are discussed in section 2.1.4 of Chapter 2.

On the business side of MP, the provider space is evolving. Traditionally, financial institutions would provide MP services. Independent providers have begun to provide payment services. Typical examples of such providers are PayPal and Google Wallet. These providers enable users to have a single access to all their payment requirements. Users, who register to the service and provide their card (credit/debit) related information, can make payments

using their cards. The provider will initiate the payment on the user's behalf and when necessary, as in the case of debit cards, the user will confirm the payment by authenticating online with the issuer.

Users can make instant payments to other members of the same provider. So, the payment made by a payer to a payee will cause an instant transfer of value to the payee's account, if both the payer and payee are members of the same provider. Inter-provider transfers typically use the services of clearing houses and are dependent completely on the service times of the clearing house for the transfer of value to the payee's account. Therefore, inter-provider transfers delay the availability of funds for the payee.

This, ironically, brings back the situation the card companies faced during their evolution. The payer and the payee required to be members of the same payment service provider for the lowest cost of the payment transaction and for instant payments. Inter-provider payments are expensive compared to intra-provider transfers. This is a significant problem that impedes the adoption of MP services today. The problem is that while the payment process is fast and available to use anytime, anywhere, the funds are not available to the payee, instantly.

The Banking industry has addressed the funds availability for the payee by implementing fast payment clearing systems supplemented by services such as the Real Time Gross Settlements (RTGS) (Dent, A., & Dison, W. (2012)). However, these schemes are for high value payments only. Small businesses (payees), who only deal with low value payments or even cash payments which are typically about £10 (BRC 2012), will benefit from an instant fund availability following a payment. Such a facility should lead to higher adoption of the MP services, since the payees will see the value in supporting MP.

From a business and infrastructure perspective, there are two requirements for instant fund availability – a completely interoperable payments process that can facilitate instant transfers and a physical computing and network infrastructure to support the interoperability. This forms the basis of our motivation for the research.

Payment primarily addresses the need of the payer. It does not address the availability of funds to the payee, following a payment. Literature addresses

various means of enabling MP such as protocols, security, wallets, etc. and business related issues relating to service provider business models, Regulatory issues and standards, studies on MP adoption and the lack of it and so on. What is clearly missing in the literature is an analysis of processes beyond the completion of the payment and funds availability to the payee.

In this context, our questions are the following:

1. Each mode of payment by a user (credit card/debit card/direct debit) requires a separate access to the respective payment provider. Providers such as PayPal provide the users with a service where they have a unified access to their payment modes and can instruct PayPal to make a payment on their behalf, using payment instrument of choice of the user, other than cash. However, payments between users who are members of different providers are still routed via the banking infrastructure
2. *What is necessary to provide interoperability between the various payment providers?* Banks and similar financial institutions use the SWIFT infrastructure for payment interoperability between them. Clearly, there is a similar need for an interoperable facility between the payment providers who are not banks or credit card companies.
3. *Is this need for interoperability being addressed by the regulatory authorities?* Payment service providers are not classified as Banks. Regulators have just about begun to address the evolution of the MP eco-space and have acknowledged the arrival of independent payment service providers who are neither banks nor credit card companies. While there is this acknowledgement, the regulatory guidelines for several functional and operational aspects for the independent payment service providers are yet to evolve.
4. *What is necessary to transition cash payments which have an average transfer value of £10* (BRC 2012) *to mobile device platforms?* Cash payments provide the payee with instant funds availability. Small businesses require such availability One of the impeding factors for making the very low value payments which represent cash transaction values is the cost of the payment transaction. From a merchant's

perspective, it is the cost of payment collection. That cost for debit card transactions is about 9p per transaction (BRC 2012).

5. *Will facilitating cash payments using mobile devices accelerate adoption of MP?* More than half the number of payments made in 2012 are in cash (BRC 2012). These are of low value but constitute a large volume. Card based payments have well established means of being dealt with online and via mobile devices (typically via wallets). Enabling users to make low value payments is not a significant problem, technically, but ensuring that these low value payments are available to the payee/merchant instantly is the objective. Should this be made possible with the inter payment service provider operability (Q1, mentioned above) and with the reduced cost of transaction (Q2, also mentioned above), such payments using mobile devices can begin to grow. Cash payments, when common place, makes it obvious that the overall MP adoption will increase.
6. *Is it possible to evolve to cashless payments without having to resort to electronic currency?* With the reduced costs of low value transactions and a large proliferation of MP, all payments can be done in real time and the payees will receive the transfer of value, instantly. All other payment modes are accessible and usable with mobile devices. This leads us to a situation where the use of currency and coins (cash) will reduce to a large extent. Therefore, it is possible to evolve towards a cashless payment system. However, there could be cash payments of a transfer of value equal to or less than the cost of the transaction where such payments may become infeasible. Such instances may still require the use of currency until there are other means by which such payments become feasible.

The user experience of mobile voice and data services impact the user adoption. The data services are provider and tariff dependent. Access speeds and hence throughputs tend to vary depending upon the location (signal strength and coverage) and the access load on the base station (number of associations). Traffic from services such as MP are typically made up of short packets and tend to use connection oriented protocols for transport. Ideally, packet retransmissions should be avoided so that the service delays are

minimised. Mobile payment services will benefit if the mobile network operator provides a consistent service level to the users. Therefore, a few questions arise from a networking perspective, in the context of mobile payments.

1. *What would the user experience be at a large super store where there are several users attempting to make a mobile payment at the same time?*
2. A related question to this is *How would the mobile network operator handle mobile payments at a super store where several users would concurrently access its data services to make mobile payments?*
3. In general, *how would the MNO handle a scenario which involves a large number of concurrent payments and be able to provide a good user experience?*

These questions are important and indicate the critical role of the MNO in the context of mobile payments. Existing technologies may require over provisioning of bandwidth to sustain a consistent user experience. This will result in the mobile network operator offsetting costs to the mobile payment service. However, there are emerging technologies such as Software Defined Networking which hold a promise for dynamic provisioning of bandwidth. Deployment of software defined networking can optimise the bandwidth usage on the provider network and result in a low impact on the cost of the services to the end user. The overall objective is to ensure that the network access and usage costs are not severely impacted with the need for a guaranteed service level for mobile payment services. The manner in which these costs add on will have an impact on the adoption of the mobile payment services.

Our primary focus of the research is on two of the core questions mentioned above – to propose a standardised means of interoperability between payment service providers to enable instantaneous transfer of value between the members of the providers. Towards this, a protocol is designed and a prototype implemented and evaluated. In addition to this, the feasibility of making low value transfers using mobile payments as a substitute for cash payments will be explored.

1.2.1 Assumptions

The research work proceeds making the following assumptions which it deems are changes that are extremely likely in due course of time.

1. Users
    - The personal device used for payments will be a mobile phone or any mobile device that also has access via a subscription to the mobile network access provider. The subscription with a network provider serves for an additional point of authentication for the device being used for payments.
2. Regulations
    - The regulatory authorities see the need for non-banks such as payment service providers to perform settlements.
    - The regulatory authorities permit the payment service providers to perform low value settlements between themselves, directly, since this involves a lower financial risk for the participating providers.
    - The regulatory authorities will provide broad guidelines for the interconnectivity and services for such low value settlements between the payment service providers
3. Mobile Devices
    - All mobile phones will be 4G enabled and will either be smart phones or feature phones with high speed network access.
    - The phones will also be WiFi enabled
4. Network Access
    - 4G will proliferate sufficiently to provide ubiquitous access
    - Mobile network operators will also deploy WiFi access in dense areas to offset traffic from the radio access network
    - Roaming charges will reduce significantly since mobile termination charges are reducing almost exponentially.
5. Point of Sale (PoS) Terminals
    - All PoS terminals will be enabled with contactless data transfer capability. Contending technologies are NFC and Bluetooth LE (also known as Bluetooth Smart). These technologies enable very short range communication using low power and are

primarily used to exchange information between the PoS and the payer's mobile phone for purposes of making a payment.

- Vending machines that provide goods/services are also enabled with such contactless technologies to enable payments.
- The vending machine is not connected to any specific network. It communicates via the payer's mobile device by sending messages to its provider. With this possibility, the investment on providing an "always on" network connectivity for vending machines is eliminated. This might help in reducing the overall transaction costs.

1.3 Research Goal – A Summary

The primary objective of the research will be to facilitate a means of providing interoperability between the payment service providers. In our context, payment service provider implies an independent payment service provider who collaborates with various actors in the eco-system such as mobile network operators for access, Trusted service managers to provide the payment service platform on the mobile devices and banks and credit card companies to transact with on behalf of the user. The need for interoperability between such providers is illustrated in scenario 1, below.

Scenario 1 – User A, a member of provider P_1 wants to make a payment of £N to User B, a member of provider P_2. Currently, such a transfer requires that both A and B be members of a bank or a similar institution and the transfer of funds is made between their accounts in their banks. Two problems arise – Firstly, User A has to initially transfer money from the account with the provider P_1 the account with the bank and subsequently initiate another transfer to user B's bank account. User B will then have to transfer those funds from the bank account to the account with the provider P_2 . Secondly, this transfer of funds take a large amount of time. In other words, the funds are available for use to B after a substantial delay (of about 4-6 days).

Presently, the payment service providers do not have a direct means of exchanging payment information as well as the transfer of value between themselves. The financial services sector has a process for making payment

transfers between participating institutions such as banks, as a part of the settlement services. Settlements are governed by specific regulations. Regulations currently only authorise institutions registered as banks to provide settlements.

The inter payment service provider interoperability addresses the settlement between the providers for transfer of funds between their member accounts. This is the first objective of this research and is addressed by designing a payment protocol that provides support for the payment process as well as to initiate and complete the inter provider funds transfer in real time.

Scenario 2 – User A requires to pay a parking fee of 50p and subsequently requires to pay £1.35 for a snack. The user can make these payments only in cash and cannot use either a debit or credit card. The limiting factor is the cost of the transaction. Can such payments be made electronically via mobile devices?

There are two specific issues here – identify the potential means to reduce transaction cost so that small payments via mobile devices are feasible and how expensive would upgrades of the PoS for such payments be? The latter influences the cost of the transaction which requires to be minimised. However, our focus will be on identifying potential for transaction cost reduction, excluding the PoS upgrades and related migration costs. This is the second objective of this research. The impact of making such payments feasible will be a step towards a cashless society.

The overall goal of this research is the following:

1 Facilitate interoperability between payment service providers to enable transfer of value between their respective members. Define and design a protocol for interoperability as well as for payments. Each payment will initiate a transfer of value. The transfer of funds between the providers should be done in near real time. Such transfers will hold for small value payments which implies lower financial risks for the payment service providers.

2 Suggest a interoperability infrastructure framework for interoperability between providers. The infrastructure should ensure that providers physically interconnect with each other for purposes of interoperability.

Further, the connectivity should not be more than one network hop between any two interoperable providers.

3 Attempt to minimise the transaction cost components such that low value payments are feasible using mobile devices.

1.4 Thesis Contribution

The thesis details the contributions made to knowledge in two ways – the conceptual contributions and the development contributions.

1.4.1 Conceptual Contribution

Understanding and investigation of the processes and evolving services in the payment services market provided the basis for the conceptual contributions in this thesis.

- Mobile payments are classified in several ways based on different criteria. While most of the classifications are flat in nature, a hierarchical classification is proposed. The hierarchy for mobile payment begins with two branches which are Remote Payments and Proximity payments. Each of these branches are further classified using Medium of payment, Value, Technology, Terms and Relationship. The details of this classification are in Chapter 3 and published as

  Aljohani, A.; Al-Begain, K., "Transaction-centric Mobile-Payment Classification Model," ***Next Generation Mobile Apps, Services and Technologies (NGMAST), 2013 Seventh International Conference on*** **, vol., no., pp.68,74, 25-27 Sept. 2013**

- Several studies on mobile payment systems do acknowledge the fact that mobile network operators play a critical role in mobile payment services. They provide the means of access to the payment services. From a services perspective, there are clearly three functional components – the access function to the mobile payment services, the mobile payment service and the back end function of settlements which facilitates the transfer of funds corresponding to the payer's request to transfer a value. The second conceptual contribution of the thesis is a technical perspective of the payment services presented as

a layered model. The details of this three layer model for payment services are in Chapter 4 and they have been published as **Aljohani, A., "Mobile Payments with Instant Settlements", *Next Generation Mobile Apps, Services and Technologies (NGMAST), 2014 Eightth International Conference***.

- While all mobile payment systems address the payment initiation and confirmation, the transfer of value to the payee is not instantaneous. This is particularly true in the case of payment service providers who are not banks and rely on institutions like banks to perform the actual transfer of value. For non-bank payment service providers to perform transfer of value, they require to be interconnected and interoperate. Instant transfer of value is specifically important for small retail businesses since they rely heavily on cash flow to sustain their businesses and cannot afford credit on payments. The third conceptual contribution is to propose the interoperability for the evolving payment services market. The details of the protocol are in Chapter 4
- Interoperability between providers requires to be facilitated. The fourth conceptual contribution is the proposal of a protocol for interoperability of services between providers. The protocol performs the payment function from the user end and completes the transfer of value to the payee using the interoperability platform, in near real time. The functional and operational details of the protocol are in Chapter 5

1.4.2 Developmental Contribution

The developmental contribution arises from the implementation of the conceptual contribution. The primary contribution is the implementation of the payment and interoperability protocol which is termed as Unified Mobile Payment Transaction Exchange Service (UMTES) protocol. The core protocol is implemented as a library that can be integrated with applications.

The secondary contribution is an example application that is developed using the payment system library. The application emulates a payment requirement, uses UMTES to make a payment. A similar application, emulating a payee displays the receipt of funds into its account. These applications use an

emulated infrastructure setup to demonstrate the functioning of the protocol and other related features of the service.

In summary, the research provides conceptual contributions of which the important contributions are demonstrated with implementations. The implementations are the developmental contributions.

1.5 Thesis Outline

The research problem is established in the current chapter and the rest of the thesis is organised as follows:

The definitions of a payment, its components and the interactions form the beginning of Chapter 2. Further, the definition of mobile payments, how mobile payments are distinct from m-commerce or mobile banking are illustrated in this chapter. It then discusses the various mobile payment models from the literature and illustrates the differences between them. The independent payment services provider model chosen for purposes of the research is illustrated. The chapter ends discussing mobile payments service adoption and the reasons why the proliferation is not as it is expected to be.

The survey of available literature on mobile payments in the context of the motivating factors are discussed in chapter 3. The methodology of the literature survey is presented. The literature review comprises of three phases each of which addresses a specific issues in mobile payment. Phase one discusses the classification of mobile payments and proceeds to propose a hierarchical classification for mobile payments. Phase 2 discusses the mobile eco-system - the stake holders, the technology enablers and the evolution of the mobile device. Phase 3 takes a look at the standards and consortiums that concern mobile payments. The survey then illustrates where the gap in the research exists and ends mentioning the scope of the study and research.

Chapter 4 provides a new perspective of the payment services. The various functional components of the payment services are grouped into layers and presented as a three layered functional model. This model is used to illustrate

the payment function and its fulfilment. The service is defined with respect to the model and the chapter ends with illustrating the complete service flow indicating the payment, the fulfilment of the payment and the transfer of funds to the payee’s account.

Chapter 5 details the UMTES protocol from a functional and operational perspective. It provides the details of the UMTES service elements that enable a transaction flow. This is followed with an illustration of the data that is exchanged between the peer entities. Two specific payment scenarios are discussed and the data exchanged between the actors is illustrated.

Chapter 6 details the evaluation of the implementation on a typical infrastructure and provides estimates of the total transaction time. The estimates are based on various statistics available in literature. Following this, a measurement of transaction delays are made on a simulated network. Then, a comparison of the estimated transaction time is made with the delay observations, made by the industry.

Chapter 7, the final chapter, concludes the thesis with a summary of the study, lists the achievements with respect to the objectives set and suggests the possible enhancements to the research and implementation of the payment system.

Chapter 2
Mobile Payments

2.1 Background

Telecommunications services have evolved over the last decade to provide data access services over their networks that were primarily built to provide voice services. With this convergence of voice and data services over a single mobile network infrastructure, mobile data access services have seen a large proliferation in the last few years. These services have been available as wireless broadband access using 3G and 4G network access technologies. Mobile network operators (MNOs) are in the process of enhancing their data carrying capacity due to the large demand for mobile data access. The fact that the user can be mobile (*i.e.,* the devices use wireless access to the Internet and can switch across wireless access technologies without interrupting the services being accessed by the user) enables them to access networked services, *Anywhere, Anytime*. With mobile phones evolving into smart phones and the proliferation of smart phones expected to be at a 10 % compound annual growth rate during 2012-2016 (Technavio 2012)., MNOs are looking at various opportunities to increase revenues and provide a larger portfolio of services.

Mobile devices like Smart Phones, Personal Digital Assistants (PDAs), and Tablets have currently an increased proliferation. Key factors contributing to this growth are the decline in smart phone prices and the rapid technology advancements of smart phones.. These devices have a reasonable computing power and memory resources as well as Internet connectivity, primarily through Wireless Broadband (3G, 4G, WiMax, etc.) and Wireless LANs. End users are able to perform a range of tasks using services such as e-mail, on-line video and audio streaming, video/audio conferencing, online gaming and so on. These services are accessed through various applications (apps) that are front-ends to the services accessed by the user.

In the recent past, these devices have been used as a means to access banking services other than withdrawals. Such online access to banking

services have become very popular and are being adopted widely by end users. These services are termed as Mobile Banking Services (m-Banking). Initially, access to user account information alone was provided but subsequently, some banks have permitted authorisation of money transfers to mobile users. Typically, these services have been made available via an application that is distributed by the bank. The application runs on the mobile device and is considered as a trusted client by the banking service.

Mobile banking services have been possible due to the availability of a robust mobile service provider (MSP) infrastructure and services. The MSP provides Internet access to its subscribers, thereby enabling its community to participate in online services accessible via the Internet. The evolution of e-commerce into mobile-banking is enabled by the convergence of the Telecommunications and the Internet, the proliferation of mobile telecommunication networks and mobile devices and consequently the evolution of support for m-banking from the financial institutions.

Mobile user services portfolio has now evolved to include making payments for purchases. The user should be able to make a payment to the seller from whom she/he has purchased goods or a service by using his mobile device (and not her/his physical wallet). Such payments are termed as Mobile Payments (MP). They are initiated, authorised and confirmed by an end user using a mobile device. MPs are constantly evolving and growing steadily in volumes, over the last few years.

Gille 2005 lists the mobility attributes that characterise the transition from e-commerce to m-commerce and affects the service provision by the payment providers as it does the user expectations. The attributes are

1. **Ubiquity** - access to information and services independent of the current location and in real-time
2. **Reachability** – mobile device when powered on are instantly connected to the network and remain connected to the network until they are either specifically logged out or powered off
3. **Security** – apart from operating the service with trusted partners, a new set of potential threats in the mobile environment have to be dealt with

4. **Convenience** – the mobile devices, such as phones have a higher level of ease of use and therefore providing m-commerce services via the device will have a convenience factor
5. **Personalisation** – mobile devices are almost always personal devices and not shared. Providing personalised information and services will be beneficial to both the user and the provider
6. **Location Reference** – can be a basis for directing personalised information as well as for purposes of authentication

Mobile payment services are based on these attributes too. It is these mobility attributes that enable value-added services (VAS) and provide product-differentiation. Applying different combinations of the attributes provide *location-based* services, *situation-based* services and *person-based* services.

2.1.1 Payments and Mobile Payments

Payment is a part of the Purchase/Procurement process. Consequently, it is

Figure 1: The Purchase Process - functional components, simplified

part of a contract/agreement between the buyer and the seller. The contract specifies the terms of payment and the payment is made by the buyer to the seller, in exchange for the goods that are delivered as per the contract. Fig 1 represents this simplified view of the functional components of a purchase

process. The goods are quoted for by the seller, the buyer agrees to buy the goods and delivers them upon receiving the payment. Our focus is on payment and the means that the seller uses to transfer funds to the buyer.

2.1.1.1 Payments

Payments are effected using *Payment Instruments*. Payment Instruments (PI) are the means provided to the user by the financial institution (Banks, Credit card service providers, termed in general as Payment Service Providers – PSPs, etc.) she/he is subscribed to. A PI enables a *Payment Transaction* (PT) whose execution constitutes a *Payment Service* (PS) provided by a PSP. The PT is the manifestation of the execution process that results in providing the PS.

The definition of Payment Instrument by the Payments Council, UK (UKPC 2012) is as follows:

"payment instrument" means any:

(a) personalised device; or

(b) personalised set of procedures agreed between the payment service

user and the payment service provider, used by the payment service user in order to initiate a payment order

The term "device" included physical devices such as cards and SIM cards. It was extended to include mobile phones, later, the same year and read as follows:

This definition is meant to cover physical devices (such as cards or mobile phones) and/or [a] set of procedures (such as PIN codes TAN codes, digipass, login/password etc) which a payment service user can use to give instructions to his payment service provider in order to execute a payment transaction.

A *Payment Order* (PO) is an advice to the financial institution about a payment but does not constitute a payment procedure or a payment itself. It is an instruction from a payer or a payee to the PSP to initiate a payment. A PO can result in a PT if all the terms of the contract (between the payer/payee and the PSP as well as legislation covering the service provision) are met, there are enough resources in the payment initiator's account for the value

transfer/deduction and all information necessary for the transaction are provided by the payment initiator. A PO may be revoked if these are not met. If all the terms are met, the user requires to confirm to the bank to proceed with the transfer of value to the payee. The bank then effects the transfer of value, resulting in a debit and a credit to the payer and payee accounts. The PO therefore results in a PT which causes the transfer of value between the accounts.

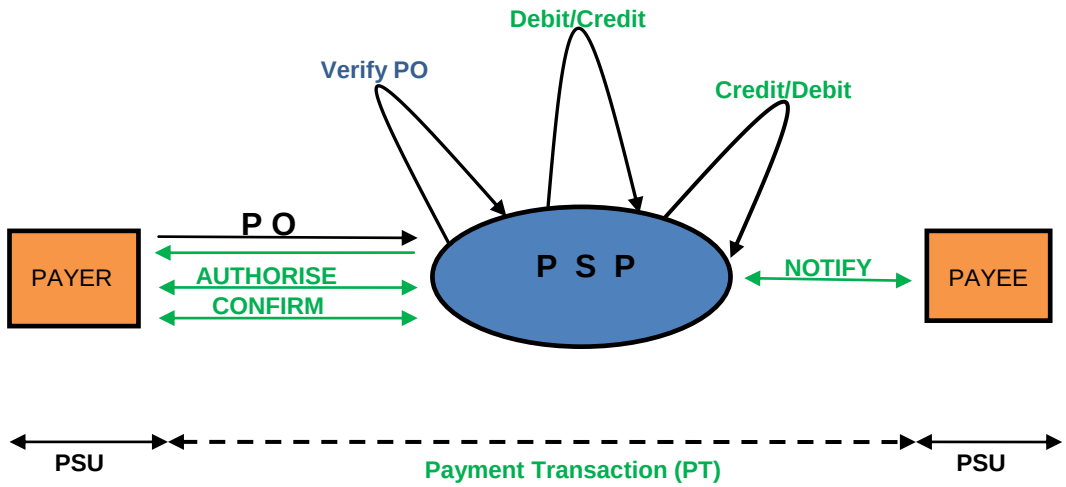


Figure 2: Payment Order and Payment Transaction Semantics

Figure 2 illustrates the interaction between two Payment Service Users (PSU), the payer and the payee through the PSP when availing the payment service. Once the PO, sent by the payer is verified, the payment transaction is initiated and the payer authorises and confirms the request for value transfer to the PSP. The transfer of value is indicated as the “Debit/Credit” and “Credit/Debit” actions in Fig 2.

In the context of mobile payment, a mobile device is the access front-end to a PSU, the payer, for interaction with the PSP. The payment process is completed with the PSU initiating, authorising and confirming to the PSP, a transfer of value to another PSU, the payee. The payer could use a payment instrument of her/his choice to make the payment unless the payee limits this choice to the payer.

Fig 2 is a comprehensive illustration in the sense that it does not indicate a generic scenario. For eg., it is not necessary that both the payer and the payee be subscribed to the same PSP for payment services. They could be subscribed to different PSPs and still transact. In such a case, the payer's PSP and the payee's PSP will use a separate entity called as a Clearing House that will settle the payments between the interacting PSPs. This process of transfer of value across PSPs via a clearing house is termed as Settlement. The Settlement process happens in the clearing house and results in transfer of value from one PSP's subscriber (payer) to another PSP's subscriber (payee). All settlement transactions are logged in the clearing house for future reconciliation and audit. This functional architecture is illustrated in Fig 3.

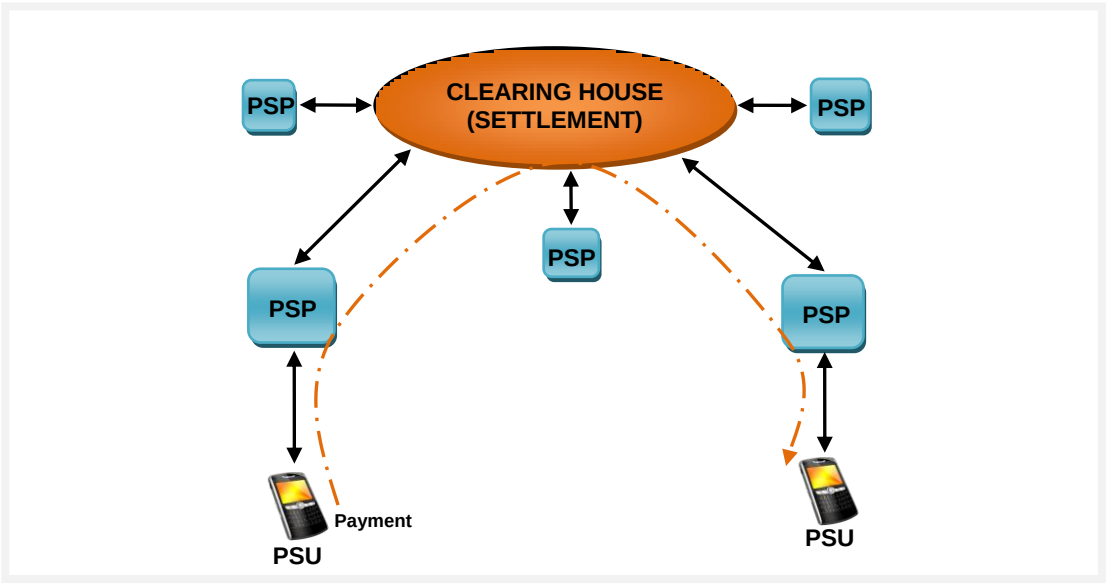


Figure 3: Clearing House, Settlement and PSPs

A PSU initiates and completes a payment to another PSU using a mobile device. Each of the PSUs are subscribed to a different PSP. The PSPs interact via a clearing house and perform the transfer of value between the two PSPs and log the transaction (details of the settlement) at the clearing house.

Payments are typically to and from individuals, and between individuals, companies and public authorities.

Payments can be classified using a great number of parameters, such as the medium (cash, paper, electronic), the size (micropayment or not), the time of payment (prepaid, pay-as-you-go, post paid), or the place of purchase (real-world or online). These criteria can be used to create demarcations between different payment models. We elaborate and discuss the use of such a classification, later.

2.1.1.2 Payment Costs

The payment process entails costs to the organisations providing the service. Each part of the transaction has a cost to the participating users, the payer and the payee. Typically, the costs components of the payment transaction are – Service access costs and Service costs.

The service access costs include the costs of access for the payer and the payee. These are the costs incurred in the PSU accessing the PSPs service infrastructure. Typically, a bank or a credit card organisation owns its captive network infrastructure and will charge this component towards the user authentication and user traffic for the transaction.

The service costs include the costs of providing the service and the costs charged by the settlement service, if it is an inter-bank transaction. These costs are recovered from the PSUs. The cost of the settlement is borne by the payee.

2.1.2 Mobile Payments

Payments executed by a PSU using a mobile device such as a mobile phone, a smart phone or a Personal Digital Assistant (PDA) are termed as mobile payments. A formal definition that has evolved for mobile payments is “A mobile payment is any payment where a mobile device is used to initiate, authorize and confirm a transfer of value in return for goods and services (Pousttchi, 2003; Au and Kauffman, 2008).”

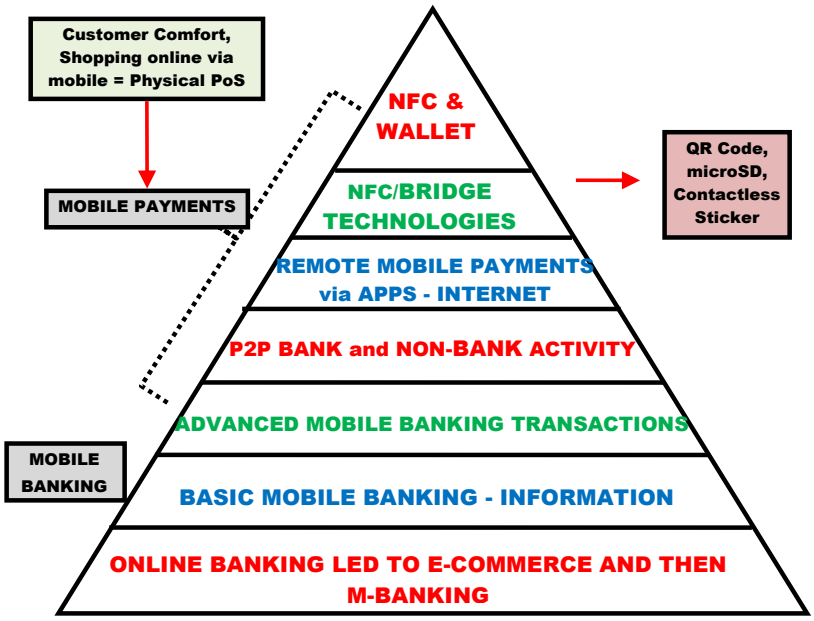


Figure 4: Evolution of MP from Mobile Banking (Crowe M (2012))

MP has evolved from Mobile Banking (MB). MB initially provided access to banking information for a user and added the capability of performing a few banking transactions. MP evolved due to two enablers - the specific need of user to make payments across merchants or end users who were with different banking/credit institutions and the arrival of contactless technology such as Near Field Communications (NFC) and Radio Frequency ID (RFID). NFC would potentially be dominant at various forms (till, vending machines, etc.) of points of sale (PoS) . The potential for shopping online and making a payment when mobile, using the mobile device brought up the concept of Virtual PoS.

The significant change in the context of payments (Fig. 3) is the inclusion of additional actors into the MP eco-system. The dominant actor is the Mobile Network Operator (MNO). The MNO provides for the access between the PSU and the PSP and assumes a very important role in the MP service scenario.

Traditional Payment System	Mobile Payment System
• Financial institutions • Customers & merchants • Payment card networks • Clearing/settlement organizations • Third party processors • Online payment providers	• Mobile Carriers • Handset Manufacturers and OS vendors • Chip makers • Mobile solution providers • Bill-to-mobile vendors

Table 1: Additional actors in the MP context (Crowe M (2012))

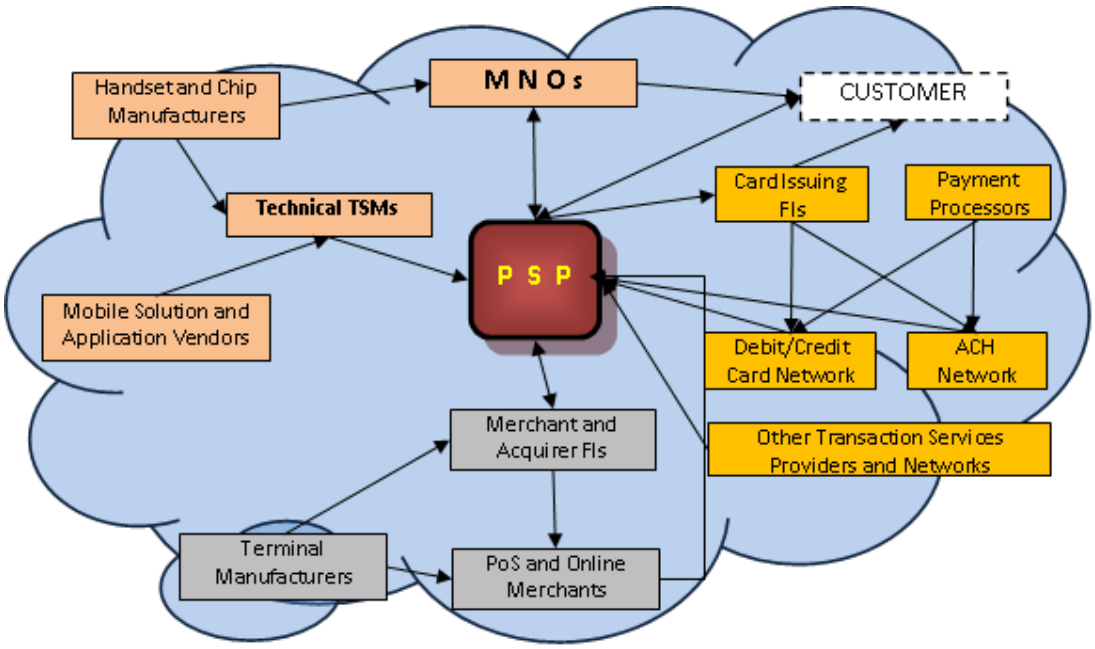


Figure 5: Mobile Payments Eco-system (Crowe M (2012))

The MP eco-system is fairly complex. There are additional actors from the mobility dimension that influence the service as a whole. They are listed in Table 1. Fig.4 illustrates the eco-system and its various components. Each component impact the service provision as well as the costs of service provision.

There are four key groups that provide the various elements of the MP service and need to interact. The MNO, the mobile device manufacturers, the mobile application vendors and the providers of technical services for the MP service (marked in orange) constitute one group. This group provides the basic infrastructure for mobile access, the end user device as well as the technology support for the service. The Merchants, the FIs that they are members of and

the Terminal manufacturer who provides payment terminals to the merchants (marked in gray) constitute another group. This group provides the merchant side requirements of service access and the service terminal. The issuing FIs, the payment processors, the wide area network that interconnects various end points to provide the payment services (marked in yellow) form another group. This group provides interconnectivity between various payment processors, merchants and customers and with transaction service providers as well as transfer-of-value services between the merchant and the customer. Finally, there is the customer that interacts with all the groups as part of the payment service.

All these groups influence the MP service provision. Fig 4 illustrates a simplified view of the relationships and interactions between the various entities of the four groups mentioned above. A PSP is expected interact with all of these groups, in addition to its own value additions to provide the payment service.

It clearly emerges that the MP service is dependent upon the following – The User device and its configuration, the Merchant terminal, the access method to make payments and the payment process. It is the interplay of these dependencies that influence the MP service.

The MNO can play multiple roles in the MP context. The primary role is to provide the basic infrastructure for Internet access to mobile devices. The additional role is to provide mobile access to services other than the basic services - Voice and Internet access services. Such additional services are termed as Mobile Value Added Services (MVAS). The primary objective of providing the MVAS is to increase the average revenue per user (ARPU) and increase revenues, overall. In order to support MVAS, the MNO typically invests in infrastructure and skills necessary to sustain the MVAS. One such MVAS is mobile payments.

The scope for the role that the MNO can play in the context of MP is a business decision that hinges on the financial risk the MNO is willing to take on a per-customer basis. Based on this decision, the MNO can be

a) an access and connectivity infrastructure provider – these are the basic MNO services
b) a payment service provider for users of its network to procure services and products hosted within the network – these are MVAS that support the MNOs user base and typically comprise value top-ups, downloading of ring tones, etc. This entails procuring goods/services from the MNO. The MNO is the vendor. The user traffic on the MNO network for this kind of MVAS remains within the MNOs network. The cost implications of this service are therefore low.
c) a generic payment service provider for users of its network to procure services and products from any source – this is a MVAS that is provided in collaboration with third parties. The user traffic for such MVAS flows in and out of the MNOs network. The cost implications are higher due to the fact that there are additional parties involved and the user traffic now flows across the MNOs network and external networks.

In the context of MP, the MNOs are an inseparable part of the service. The role that they intend to play as part of the payment services gives rise to different business and service models for the MP services.

2.1.3 Mobile Payment Models

Traditional payment services are hosted by banks and credit card companies. Credit card services have proliferated to such a large extent that a considerable volume of the payment services uses this mode of payment. Banks and credit card companies have been directly providing these services. Banks provide these services by tying up with the credit card companies. These organisations have their own captive networks to carry the payment traffic and interconnect and share their network resources to provide the payment services. In the context of MP the MNO, a third party service provider, becomes part of the service provision.

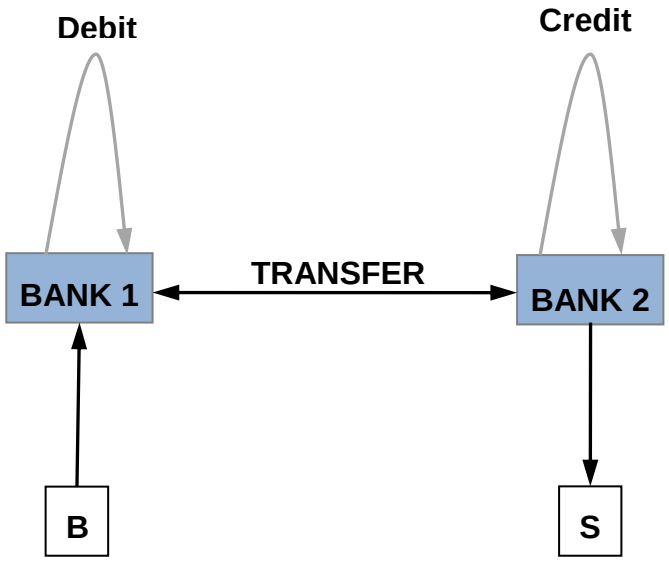


Figure 6: Bank-centric model - the bank owns and provides the entire service

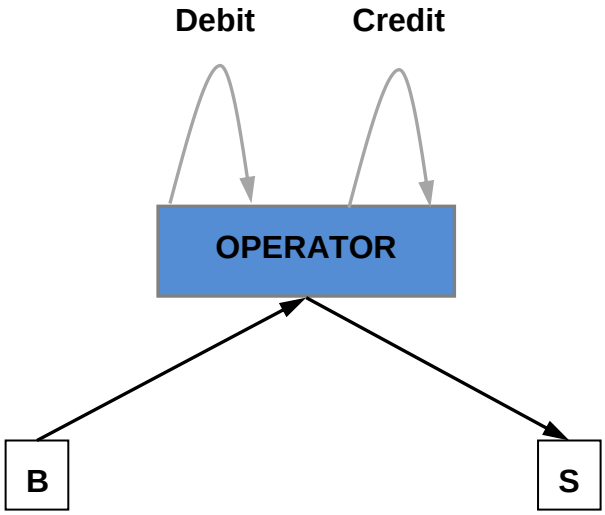


Figure 7: Operator-centric model - the operator owns and provides the entire service

Depending upon the actors and their roles in MP service provision, there are four distinct models for mobile payment (Chaix, Laetitia; Torre, Dominique (2012)). They are

- the bank centric model: a bank provides the MP functionality, manages the transactions and takes the financial risks (Fig. 6).

- the operator centric model: similar to the bank centric model but with the operator in place of the bank (Fig. 7).
- the collaborative model: financial intermediaries and MNOs collaborate in providing the service functionality and share the financial risks. Fig. 8 illustrates a collaborative model between banks and MNOs. An inquiry by the Smart Card Alliance shows that the collaborative model is considered by 86% of the participants as having the greatest potential for long term propagation (Chaix, Laetitia; Torre, Dominique (2012)).
- the Independent Payment service provider (IPSP) model: in this model(Fig. 9), a third party of confidence operates as an independent and “neutral" intermediary between financial agents and operators. Google or PayPal are associated with this model.

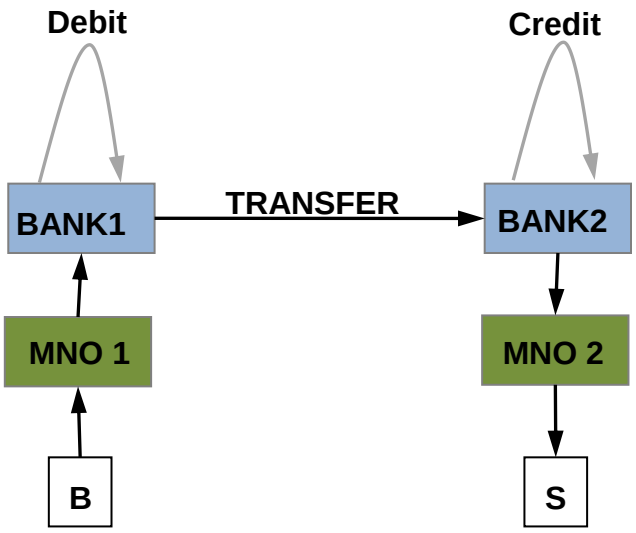


Figure 8: Collaborative Model - Banks and MNOs own and provide the service

It was expected that the market would tend towards a collaborative model of MP services provision involving the banks, the MNO and other third party service providers. However, recent trends indicate the successful emergence of independent PSPs who provide an integrated payments system for end users.

Table 2 indicates the potential for revenues from an MP service based on the MP services model. ‰ indicates revenues generated by the payment service traffic on the access network. Regardless of the model, the MNO stands to gain by simply providing mobile access to the payment service users. If it

provides a specific quality treatment for the traffic generated by the payment service (such as priority), then it could charge a premium rate for that traffic. √ indicates revenues from the MP service provider. In a collaborative model, the collaborators share the revenue from the MP service whereas in an IPSP model, all the actors have a share of the revenue. ☼ indicates the actors who are the primary investors in providing the service.

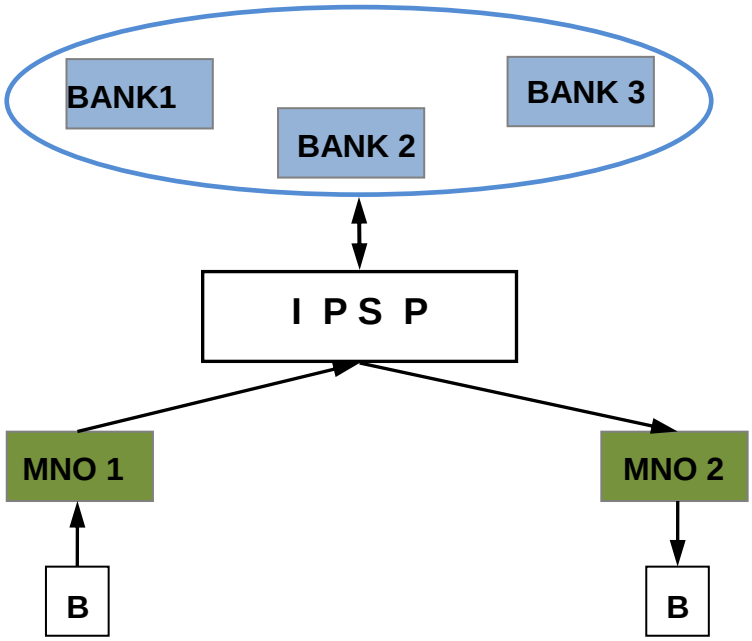


Figure 9: Independent PSP (IPSP) model - The IPSP owns and operates the service an provides a single access point to the user

Actors/Model	M N O	B A N K	I P S P	OPERATOR
Bank	‰	√ ☼		
Operator	‰			√ ☼
Collaborative	‰ √ ☼	√ ☼		
IPSP	‰ √	√	√ ☼	
Legend: **‰ :** Revenue from Payment Traffic**,** √ **:** Revenue from the MPSP in a collaborative model, ☼ **:** Revenue as Primary investors in the payment service				

Table 2: Actors vs Models - Potential Revenues from an MP service

Payments can be classified based on the medium of payment (cash or non-cash), by value of transfer (micro/macro payments), mode of purchase (PoS,

Virtual PoS, online) and by the payment terms/contract (subscription/membership, pay-per-use, pre-paid).

2.1.4 Mobile Payment Service Adoption

Electronic and Mobile payments have been around for a decade. It has seen varying adoption and success rates. It has not proliferated western markets and is believed to be slowing down (Chaix, Laetitia; Torre, Dominique (2012)). The major reasons for this slow down are

- The service models are derived either on a technical basis or on an economic basis but not with a comprehensive service orientation (Pousttchi, K., Schiessler, M., & Wiedemann, D. G. (2009)). The resulting service offering is not appealing to the large user community. The two reasons for this are:
  1. Technical – failure to converge on a solution for storing confidential information on the mobile device, *i.e.*, the Secure Element (SE). The choice was between implementing this as secure chip on the device (the OEM's domain) and implementing it on the SIM card (the Operator's domain). Though the decision was in favour of the SIM, there are both solutions in the market today with the stake holders competing for the market. Clearly, this has led to different implementations that have tended to be proprietary in use.
  2. Economical – the various payment services models that are feasible and have evolved but economic viability requires the actors in these models to work together to provide the services. The primary problem has been that the newer models require a non-financial partner/s to participate in the service provision. The banking and credit card industry earns about 25 to 30 % of their revenues from payment services (Carton et al, 2012). Newer actors in the payment services market with newer modes of payment imply that these revenues will have to be shared by these organisations with their collaborators. Adding to these revenues to provide for collaborators' RoI will result in loading the end users and sellers with the additional costs for making payments. The end users will therefore be accorded an expensive service for convenience. The industry is still attempting to work out the

feasibility of such a collaborative business model. Therefore, MP services have not been adopted on a large scale.

- The transfer of value (payment) falls into two categories – Low value and High Value. The low value transactions are higher in volume compared to the high value transactions whereas the transaction value remains somewhat constant and depends on the payment instrument used. MP proliferation is certain if it can cater to the low value payments. The transaction cost for a mobile payment should be sufficiently low so as to make both low value and high value transfers feasible for the PSP as well as the PSU. Various means, including e-Wallets and e-Currency are evolving to achieve this objective. The British Retail Consortium quoted in 2008 that further progress and technology adoption should come at *no cost to the public* and no *additional profit to the Banks.* This will be the key to the adoption of MP.
- Security & Privacy – There have been several approaches to provide security for MP. However, most schemes assume the computing power and memory resources on mobile devices are low causing the security implementation to be rather complex as well as time-consuming. Present day smart phones are equipped with multiple core processors and have access to large on-board memory as well as secondary memory via SD cards. Asymmetric key cryptography can be deployed on the phones independent of the involvement of the mobile operators.

The MP market is moving towards an IPSP model where third party organisations front-end with the users via the network and provide them with payment services regardless who they bank with. This model provides each of the actors involved to concentrate on their core business while the IPSP coordinates all the payment functions. Our objective is to engineer a Safe, Simple and Speedy (Chaix, Laetitia; Torre, Dominique (2012)) means to carry out the payment function from a mobile device.

Towards this, we intend to propose a payment framework which will describe the functional components of the framework and their interactions. We will then detail a payment protocol that is to be deployed on that framework. The

protocol will provide a means to the user to make a payment using an appropriate payment instrument, electronically.

2.2 Motivation

The need for research is motivated by three prime issues mentioned below. These issues are dealt with in-depth in course of the research and the expected outcomes are mentioned under the heading, Objectives.

1. Heterogeneous Mobile-payment Technologies & Solutions

   The heterogeneity in technologies exist in various forms – user-side payment service access technology (IP-based, SMS-based, USSD-based), payment service access networks (a separate network for each PSP), user-side payment service access devices (smart phones, tablets, feature phones and plain mobile phones) and merchant-side payment service access devices (one device for each PSP, one device for type of user information collection – contact (magnet stripe-only card, chip-and-pin card, etc.) and contactless. Clearly, a merchant will require to have a host of devices and connect to various networks based on the user payment context. Ideally, the merchant should have one integrated device that can support both contact/contactless technologies, access any PSP and connect to one network to access the payment service, regardless of the PSP.

   The heterogeneity in the solutions exist in the payment processes, payment interfaces and the payment applications. Each PSP strives to provide service to both the merchant and the customer. From a customer's perspective, there is no interoperability between the various payment services. Interoperability is discussed separately, next.

   Literature suggests that a common minimum set of requirements for an MP solution are Usability, universality/interoperability, Low cost and High-speed of the transaction and security. In order to increase MP adoption, it is essential to have a solution that fulfils all of the above requirements. Existing MP solutions are very heterogeneous in nature. Each of the solutions offer specific advantages and disadvantage with

respect to the MP requirements. However, most solutions do not provide universality, interoperability and high-level security that is required by the MP players. IP based solutions provide the abstraction required to normalise the access layers for the existing heterogeneous MP solutions. Therefore a MP solution based on IP can be independent of the technology/network that was used to trigger a payment transaction or the technology/network used to complete the transaction. Consequently, for example, an existing SMS-based solution can be migrated to an IP-based SMS solution before migrating to an ideal solution. IP supports better security with IPv6 and its privacy extensions that use IPSEC as well as facilitate the use of secure transport protocols that are used in e-payment systems in MP systems. This is the prime motivation for the research work. We intend to propose an integrated payment service access architecture and use a single payment protocol to enable the integrated mobile payment service.

2. Lack of standardisation and interoperability

Although MP has a great potential for large scale deployment from a convenience point of view, there is little evidence of large scale deployments of the service. Current deployments are limited to a small range of products initiated for mobile commerce transactions and services for niche markets. They are limited in scope, limited in customer reach and are neither open nor standardized. There are several international consortia such as SIMPAY (www.simpay.com), Paycircle (www.paycircle.org), Mobey Forum (www.mobeyforum.org), Mobile Payment Forum (mobilepaymentforum.org) , Liberty Alliance, etc working towards consolidating requirements and attempting to define a normalised service. Each of the above consortia is either driven by mobile operators and banks or third-party driven.

Currently, the mobile payment services market is in a pre-standardization phase where no collective standards have been achieved and where various industries and consortia, most notably the

financial and telecommunication industries, compete to form the dominant standard (Lim, 2005b). Some studies which have looked at the mobile payment services market from the point of view of multiple actors have discussed the standardization of mobile payments and emphasized the need for a technological and organizational consensus between the players in the industry (Ondrus et al, 2006a 2006b 2006c). This consensus can be achieved only with an industry-wide agreement on a normalised payment services architecture, roles of various actors participating in the payment service and an assurance of the Return on Investment (RoI). The need for a normalised payment services architecture that can provide a standard service profile and a set of standard interfaces to the associated financial systems is a strong motivation for research.

This lack of interoperability amongst the MP solutions and players is one other motivation for this research. A new generic MP service platform could be designed on the basis of IP Multimedia Subsystem (IMS) which is a standardized next-generation mobile telecommunication architecture. This offers a layered, standardised architecture for payment services that is interoperable across payment systems. IP based access can provide for universal access to the payment services. With the rapid proliferation of next-generation mobile services, MP could easily be adopted as a MVAS on provider networks and scale.

3. Lack of Security

Security concerns with the existing MP mechanisms have been a bottleneck in their large-scale adoption. A traditional mobile infrastructure is not conducive for a payment service with strong authentication and cryptographic algorithm. A mobile phone with IP can be treated as an IP end point. Therefore, any classical internet model of transaction and security can be applied directly. Many mature

security frameworks such as S/MIME, IPSec, SSL/TLS can be implemented on IP, thus enhancing the overall security of the service.

The user perception of security should be strong enough to provide confidence to the users to use the service (Schneiderman, 2000). Mobile payment brings in a different set of concerns to security. User device security concerns (theft, data loss and damage), in addition to transaction security forms an important requirement (Chari et al, (2000)). PSPs who are not traditional FIs or are new in the market are also a concern for the PSU. The PSP's credibility, capability to deliver and sustain the service, the security of user information at the PSP are among the concerns raised by potential users of the MP services. A security breach can result in invasion of privacy and financial loss (Egger F, Abrazhevich D, 2001). Overall, security in MP cannot be a mere extension of security in electronic payments.

These three important factors form the major motivation for the research. The reasons for the lack of commercial adoption are manifold and range from economic to technical to user adoption. Our focus is on technical concerns of the service as well as those that impact the economic and user adoption concerns. There is no focus on standardisation relates issues, apart from an understanding of the state-of-the-art. The research addresses the need to have a common interoperable platform for MP, independent of the type of payment, its value, the provider or the user device and its access technology.

2.3 Research Problem

The focus of the research is to identify and propose a comprehensive MP solution that addresses the technology issues that hinder the proliferation of MP services. The research problems that are encountered enroute to designing a MP solution are listed below:

1. The heterogeneity in the MP landscape spans across several components of its eco-system such as mobile technologies, user devices, MP service access, MP security and MP goods. This heterogeneity is impeding the large-scale commercial deployment of

mobile payment systems. There is a need to identify the technology related impact factors and address them.

2. There is a need to identify the requirements and expectations of the users, and draw the service requirements from them. A mapping of the operational features of the existing solutions to the service requirements is necessary to ascertain that there are no further gaps to be addressed. This will not be addressed as part of our work.
3. MP is classified based on a number of functional characteristics such as payment methods, payment value, mode of access, etc. There is a need for a new classification model from which the characteristics of a unified and generic payment platform can be drawn. These characteristics will help to design the unified and generic payment platform that will address the problem of heterogeneity, comprehensively.
4. MP economic models in the market are tending towards collaborative models. There is a need to design a payment services architecture and components such that the architecture is generic enough to accommodate any of the four well known economic models, regardless of the actors and their roles.
5. Finally, to provide the operability to the unified and generic payment service, there is a need to design a protocol that will perform both signalling and data transfer between the two transacting entities. The protocol should be simple, safe and secure and provide usability, interoperability and a perceivable security to the end user.

The overall problem is stated as follows – The heterogeneity in the payments landscape has increased the complexity of components, actors and their roles with the added dimension of mobility. Therefore, there is a need to examine the impact of the evolving economic models of service provision in the market, reassess the user requirements and expectations, propose a generic payment service architecture which is model/user agnostic, design a service that provides a unified access to all types of payment services and design a protocol that will provide the operability to the service.

Chapter 3
Literature Review

3.1 Background

The Internet has revolutionized every aspect of society particularly personal and business interactions. The flourishing E-Commerce industry is a direct consequence of the growth of the Internet and Internet technologies. The technological developments in the Internet and wireless communications including the recent NFC technologies have merged with the electronic commerce in promising ways to transform the consumer-merchant interaction. A vital part of this interaction is payment for the goods purchased. E-Payment systems (EPS) were introduced to manage the business critical aspect of e-commerce, i.e. financial transactions. The electronic payments industry traditionally included the credit and debit card systems, online banking and electronic bills. The electronic payments industry was largely dependent on the network that moved money between consumer and merchant bank accounts using computers, software, and communication links.

EPS has several favourable characteristics such as security, scalability, anonymity, reliability, efficiency and conveniences when compared to traditional payment methods (Kousaridas et al., 2008). In countries such as France, UK and US e-payment systems are well established, while the Asia Pacific region shows prospects (Kim et al, 2010).

The past decade has witnessed enormous growth in mobile communication technologies, mobile devices and applications and services that make use of the above advancements (BII Report, 2012). Mobile-Commerce is a natural extension of e-commerce that was introduced to tap the potential of mobile technologies and the increasing capabilities of mobile devices. Both e-commerce and m-commerce hinges heavily around trust and security. Mobile-Payment was a natural and a complementing evaluation of e-payment mechanism. However, the two mechanisms differ in the aspect of anonymity. E-payment transactions take place with users who are typically associated with multiple end-devices which offers the feature of anonymity to the

transactions while posing the challenge of security, identity management and trust. However, mobile-payment transactions occur with users who are normally associated with one mobile device that acts as their Personal Trusted Device (PTD) making the transaction transparent as well as enables security, identity and trust (Karnouskos, 2004). Thus M-payment cannot be viewed as having a mobile interface to the existing Internet transaction, but as a mechanism that involves different business models, different interaction amongst the players involved. Finally, it differs greatly due to the capabilities of the end-device (Jelassi and Enders, 2005).

3.1.1 Mobile Payment Literature Review Methodology

Mobile Payments have been a subject area of research for scholars from various fields such as technology, financial sector and business. A significant amount of published literature exists under the broad theme of mobile payment. Most studied aspects of mobile payment in contemporary research are mobile payment technologies, consumer perspectives of mobile payments, m-payment business models and m-payment adoption. However, Mobile Payment technology research is still fragmented. There is no evidence of significant academic work dedicated to a unified mobile payment platform from the technology perspective. Therefore the literature survey conducted as part of this research adopts the methodology as depicted in the fig. 10.

The first phase, aims to clarify some key concepts, definitions and mis-conceptions of mobile payment . By reviewing existing literature in phase one a holistic classification of mobile payment is presented.

The second phase of literature survey focuses on the heterogeneous mobile payment ecosystem particularly focussing on the technological perspective. The aim of the research is to identify the gap in research that are essential to be covered future research.

The third and final phase of literature review focuses on the various standards and consortiums related to mobile payment and the current status of mobile payment adoption.

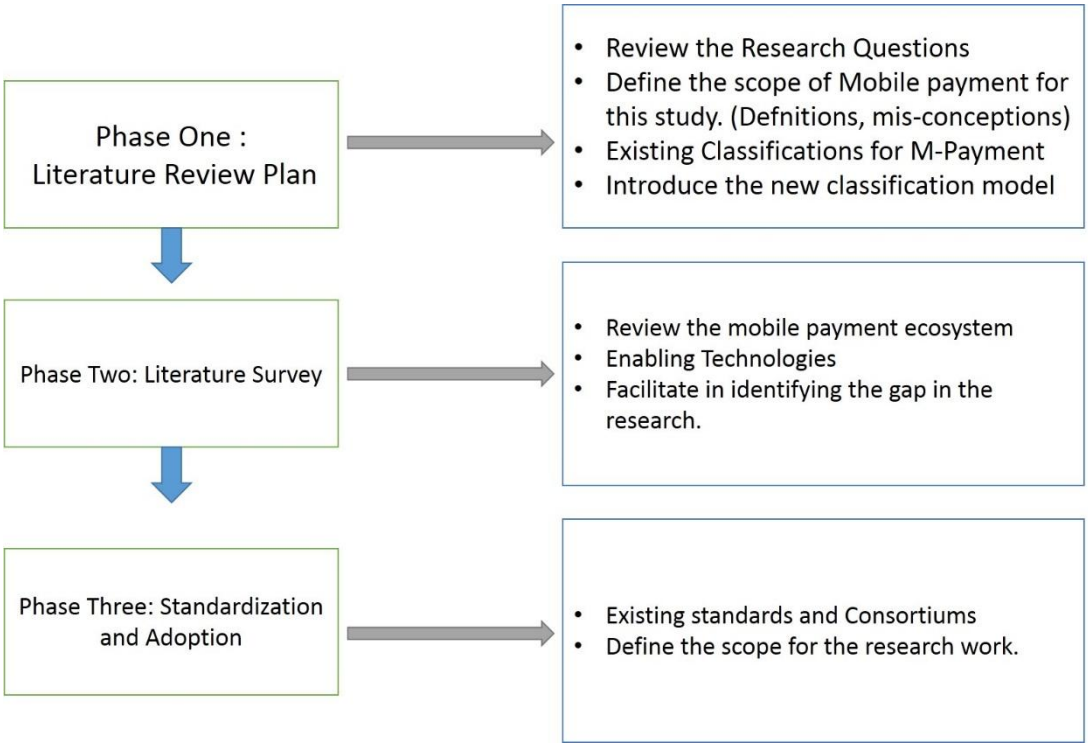


Figure 10: Literature Review Methodology

Literature review concludes by identifying the gaps for future research and defining the scope of the current study.

The research started with a wide and systematic research of materials in the leading databases for online journals and conference materials: IEEE Explore, ACM Transactions, Science Direct, and Google Scholar. The analysis also went “backwards”, by identifying other works of the authors and citations to be reviewed in addition to the articles downloaded from the database. In order to conduct an organized literature review, the literature search and archiving was based on the following three key criteria:

- Literature work relating to mobile payment classification and in defining the various mobile payment instruments.
- Literature relating to the technologies enabling mobile payment and fragmented state of deployment of these technologies
- Literature that is in scope and fits within most the aspects of the scope of this research i.e., related work that has focused on a uniform mobile payment platform or framework.

3.2 Definition and Classification of Mobile Payments

3.2.1. Mobile Payment Definition and Mis-Conceptions

Mobile-Payment is not about accessing E-payment services using a mobile device. Although, this is possible by developing a mobile version of the EPS in the form of a mobile application or a mobile website. However, in general, designing and implementing payment procedures for the mobile world differs from the Internet applications due to the different contexts in which the two approaches operate (Hartmann, 2006).

M-Payment and Mobile-Banking are two different things. Although Banks could offer their services through a mobile device, M-payment is a more generic service which needs to be universally available. It is a service that involves players other than financial institutions and banks alone. Mobile-banking are usually narrow in scope, tied up with banking procedures and hence can be viewed as a sub-domain of M-Payment systems (Karnouskos, 2004).

There are several definitions of mobile payment that exists which share some common elements as well as differences. Listed below are some common definitions based on the literature survey:

- Krueger 2001: *«Mobile payment can be defined as a payment that is carried out with a handheld device such as a mobile phone or a PDA (personal digital assistant)»*;
- Zmijewska 2004: *«Payments in which at least one part of the transaction is conducted using a mobile device (such as a mobile phone, smartphone, or Personal Digital Assistant) through a mobile telecommunications network, or via various wireless technologies»;*
- Karnouskos and Fokus, 2004: *«A mobile payment or m-payment is any payment where a mobile device is used to initiate, authorize and confirm an exchange of financial value in return for goods and services»;*
- Turwoski and Pousttchi: 2004 *«it is a type of electronic payment transaction procedure in which at least the payer employs mobile*

communication techniques in conjunction with mobile devices for the initiation, authorization or realization of payment»;

- Au and Kauffman 2008*: «as any payment where a mobile device is used to initiate, authorize and confirm an exchange of financial value in return for goods and services»;*
- Pousttchi 2008: *«m-payments are defined as a type of payment transaction processing in which the payer uses mobile communication techniques in conjunction with mobile devices for initiation, authorization, or completion of payment»;*
- Dhalberg et al. 2008: *«Mobile payments are payments for goods, services, and bills with a mobile device (such as a mobile phone, smart-phone, or personal digital assistant (PDA)) by taking advantage of wireless and other communication technologies».*

Most definitions agree that a mobile device plays a key role in m-payment is a distinguishing characteristic when compared to other forms of payment. Regarding the function of mobile payments, all definitions refer to the transfer of monetary value. Differences can be found when it comes to the phases of the payment process that are considered to be part of the mobile payment (Henkel).

For the purpose of this research work, the definition of mobile payment is limited to what is quoted by Karnouskos and Fokus (2004) as “ Any payment where a mobile device is used in order to initiate, activate, and/or confirm this payment can be considered a mobile payment."

3.2.2 Mobile Payment Classification

Categorizing mobile payment systems let researchers organize their knowledge. It puts things into perspective, and reveals the big picture. It enables a better understanding of the current situation, and provides a summary of what is happening. Classifying reveals the current situation across many dimensions, so the view is complete, hence this forms the most critical part of the preliminary research work undertaken.

The initial literature review is focussed on investigating exist classifying models of mobile payment systems. Most models are based on very few criteria. Seah et al. (2001) categorizes m-payment systems from the devices perspective i.e. devices with or without payment applications or payment capabilities. Kountz's (2002) categorise based on the value of payments, settlement method, and content type. Schwiderski and Knospe (2002) proposes a categorization based on the means or channel of payment such as the smart card, credit/debit card, bank account or in the form of currency on the mobile device. Since the above methods of classification are very narrow in scope and definition, it does not enable to fully analyse the existing systems.

Buhan et al. (2002) propose a more detailed analysis. They believe that potential systems fall into the following categories: transaction settlement (pre-paid or post-paid), transaction type (pay per view, per unit, subscription), content type (ticketing, voting, digital goods, hard goods), and content value (micro or macro).

A more comprehensive view of the mobile payments market and its many dimensions is presented by Telecom Media Networks (2003). Systems are divided by means, size, seller/buyer origin, type of purchase, place of purchase, clearing or settlement method, type or transaction, the time of payment, geography, and location of payer's account's details.

Ondrus (2003) proposes a new multidimensional table. Its categories include: m-payment solution type (client-based, server-based, or hybrid), solution providers (MNO, financial, newcomer), relationship (B2C, P2P), location (F2F, remote), and payment time (pre, direct, or post). The system is not meant to be exhaustive; according to the author, it's meant to judge the flexibility and limitations of a system only.

Bradford (2003) presents a user-centric categorization as the most important component in mobile payment systems is the user. Much research work is dedicated to the study of usability as a critical success factor of mobile-

payment systems (Northstream, 2002). Mobile usability tests (Duda et al., 2002) indicated that the leading determining factors for a general acceptance of mobile data services are the experienced utility and usability. The authors conclude that usability is therefore a strategic factor of success, as much as the benefit of the service for the user. Kreyer et al. (2002) support the statement that the consumer is the key to the acceptance of a new payment method. Since eventually it is the consumer who decides whether or not a new system is accepted, it only seems logical to devise a classifying system from the consumer's point of view.

3.2.2.1 Hierarchical Classification

Payments can be classified using several characteristics. They are:

- Medium of payment: Payment by cash, by cheque (paper), electronic (bank transfers) and online
- Value of payment: The transfer value in the payment process as Micro-payments which are low value payments, typically those that we transact using cash – notes and coins and Macro-payments, typically those that are traditionally paid by cheque or by credit cards. Recall that payments through credit cards require a minimum value of payment to make them feasible for the consumer and the merchant in terms of the transaction charges and payment changes.
- Terms of payment: The terms of contract for the payment. This could be one of Subscription/Membership (post-paid), Pay in advance (Pre-paid) and Pay for use (pay-as-you-go).
- Location of PoS: Physical, meaning a real-world PoS terminal and Virtual, meaning that the PoS is online.

The characteristics of classification can be very much more. In most cases, there is an almost complete overlap. For example, a classification based on the payment instrument used – Cash, Cheque, Debit Card, Credit Card and Direct Transfer. This classification almost completely matches with a classification by payment value, Macro and Micro payments. Cash and Debit Card would fall under Micro payments whereas Cheque, Credit Card and Direct Transfers would fall under Macro Payments. This is the reason such classification characteristics have been omitted and the most generic characteristics (listed above) have been chosen.

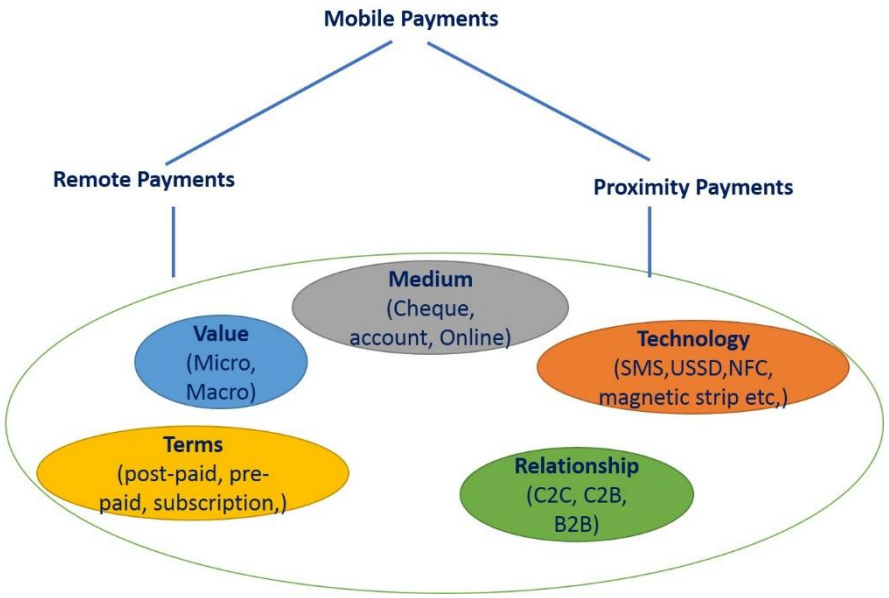


Figure 11: Hierarchical Classification of Mobile Payments

Notice, that the location of the PoS, by far, seems the most generic characteristic from the payment perspective. The payments can be classified as Remote payments and Proximity payments. The term “Proximity” has a technical connotation in recent literature and is used in the context of contactless payments. Regardless of this, all elements of the types of payments mentioned above can be categorised under either of remote or proximity payment. This prompts a hierarchical approach to payments classification with remote and proximity as classification parameters at tier 1 (Fig. 11).

3.2.2.1.1 Tier 1 – Proximity and Remote

Flatraaker (2008) mentions a consumer-centric approach for MP classification as “proximity” payments and “remote” payments. It is regarded as consumer-centric since the focus is on the consumer’s choice of the payment mode. The payment for a particular good could be made at a physical PoS or via the Internet. It should be noted that this classification coincides with a technology based classification since proximity and remote payments require different access technologies although the device used for access, the smart phone, remains the same. This is the first tier of the classification hierarchy.

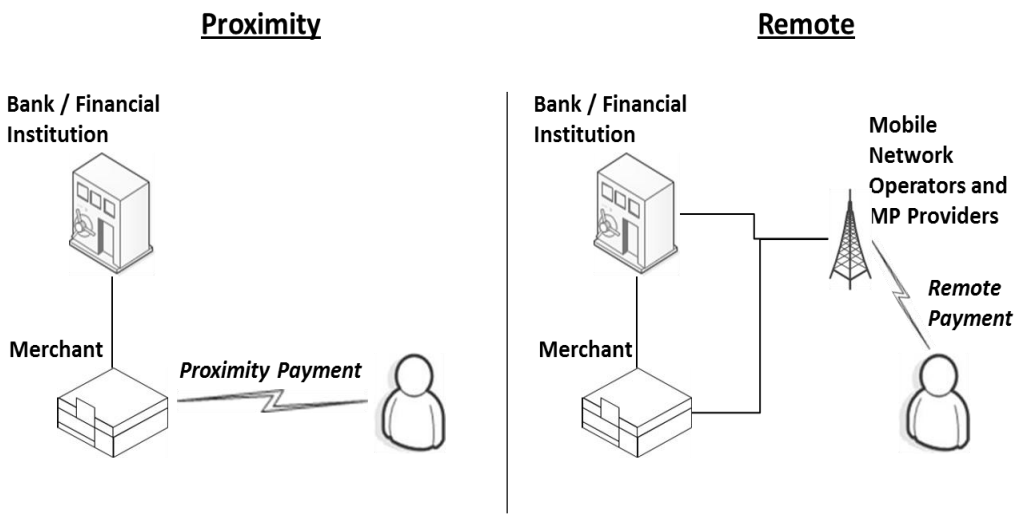


Figure 12: Proximity payments vs Remote payments

Features	Mobile Remote	Mobile proximity
Use Case	The user purchases digital good or service over the web and pays for the service with an SMS.	The user purchases food at a physical store and pays for the purchase with a contactless Credit Card.
Wireless Data Standards	Mobile Data (GPRS, UMTS, EVDO, LTE, HSxPA)	Wireless Proximity Data NFC, IR, RFID, Wi-Fi, UWB
Communication Protocols	SMS, WAP, HTTP, WSDL	HTTP, EDI, XBRL
Charging of purchase	Mostly directly to User's Phone Bill (also to credit card and to other electronic wallets)	Mostly to user's credit card or banking account
Device	Mobile Phone, Smartphone, Pad (Anything equipped with a Mobile SIM Card)	Mostly Cards and NFC /RFID dedicated devices
Reference Point of Sales	Web or Mobile Store / Site / App	At the Store/till/vending/ ticketing machine

Table 3: Key Distinguishing features: Proximity vs Remote Mobile Payment (Source: Dewan and Chen (2005))

Dewan and Chen (2005) illustrate the categorization (ref. Table 3) of the term proximity and remote listing various activities pertaining to the payment ranging from the location of the merchant to the protocols and standards used. Notice that the smart/mobile phone is missing from the proximity category in Table 3. Smart phones arrived in the market, later.

3.2.2.1.2 Tier 2 – Medium, Mode, Value and Terms

The second tier of the classification consists of payment characteristics which are Medium of payment (cash or non-cash; non-cash implies both card based and coupon/voucher based payments), the transfer value (Micro or Macro), Mode of purchase (PoS, Virtual PoS, online) and terms of payment (Subscription, pre-paid, etc.) that are under proximity and remote. Notice that these are already mentioned in the list of payment characteristics, earlier. These are generic categories and serve to classify components under proximity and remote.

3.2.2.1.2.1 Based on Value

The typical values that distinguish Micro and Macro payments in literature are listed below.

- Micro payments – less than 5$
- Medium Payments – Between 5$ - 25$
- Macro payments - above 25$

Value-Based	Proximity	Remote
Macro	Retail Purchase at POs, Loyalty Coupons etc.	Online purchase, m-banking, P2P remittance etc.
Micro	Vending machines, parking, cinema tickets, Tolls etc.	Digital Content, P2P remittance etc.

Table 4: Value based classification

Table 4 illustrates the value based classification of payments into micro and macro payments and against proximity and remote payments. Each combination lists the typical payment context for that combination.

From a payments perspective, Medium payment covers a typical value for debit cards as payment instruments. In the UK market, the average value of cash payments was approximately £ 10 for the year 2012 (BRC 2012). It is estimated that this value will distinguish micro payments from macro

payments. That is, payments up to £ 10 will be considered as micro payments. It remains to be seen how the market evolves on these definitions. For purposes of our research, we consider payments up to £10 as micro payments.

3.2.2.1.2.2 Based on Technology

Technology based classification is done based on various factors that influence the payment process such as the access technology, the protocols used, the application technology used, security provisions made and so on. These are all related technologies which are used to develop and produce mobile payment services. Some of these technologies develop slowly, such as mobile network technology or transaction protocols. Some other technologies have very short development cycles, such as mobile handsets and their components. Continuous development of technologies facilitates more reliable, user friendly, versatile, and functional rich mobile payment services (Dhalberg et al. 2007).

Seven technologies have been identified as enabling Mobile Payment business models (Pousttchi et al. 2007): IVR, Calling Line Identification Presentation (call capture, CLIP), SMS, Unstructured Supplementary Service Data (USSD), Wireless Application Protocol (WAP), Near Field Communication (NFC), Java 2 Platform Micro Edition (J2ME), and, finally, Subscriber Identity Module Application Toolkit (SIM Toolkit). Other recent enabling technologies for m-payment are the Magnetic Strip card and Smart Cards.

	Proximity	**Remote**
Technology-based	Contact-less cards, magnetic strip card, smart cards, NFC	SMS, Mobile Internet, USSD, IVR, CLIP, J2ME etc.

Table 5: Technology based classification

3.2.2.1.2.3 Based on Payment Relationship

Electronic and Mobile payments have been around for a decade. It has seen varying adoption and success rates. It has not proliferated western markets and is

believed to be slowing down (Chaix, Laetitia; Torre, Dominique (2012), Damsgaard and Hedman, (2009)). The major reason for this slowdown are that the service models are derived either on a technical basis or on an economic basis but not with a comprehensive service orientation (Pousttchi, K., Schiessler, M., & Wiedemann, D. G. (2009)). The resulting service offering is not appealing to the large user community and overall revenues are poor. Similar views about the cause for lack of MP proliferation are mentioned; poor revenue sharing amongst the actors of the service (Ballon and Van Bossyut (2006)) and using static business models in the complex MP services environment (Cousaris et al (2006)). This makes a case to consider classifying mobile payments from a service value chain perspective. It would enable an insight into the role of the actors, the processing functions and the service elements (Table 6).

3.2.2.2 Mobile Payment as Value Network

Value networks are defined as a set of roles and interactions that generates a specific business, economic, or social good (Allee V (2011)). A generic example of such roles and interactions/dependencies is illustrated in Fig. 13. This provides us an estimate of the complexity of the value network and the number of value parameters that need to be considered to ensure that all the actors are benefited as well as perceived as an active and valuable partner/contributor in the service provision.

In our context, the value parameters remain almost the same. We can map the actors in the MP context – Consumers, Merchants, MNOs, Mobile device manufacturers, FIs, Software and technology providers (application developers) and Regulators (Dahlberg et al (2007)) – to the generic actors in this example.

Firstpartner (2012) presents a mobile payment classification based on the payment processing value chain (Table 6). They present a matrix of payment service elements and the MP provider classification. It illustrates the actors involved and the roles they play in providing the service. The service elements are functions in a payment process between the consumer and the merchant.

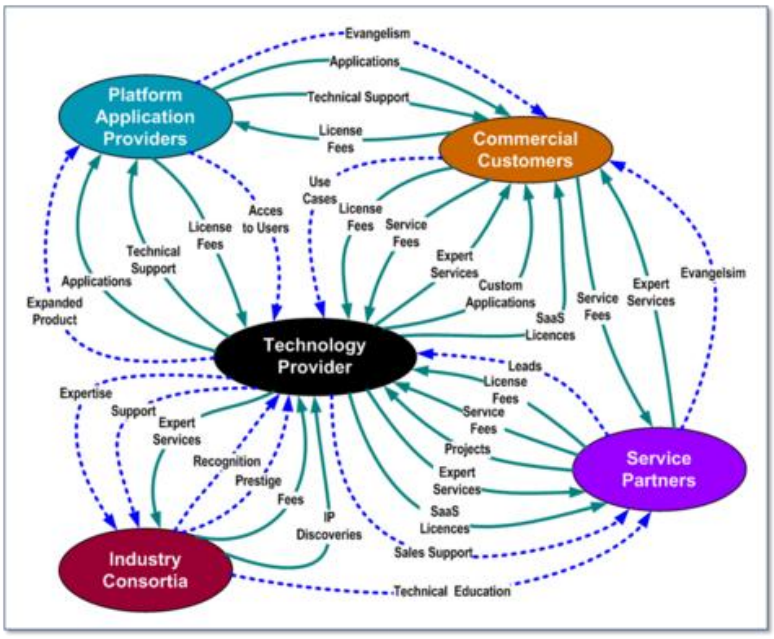


Figure 13: An example value network (Allee V (2011))

		Source of Funds	Consumer account provider	Funds Transfer	Funds Withdrawal / Settlement	
Four Parties	CUSTOMER	Bank	Issuer	Card Network	• Acquirer • PSP	MERCHANT / RECIPIENT
E-Wallet		• Card • Stored Value • Bank	Wallet Provider			
Mobile Money Transfer		• Carrier Bill • Mobile Money Agent	Mobile Network Operator Partner Bank	Bank / Interbank Network	• Mobile Wallet • Agent • Bank	
Carrier Billing		Carrier Bill / Prepaid Balance	Mobile Network Operator	Mobile PSP		

Table 6: Classification based on Payment Processing Value Chain (FirstPartner (2013))

The transaction fee is paid by the merchant and is divided across the actors providing different service roles. Such a classification represents the functional roles of each of the actors while they provide value to the service, overall.

3.3 The Eco-system and Technology Enablers

3.3.1 Mobile Payment Eco-system

The mobile payment eco-system (Fig. 14) primarily consists of all the stakeholders in the m-payment model, the enabling technologies, the various payment instruments and m-payment methods and lastly the consumers as depicted in the figure below. In our study, although the consumers are considered to be part of the m-payment stakeholders, user-centric perception of the existing and future m-payment solutions are presented in the thesis.

3.3.2 M-Payment Stake Holders

The main parties in the mobile payment landscape are depicted in Figure 15, the customer (payer) and the merchant (payee) are the two central players and they transact with each other via the mobile payment process which is facilitated by mobile network operators (MNO). The other players of the mobile payment landscape are the financial institutions (e.g. Banks, credit card companies, etc.) , the government (legislators and regulators), and lastly, the device manufacturers, software and service providers. MNOs typically have a large customer base, and control the end user mobile device to a large extent. Hence they have a huge influence on the MP model. However, they cannot independently handle an MP system, as they have limited experience in payment services and the risks associated with them. On the contrary, the financial institutions have the necessary experience to handle the payment services in a secure manner. Therefore, cooperation of both sides is key for a successful mobile payment model. The device manufacturers also play a significant role, as they control the technology and capabilities of the end-device, which influences the implementation and deployment of an MP service. Therefore it is important that the manufacturers cooperate with each other and with other MP players to develop a common approach to mobile device capabilities. Finally, software providers develop the required software that is standards compliant that connects the different parts of the MP process. The service provider’s role is to market the service while customizing to the end-user’s needs. MNOs or banks typically act as the service provider

and can also offer limited MP services on their own as presented in Choi et al, (2006) and Wrona et al (2002).

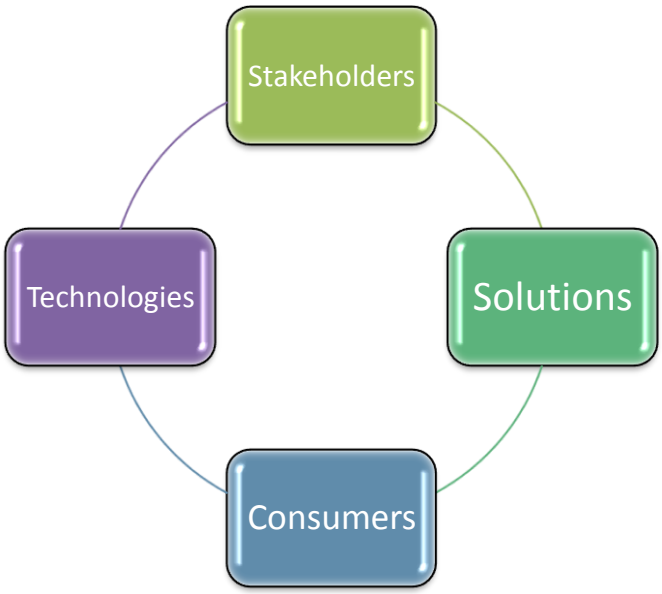


Figure 14: M-Payment ecosystem components

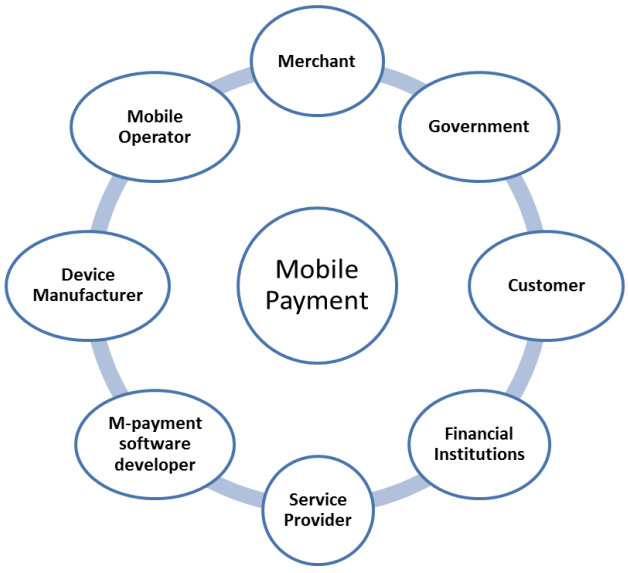


Figure 15: M-Payment Stakeholders

3.3.3 Technology Enablers

The technology that enables the initiation of mobile payment such as a mobile device, payment instrument etc., forms one part of the technology enablers. The other part is the technology infrastructure that enables transmission of m-

payment data and facilitates in conducting m-payment, such as the mobile technology.

3.3.3.1 Mobile Devices Evolution

Mobile phones have proliferated densely across the globe, over the last decade. According to the ITU, in 2013, there are almost as many mobile-cellular subscriptions as people in the world (Fig. 16), with more than half in the Asia-Pacific region (3.5 billion out of 6.8 billion total subscriptions). The account for active, inactive subscriptions as well as users with dual-SIM devices and tablet users. Mobile-cellular penetration rates stand at 96% globally; 128% in developed countries; and 89% in developing countries (ITU (2013)).

Mobile phones have evolved over the last three decades into feature phones and smart phones. Smart phones were first seen about 8 – 9 years ago. Feature phones were fore-runners of smart phones. The most distinguishing differences between feature and smart phones are that feature phones have lower speed CPUs, screen size, form factor and data speeds compared to smart phones. They do not have an open ecosystem for applications on the phone and rely on proprietary implementations of the applications and operating system by the handset manufacturer. From a functionality perspective, feature phones do have Internet access as well as applications to access email and popular social network sites. They beat the smart phones in price and are expected to replace all basic mobile phones across the world.

The Oxford Dictionary mentions both the terms feature phone and smart phone and has indeed made the difference clear, relatively. A smart phone (noun) is a mobile phone that is able to perform many of the functions of a computer, typically having a relatively large screen and an operating system capable of running general-purpose applications. Whereas a feature phone (noun) is a mobile phone that incorporates features such as the ability to access the Internet and store and play music but lacks the advanced functionality of a Smartphone. Smart phones are a recent phenomenon and their proliferation across the globe is increasing rapidly. The proliferation of the

feature phone per se is far higher than the smart phone. However, statistics indicate that the overall picture is changing. The overall growth rate of smart phones is expected to cross that of feature phones which have been higher so far. It is estimated that while the number of smart phones shipped in 2016 will double that at present (694 million units to 1342 units), the feature phone shipments will drop by about 14 % (770 mu to 660) and basic mobile phones will drop by about 50 % (122 mu to 58). Tablet shipments are expected to rise three times over. (Canalys (2013)).

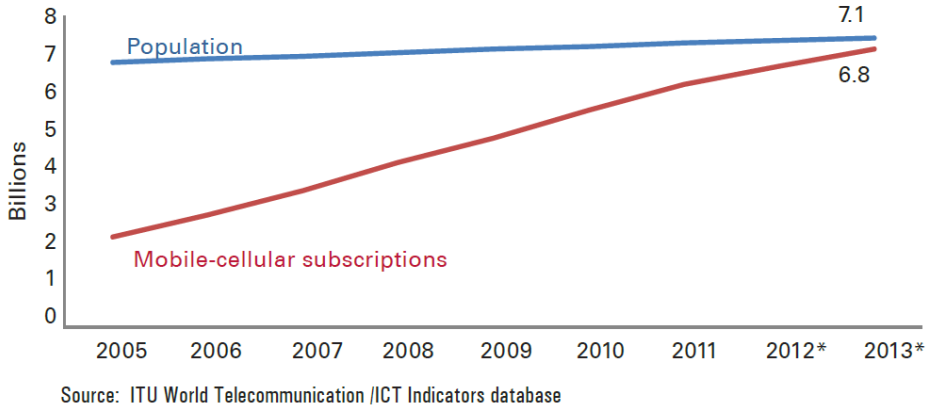


Figure 16: Global mobile phone subscription, * = estimates (ITU (2013))

Existing MP systems have evolved by using SMS services on mobile networks as part of the service function. This was because of the fact that the lowest common functional denominator across the mobile phone functions was SMS. With the proliferation of feature phones and smart phones, the MP services can look forward to an all IP based services. Mobile users and MNOs have, in a sense, bootstrapped the market for MP. Users purchasing digital content online from the MNOs (such as ringtones, alerts/notifications, etc.) have either been billed by the MNO or paid the MNO from their pre-paid account with the MNO. This puts the MNOs in a very advantageous position with respect to the micro payments market.

3.3.3.2 Mobile Infrastructure Technology

The mobile infrastructure is an active participant in the payment process. It facilitates the transfer of information from the user's mobile phone to the

PSP's service end point which could either be resident on the mobile network or interconnected to the MNO's network. The MNO's network should provide an interface to the PSP's service end point.

The infrastructure has to support access to the MNO network, transport the user's information using the appropriate service protocols. Should the payment service requires any other aspect of the core MNO service, such as an SMS, the MNO should provide the service via the interface.

The functional service components of the MNO's network that participate in the payment process are largely identified by their function. They are:

- Short Message Service (SMS) – is a basic core service of an MNO's service offering. SMSes are part of the payment process and are used for authentication and billing. Value Added Service Providers (VASP), such as a PSP, can use these services to send or receive messages to/from a user. The MNO charges the VASP or the user for what is termed as a premium SMS or (P-SMS). If the VASP sends the SMS, it is termed as P-SMS, Mobile Terminated (P-SMS-MT). If the user sends the SMS to the VASP, it is termed as P-SMS, Mobile Originated (P-SMS-MO). The charges for a P-SMS-MO is billed to a post-paid user or deducted from the credit of a pre-paid user. The VASP has an interface to the MNO's operations centre using a protocol such as SMPP over IP.

- Universal Supplementary Service Data (USSD) – is not a store-and-forward service like SMS. It provides a two-way connection between the user and the MNO service and used for instant messaging between the user and the network. This service is typically used by the MNOs for servicing "Balance queries" from pre-paid users. MP services use USSD to charge the user for the payment amount either to his bill or deduct it from the available pre-paid credit.

- Wireless Application Protocol (WAP) and Internet access – are used to access the Internet and access the MNO infrastructure using WAP.

USSD is used for this service. WAP is largely deprecated /discouraged recently to the point that smart phones do not have an implementation of WAP included. WAP served as the protocol stack for MNOs to provide interactive services. WAP billing enabled users to purchase content from WAP enabled sites. Users were identified by their MSISDN which was sent as part of the WAP protocol request. Their purchase was charged either to their bill or deducted from their credit. With the advent of feature phones and smart phones, all services went completely IP based and interactive services used HTTP. WAP 2.0 is still in operation across MNOs but WAP based services are on the decline.

- Interactive Voice Response (IVR) – was used for charging the user by verifying the user's Identity and PIN interactively via a GSM voice call.

These are the various functional components of the MNO network that provide support for the MP services. Note that mobile based payments are well established as a VAS provided by the MNOs themselves, using these functional components. MP service providers use these functional components as service enablers to provide MP services.

3.3.3.3 Categories of items purchased

Although in the literature there is a reference to the use of Mobile Payments for the purchase of a wide variety of goods and services, when the system is narrowed to Operator Billed Mobile Remote Payments, cases and studies make reference almost exclusively to the purchase of digital content and virtual goods. Ticketing and Couponing also seem viable. More specifically main items and services users purchase via Operator Billing are:

- Mobile Content: from traditional content such as Ringtones, Wallpapers and basic games to rich multimedia content and apps for smart phones.
- Web and Digital Content such as music and video files, software or streaming access (Mallat and Tuunainen 2008).
- Virtual Goods such as bonus points and features for online and mobile games. These include features to be used in MMOGs (Massive

Multiplayer Online Games) or customizations and digital items to be utilized within virtual online and mobile communities.

- Ticketing: Includes payment for car parking services (Östberg, 2003), public transportation services (Mallat et al., 2006; Mallat et al., 2006).

3.3.3.4 Mobile Payment Protocols

To explore the mobile payment mechanisms designed so far, the lead is taken from the observations of Dahlberg, T., Mallat, N., Ondrus, J., & Zmijewska, A. (2008) and Slade, E. L., Williams, M. D., & Dwivedi, Y. K. (2013). There are several references to mobile payment protocols in literature. S. Kungpisdan, B. Srinivasan, P.D. Le (2003, 2004a, 2004b) in their papers developed a version of the SET protocol for use with mobile devices and discussed various aspects of the payment protocols. Subsequently, there have been many other protocol proposals mentioning the heavy computing requirements of the protocol proposed by S. Kungpisdan, B. Srinivasan, P.D. Le (2003).

Shedid, S.M. (2010) suggests modifications to the SET protocol, terms it as MSET and compares it with the proposal of S. Kungpisdan, B. Srinivasan, P.D. Le (2003) from a security perspective and , Shedid, S.M.; Kouta, M. (2010) illustrates how the security objectives are met. All modifications suggested are from a perspective of the low client computing capability which can lead to large transaction times. Tripathi, D.M. (2011) points that MSET protocol lacks the Non-Repudiation property of transaction. Tripathi, D.M.; Ojha, A. (2012) follow up with a lightweight protocol for mobile payment which can work on resource constrained mobile devices.

The most recent protocol proposal is from Isaac, J. T., & Zeadally, S. (2013) who have compared the performance of their proposal, in terms of security operations and performance with that of S. Kungpisdan, B. Srinivasan, P.D. Le (2003) and illustrated that their proposal is both economical in terms of resources as well as quicker. Their work is based on a set of earlier work Isaac, J.T.; Camara, J.S. (2007a) and Isaac, J.T.; Camara, J.S. (2007b). All the protocol proposals mentioned thus far consider the classical payment

model that involves the Issuer, the Acquirer, a payment gateway, the payer and the payee.

There are other proposals and implementations that are interesting from a protocol perspective. They attempt to offer a P2P solution with direct interaction between the payer and the payee. Such protocol proposals use NFC technology to exchange payments between mobile phones. Many of them deal with substitutes for currency such as e-cash or tokens. In addition to such proposals, there are other proposals which mention implementation of mobile payments in specific scenarios and provide performance measurements as well as some measures on acceptability. Janne Lukkari, Jani Korhonen, and Timo Ojala. (2004) illustrate an order-pay system to order a meal at a campus restaurant where the ordering and payment is done via a mobile phone. Yen Choon Ching and Heinz Kreft. (2008) propose a framework for P2P payments using transferable value tokens and term it as fairCash. They illustrate the basis for determining the validity of the tokens and ensuring that there is no fraud. Vili Lehdonvirta et al (2009) model the usability and security trade off as a problem of minimising transaction costs and term their proposed scheme as UbiPay. Balan et al (2009) present an NFC based mobile payment scheme to replace cash transactions and claim that the scheme outperforms cash payments in terms of speed and cognitive load, in common payment situations. Roehrs, A.; da Costa, C.A.; Barbosa, J.L.V. (2012) propose a system named 4iPay and demonstrate an implementation on Android with transaction times of 16.5 seconds on 3G and 1.5 seconds on NFC. They then compare the various proposals to illustrate that 4iPay meets all desirable characteristics of mobile payments.

We draw from this comparison and extend it to illustrate the differences between the approaches using Tables 7, 8, and 9.

Functionality	SmartRestaurant (2004)	FairCASH (2008)	UbiPay (2009)	mFerio (2009)	4iPay (2012)	PCMS (2013)
Solution Model	Payment Gateway	Wallet	Wallet	Wallet	Payment Gateway/ Wallet	Payment Gateway Centric
Architecture	Client-Server	P2P	P2P	P2P	Client-Server, P2P	Client-Server
Payment Types	P2B	P2P, P2B	P2P	P2P	P2P, P2B	P2B
Payment Instruments	Transfers	e-cash	Transfers	No	CC, DC, Bank Account *	CC, DC, Bank Account
E-cash/Tokens	No	e-coin	No	Secure Token	No	No
Communication Technologies	WiFi, WAP, Ethernet, USB	NFC, Bluetooth, WiFi, Ethernet, USB	NFC, Bluetooth, WiFi	NFC, Bluetooth, WiFi	NFC, Bluetooth, WiFi, WAP, Ethernet, USB, SMS	WiFi, 3G
Location Awareness	Yes	No	Yes	No	Yes	No
Target Device/s	Mobile Phone, Digital TV	Mobile Phone, Digital TV	Mobile Phone	Mobile Phone	Mobile Phone, Digital TV	Mobile Phone, PDAs
User Configurability	Yes	No	Yes	No	Yes	No

Table 7: A functional comparison of mobile payment schemes. A * indicates that the particular attribute is implied and not specifically mentioned in the proposal

Table 7 provides the functional comparison. In column 1, Solution model gives an idea of the basic service the protocol supports, Architecture shows the actor interaction, Payment types indicates the combinations of the class of the payer and payee, followed by the payment instruments supported. E-cash/Tokens indicates whether the protocol supports an account based solution or a cash/token based solution for P2P interaction. The communication technologies supported are listed next. For a networked application, the communication technology used depends upon the device capabilities and the coded implementation support. Location Awareness indicates whether location details are shared as part of the basic function. Target devices for the potential implementation are listed next. The User configurability indicates the facility for the user to configure various aspects of payment.

Functionality	SmartRestaurant (2004)	FairCASH (2008)	UbiPay (2009)	mFerio (2009)	4iPay (2012)	PCMS (2013)
Architecture	Client-Server	P2P	P2P	P2P	Client-Server, P2P	Client-Server
Payer to Payee	Via Server	Direct	Direct	Direct	Direct and via server	Via Server
Secure Data Exchange	Yes	Yes	NA*	Yes*	Yes	Yes
Payer, Payee Authentication	Yes	Yes	Yes	Yes	Yes	Yes
Settlement	No	instant	Instant	Instant	No*	No
Anonymity	No	No*	No*	Yes*	No*	Yes
Single Click Payment	Yes	Yes	NA*	Yes*	Yes	Yes*

Table 8: Operational comparison of mobile payment schemes. A * indicates that the particular attribute is implied and not specifically mentioned in the proposal

Functionality	SmartRestaurant (2004)	FairCASH (2008)	UbiPay (2009)	mFerio (2009)	4iPay (2012)	PCMS (2013)
Inter-PSP	No	No	No	No	No	No
With Card Networks	Yes*	No	No	No	Yes*	Yes
With Bank Gateways	Yes*	No	No	No	Yes*	No*

Table 9: Interoperability features of mobile payment schemes. A * indicates that the particular attribute is implied and not specifically mentioned in the proposal

Table 8 provides an operational comparison of the various proposals. The routing of the payment between the two end points is indicated against Payer to Payee, in Column 1, Table 8. Secure Data Exchange indicates whether the transaction data is exchanged in a secure manner. Settlement indicates when the Payee receives funds that can be used for other transfers of value, once the Payer has made the payment. Anonymity is a key factor that is referred in literature in the context of payment information. It refers to the fact that the transaction information is recorded but it does not reveal the details of the purchase or the identity of the payer to the payee. Single click payment

indicates the capability of the solution to reduce the user operation to make a payment, down to a single click/touch, after an authentication procedure.

Table 9 provides an idea of the interoperability features of the proposals. Inter-PSP operability is never direct and all interactions are via a payment gateway. Similar interworking with card networks and bank gateways are listed.

Table 7, overall, depicts an evolution of focus of mobile payments from a client-server based model to a P2P, initially, but the focus is now shared between the two. This is an indication for the need to integrate the payment solution so the user is transparent to the type of payment. The proliferation of e-coins, e-cash and tokens in payments does seem to be low. Yen Choon Ching and Heinz Kreft. (2008) illustrate the operational framework necessary to sustain an implementation of e-cash. Regulatory issues with e-cash remain and initiatives such as Bitcoin (Brito, J., & Castillo, A. (2013), Bollen, R. (2013)), introduced in 2009, are still uncertain in terms of acceptance, across the world. Tokens and vouchers are accepted in closed environments and not freely exchangeable. So, the need for an account-based system for payments and value transfer is clear.

The target device for implementing mobile payment is the phone. However, the devices that the payments need to be made from will now extend to various ICT devices used in the home (set top boxes, smart meters, etc.) as well as at other places (electric vehicle charging points). More importantly, both the payer and payee devices will require to communicate to effect the payment. Therefore, payment capabilities must be extended across the devices, as part of their service access or service provision. This is an important observation that impacts the solution proposed in this study.

Table 8 primarily illustrates that instant settlement is a missing ingredient in account based payment systems. This is another requirement that needs to be considered for the solution as are payer and payee authentication single click payment and anonymity.

Table 9 illustrates the need for interoperability between various kind of payment systems. This is one of the major attributes that is considered for the solution design in this study. Instant settlement and inter-provider interoperability form the primary part of the research problem.

3.4 Standards

3.4.1 MP Standards and Consortiums

There are several groups that are addressing MP as a service. Industry Working Groups, Manufacturer forums, Technology Forums, Regulatory bodies are some of them. A comprehensive standard is yet to evolve. It is expected that this will take some time since the MP market is evolving and collaborations across the financial and technical investors are foreseen for providing MP services. In addition, Independent MP service providers are expected. To accommodate this expansion of the eco-system, initial regulatory guidelines are necessary. For example, independent MP service providers must be permitted to provide credit and manage public funds. Such requirements delay service definitions and standardisation.

A list of standards organization and industry-led forums that are active and relevant to M-payment solutions development and deployment within the European sub-continent are listed as follows:

- The International Organisation for Standards (ISO) is the world's largest developer and publisher of International Standards. ISO has different committees which specify technical standards used in mobile payments such as standards for integrated circuit cards, communication protocols such as NFC, security mechanisms and is also is involved with mobile payments in ISO TC68.
- The European Telecommunications Standards Institute (ETSI) produces globally applicable standards for Information and Communications Technologies, including fixed, mobile, radio, converged, broadcast and internet technologies. ETSI defines GSM, UMTS telecommunication protocols and the UICC including all the access protocols.

- EMVCo manages, maintains and enhances the EMV® Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, including point of sale (POS) terminals and ATMs. EMVCo also establishes and administers testing and approval processes to evaluate compliance with the EMV Specifications. EMVCo is currently owned by American Express, JCB, MasterCard and Visa.
- Global Platform (GP) is the leading international association focused on establishing and maintaining an interoperable and sustainable infrastructure for smart card deployments. Its technology supports multi-application, multi-actor and multi-business model implementations, which delivers benefits to issuing banks, service providers and technology providers.
- The GSMA represents the interests of the worldwide mobile communications industry. Spanning more than 200 countries, the GSMA unites nearly 800 of the world's mobile operators, as well as more than 200 companies in the broader mobile ecosystem, including mobile handset manufacturers, software companies, equipment providers, Internet companies, and media and entertainment organisations. The GSMA is focused on innovating, incubating and creating new opportunities for its membership, all with the end goal of driving the growth of the mobile communications industry.
- Mobey Forum is a global, financial industry driven forum, whose mission is to facilitate banks to offer mobile financial services through insight from pilots, cross-industry collaboration, analysis, experience-sharing, experiments and co-operation and communication with relevant external stakeholders.
- The Near Field Communication (NFC) Forum is a non-profit industry association that promotes the use of NFC short-range wireless interaction in consumer electronics, mobile devices and PCs.
- In Europe, the European Payment Council (EPC, 2013) is the decision making and coordination body of the European banking industry in relation to payments. The EPC develops the payment schemes and frameworks to realize the Single Euro Payments Area (SEPA). SEPA is an infrastructural initiative from the European Commission and the

European Central Bank to create a common payment market across Europe

3.4.2 Regulation and Standardization Challenges

Regulation has not kept pace with mobile payment innovations. Most non-banks rely on traditional funding sources such as Credit, debit, prepaid cards etc. Furthermore, mobile carriers and alternative payment providers are less familiar with banking laws. There is a lack of specific guidance and legal framework for mobile payments where coverage and liability unclear. This creates a large gap for mobile payment adoption.

3.5 The Gap

The current challenges in large-scale deployment, acceptance of MP mechanisms can be seen as the gap in M-payment research.

3.5.1 Payment Industry standardization Problems

The onus is on the payments industry to provide a method that both buyers and sellers could use to complete the payment transactions. In order to facilitate large-scale trade on e-commerce it was essential to introduce a uniform and standardized method of payment. There needs to be consensus among the buyers and sellers to create a standardized payment method.

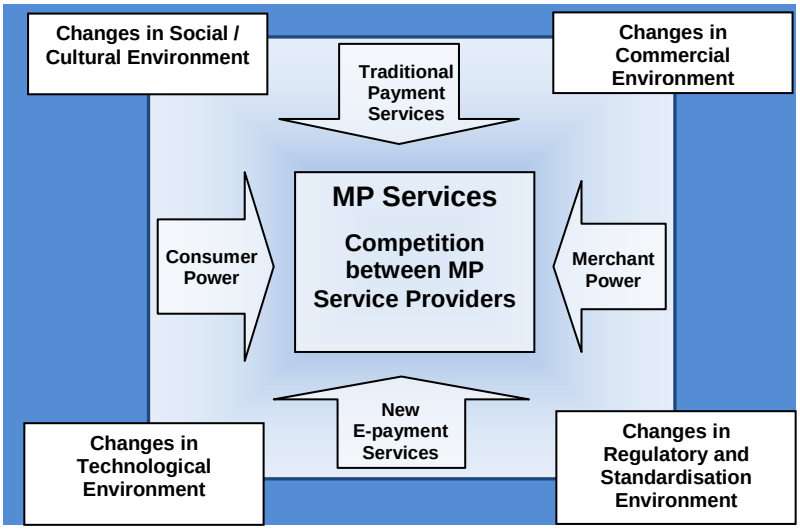


Figure 17: Framework of factors impacting MP services

As observed by Evans and Schmalensee (2009) there exists a 'chicken and egg' problem with the payment industry. The authors have observed that the

buyers are not be willing to use a payments instrument if it is not widely accepted across all vendors and , and sellers are not willing to accept a payment instrument when only few shoppers are willing to pay with it. Therefore, players willing to introduce new payment instruments are expected to solve this fundamental issue. This is more challenging as these players need to compete against well established, secure and convenient payment methods through which transactions take only a few seconds to complete. It is hard to convince merchants and consumers to change when what they currently rely on works very well

3.5.2 Large-Scale Adoption Problems – From the Provider Perspective

The payments market is a *two-sided market* and serves two distinct user groups who are inter-dependent and facilitates the business. A market is termed as two-sided if the platform can affect the volume of transactions by increasing the charge on one side and decreasing the charge equally on the other side; the pricing structure matters and it should be designed so as to bring both sides on board (Rochet J; Tirole J., (2006)). In our context, the MP service is the platform, the consumers are on one side and the merchants on the other. The merchants need to pay for infrastructure and the transaction of the payment service whereas the consumer has to pay for the facility and convenience. The MP service provider should balance out the charges between the two sides to ensure that the service is found attractive enough for the consumers to adopt.

Mallat, N. & Tuunainen, V. K.(2008) identify the barriers to adoption to include complexity of the systems, unfavourable revenue sharing models, lack of critical mass, and lack of standardization. For the merchants to invest in the service, they must perceive the existence of a *critical mass* of consumers on the service (Dahlberg *et al.*, 2007; Contini D *et al.*, 2011; Begonha *et al.*, 2002; Remco Boer and Boer, 2010; Jeroen de Bel and Gâza, 2011). MP services, so far have failed to attract this critical mass for adoption (Pousttchi *et al.*, 2009; Mallat, 2006) and are believed to be slowing down (Chaix, Laetitia; Torre, Dominique (2012)). The MP services require the following characteristics - simplicity and usability, universality, interoperability, security, privacy and trust, cost, speed, and capability for cross border payments (Dahlberg *et al.*, 2007;

Karnouskos and Fokus, 2004; Antovski and Gusev, 2003; Pousttchi, 2003) to enable adoption and reach critical mass. Achieving critical mass is an indication of the universality of the solution since it is a key factor in driving adoption of the service (Van der Heijden, 2002).

However, mobile based Internet access (ITU (2013)) to other services, including mobile banking are on the rise (NMG 2013). Users remain ambivalent about their use of mobiles quoting the fear of their data falling into the wrong hands in a recent survey and 69% cited security reasons (NMG 2013). Nevertheless, MP is expected to take off in two to five years, from now. The current challenges in large-scale deployment, acceptance of MP mechanisms can be seen as the gap in MP research.

3.5.3 Large Scale Adoption Problems – Consumer Perspective

The consumer is on the other side of the two-sided MP market. While the merchant adoption has largely been impeded due to a lack of business/ revenue models and a lack of service standardisation. The consumer side adoption barrier is mainly due to an uncertainty of the benefits to them and the security perception of the service.

Technically, users are enabled to use mobile devices and device proliferation has risen to very high levels. They are aware of the risks of online services and experienced mobile payment service users of the services provided by their MNOs. So, they are prepared to use the services should they see the services as secure and convenient and not simply another way of payment which they have a choice of. PCI has published guidelines for mobile payment acceptance as well as security guidelines for merchant adoption in February 2013. Similarly, the Trusted Computing Group has guidelines for the use of Mobile Trusted Module (MTM) for use of mobile devices for banking and payments (TCG (2011)). Security is indeed being addressed and what is currently lacking is the security requirements for the payment process.

Summarising the perspectives of MP services of each of the actors from literature by Pousttchi and Zenker (2003), Pousttchi (2003), Van Der Heijden (2002), Mallat, et al (2004), Ondrus and Pigneur (2005), a list of requirements from the vendor perspective, customer perspective, mobile operator and financial institution's perspective is listed in Table 10.

3.5.4 Requirements and Expectations of the Mobile-Payment Players

As part of investigating the gaps that exist within the current mobile-payment systems, it is essential to identify the basic functional requirements of all the mobile-payment players as well as their expectations from a global, standardized mobile-payment platform based on the literature presented in Zheng and Chen (2005), McKitterick (2003), Rahimian et al (2008), Ondrus and Pigneur (2006) and Min and Li (2009). Table 10 summarizes the list of requirements for each of the MP stakeholder.

MP Players	Requirements / Expectations
Merchant Requirements	• Faster transaction time/ Minimum number of transactions. • Low Capital investment, low running cost. • Integration with existing payment methods. • High-level Security and trust. • Configuring/customizing the service. • Real-time status of MP transactions.
Financial Institutions	• Branding and customer loyalty. • Ownership or co-ownership of the MP service. • Secure and trusted payment service. • Minimal fraud /Loss. • Lower capital and operational cost.
Mobile Operator	• Lower capital and operational costs. • Increased customer loyalty. • Added value to existing services. • New revenue channels. • Increase in Average Revenue Per User [ARPU] • Service with low time to market .
Device Manufacturers	• Open , interoperable widely used standards. • Low cost of new features/technologies to be integrated. • Multi-application capability.

Customer	• Minimal Learning Curve. • Trusted and secure solution. • Personalized service. • Service availability. • Low cost of usage. • Interoperability between mobile operators, devices and financial institutions. • Real-time transaction status. • Universal payment mechanism using any device, anywhere in any currency. • Scope for person-to-person transaction.

Table 10: Stakeholder perspectives on MP services

Based on the above table, a common set of design features that is expected of a comprehensive mobile payment model is listed as follows:

3.5.4.1 Simplicity and Usability

The generic mobile payment platform should be easy to implement for all the players involved. The specifications should be based on open standards keeping it simple resulting in a short learning curve.

ISO defines usability as “The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use”. Simplicity and usability leads to system acceptability. Nielsen’s concept of system acceptability argues that the model must also be useful, practical and socially acceptable (Nielsen, 1993) (Fig 3). Ultimately adoption is likely to influenced by the ability to use the model in a way that is convenient to all the parties involved (Valcourt et al, 2005).

3.5.4.2 Interoperability and Universality

The term micropayment is widely used to describe transactions of a low value, but there is no standard amount at which a payment becomes a micropayment. The challenge for micro-payments is that the cost of processing is high compared to its value. As a consequence some vendors have introduced a minimum transaction value for EFT payments, while the payments of high values are processed by all vendors. It is essential for the mobile-payment system to accept any amount paid through any channel such

as a credit/debit card, bank account transfer or digital wallets, etc., as presented by Choi et al (2006)

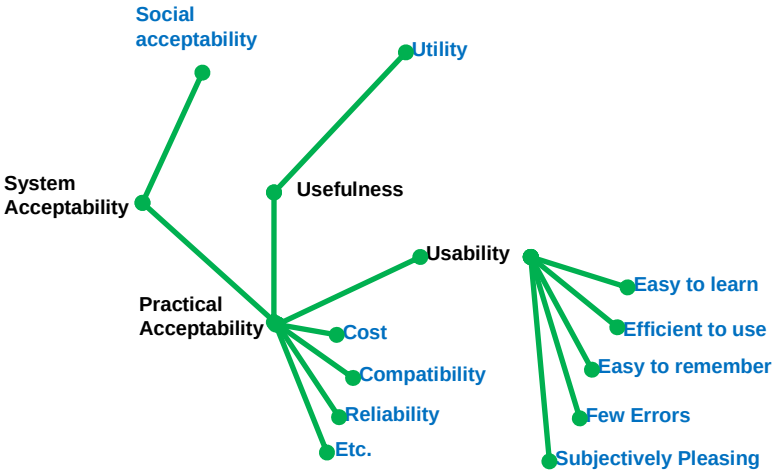


Figure 18: Model attributes of system acceptability (Nielsen 1993)

Similarly, there are a wide variety of mobile devices in the market with varying capabilities, and that which connect using varying access technologies such as WiFi, GPRS, 3G, LTE etc. It is essential for the mobile payment mechanisms to be universally accessible irrespective of the amount of payment, channel of payment or the devices and technology used.

In order to achieve the universality, there is a need for a paradigm shift in the way mobile-payment ecosystem is categorized and in its operation.

3.5.4.3 Cost and Speed of Transaction

It is essential to keep the cost of the transaction as low as possible for all the players involved in its large scale adoption. Traditionally, transaction costs were borne by the vendors/merchants, however there may be a change in this in the future where costs may be transferred to the customer for the services received or the cost may be shared between multiple players.

Similarly the speed of transaction is a critical parameter that decides the uptake of the technology. Especially from the user's perspective and for the efficiency of the mobile payment system, the number of transactions is required to be kept at a minimum (Herzberg, 2003).

3.5.4.4 Security, Integrity, Privacy and Trust

It is essential for the mobile payment platform to provide a level of security that is acceptable to all parties involved in a transaction. All users must be able to transparently aware of the data that is passed on all the players involved and the measures taken to secure the transaction and preserve its integrity. This needs to be implemented in such a way that they can trust the protocol and, for any given transaction, quickly decide whether it is appropriate to proceed.
Encryption is a given, but the methods of encryption require careful consideration. Although the latest mobile devices have significant processing capabilities, previous generation feature phones and tablets (still in widespread use) might struggle with high level cryptographic algorithms such as public key cryptography (Linck et al, 2006)

Each party involved in a transaction will require a means of authenticating those with which it interacts. To initiate a secure transaction the consumer must firstly be able to verify that the service they are about to use is what they believe it to be (and not a clone). Subsequently the service needs to determine that the consumer is who they purport to be and then, during the processing the transaction, each party must be able to authenticate those others with which it interacts. For servers this might be achieved using digital certificates and certificate authorities; For human user authentication could involve:

- Something they know (e.g. Secret PIN number or password)
- Something they have (e.g. Device)
- Something they are (e.g. Fingerprint)
- Using a robust (preferably a multi - factor) but sufficiently fast procedure for authenticating human users is essential for the success of any mobile payment system.

The approaches used for all aspects of authentication must be such that man-in-the-middle attacks are not feasible and that eavesdropping only provides meaningless data.

The concept of privacy needs to be protected such that parties involved in payment processing do not necessarily need to know what the payment is actually for, only the amount that is to be transferred and relevant details of the payee.

There might be circumstances where a consumer wants to pass on further details about themselves in order to receive future communication from the vendor or where they would elect to provide details of their purchasing habits to a third party to assist with fraud detection (Karnouskos et al, 2004).

With regard to both security and privacy, all users of the framework must be able to understand the policies without having to read any fine print and trust that by using it the data will not be compromised or used in any way to which that have not consented.

3.6 Scope of Current Study

1. The research is not limited to any geographic territory or area, however the standards and regulations related to the European sub-continent is considered as part of the research.
2. The research focuses both on Mobile Remote Payments as well as proximity/contactless based payments. UMTES is designed to be a solution for both.
3. The research attempts to illustrate the feasibility of the operation of UMTES on mobile networks by way of estimating the network delays as well as evaluating the network delays using simulation.
4. The research covers technology-based aspects to the mobile payment deployment and implementation. The strategic phase of the adoption, that is the decision making process of adopting the mobile payment system is out of scope.
5. The proposal made in this study may or may not comply with the existing regulations across the world. Such a discussion is out of scope of the study.

Chapter 4
Unified Mobile Payment Transaction Exchange Service (UMTES)

UMTES as a service will be defined by two components namely, the service architecture and the service definition. The service architecture will define the functional components of the service and its layout in terms of a functional topology. These functional components are resident on the end points of service. The service definition will illustrate the functional interaction between the architecture components and will include the functional scope of the service. The service definition that includes the functional interaction between the end points is represented as a protocol. The following sections detail the architecture and the service definition. They are addressed as a generic payment system to illustrate that UMTES architecture can be mapped on to any existing payments system.

4.1 MP Service Architecture

A Payments System is a funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions (EPC 492-09 (2012)). Payments system architecture is the set of physical and logical structures that allow institutions to exchange payment instructions, initiate settlement and perform any additional functions associated with a payment (RBI-AU (2012)). A payment service rides over these structures to fulfil the customer's payment needs. In the context of MP, the structures that provide a customer the ability for mobile access to the payment services adds on to the structures of the traditional payment systems.

The MP service architecture comprises the functional components of the service. These functional components are detailed in two parts. First, the actors in the MP service and their relationship is illustrated. Following this, the specific functional components of the MP service are illustrated.

4.1.1 Actors in the MP Service

The actors in the service depends upon the model of MP service provision. Chaix, L., & Torre, D. (2011) suggest that the mobile payments service provision will require to be collaborative but tend towards independent providers, who are neither banks nor MNOs, providing payment services. The

European Payments Council anticipates the entry of such providers into the payments eco-system and mentions this in (EPC 492-09 (2012)). The Independent PSP (IPSP) model is considered for the study.

The IPSP is accessed by the payer (buyer) via a mobile network infrastructure which is owned by an MNO and interacts with the payee (seller/merchant), the financial institutions (such as banks), with the support of a Trusted Service Manager (TSM). Each of the actors can play a single or multiple functional roles. The most generic case is with one role being performed by each of the actors – their core business competency.

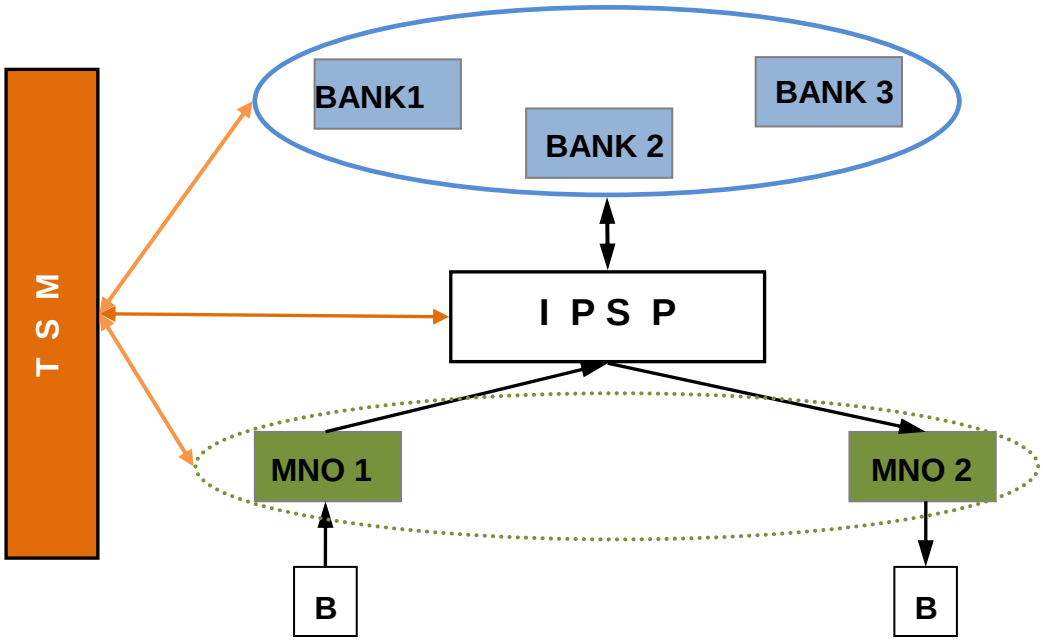


Figure 19: The Independent PSP model overlaid with the TSM interactions for Mobile Contactless Payments

The TSM is necessary since mobile contactless payments are included in the consumer's payment service portfolio. EPC 220-08 (2010) defines the mandatory role of the TSM as a third party provider of the service management required to enable, maintain and manage the user's personal and security data on the mobile device by interacting with the financial institutions and the MNOs. The TSMs are not involved in the payment transactions.

The IPSP model in Fig 9 (ref. §2.1.3) is overlaid with the TSM and its interactions with the Financial Institutions, the IPSP and the MNOs (fig. 19). The IPSP requires to interact with the TSM if it plays the role of the Issuer,

which would be the case if the IPSP provided a e-coin service or issued its own branded credit cards.

4.1.2 A Layered Model for MP Services

From Fig 19, it is evident that the MP service spans across the actors and the fulfilment of a customer/payer's payment request will traverse all the actors that participate in the service. There are three broad categories that the payment service functions would fall into – access to the payment service, the payment control functions and the payment settlement functions.

The access function provides the PSU access to the payment service. The PSU and MNO are the actors involved in this function. The control functions include all functions that are necessary to coordinate the initiate-authorise-confirm cycle of the payment. This includes the end point functions for the payment request, originating the request functions for the payment settlement and notifications to the payer and the payee. The actor involved for the control functions is the IPSP. The settlement functions include the value subtraction, value addition and appropriate responses to the requests from the control functions.

From this functional categorisation, the service model in Fig. 14 can be divided into three layers – the Payment Service Access (PSA) layer, the Payment Service Control (PSC) layer and the Payment Service Settlement (PSS) layer. The TSM that performs the role of service management interacts with all the three layers. This is termed as the Three Layer Model (TLM) for payment services (Fig. 20).

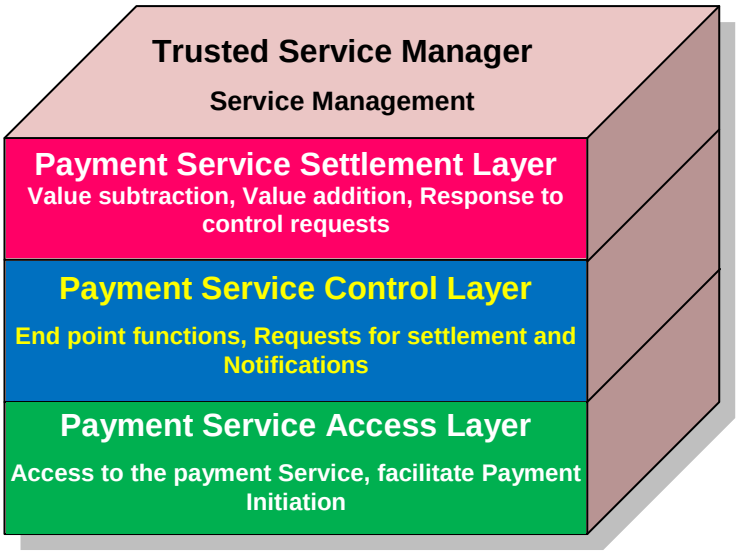


Figure 20: The Three Layer Model for Payment Services

These layers are indicated in the IPSP service model and depicts the actors in each of the service layers (Fig. 16). These layers, in the broader context of the ISO OSI layered internetwork model, are at the application layer.

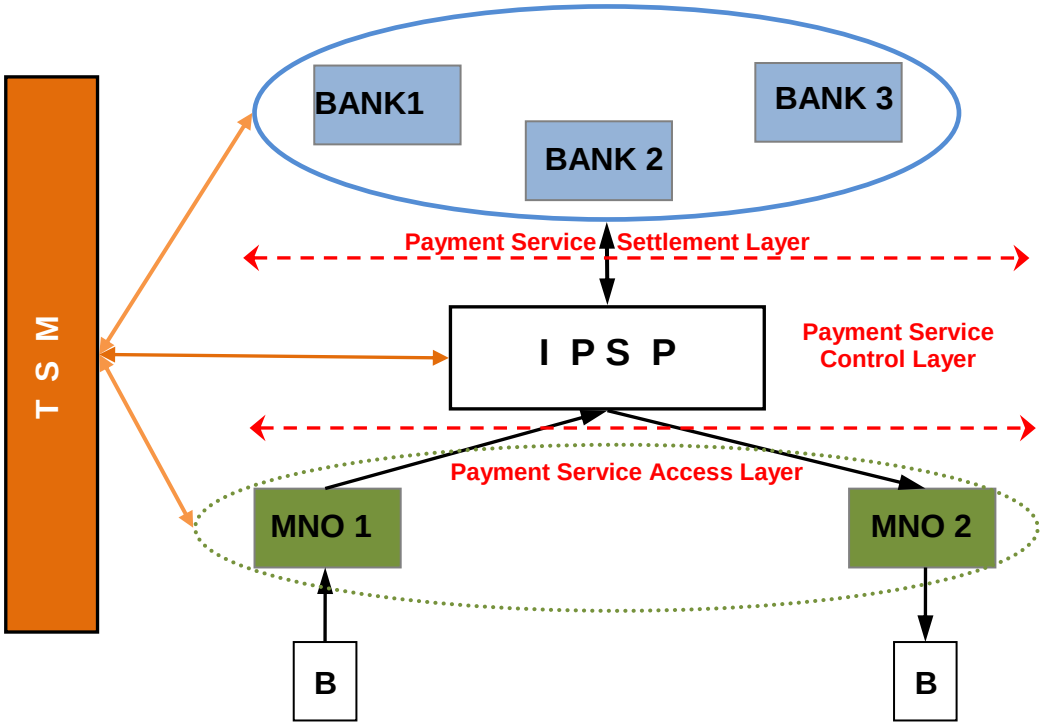


Figure 21: The IPSP model with the three payment service layers

Fig. 16 shows the three payment service layers. Notice that the PSS layer is a collection of actors who are Banks and/or Financial Institutions. Similar to the PSS layer, the PSC and the PSA layers can be a collection of IPSPs and MNOs respectively. Therefore, the most generic model will contain four sets of actors, one set each corresponding to each of the layers and a fourth containing a set of TSMs (Fig. 21).

4.1.3 The MP Service Architecture

The MP service provides an end user the capability to initiate, authorise and confirm a payment to be made to another user/service_provider/device who/which is typically a seller. This service is availed by the user using a mobile device. An application on the mobile device would provide access to the MP service and fulfil the user's request for payment. This application would access the PSP to fulfil the user's payment request. The request originates from the PSA layer and is passed on to the PSC layer.

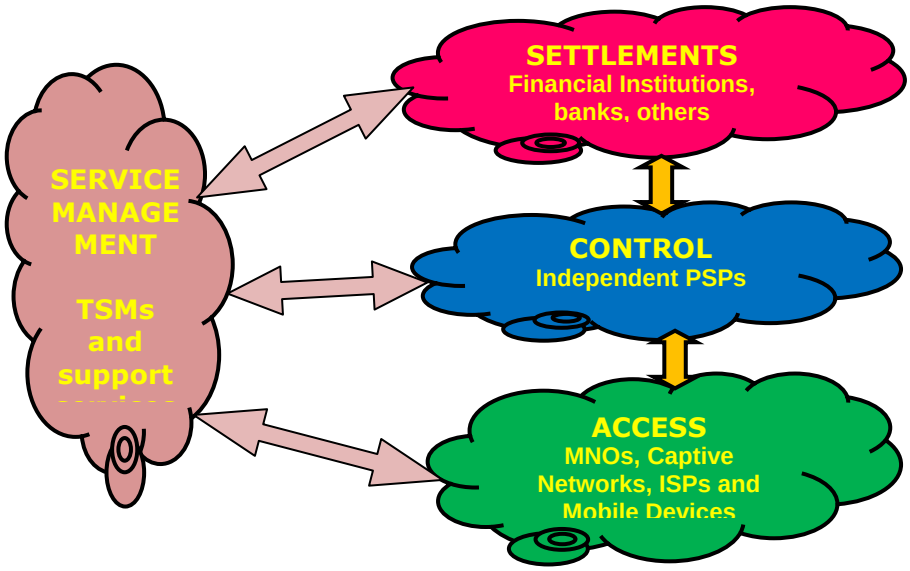


Figure 22: The Generalised Three layer model for Payment Services

The MP service provider, in the PSC layer, receives the payment request from the user in the PSA layer and fulfils it by interacting with the elements of the PSS layer.

The interaction between the layers will be via interfaces which are a part of the PSC layer. There is one interface each for the layer above and the layer below. Each interface comprises of two interface units – the physical interface unit (PIU) and the service interface unit (SIU). Each interface unit defines the mode and type of interconnection between the layers. The PIU defines the physical interconnection of the PSC layer infrastructure and the infrastructure of the adjacent layer. The SIU defines the service end point of the service for the adjacent layer (Fig. 18).

A PSU using a mobile device accesses the service infrastructure through the PIU of the mobile device and that of the access layer. The MP service element (application) on the mobile device uses the payment service interface resident on the mobile device and interacts with its equivalent on the IPSP, via the SIU at the PSC layer. The service element on the IPSP interacts with the service elements of the PSS layer via the SIU on the interface. The SIU provides, in addition to being a service end point, a gateway service that relays (with

appropriate security measures) the requests from the PSC to the PSS and from the PSS to the PSC layer.

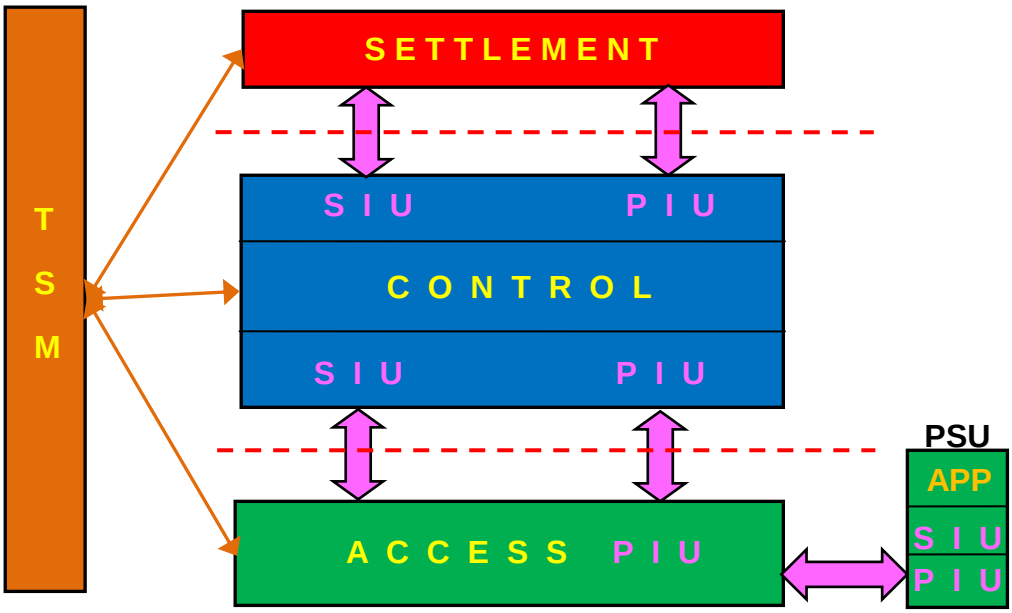


Figure 23: Payment Service Architecture showing the interfaces between layers. The PSU is part of the PSA layer

4.1.4 Service Elements

Each layer has service elements which utilise the SIU to provide the service. Recall that the PIU provides the physical point of interconnectivity between the layers. The service elements in each of the layers perform the major functions of the layers. The service elements of each layer are listed individually and explained in the following sub-sections.

4.1.4.1 Service Elements of the PSA

The access layer manifests as the mobile network that provides access to the payment service. It enables the access from the mobile device to the payment service elements in the control layer. It performs three major functions while providing access to the services in the control layer. They are Authentication, Authorisation and Monitoring. All these functions are part of the mobile network operations and exist as part of their basic telecommunications service. Each of these functions are defined below

- Authentication: The mobile device, its identity and service access credentials are checked by the mobile network operator. Upon

verification, the device is permitted to connect to the network and will remain part of the network. The device will be permitted to roam across other mobile network operator networks with whom such roaming agreements are in place.

- Authorisation: After the mobile device identity is verified and permitted to connect to the network, its service profile is applied within the network. Such service profiles are based on the service the mobile user subscribes to.
- Monitoring: Once the device is connected to the network and the service profiles are applied, the network operator monitors all activity of the mobile device from a usage perspective. Such monitoring is primarily for billing purposes and could also include security requirements.

The PIU in this layer provides the physical interconnectivity with the upper layer on one end and the mobile device on the other end. Notice that the physical interfaces interconnecting the mobile device is wireless whereas that interconnecting the PSC is typically, a wired interface.

The wireless interconnectivity used by the mobile device could use any of the wireless access technologies such as 3G, LTE, WiMAX, WiFi and so on to utilise the wireless broadband service provided by the mobile network operator. In contrast, the interconnectivity between the PSA and PSC is typically a wired interconnection that facilitates a large bandwidth resource for data traffic between the two layers. Multi-homing is used to ensure that there is sufficient redundancy and fault tolerance built in to accommodate failure of interconnectivity.

The SIU of the mobile device uses the SIU of the PSC as its access interface to the payment service. There is no specific SIU in the PSA since the PSA does not participate in the payment service but only serves to provide a physical access and path to the payment services. From a stake holder perspective, this means that the mobile network operator does not directly participate in the payment service function; they only enable physical access from the mobile device to the service.

4.1.4.2 Service Elements of the PSC

Authentication, Authorisation, privacy, payment context router, wallet/pouch, inter-PSP transfers, settlements interface

The PSC provides the core payment service functions and interfaces with the PSA and PSS layers. The interfaces provide access to and from the service

elements within the layer. The payment service application on the mobile device uses the SIU on the device to access the payment service via the SIU of the PSC. The access path is via the PIU of the device, the PSA and the PSC.

The PSC supports various functions of the payment service. The major functions are Authentication, Authorisation, Privacy processing, Payment context processing, wallet/pouch processing, inter-PSP communication and logging. Each of these functions are defined below.

- Authentication: The user, the device being used to access the service and the payment service application are authenticated as valid entities to use the service.
- Authorisation: The service profile of the user is activated, after the authentication. The service profile is partly decided by the subscription type and partly configurable by the user.
- Privacy Processing: The application on the user's mobile device and the PSC negotiate specific security parameters for the service interaction.
- Payment Context Processing: The context of the payment is ascertained based on the payment details. User preferences for the mode of payment (card, direct debit, low value payment, etc.) are applied, if specified or the default payment mode indicated is applied. The payment context processor redirects payment requests to the inter-PSP communication, if the transfers are destined to a user registered with another PSP. Similarly, the requests are directed to the wallet/pouch processing unit if the payment requests are of low value.
- Wallet/pouch processing: The support for low value payments is done via this unit. The wallet/pouch needs to be charged with value prior to its use. Such a charging is typically done from a primary funding source indicated by the user.
- Inter-PSP communication: this unit enables communication between the PSPs for purposes of transfer of value. This unit is different from the settlements unit and takes care of direct transfer of value between the PSPs which are not either banks or card issuing payment service providers..
- Settlements: The payment context processor redirects payment requests to this unit if the transfer of value is through a financial institution such as a bank which have established settlement

procedures via a clearing house. This unit interacts with the PSS layer via the SIU of the PSC.

- Logging: All transactions are logged in the system and the logged information is kept private.

4.1.4.3 Service Elements of the PSS

The settlements layer provides the critical functionality of the actual transfer of value between the financial institutions of the payer and the payee. The settlement functions are entirely handled by the financial institutions. The PSC service elements interface with the PSS services via the SIU of the two layers. The major function of the PSS is the transfer of value between the financial institutions via the Clearing House (CH). These settlement procedures are standardised, comply with regulatory requirements and have been operational for a long time.

4.1.5 Ownership of the Service Elements

Recall from section 4.1.1 that the model we consider for study is the independent PSP model. From the perspective of an independent PSP the functions of the PSS layer are not completely owned by the independent PSP as are the functions of the PSC. The functions of the PSC are completely owned by the independent PSP and these service elements initiate from and respond to requests from the payment service application on the mobile device. The PSA layer, as mentioned earlier, provides an access path between the mobile device and the services of the independent PSP.

4.2 MP Service Definition

There are several aspects to the MP service that form part of the definition. Each of these are listed separately, below.

4.2.1 The Core Service

The MP service is an extended service provided by a payment service provider who already has services that are executed using traditional means including online payments. The MP service is therefore considered as a specific instance of an online payment where the control is autonomously available with the user.

The autonomous control is provided by a mobile application, a software executed on a mobile device, owned by the user. The mobile application is distributed and maintained by a Trusted Service Manager.

The mobile payment service provides a user, the payer, the ability to initiate, authorise and confirm a payment to a payee, using a mobile device. The payer can choose the source of funds as well as the mode of payment for each payment, either by specifying preferences or by choosing them before initiating a payment.

The payment service provides a wallet/pouch for the purpose of low value payments that are of values typical of cash payments. The term “pouch” is preferred over the term “wallet” since low value payments, in the currency system, are typically handled by using coins. Coins are typically stored in the pouch of the wallet. While the term “wallet” signifies the larger service component that stores all the card related information and the account information of the user, the term “pouch” signifies a fund store for the low value payments.

Funds are transferred *a priori* from a source indicated by the user to the pouch. The funds from the pouch can be utilised by the user until the funds in the pouch are exhausted. At this time, another transfer of funds will be necessary to top up the pouch with funds. The source for such transfers can either be chosen or indicated as a preference. Limits on the value of the transfers and the number of transfers can also be imposed by way of configuration. Upon reaching these limits, the user is notified and attempts to make payments are aborted.

All transactions relating to the pouch will initiate instant transfer of value if the payee is another independent payment service provider, that is, the payee payment service provider is not a bank or a similar financial institution that uses the services of a clearing house for settlements.

The MP service supports payments via other payment instruments such as credit/debit cards by connecting to the appropriate gateways for such payments. These are auxiliary services that are triggered by the payment protocol upon a demand from the user for such a payment. The delays in transfer of value for such payments is governed by the settlement policies of those providers.

Each of the participants in the service have a distinct identification. The user has an identification as part of her/his registration with the provider, which the provider uses for authentication as well as to address messages and notifications to. The provider has a distinct identification which the user uses to address when requiring to make a payment. The providers identity is distinct

across the provider space to enable payee to make payment requests to the appropriate providers.

4.2.2 The Security Support

There are three broad security concerns in the service provision, namely, secure access to the device and its services, secure access to the service provider to access and use the service and secure data transfer of all authentication and payment related information during the payment process.

The device used by the user for purposes of payment has to provide secure access to its services such that only the real owner has access to services. Current day devices provide finger print based authentication (Eg: iPhone 5 with IOS7), facial recognition based authentication (Eg: Google Nexus 5 with Android KitKat), in addition to traditional PIN and password based authentication.

The device and the payment application attempting to make a payment are both authenticated by the payment service provider. The application coveys its own identity along with the device identity, both of which are pre-registered with the PSP. Note that the device is also authenticated by the mobile network before it can use the access services of that network.

The data security for the entire session is taken care in two steps. The end-to-end connection for data transfer on the network is via secure sockets layer (SSL). This ensures a peer negotiated security association that results in encrypted data between the payment service provider and the user. A similar connection is made for the inter-operation between two payment service providers. The application that uses the payment protocol also negotiates a security association with its peer and encrypts data before it is sent to the SSL end point for further delivery. In effect, there is a dual encryption of data, as seen on the network.

The security model of the application used for the payment services broadly mimics the security model of the GSM system. The security process in the system is mentioned in § 4.6 as part of the design objectives of the payment protocol. The security requirements for the service follow the recommendations laid out in ECB 2013 and PCI-DSS 2013.

4.2.3 The Application

The application used for payment services on the mobile device is built and distributed to registered users by a trusted service manager entity in the eco-system.

Each application is provided with a distinct identity which is used in the authentication process. The application is treated as a software asset that is provided to the user by the payment service provider and meant for her/his personal use on a device, pre-registered by the payment service provider.

The trusted service manager also performs all the necessary security instrumentation required by the application. A part of the information required for such instrumentation is provided by the payment service provider. Typically, these applications are provided to the user, over-the-air (OTA).

4.3 The UMTES Service Context

The Unified Mobile Payment Transaction Exchange Service (UMTES) is proposed as the protocol that will enable the mobile payment service using the architecture described in the earlier sections. UMTES manifests itself as an application layer protocol that is used by the payment applications. There are two functional application entities that comprise the service – the application entity that runs on the provider side (server side) and the application entity that runs on the mobile device (client). These application entities are built with UMTES support and they utilise the UMTES protocol to communicate the payment functions. The functional elements of UMTES are designed with a specific scope of the overall service.

The functional scope of the service is described below. It lists out the service environment, what the service is for and how it can be used by the end users. These details form the basis of the functional design of UMTES.

4.3.1 What does the service provide?

The payment service provides the users of the service a capability to make a payment to another party using a specific means of payment (payment instrument) supported by the service. Presently, the service is designed to make payments from the user's account with the PSP as a source of funds. The value of the payment made is instantly transferred as part of the payment transaction. Support for payments using alternate payment instruments to make payments is provided as part of the basic design. Additionally, a user is able to transfer funds from a primary source such as a bank or a similar

financial institution. The users will be able to perform all operations using an application program that will run on their smart phones.

Using this application, the user is able to make a payment to a business or another individual for services or goods received. The payment to a business could either be a purchase of goods or services at a store, online or via a vending machine. All the participating entities should support the common payment protocol supported by the application.

4.3.2 The Target Audience

The service is intended for smart phone users. The service is limited to smart phone users for two reasons – that the compute power available on smart phones is necessary to provide sufficient data security and that the application development environment for smart phones is open and there is a well-defined system available for distribution of applications. This is in comparison to feature phones that have less resources and often run proprietary applications only.

4.3.3 Type of Payments

The service supports what is termed as “Retail Payments”. Retail payments usually involve an individual as one counterparty and an individual, firm or government agency as the other. The counterparties can be engaged either in a transaction-by-transaction relationship involving one-time payments or in a contractual relationship involving recurring payments (CPSS, 1999). The payments can be face-to-face or remote. Some frequent, small-value, business-to-business payments might also be characterised as retail payments.

Not all individual retail payments are for small amounts, but compared to the large-value payments related to financial transactions between institutions, they have a much smaller average value and much greater daily volumes. They also involve a much broader range of payment instruments and transaction systems (Gopinath S, 2009).

The application is intended to address retail payments based on value. In the context of retail payments, payments up to and including a value of £5 (or £10) are termed as micropayments and those above are referred to as macro payments. The impact is on the security overhead associated with these payments; a reduced value implies a lower risk to the user, as well as the PSP and there is scope to reduce the security overhead and, in general, the transaction overhead based on these factors.

In case of micropayments, the transfer of value between the two end users will be completed in real time. Note that this is traditionally considered as part of the settlement process. The transfer of value for macro payments too can be instantaneous if the transfer of value is between the two independent PSPs and does not involve a financial institution such as a bank.

4.3.4 The Application

The application that runs on the user mobile will be treated as a software asset owned by the PSP and leased to the user as part of the subscription. Therefore, the maintenance of the application (updates and releases) will be the responsibility of the provider. Generally, this function is fulfilled by the TSM.

The TSM will generate a version of the application for use of the subscriber the information. The application will be tagged with a “time-to-live” (ttl). Upon the expiry of the ttl on in anticipation of it, the provider should extend the lease of the application to the user. This is done to ensure that the application is tracked and used with the device it is registered to be used with.

The application is launched for use. A “pop-up” screen appears when the user receives a payment request from the seller displaying the details of the payment request received and prompts the user to make the payment.

4.3.5 Security

There are three factors considered with respect to security of the entire service. They are – the user and device authentication, the application authentication and the privacy of data transfer over the network. The user and device authentication is part of the initial authentication process. Similarly, the application is authenticated for its identity. The data transfer between the device and the provider is over a secure connection, thereby keeping the data private.

These factors address the primary security concerns of identifying the end points (payer and payee) and the privacy of data when transferred over the network.

The security association between the user and the provider can further be supplemented using a security scheme within the application.

4.3.6 Standards and Compliance

The overall design complies with the requirements and recommendations of some important agencies in the mobile payments eco-system. A TSM with the role recommended in the GSMA is included in the discussions. The

implementation of the TSM however is trivialised to a URL from where the application has to be downloaded.

The data representation is in JSON/XML in line with the ISO-IEC 20022 standard for financial message exchange. Most financial systems are in the process of complying with the ISO-IEC 20022 and hence the choice of using the same data representation as in the standard.

4.4 The UMTES Protocol

The protocol is intended to facilitate a user, a payer, to make a payment to a payee. The user makes the payment using a smart phone, in response to a payment request made by the payee. The payee could originate the payment request via a mobile PoS or via a desktop PoS. The payer and the payee communicate with each other through their respective payment service providers. Once the payment is complete, the payee is notified about the status of the payment. A payment process is deemed complete upon the payee receiving a notification indicating the success of the transaction or a failure with the reason specified.

The transfer of value corresponding to the payment made is initiated as part of the payment process if the value is below a certain limit, which is configurable.

Towards achieving the payment process mentioned above the UMTES protocol is detailed in the following sections.

4.4.1 The UMTES Model

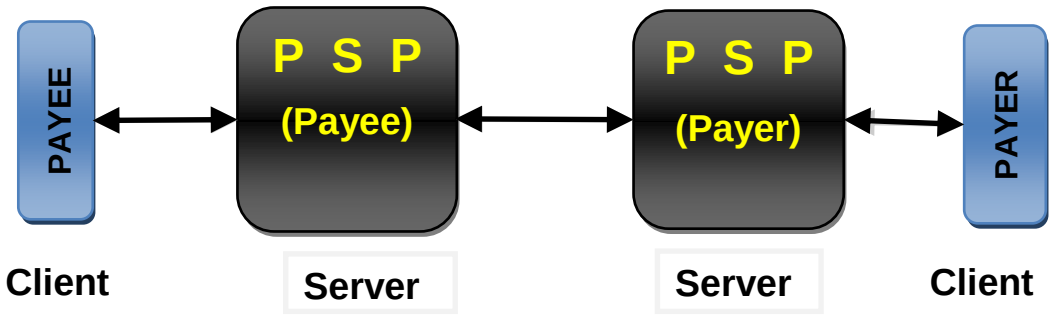


Figure 24: The generic UMTES service model

The UMTES design is illustrated in Figure 24. The primary actors in the functional model consist of the Payer and the Payee and their respective

payment service providers. The Payer and Payee are clients to their respective PSPs which are servers that provide the service. When the Payee has a payment request to make to the Payer, it sets up a two way connection with its payment service provider. The responsibility of the client is to place the payment request and await the progress of the payment process until it receives a notification of status. The status could be a confirmation or a notification indicating the reason for the failure of the process.

The Payee PSP server, upon receiving the payment request from its client, forwards it to the Payer PSP server for onward processing on a two way connection. The Payee PSP server either initiates this two way connection or uses a pre-existing connection between them. The Payee PSP server is responsible to ensure that the Payee's request is forwarded to the Payer PSP and convey the notifications it receives from the Payer PSP, to the Payee client.

In a similar manner, the Payer PSP server interacts with the Payer client to process the payment by obtaining its authorisation and confirmation over a two way connection.

The client and servers interact by way of command and response mechanism. The client sends a command to the server and the server returns a response to the command. The response indicates the status of the execution of the command. The response may indicate that the command was accepted, that additional commands are expected, or that a temporary or permanent error condition exists.

The command sequence is fixed and therefore operates sequentially. Each command is sent along with associated data. The responses, in addition to the status of the command may include associated data, depending upon the context.

The entire payment process is executed in a lock-step manner with one command at a time. Once the set of commands are executed, the connection between the client and server is shut down. One payment is made in a single connection and no more.

In addition to the client to server communication, there is communication between the servers. The communication between the servers is in two contexts – to forward a payment request from a payee to the payer PSP and to perform a transfer of value between the two PSPs. The first context is routine and merely a forwarding action, given that a payment request from the payee needs to be forwarded to the payer for authorisation and confirmation of

the payment. The second context for communication between the two servers is for a transfer of value between the PSPs. In both the contexts, it is the payee PSP server that opens a two way connection between itself and the payer PSP server. Once the payment process is finished, the connection between the servers is either shut down or retained to provide connectivity for other transactions to avoid the connection set up delay.

There are two primary characteristics of the model. They are – the entire payment process involves four entities and the process is completed in real time.

4.4.2 Design of the UMTES Model

The design decisions for the UMTES model are discussed in this section. The discussion will provide the basis for the choices made in the model.

4.4.2.1 The Payment Process

Recall that only a payment is intended to be initiated, authorised and confirmed in the transaction between the actors. In specific contexts (micro payments), a transfer of value has to be initiated as part of the transaction. The transfer of value is traditionally a part of the settlement process and decoupled from the payment process. However, the transfer of value (settlement) is included in case of low value payments to emulate a cash transaction where the transfer of value is instantaneous. The various actions/ processes leading up to the payment are out of scope.

4.4.2.2 The actors in the process

For making a payment, three of the actors require to interact. The payee provides the payment information to the payer, the payer reviews the information and instructs her/his PSP to make the payment and the PSP sends a notification to the payee indicating the status of the payment made. This happens in real time. Including the settlement for the micro payments requires the fourth actor – the Payee's PSP also to be a part of the process. This is a significant difference with respect to payments.

So, the payment process is a real time transaction that involves four actors.

4.4.2.3 Real time, end-to-end

Payments made electronically are real time payments The transfer of value is included for micro payments and this amounts to a settlement process. The entire process, that includes the payment and settlement in case of micro payments, is a real time process. The settlement therefore is part of the real time payment process. The real time transfer of value is intended to provide

an instantaneous availability of the transferred funds to the payee. Recall that the real time transfer of value for micro payments provides a sufficient condition to replace cash payments.

4.4.2.4 Transport connections between the actors

The connections between the actors refers to the service level connectivity between the actors. Each client (payee, payer) connects to their respective server using a secure transport connection. TCP is chosen for the transport connection over UDP to ensure that there is guaranteed packet delivery, given that the connection to the server has a wireless access segment. Transport Layer Security (TLS) is used over TCP for data privacy on the network. TLS provides the end points for privacy on the client and on the server. In addition to the use of TLS,UMTES provides independent privacy support for exchange of data with its application peer.

The transport connections between the client and the servers are established when needed. After the transaction is completed, these connections are compulsorily shut down. In contrast, the transport connection between the servers are set up on a one time basis and tend to be reused by several transactions. The lower level connectivity, typically at the network layer, would be established with secure end points on the network such as in an IPSEC based tunnel between the two networks hosting the servers.

4.4.2.5 Security components

The broad security objectives for the service are authentication and data privacy. Both these aspects are taken care of by the application and are part of the basic model. They are elaborated in the course of the UMTES description.

The primary concern for security is impacted by two factors – the mobile device and the data transfers. The mobile device is vulnerable to three factors – the access to the device, the loss of the device and the data transmitted over the air in the radio access network. The wired network and the servers have to be protected against other vulnerabilities. These factors are in addition to the vulnerabilities that the application may present when using the network service infrastructure (links, routers, server OS and other intermediate equipment).

The design of the UMTES model incorporates the use of TLS. TLS addresses the data privacy concerns on the network. TLS provides an end-to-end privacy mechanism between the mobile device and the server. In addition to this, the

application provides for end-to-end privacy with the use of the privacy mechanisms supported by UMTES.

Data privacy on the network (IP layer and below) is taken care of individually by the wireless access network (Radio Access Network) segment and the wired network infrastructure segment. These privacy mechanisms are in addition to those used by the transport layer and application.

There are two additional procedures that are enforced on the UMTES model from a security perspective. They are the following:

1. The clients (payer and payee) will only connect to and interact with their respective servers (service providers). This ensures that the clients are authenticated by their respective providers before the payment process begins.
2. The clients do not interact with each other directly but indirectly through their respective servers. Each message that is exchanged between them is authenticated by the respective servers.

By keeping the client and servers tightly coupled, the clients are identified and the interaction is monitored.

4.5 UMTES Terminology

There are several terms used in the context of detailing UMTES. These terms are formally defined in this section. The definition of the terms include the UMTES context that they are used in. Some of the definitions may be repetitive. Nevertheless, they are included for sake of completeness. Following the detail of the terminology, the operational details of UMTES is provided.

4.5.1 Addressing the Actors

There are four actors that interact in the context of UMTES. The actor who makes the payment is termed as the Payer. The actor who receives the payment is termed as the Payee. The Payee always interacts with the Payee PSP and the Payer always interacts with the Payer PSP. The Payee PSP and the Payer PSP interact to provide the exchange of messages between the Payee and the Payer.

In general, the Payer and Payee are users of the service. In order to use the service, they require to be registered as users with their respective PSPs.

4.5.2 Account

An account is the basic object that is assigned to a registered user of the service. This is termed as the User Account and used interchangeably with the term Account. Associated with this account is the information about the user, her/his identities in the scope of the service, information about the mobile devices that may be used for payment, authentication information, the preferences of the user with respect to her/his usage and the limits imposed on the user's extent of usage of the service (maximum value of withdrawal, number of withdrawals per day, etc.). Such information is termed as User Registration Information (URI). Each PSP will maintain such information for every registered user.

An account is also the source of funds associated with the user. Funds are either deposited into this account or withdrawn from it when a payment is made. UMTES provides the means for the deposit and withdrawal in the overall context of the payment. The movement of funds into and from the account is recorded as events and the non-committed value of the funds is readily available all the time. This is termed User Account Information (UAI).

The URI and UAI form the most important user information that is necessary for every transaction that the user initiates.

4.5.3 Identification of actors

The actors participating in the service require to have an identification within the context of the service. This is applicable to both the users as well as the PSPs. The scope of the implementation of the payment service could be global, thereby requiring a globally distinct identity for the users as well as the PSPs.

4.5.3.1 User Identity

In the online context, several services exploit the fact that email addresses of the users are globally unique. Every user has a unique identification (id) within the domain of the email service provider. The domain is identified by a fully qualified domain name (FQDN) which is globally unique. Thus a combination of the user-id and the service provider's domain name provides a globally unique id. UMTES retains this as the primary user identification for the service.

There have been other proposals for unique identification of users. The International Mobile Subscriber Identity is globally unique. The IMSI is a candidate for a globally unique identity in the mobile payment service. Note that the access to the service is via a mobile service provider. Using this as

the identification for the user has the advantage of the user having been authenticated by the mobile service provider. The subscriber identity on the mobile network is being used as a user identity for making person-to-person payments in a service which is expected to start in June 2014 (UKPC 2013). This service will enable secure payments to be made directly to or from an account without the need to disclose the sort code and account number, by simply using a mobile phone number as a proxy.

Like the IMSI, the IP address of the user is another potential means of identifying the user. The IPv6 address assigned to the user device can be a potential unique identity (Murugesan, R. K., & Ramadass, S. (2010)). Another proposal mentions the use of a personal IPv6 address and its use on a Customer Identity Module (CIM) card that will enable users to use their IPv6 address on any device they wish to use to access services Ganchev, I., & O'Droma, M. (2007).

In the context of UMTES, the IPv6 address could be used as an additional identity factor where applicable. This applicability is dependent upon the implementation of Mobile IPv6 support across the mobile service providers.

The primary user identity visible to the external world would be the user's email id. This identity may be mapped internally, within the scope of the PSP to other forms of identity which could include a specific numbering scheme that the implementation might want to adopt.

4.5.3.2 The PSP ID

PSPs require to have unique IDs since they participate in inter-PSP exchange of value. A user account is attached to a PSP and in order to route a transfer of value to a specific account, the PSP must first be identified and the transfer of value to its user, routed via that PSP. For purposes of this routing, each PSP requires to have a unique ID.

In the context of banks, the International Bank Account Number (IBAN) is used to uniquely identify a user account, globally. The IBAN, is hierarchical in structure (ISO 13616 2007). The first level segregation is country wise, followed by the identity of the bank, the branch and followed by the account number of the user in that branch. Therefore the destination bank routing is done using a part of the IBAN. Notice that the IBAN is inherently location based and does not suit the online ecosystem where location of the PSP is not specifically relevant.

Another unique identification system that can be considered is the payment card numbering system. The numbering conforms to ISO 7812 and defines a

numbering system for the identification of issuers of cards that require an issuer identification number (IIN) to operate in international, inter-industry and/or intra-industry interchange (ISO 7812 (2006)). The card numbering system consists of a seven digit IIN to identify the card issuer. This numbering system is hierarchical like the IBAN but it is card issuer centric and not location centric like the IBAN. In this manner it is better suited for use with the mobile payment ecosystem. This could potentially be used as the PSP identifier.

So, the PSP ID could potentially be a IIN, if the industry decides to adopt the ISO 7812 to identify PSPs. This will most probably be the choice of the industry because the banking industry already adopts this approach for their debit cards. Newer PSPs also belong to the banking/finance category. They also provide user accounts that contain funds and could potentially issue cards. These cards could be physical or given the movement to mobile payments, it could be an electronic card in an electronic wallet. With this. the PSPs will have a unique ID for every customer as well as themselves. The user account part of the card number could internally be aliased to the actual user account details. With this, the user will have multiple identities which can be used depending upon the means she/he chooses to pay – online (via the web), using the email id or via her/his wallet using the e-card or from her/his mobile device using a service like UMTES.

UMTES chooses to use a ISO 7816 numbering scheme for globally identifying the PSP and the user account. For experimental purposes, the Major Industry Identifier (MII), the first digit of the ISO 7812 Issuer Identifier is chosen as 7. This is marked for assignment to the Petroleum industry and other future industry assignments. Choosing this ensures that there will be no clash with the numbers in circulation when the UMTES service is tested. The six digit IIN and the user account number and the single digit checksum will be allocated and utilised when the implementation of the UMTES service is discussed, later.

4.5.4 Making a payment

Making a payment implies indicating a source of funds for withdrawn from which a specific value is marked for transfer to the actor who receives the payment. In the case of a micro payment, the term ‘making a payment’ also includes a transfer of value from the payer’s account to the payee’s account on their respective providers.

One payment is permitted per connection from a mobile device. This limitation is set as a service characteristic to ensure that multiple payments are not possible within a single authorise-confirm phase. In addition to making the user doubly aware of the payments being made, such a limitation can help to mitigate malicious spoofing attacks.

4.5.5 Transaction

A payment transaction is a complete cycle of payment initiation, authorisation and confirmation. A payment transaction is deemed completed when the complete payment cycle is successfully executed and the payment made. In case of micro payments, the payment cycle includes the transfer of value between the sending and receiving parties.

The payment transaction requires information from the user registration information as well as the user account information when initiating the payment. The payment initiation is successful based on the user authentication being successful, the user preferences being appropriately applied and user account information returning the availability of funds as available. Beyond this. the other phases of the transaction – authorisation and confirmation require to be successful. In the context of micro payments, the transfer of value phase also has to be successful before the transaction is deemed as successfully completed.

The transaction is deemed aborted if either of the necessary phases are unsuccessful. Once aborted, the application requires to reset it connection and restart the process all over again.

4.5.6 Commands and Responses

The client and server interact using a command-response mechanism. The client sends the commands and the server sends an appropriate response to the command. A response is considered as an acknowledgement, either positive or negative.

Commands are verbs that initiate action on the server side. The commands contain two parts the verb and the associated data sent from the client to the server. The data can contain multiple sets of data and is always encrypted before being sent as part of the application protocol data unit.

Responses contain two parts, a status code and associated data, if any. The data is encrypted as in the case of the command.

The status code indicates the status of the command response. The status could be either of success or failure. In the event of a failure, the reason of the

failure is encoded in the status code. In the context of a failure, the status code is referred to as an error code. The two terms are used interchangeably although one is a specific instance of the other.

4.5.7 Message

Message is a term used to denote a combination of a command and its associated data. The same term is used to denote a response and its associated data. The message structure, format and information are discussed in a later section.

The term Message is used in order to be consistent with the terminology used in the Finance industry in the context of payments. This is the first point of alignment with the ISO 20022 standard for Financial Services Messaging.

4.5.8 Clients and Servers

The clients and servers are application programs that use TCP/IP to communicate with each other. These programs, therefore, will be able to interconnect and communicate on any Internet enabled infrastructure. As mentioned earlier, the clients will reside on the mobile device and communicate with a server which is accessible via the Internet and typically housed in a provider’s data centre.

4.6 Design objectives for the payment protocol

The payment protocol is intended to provide a simple, speedy and secure payment service that is accessible from mobile devices. Typically, the payment protocol operates across a 4G network which has relatively high uplink and downlink bandwidth when compared to a 3G network. Each of the three design objectives are elaborated below:

4.6.1 Simple

1. The protocol should be a simple, linearly operating protocol without a complicated state transition. Any non-compliant protocol action such as an out-of-sequence command or a time out should abort the ongoing transaction and force a restart.
2. The protocol data units (PDU) should be concise enough so that the amount of data transfers for the service must be minimal. Consequently, the amount of PDU processing should be minimal permitting a sufficient delay budget for security processing which is an important requirement.

3. The protocol should be sufficiently specific to avoid any ambiguous error conditions.
4. The protocol verbs should be distinct and explicit with respect to the actions they represent.
5. The UI for the application that provides access to the service should be simple and easy to use. Therefore, the impact of the protocol if any, on the UI must be minimal.

4.6.2 Speedy

1. The protocol processing on the mobile device should be designed to avoid any input-output (I/O) operations on local storage to ensure that operational delays are minimised. All operations should be memory bound within the running environment of the application on the mobile device.
2. The size of the application PDU (APDU) should be such that the total size of the transmitted frame at the link layer should be aligned with the size of the maximum transmission unit (MTU) of the device. On LTE and 3G networks, the typical MTU size is set at 1428/1492/1500/1502 bytes, depending on the network provider. Therefore, the APDU plus all the headers should be less than 1428 bytes.
3. The security elements should be chosen such that the time taken for security processing should be low to ensure that the overall processing at the mobile device does not delay the transaction itself. This is specifically important since every APDU is encrypted before being handed over to the layers below, for transportation. In addition, the transport layer deploys security mechanism and the choice of the algorithm and therefore the processing requirement, is limited by the standards and interoperability

4.6.3 Secure

1. The security elements of the service should primarily be managed by a Trusted Service Manager (TSM). However, these management aspects are meant for the coded implementation and realisation of the payment services using the protocol that will be designed. The security elements include the application program executable (which is the software asset of the service provider) and the services required to generate, distribute and maintain the application program executable

   a. a signed application executable that is custom generated for each user with the user identity and information encoded and embedded within the application executable.
   b. Over-the-air (OTA) updates for the application executable and/or validation
   c. Dynamic code loading during run time of the program executable must be avoided (Poeplau et al 2014)
2. The security aspects of the protocol are mentioned below. These aspects go into the protocol function design as well as the protocol processing at the service end points – the mobile device and the PSP.
3. The authentication of the user and the user device is managed at the PSP side. The protocol functions enable the user authentication, the device authentication as well as the authentication of the software asset, referring to the user's registration information and other details stored by the PSP.
4. The location of the user as well as the location of the PoS should be used effectively for purposes of validation of the payer and payee.
5. To enable (i) above, the protocol should have a distinct registration phase and a transaction phase. The protocol should include both phases in a "session". Functionally, a session could have a single registration phase followed by multiple transaction phases.
6. The registration phase should be followed by periodically acknowledging the PSP side that the registration is valid and transactions can occur.
7. Every APDU exchanged must have a time stamp from the originating side. This ensures that the data is recent and can mitigate any replay attacks.
8. In order to reduce the processing required for encryption and authentication of the application PDUs, symmetric encryption should be deployed to the extent possible, without compromising the resistance to security attacks such as man-in-the-middle (MITM) and denial-of-service (DoS) attacks
9. Key management for secure data transfers must be implemented as part of the protocol while ensuring that the key management data exchanges do not load or extend the basic functional protocol. To the extent possible, the key management data should piggy-back on the application data as part of the application packet.
10. The application protocol uses a secure transport layer for secure data transfers as well as authentication of the transport end points.

Therefore, the extent of security implemented at the application layer must complement the security at the transport layer.

In summary, the APDUs must be short and contain enough information necessary for the exchange of information for payment. Each of the APDUs should be encrypted with a key shared between the mobile user and the PSP. The APDU should be signed and the signature appended to the APDU before handing over to the transport layer.

The protocol design is based on these design objectives. With these objectives, the protocol is expected to be comprehensive and concise to provide the specific function of an interoperable payment service.

4.7 Conclusion

In this chapter, the service architecture for the MP service was illustrated and its components defined. A three layer model was derived and the service components of each layer were illustrated. The three layer model is proposed as a generic model for mobile payment services.

The MP service definition was evolved in three parts. The core service detailed the individual functions that form the service as well as the basic features. The security support for the service is detailed mentioning the security support in the application and between the end points. The application for the payment service is distributed and managed by the trusted service manager, on behalf of the payment service provider.

Finally, the design objectives for the protocol were discussed. The three broad objectives, namely, Simple, Speedy and Secure were elaborated. The details illustrate the approach taken towards the functional and structural design of the protocol.

Chapter 5
Implementation of the Unified Mobile Transaction Exchange Service (UMTES)

5.1 The UMTES Protocol

UMTES participants, that is the payer, the payee and their respective PSPs, communicate using the UMTES protocol to provide the payment service. The UMTES protocol functions from the application layer and communicates with its peer layer entity on the server. It uses SSL for privacy of its communications. The layered stack on the server and clients side is shown in the Figure 25.

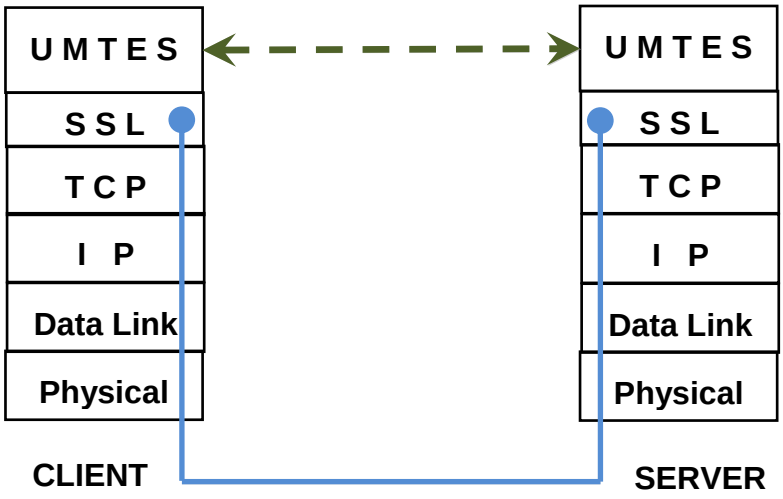


Figure 25: UMTES Protocol Stack on the Client and the Server

The protocol stacks on the client and server are similar. When the two entities communicate, and end-to-end SSL connection is set up between them. Notice that the SSL works from above the TCP layer. It first establishes a secure session with the server and passes on the encrypted data to the TCP layer for onward transmission. UMTES uses this secure connection to the server to send its data. This is indicated by the dashed arrow between the UMTES peer layers. Recall that the application sits above the UMTES layer.

5.1.1 Objectives of the UMTES Protocol

The overall objectives of the protocol are divided into three – the functional objectives, the operational objectives and implementation objectives.

Functionally, the UMTES protocol is expected to facilitate a user to make a payment using a smart phone. The payment is made using the services of a PSP with whom the user is registered. Payments can be made to recipients who are registered with the same PSP as the user or with another PSP. The protocol should ensure that the communication should be secure. Towards this two specific functions are necessary – the identities of the payer and the payee must be established before a payee requests for a payment and all data exchanged should be private. The protocol should utilise as many standardised components as possible to achieve its functional objectives so that its implementations could be deployed on a wide variety of interoperable platforms. Towards this, UMTES will use the standard TCP/IP suite of communication protocols and Secure Sockets Layer (SSL).
Operationally, UMTES aims to provide secure communication between the client and the server so that all the payment related information exchanged between them is private. The protocol aims to minimise processing delays since the entire payment process has to happen in real time. The processing delays are referred to in the context of the number of protocol exchanges to complete a payment, the authentication procedure and privacy mechanisms utilised for secure data transfer. In addition to this, the operational costs have to be minimised. Operational costs refer to the costs incurred for mobile access to the payment service as well as the costs incurred to provide the infrastructure support for the service. Towards this, it is assumed that the access to the payment service via a mobile network will be a standard access and that the mobile network provider will not accede any additional privilege either to the customer or to the traffic to access the payment services. Providing any such additional privilege will imply additional costs and will add to the overall costs. Similarly, it is assumed that the server hosting and operations are performed on a shared infrastructure in a location that is approved by the relation and oversight authorities of the financial industry.

UMTES has implementation related objectives. The implementation will require to integrate as seamlessly as possible into existing applications. The implementation will require to be in multiple forms – as a payment plug-in for browsers, as an applications programming interface (API) to develop applications that will potentially use UMTES for payments. The API should be supported with functional components of the UMTES protocol available as

shared libraries or class libraries. With such an API available, the payment capability can be integrated into various applications. UMTES could function as a common underlying payment protocol for various types of applications, browser-based, applications requiring inline payment (such as in pay-for-use services like video streaming, etc.), as well as applications requiring a online payment. The implementation is discussed in the chapter on Implementation, following this chapter.

5.1.2 Payment Scenarios Supported by UMTES

UMTES is expected to facilitate a few scenarios, initially. The protocol should be extensible to facilitate any kind of payment scenario. The initial support is focussed on micro payments. Therefore, the following generic payment scenarios are considered:

Payment at a physical PoS location such as in a store or to an individual vendor like one in a farmers' market: The PoS in such cases will either be a desktop PoS or a mobile PoS (smart phone with a PoS application) that support UMTES. Upon identifying items for purchase, the payee addresses the user and makes a payment request. The payment request is made via the payee's PSP to the payer. The payer receives the payment request, authorises it and confirms the payment to her/his PSP. Upon this, the payer's PSP initiates a transfer of value to the payee PSP and notifies the payee upon successful completion. When the payee receives the notification, the goods are delivered to the payer.

Payment to a vending machine such as in a coffee machine or a ticket vending machine: Recall that in such devices, it is assumed that they are not online and hence cannot communicate independently. The user makes a choice of items to purchase, the vending machine makes a payment request to the payer and uses the payer's network access to send the payment request to its PSP for processing. Once the payment is processed, the notification is sent to the payer for passing it on to the vending machine which would then deliver the goods. The communication between the payer and payee would be by using contactless technologies like NFC or Bluetooth LE. Unlike in the earlier scenario, the vending machine need not support UMTES since it does not communicate directly with the PSP.

UMTES is easily extendable, by means of code implementation, to online remote payments where the payee is remote and accessible online. The operation remains the same. The difference is that the payee has the user information registered already (eg., online stores or services like video-on-

demand, ticket booking, etc.) and does not require the equivalent of a swipe to gather user information.

5.1.3 Operational Overview of UMTES

UMTES enables a payer to make a payment to a payee, using a mobile device. The payer and the payee use their respective PSPs to communicate the payment request and receive the notification of payment. Direct communication between them is not permitted. The application on the mobile device and the server use UMTES to communicate. UMTES works in a lock-step manner using a command response mode. The clients send commands and the server responds to them, indicating the status of their completion. Upon the completion of the payment process, the payee receives a notification of a successful payment. Figure 26 gives an operational overview of the protocol indicating the actors involved, the protocol interactions between the actors, the type of messages exchanged and the various phases of operation of UMTES. The five different phases are illustrated in separate colours.

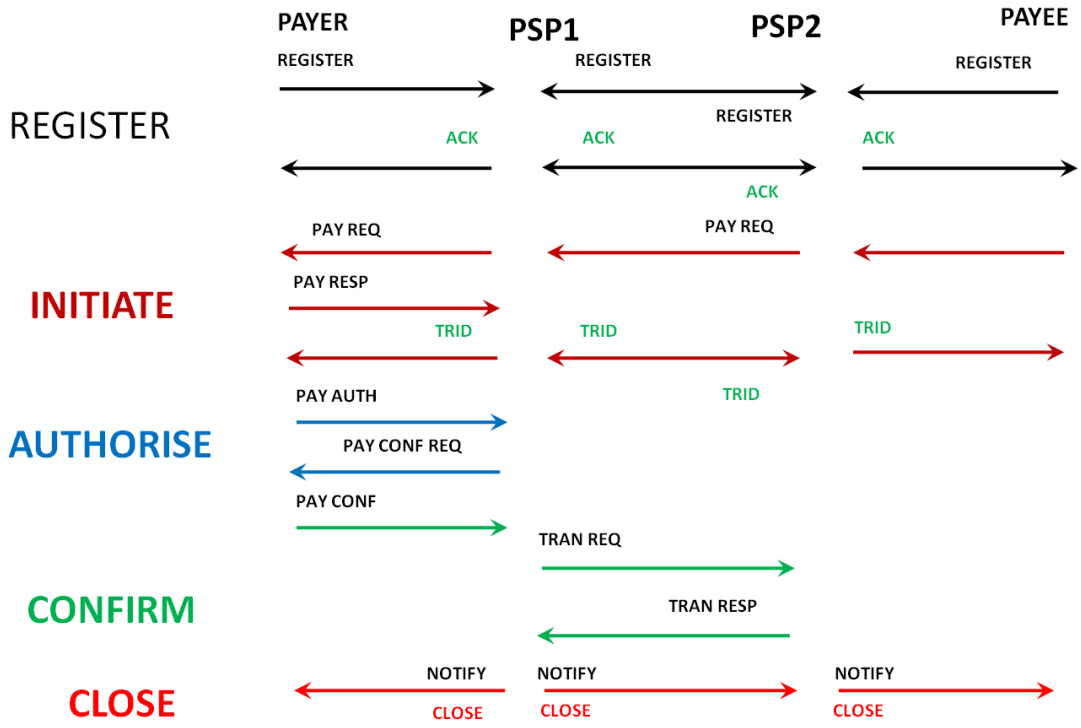


Figure 26: An overview of the UMTES protocol operation

The payment process is always initiated by the payee. The payee's PSP authenticates the payee and forwards the request to the payer's PSP. The payer's PSP validates the payee PSP's forwarding request and forwards the payment request to the payer. The payer then responds to the payment request by authorising and confirming the payment. The payer's PSP responds to the payee's PSP mentioning that the request is accepted and

under process. Upon the payer's confirmation, the payer's PSP initiates a transfer of value to the payee's account on the payee's PSP. When successful, the payer's PSP closes the transaction and notifies the status of the payment to the payee.

The payment transaction aborts with a failed status code upon a timeout of a response (for any reason) or if the data in the payload is erroneous or invalid. One payment per connection is permitted and multiple payments are not permitted in a single attempt. This follows from the fact that it is very unlikely that multiple payments are made at one time unless payment requests are batched. After every successful payment, a cooling period is imposed before another payment is initiated. This period is tentatively fixed at two minutes and is modelled after a user making purchases at a farmers market or at an indoor market in a town.

5.2 UMTES Protocol Description

This section details the description of the various protocol components of the UMTES protocol. An overview of the UMTES functional procedures is first mentioned and that is followed by the details of the UMTES commands, command sequences and the payment transaction.

5.2.1 UMTES Procedures – An Overview

The overall procedure consists of two parts, a user registration procedure followed by payment transactions. The registration is mandatory for all users intending to use the payment services of the PSP. Following the registration, a user could use the service to make payments.

5.2.1.1 User Registration

The user registration procedure is a one-time activity that is necessary for a user to be provided with the required software/application, the access to the service through the application and the authorisation to use the service. This procedure is done online, usually via a browser based interaction.

The user registration procedure collects several details of the user into a user registration database. Along with obvious details such as contact details and billing address, the registration process requires information about the mobile devices the user intends to use for payments. Typically, the IMEI and the IMSI of the devices intended to be used for payments is collected from the user and included as part of the user information in the registration database. Payment

transactions originating from mobile devices with these device identities will be permitted by the service.

The primary identity of the user in the context of the service is her/his email id. When the user starts the mobile payment application on her/his smart phone, this primary identity is used to identify the user of the service.

Upon gathering all the details of the user, the application meant for use by the specific user is generated using some elements of the user's registration. The application program for the specific user device is generated and distributed to the user by the TSM. Having received the application means for her/his exclusive use, the user is equipped to use the payment service provided by her/his PSP.

5.2.1.2 Payment Transactions

A user with the mobile payment application provided for her/his exclusive use is ready to initiate payment transactions. The payment transaction is initiated by the payee and has five distinct phases to it – Register, Initiate, Authorise, Confirm and Close. This is illustrated in Figure 26.

Once the application is started on the mobile device of the user, the application performs two basic functions. It first verifies whether it is executing in the intended environment and on the intended device. Next, it opens a secure transport connection with the PSP over which it opens an application session with the server. On this session, it contacts the payment service on the PSP and registers itself with the provider to indicate that it is online and ready for transactions. The details of this process are mentioned along with the description of the REGISTER command, later.

Once the application has registered its presence with the PSP, the other phases can occur. The payment initiation starts with the payee initiating the transaction with a payment request and the payer responding with the authorise and confirmation for the payment request.

The payment request originates from the payee, traverses the payee PSP, the payer PSP and reaches the payer. Once the payer responds to the payment request by validating the payment request to the payer PSP, the payer PSP notifies the payee PSP and in turn the payee that the payment is under process. From this point onwards, the interactions are between the payer and the payer PSP, until the payer confirms the payment. Once the payment is confirmed, the payer PSP performs a transfer of value to the payee PSP and upon a successful transfer, the payee PSP closes the transaction with a success notification to the payer, to the payee PSP and onward to the payee.

Closing the transaction implies that the application closes the session with the server.

Note that closing the application session does not imply that the application shuts down on the mobile device. It remains active and online. The secure transport connection set up during the initial pre-registration phase remains as is. Until this connection is open, the user and the device are marked as online and ready at the PSP.

In the course of the transaction, any kind of error leads to the transaction aborting and the application session closing down with appropriate notifications to the participants. A restart of the payment will require a new application session to be started.

5.2.2 UMTES Commands

Each phase in the UMTES protocol has a separate command and each command has a distinct response. Each of the commands are functionally described here.

REGISTER: Register initiates a mandatory pre-transaction step for the user to login to the payment service. The application starts up on the mobile device, and initiates a secure transport connection initiated with the PSP. The application begins a session with the server. The payer/payee register their online presence with their PSPs by logging in to the service. Once the user is registered, the user remains online until the application program on the mobile device is stopped.

INITIATE: The payee initiates a request for the payment from the payer. This request, addressed to the payer is sent to the payee's PSP. It contains the payee ID and the payment amount. Sending this request constitutes the beginning of the payment transaction.

AUTHORISE: The payer authorises the payment reiterating the payee ID, mode of payment and the payment amount. This amount is the value that requires to be transferred from the payer's account to the payee's account and referred to as the transfer value, here on.

CONFIRM: The payer confirms the payment to the PSP once the PSP verifies the payer funds availability

TRANSFER: Transfer follows a confirmation for the transfer of value by the payer. The payer PSP transfers the value to the payee PSP and obtains an acknowledgement for the value received in the payee's account

REFRESH: Refresh reiterates its online presence to the PSP. This is done periodically to ensure that the PSP knows the status of the application on the mobile device.

SWIPE: Swipe is an independent action where the id of either the payer or the payee is provided to the other (payer to payee or payee to payer). This depends upon the PoS type.

CANCEL: Originated by either the payer or the payee, and valid up until the payment confirmation is not made. This control is provided from the application as a button click. A cancel causes the transaction to abort and is functionally treated as an abort request from the payer or payee.

ABORT: An ABORT is automatically sent by the Payer's PSP in the event of timeouts and/or out-of-sequence/state requests

CLOSE: Originated by the Payer's PSP upon successful payment and transfer of funds to Payee

These commands are exchanged in a specific sequence which is illustrated in Figure 26. Further illustration of this sequence is provided when the payment scenarios are discussed later on in this chapter.

5.2.3 UMTES Command Responses

Each command sent by a client elicits a response from the corresponding server. The command responses are typically status codes that have a

Status Code (Range)	**Response Category**
1XX	Reserved (for substituting UMTES commands)
2XX	Acknowledgements (eg., 200 OK)
3XX	Authentication Errors (User, application, service authentication)
4XX	Validation Errors (Encryption, Signature Verification, Checksum)
5XX	Resource Errors (Funds, Currency, Network, Computing)
6XX	Response Time Outs
7XX to 9XX	Reserved for future use

Table 11: Categories of status codes in UMTES

standard interpretation. Along with the status codes, some responses may also have associated data that is necessary in the context of the transaction. Status codes are divided into categories. The categories map a status code to its interpretation. These codes are sent as responses to the commands. Since the protocol operation is lock-step, a response received is interpreted as a response to the most recent command sent. Table 11 provides an overview of the categories of status codes.

5.2.4 UMTES Command Response Information Exchange

The commands and responses in UMTES carry along some associated data. Such units of commands/responses and their associate data are referred to as UMTES messages. These details of the messages are discussed in this section. To enable illustrate the message content and its format in which messages are exchanged, a comprehensive notation is used. The notations are listed in the table.

Payer – P_r Payee – P_e Payer PSP – PSP_r Payee PSP – PSP_e Initial key - K_i Shared Encryption Keys between PSP_e and P_e – K_{se} PSP_r and P_r – K_{sr} PSP_e and PSP_r – K_{ser} Encryption Function – $E.K_{sj}(), j=\{e\|r\|er\}$; Eg: $E.K_{sr}(K_i)$ Payer Location – L_r Payee Location – L_e	Currency – C Amount Payable – A Payment Instrument – PI; $PI=\{CC\|DC\|OLB\|TRF\}$ CC=Credit Card, DC=Debit Card, OLB=Online Banking TRF=Transfer Payment Instrument Attributes PI_{attr} Payee Reference – P_{er} Payment Context – P_c $P_c = \{P_{er}, PI, PI_{attr}\}$ Transaction ID – $TRID$ Session IDs - SID_n , $n=\{e\|r\|er\|re\}$ Signature = S_{CMD}, CMD = protocol command verbs

Table 12: Notations used to illustrate the information exchange in UMTES

Note that each of the actors are identified using a role based subscript, “r” for payer side, “e” for payee side. “re” indicates the association of the payer with the payee and “er” indicates the association of the payee with the payer. Such notations indicate the direction of the interaction.

Using the notations in the table above, each of the messages will be detailed with concise definition and format. Along with this, the functional objective of the command/response is also specified. The commands are mentioned in the functional sequence of their occurrence in a typical transaction. A signature, S_{CMD} , is always appended at the end of the protocol message. The signature is not shown in the message format descriptions, explicitly.

A protocol message is sent from one peer to another. A message comprises of the command and the command arguments as well as a signature concatenated together for form the Application Protocol Data Unit (APDU). The APDUs for all protocol messages are listed in the following sub-sections.

5.2.4.1 REGISTER and ACK

REGISTER

Functional Objective: Authenticate the client (payer/payee), the mobile device from where the payment is being made and the payment app used to make the payment. Upon completing the authentication, the user is termed as online and ready at the PSP end.

Message Type: Command

Message Flow: From the payer/payee (Client) to the PSP (Server), from PSP_e to PSP_r and from PSP_r to PSP_e (the PSPs register with each other).

Message Format:

$REGI, E.K_i(Mobile\_Device\_ID, Password, Time\_Stamp)$

Message Content Description: The message content is encrypted using the initial symmetric key, Ki. It contains the mobile device ID, the IMEI, the user’s password for logging into the service and a time stamp of when the message was sent.

ACK

Functional Objective: Acknowledge to the register request when the user, device and app are authenticated and identified.

Message Type: Response

Message Flow: From the PSP (Server) to the payer/payee (Client), from PSP_e to PSP_r and from PSP_r to PSP_e.

Message Format:

$ACK, E.K_i(status\_code, SID_n, (Session\_rand, ttl))$

$n=\{e|r|er|re\}$

Message Content Description: The message content is encrypted using the initial symmetric key, Ki. It contains a status code that indicates the status of the registration. If the authentication has been successful, the message will contain a session identification for the device/user and a random number that is used to derive a shared key for the session. The session identification is used as an identification and not the original ID. This random number is associated with a time to live (ttl), after which the client will require to **REFRESH** its online presence.

5.2.4.2 REFRESH and ACK

Functional Objective: Continue the online status of the session with the PSP

Message Type: Command

Message Flow: From the payer/payee (Client) to the PSP (Server), from PSP_e to PSP_r and from PSP_r to PSP_e.

Message Format:

$REFR,(SIDn, E.K_{sj} (Time\_Stamp))$ where $n=\{e|r|er|re\}, j=\{e|r|er\}$

Message Content Description: The message contains the session id that is currently used by the sender and a current time stamp.

ACK

Functional Objective: Acknowledge the refresh request with a new random number and session identity.

Message Type: Response

Message Flow: From the PSP (Server) to the payer/payee (Client), from PSP_e to PSP_r and from PSP_r to PSP_e.

Message Format:

$ACK, E.K_{sj}(status\_code, SID_n, (Session\_rand_n, ttl_n))$ where $j=\{e|r|er\}, n=\{e|r|er|re\}$

Message Content Description: The message content is encrypted using the respective symmetric key. It contains a status code that indicates the status of the refresh. The status code is followed by a new session identification and a new random number for the session along with its associated ttl.

5.2.4.3 SWIPE

Functional Objective: Transfer the payer information to the payee PoS or payee information to the payer. The latter is done in the case where a PoS, such as an automated vending machine initiates its payment request through the user's mobile device.

This is the only command in UMTES that has no associated response.

Message Type: Command

Message Flow: From the payer to payee, called Direct mode indicated with a "D" in the message, or from the payee to the payer, called the Proxy mode indicated with a "P" in the message. These messages are exchanged between the payer and payee devices using either NFC or Bluetooth LE.

Message Format:

$SWIP, (D, SID_r , PSP_r , E.K_{sr}(L_r))$

$SWIP, (P, P_e, PSP_e , E.K_{se} (L_e , A , C, P_{er}))$

Message Content Description: There are two distinct SWIP messages based on the mode of operation – Direct mode or Proxy mode. Recall that in the proxy mode, the payee, typically an automated vending machine with less resources and no online network access, uses the payer's network access to send its payment request information. Therefore, the direct mode and proxy mode messages are not symmetrical in terms of message format.

SWIP includes the mode of use, the payer/payee ID, their PSP ID, the location encrypted. In proxy mode, the location, amount payable, the currency of the payable amount and the payment reference are encrypted and sent to the payer. Recall that the payment context includes the payee reference and the payment instrument.

5.2.4.4 INITIALISE (Payment Request) and ACK

Initialising a payment is a three step process. A payee initiates a payment request which reaches the payer, the payer acknowledges the request and validates it. The request is acknowledged to the payee to indicate acceptance and then the payer specifically confirms and authorises the payment, separately.

The initialise command comprises of two forms which are used in different contexts, the initialise request and the initialise transaction. Functionally, these two map on to a payment request and a payment response. The payment request is originated by the payee and the payment response by the payer, in response to the payment request. Note that the response is also a command .

INIT_REQ

Functional Objective: The initialise request is used to generate a payment request which signals the beginning of a payment transaction. With this command, the transaction is initialised and hence the name. The payment details, which include the location of the PoS, the amount payable, the currency and the payment context are encrypted and sent to the PSP. Depending on the mode of operation, the message parameters will vary.

Message Type: Command

Message Flow: In Direct mode, from the payee to payee's PSP, payee's PSP to payer's PSP and onward to the payer. In Proxy mode, from the payer to the payer's PSP and payer's PSP to the payee's PSP.

Message Format:

$INIT\_REQ, (D, SID_e , E.K_{se} (L_e , A , C , P_{er} , SID_r, PSP_r , E.K_{sr} (L_r)))$

$INIT\_REQ, (P, SID_r , E.K_{sr} (E.K_{se} (L_e , A , C , P_{er}), P_e , PSP_e)))$

Message Content Description: The message format indicates the mode of operation, first. In direct mode, the payee originates the payment request and is addressed to the payee PSP. The message contains the payee's ID followed by encrypted payment details – PoC location, the amount, currency and the payment reference. Also encrypted are the payer ID, the payer PSP ID and an encrypted location of the payer.

In the proxy mode, the payer forwards the payee's payment request to the payee PSP via the payer PSP. The message contains the payer ID, and an encrypted block containing the encrypted payment details received from the payee, the payee ID and the payee PSP ID.

INIT (Payment Response)

Functional Objective: This is a response to the payment request sent by the payee to the payer. This response conveys to the payer's PSP that the payer has confirmed that the payment request is valid and the details are correct. It

also implies a request to the payer PSP to start a payment transaction to process the payment to the payee.

The application on the payer's mobile device visually prompts for a confirmation of the payment details from the payer. The payer is expected to verify the details of the payment request from the payee and click to confirm the details. In case the user does not confirm the payment details on the payment request, the transaction is aborted with an appropriate reason given with a status code. The payment details in the request cannot be changed by the payer. However, the payment instrument can be chosen to be different than that configured in the payer's preferences. This choice has to be made manually and is included in the payment response.

Message Type: Response

Message Flow: From the payer to the payer's PSP

Message Format:

$\texttt{INIT, SID}_r\texttt{, E.K}_{sr}\texttt{(Status\_code)}$

Message Content Description: The message contains the session id to identify the payer and the status code, encrypted. The status code indicates an acceptance of payment request and format indicates the mode of operation, first. In direct mode, the payee originates the payment request and is addressed to the payee PSP. The message contains the payee's ID followed by encrypted payment details – PoC location, the amount, currency and the payment context. Also encrypted are the payer ID, the payer PSP ID and an encrypted location of the payer.

In the proxy mode, the payer forwards the payee's payment request to the payee PSP via the payer PSP. The message contains the payer ID, and an encrypted block containing the encrypted payment details received from the payee, the payee ID and the payee PSP ID.

ACK

Functional Objective: Acknowledgement to the payment response given by the payer to the payer PSP. This acknowledgement indicates that the payer PSP has accepted the payment response and is ready to initiate a transaction for a transfer of value on behalf of the payer. The acknowledgement will contain the Transaction ID which will be referred to in the further messages between the payer and the payer PSP.

A copy of this acknowledgement is also sent to the payee PSP to indicate that the payment request has been accepted and the transaction is underway.

Message Type: Response

Message Flow: From the payer PSP to the payer, payer PSP to payee PSP, payee PSP to payee

Message Format:

$ACK, E.K_{sr}(status\_code, TRID)$

$ACK, E.K_{sre}(status\_code, TRID)$

$ACK, E.K_{se}(status\_code, TRID)$

Message Content Description: The message contains a transaction ID issued by the payer PSP to the payer for use during the period of the current transaction, along with the status code. These are encrypted using the respective keys of the source and destination of the message.

5.2.4.5 AUTHORISE and ACK

Functional Objective: Authorise is a command initiated by the payer in response to the INIT acknowledgement containing the transaction ID. This command authorises the payer PSP to make a payment using the payment instrument indicated by the payer.

Message Type: Command

Message Flow: From the payer to the payer PSP

Message Format:

$AUTH, E.K_{sr}(TRID, A, P_c)$

Where $P_c = \{ P_{er}, PI, PI_{attr}\}$ and $PI = \{CC|DC|OLB|TRF\}$

Message Content Description: The message contains the transaction ID issued by the payer PSP to denote the current transaction, the amount and the payment context. Recall that the payment context contains the payment reference issued by the payee in the payment request , the choice of the payment instrument (or mode) that the payer wishes to use for the current payment and the associated details (includes card details for card payments). The choices are between the use of a credit card, a debit card, online banking or a transfer from the payer's account on the PSP. The content is encrypted using the symmetric key between the payer and the payer PSP.

ACK

Functional Objective: Acknowledgement to the payment authorisation is sent by the payer PSP. Upon receipt of the payment authorisation, the payer PSP verifies the payment context, the amount for the TRID specified and other

transaction limits specified for the payer as well as the preferences. With these verifications done, the payer PSP sends an acknowledgement to the payer to proceed with the transaction. The acknowledgment functionally implies a payment confirmation request and awaits a payment confirmation from the payer.

Message Type: Response

Message Flow: From the payer PSP to the payer

Message Format:

$ACK, E.K_{sr}(status\_code, TRID)$

Message Content Description: The message contains a transaction ID and the status code. These are encrypted using the symmetric key shared between the payer PSP and the payer.

5.2.4.6 CONFIRM

Functional Objective: Confirm is a command initiated by the payer in response to the AUTH acknowledgement. The AUTH acknowledgement is implied as a payment confirmation request. This request conveys to the user that the PSP has validated the payment authorisation made by the payer and that the attributes of the authorisation request do not violate the scope of the payer privileges provided by the PSP. The confirmation is made by reiterating the transaction ID and the amount.

The confirm command has no specific acknowledgement. Confirm triggers the transfer command between the PSPs. Therefore, the response to this command is the result of the transfer command which can either be a close command or an abort.

Message Type: Command

Message Flow: From the payer to the payer PSP

Message Format:

$CONF, E.K_{sr}(TRID, A)$

Message Content Description: The message contains the transaction ID and the amount payable. The content is encrypted using the symmetric key shared between the payer and the payer PSP.

5.2.4.7 TRANSFER and ACK

Functional Objective: Transfer is a command initiated by the payer PSP in response to a payment confirmation from the payer using CONF. The transfer

command sends the details of the payment amount the beneficiary and the details of the payment instrument depending upon the mode chosen. Transfer is intended to achieve the actual commitment of funds to the payee in case of a card based transfer and a transfer of value if the direct transfer option is chosen. Recall that the direct transfer option is required to transfer funds from the payer's account on the payer's PSP to the payee's account on the payee's PSP.

In case of a direct transfer from the payer's account on the PSP to the payee's account on his PSP, the session id of the payee and the amount is sent. The payee PSP takes the details, credits the amount into the payee's account and reports the status via an acknowledgement to the payer PSP.

In case of a card payment, the payer's card details are sent to the payee PSP for processing the payment with the card provider. The payee PSP is expected to perform the backend processing for card based payments since it represents the payee. The payee PSP initiates the access to the card issuer's gateway and provides the user card details to effect the payment.

Message Type: Command

Message Flow: From the payer PSP to the payee PSP

Message Format:

$\mathtt{TRAN,\ SID}_{re}\ \mathtt{,\ E.K}_{sre}\mathtt{(TRID,\ SID}_{e}\mathtt{,\ A,\ P}_{c}\mathtt{)}$

Message Content Description: The message contains the session ID identifying the session between the payer PSP and payee PSP. The transaction ID, the session ID of the payee as the payee's identification, the payee reference, the amount payable and the payment context.

ACK

Functional Objective: Acknowledgement to the transfer request made by the payer PSP is returned by the payee PSP. This acknowledgment ascertains that the actors responsible for committing the payment at the appropriate sources have indicated a successful commitment to the payee PSP. The payee PSP returns the status of the transfer via the acknowledgement.

Note that the payee PSP uses a separate logical channel for communicating with the payer PSP. It does not use the same logical channel that the payer PSP uses to communicate with it.

Message Type: Response

Message Flow: From the payee PSP to the payer PSP

Message Format:

$ACK, SID_{er}, E.K_{ser}(status\_code, TRID)$

Message Content Description: The message contains the session ID between the payee PSP and the payer PSP. The status of the transaction and the transaction ID are encrypted with the symmetric key shared between the payee PSP and the payer PSP.

5.2.4.8 CLOSE

Functional Objective: Close is a command initiated by the payer PSP to signal the end of a successful transaction. This command is unilateral and interpreted as a command or a response by each of the parties. The payer interprets the close command as a response to the payment confirmation and expects the status of the transaction. The payee PSP interprets it as a unilateral command to close the transaction, gracefully and the payee interprets it as a response to its payment request indicating a successful payment.

Following the receipt of a close command the payer and payee shut down their connections with their respective PSPs. They are provided with new random numbers to generate their keys for the subsequent session. The logical connections between the PSPs are typically shut down but their end-to-end connectivity remains.

The close command varies slightly in terms of the message content depending upon the mode in which the session was started. In the proxy mode, the payee identity is included in the message content and the content is flagged as proxy mode. Functionally, this serves to get the payment app on the payer's smart phone to transfer the payment information to the vending machine.

Message Type: Command

Message Flow: From the payer PSP to the payer, payer PSP to the payee PSP and from the payee PSP to the payee.

Message Format:

$CLOS, SID_n , E.K_{sn}(TRID, A, session\_rand_n)$

$CLOS, SID_m , E.K_{sm}(P, TRID, A, session\_rand_m , P_e)$

$n = \{ r|re|e \}, m = \{ r|re \}$

Message Content Description: The message contains the session ID identifying the session between the end points and the transaction ID, the

amount transferred and a random number that is issued by the PSPs to the payer and the payee.

5.2.4.9 CANCEL

Functional Objective: Cancel is a command that is originated by the payer with the intention of stopping the payment. This command is effective up until the payment confirmation is sent by the user. Once the payment is confirmed, the transaction cannot be cancelled.

Message Type: Command

Message Flow: From the payer to the payer PSP

Message Format:

$CANC, SID_r , E.K_{sr}(SID_e, A)$

Message Content Description: The message contains the session ID identifying the session between the payer and payer PSP. The session ID of the payee that identifies the payee and the payment amount are encrypted along with the symmetric key shared between the payer and the payer PSP. The cancel command, in turn, evokes an abort command from the payer PSP.

5.2.4.10 ABORT

Functional Objective: Abort is a command functionally similar to close and initiated by the payer PSP. Abort causes the transaction to stop and send an appropriate status command to all the parties.

Message Type: Command

Message Flow: From the payer to the payer PSP, payer PSP to payee PSP and payee PSP to payee

Message Format:

$ABOR, SID_n , E.K_{sn}(TRID, session\_rand_n)$

$n = \{ r|re|e \}$

Message Content Description: The message contains the session ID identifying the session between the end points and the transaction ID and a random number that is issued by the PSPs to the payer and the payee.

5.3 Payment Scenarios using UMTES

Two specific payment scenarios are described here to illustrate the use of UMTES and the typical exchange of information along with the commands and

responses. The first scenario illustrates a payment at a PoS and the second scenario illustrates a payment at a vending machine.

The payer and payee are registered users on their respective PSPs. Their registration information includes their respective card information. They have set their preferences to use their primary source of funds as the account on their PSP.

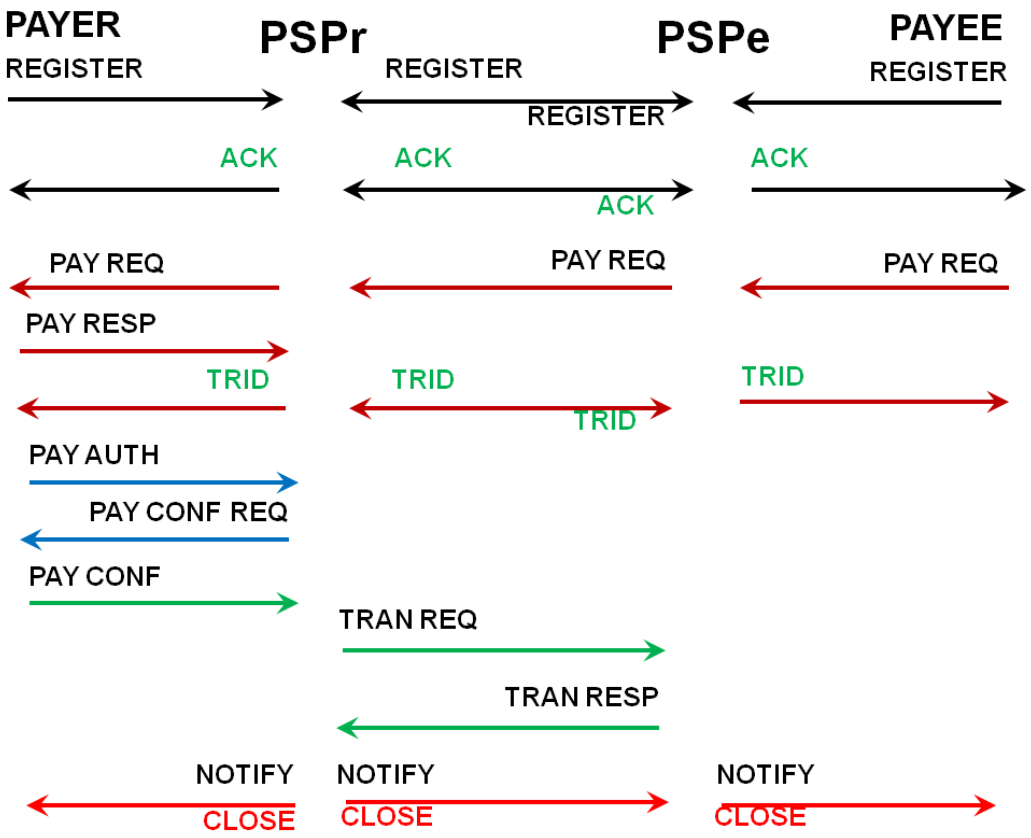


Figure 27: Functional interaction of UMTES in Direct mode

The transfer of value in both the scenarios will be from the payer's account on the payer PSP to the payee's account on the payee PSP. The transferred value will reflect as available funds to the payee, upon transfer.

The functional progression of the UMTES protocol is illustrated in the two scenarios detailed in the following sections. They illustrate typical detail in the information exchange in the protocol. Both the scenarios indicate a successful payment transaction.

5.3.1 Payment at a Point of Sale (PoS) Terminal at a Store

The payer makes a purchase at a store and intends to pay at the physical check-out counter which is manned by a sales person and a PoS terminal. This terminal supports UMTES and is NFC enabled.

The payer intends to make the payment using his smart phone. The smart phone has a payment application loaded and started up. The application supports UMTES.

Protocol Variable	Value
P_r	GB22PSP160161331926819
P_e	GB83PSP291862913316106
SID_r	7030210281782
SID_e	2871820120307
SID_{re}	181603543301
SID_{er}	103345306181
PSP_r	GB22PSP16016
PSP_e	GB83PSP29186
L_e, L_r	9.80dN71.56dW
A	32.59
TRID	7030213110
P_{er}	GR31332465

Table 13: Indicative message parameters

The information required for protocol message exchange such as identification of the PSPs, payer and the payee, the location information and the operational parameters of the protocol such as the session IDs, the transaction ID, the payee reference, the payable amount, etc. are listed in the table 13. They are indicative in the context of the function of the protocol. The initial shared key, K_i, is available with the application and used only with the register command.

In order to use the service, both the payer and the PoS register with their respective PSPs. The registration process of the payer is indicated in a table (ref. Table 14) showing the message exchanges between the payer and the PSP. For illustrative purposes, the protocol function is listed along with the

relevant message template. Alongside, the message, populated with the indicative parameters, is illustrated.

The values in the illustration correspond to the variables in the message templates for the register and the acknowledgement to the register message. The payer receives the session random number and uses it to generate a key for the following session.

Protocol action and message template used	Message with indicative parameters
PAYER registers with the PSP REGI, $E.K_i$(Mobile_Device_ID, Password, Time_Stamp)	$E.K_i$(355136053681782, WhyYung%8, 15:33)
PSP_r responds with an acknowledgement ACK, $E.K_i$(status_code, SID_r, (Session_rand, ttl))	E.Ki(200,7030210281782, (513832129, 1800))

Table 14: The information exchange for the registration process in UMTES

The PoS terminal will have a similar registration process. With the registration done, both the payer and the payee are ready to transact.

The payer has made a purchase amounting to, say £ 32.59, and intends to make this payment. The functional sequence of the protocol is indicated in the following table. Like earlier, the template and the values are shown separately, for clarity.

Protocol action and Message Template used	Message with indicative parameters
Payment Initiation PAYER swipes his ID onto the PoS **SWIP,** (D, SID_r , PSP_r , $E.K_{sr}$(L_r))	(D, 7030210281782, GB22PSP16016, E.Ksr (9.80dN71.56dW))

Payment Initiation PAYEE uses the payer ID and originates a payment request to PSPe **INIT_REQ**, (D, SID_e , $E.K_{se}$ (L_e , A , C , P_{er} , SID_r, PSP_r , $E.K_{sr}$ (L_r)))	(D, 2871820120307, $E.K_{se}$ (9.80dN71.56dW, 32.59, GBP, GR31332465, 7030210281782, GB22PSP16016, $E.K_{sr}$ (9.80dN71.56dW)))
Payment Initiation PSPe validates the source of the request as Pe and forwards the request to PSPr, which in turn forwards the request to Pr **INIT_REQ**, (D, SID_{er} , $E.K_{ser}$ (L_e , A , C , P_{er} , SID_e, PSP_e , $E.K_{sr}$ (L_r))) **INIT_REQ**, (D, SID_r , $E.K_{sr}$ (L_e , A , C , P_{er} , SID_e, PSP_e , $E.K_{sr}$ (L_r)))	From PSP_e to PSP_r (D, 103345306181, $E.K_{ser}$ (9.80dN71.56dW, 32.59, GBP, GR31332465, 7030210281782, GB22PSP16016, $E.K_{sr}$ (9.80dN71.56dW))) From PSP_r to P_r D, 7030210281782, $E.K_{sr}$ (9.80dN71.56dW, 32.59, GBP, GR31332465, 2871820120307, GB83PSP29186, $E.K_{sr}$ (9.80dN71.56dW))
Payment Initiation PAYER receives the request on his smart phone and responds, confirming the details in the payment request INIT, SID_r, $E.K_{sr}$(Status_code)	7030210281782, $E.K_{sr}$(200)

Payment Initiation PSPr receives the response and initialises a transaction and conveys the transaction ID to all the parties ACK, $E.K_{sr}$(status_code, TRID) ACK, $E.K_{sre}$(status_code, TRID) ACK, $E.K_{se}$(status_code, TRID)	$E.K_{sr}$(200, 7030213110) $E.K_{sre}$(200, 7030213110) $E.K_{se}$(200, 7030213110)
Payment Authorisation PAYER sends an authorisation to PSPr AUTH, $E.K_{sr}$(TRID, A, P_c) Where P_c = { P_{er}, PI, PI_{attr}} and PI = {CC|DC|OLB|TRF}	$E.K_{sr}$(7030210281782, 32.59, (GR31332465, TRF, NONE))
Payment Authorisation PSPr verifies the payer privileges and preferences and requests a confirmation ACK, $E.K_{sr}$(status_code, TRID)	$E.K_{sr}$(200, 7030213110)
Payment Confirmation PAYER sends a payment confirmation CONF, $E.K_{sr}$(TRID, A)	$E.K_{sr}$(7030213110, 32.59)
Payment Confirmation PSPr receives the confirmation and initiates a transfer of value to PSPe TRAN, SID_{re} , $E.K_{sre}$(TRID, SID_e, A, P_c)	181603543301 $E.K_{sre}$ (7030213110, 2871820120307, 32.59, (GR31332465, TRF, NONE))

Payment Confirmation PSPe receives the transfer request, performs the backend processing and returns an acknowledgement ACK, SID_{er}, $E.K_{ser}$(status_code, TRID)	103345306181, $E.K_{ser}$ (200, 7030213110)
Payment Close PSPr receives the acknowledgement and terminates the transaction and sends a close message each to the payer, to PSPe and the payee CLOS, SID_n , $E.K_{sn}$(TRID, A, $session\_rand_n$)	2871820120307, E.Ksr (7030213110, 9183224561) 181603543301, E.Ksre (7030213110, 6138765199) 2871820120307, E.Kse (7030213110, 32.59, 3139014367)

Table 15: The information exchange for a payment transaction

5.3.2 Payment at a Point of Sale (PoS) on a vending machine

The interaction with a vending machine is quite similar. The only difference is at the payment initiation phase and at the end of the transaction. Recall that

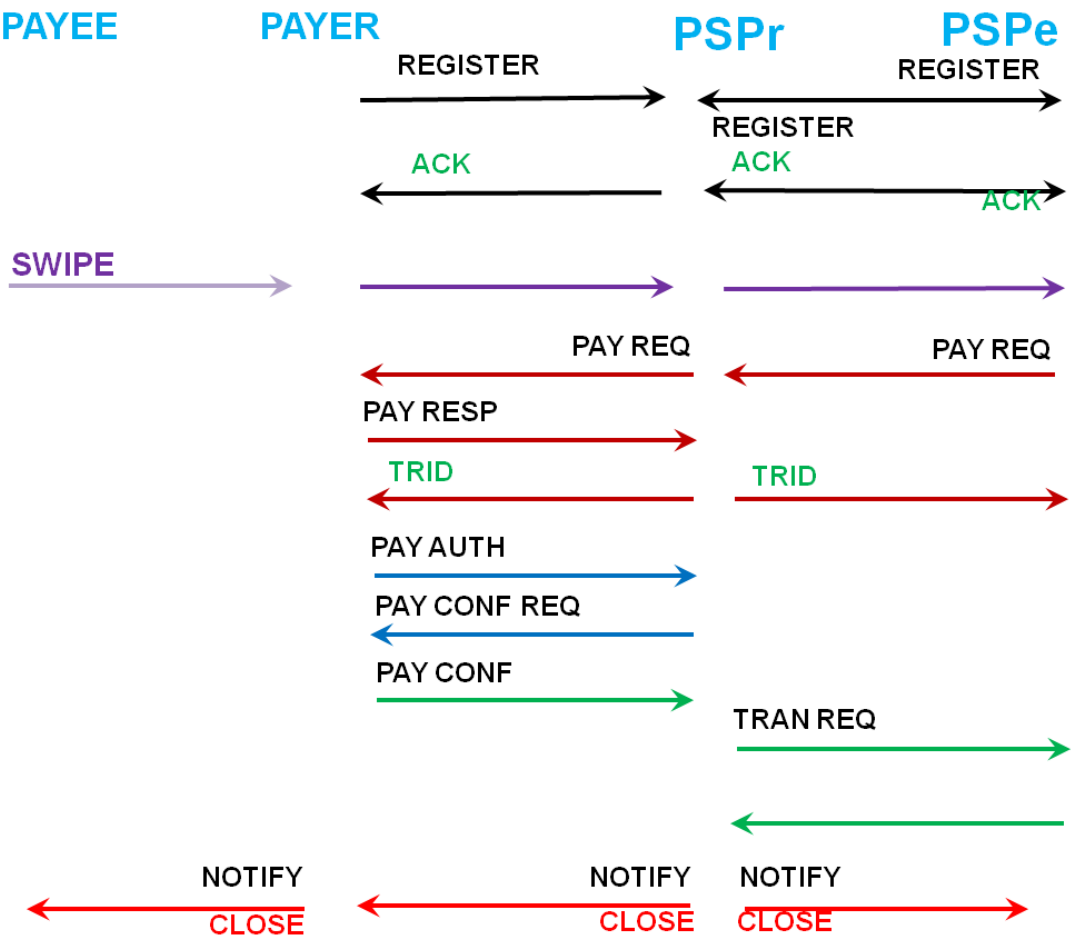


Figure 28: Functional interaction of UMTES in Proxy mode

the vending machine uses the payer's network connectivity in order to initiate the payment. This is termed as the proxy mode of payment initiation.

The payer interacts with the vending machine. This interaction typically consists of choosing the items or services and requiring to pay. At this point, the payer intends to make a payment. The process starts with the payer swiping the payment information off the vending machine.

Table 16 shows the steps that are different from the payment process for payments at a PoS.

Protocol action and Message Template used	**Message with indicative parameters**
Payment Initiation Collect information about the amount payable SWIP, (P, P_e, PSP_e ,	P, GB83PSP291862913316106, GB83PSP29186, $E.K_{se}$ (9.80dN71.56dW, 32.59, GBP, (GR31332465, TRF, NONE))

$E.K_{se}$ (L_e , A , C, P_c))	
INIT_REQ, (P, SID_r , $E.K_{sr}$ ($E.K_{se}$ (L_e , A , C , P_{er} , P_e) PSP_e)))	P, 7030210281782, $E.K_{sr}$ ($E.K_{se}$ (9.80dN71.56dW, 32.59, GBP, (GR31332465, GB83PSP291862913316106)), GB83PSP29186
INIT_REQ, (P, SID_{re} , $E.K_{sre}$ ($E.K_{se}$ (L_e , A , C , P_{er} , P_e) PSP_e)))	P, 181603543301, $E.K_{sr}$ ($E.K_{se}$ (9.80dN71.56dW, 32.59, GBP, (GR31332465, GB83PSP291862913316106)), GB83PSP29186
INIT_REQ, (P, SID_r , $E.K_{sr}$ (L_e , A , C , P_{er} , P_e, PSP_e))	P, 7030210281782, $E.K_{sr}$ (9.80dN71.56dW, 32.59, GBP, GR31332465, GB83PSP291862913316106, GB83PSP29186)
CLOS, P, SID_r , $E.K_{sr}$ (TRID, A, $session\_rand_r$, P_e)	P, 7030210281782, E.Ksr (7030213110, A, 87093342, GB83PSP291862913316106)

Table 16: The information exchange for the initialisation and close in proxy mode

5.4 Extended Payment Scenarios using UMTES

UMTES can be used for other payment scenarios such as topping up the user account on the PSP and P2P payments. In both cases, the payment request originates from the user application on the smart phone and is fulfilled by UMTES.

5.4.1 Topping up the user account on the PSP

A user will require to top up his account on the PSP with funds from another source of funds held by the user such as a bank account. This will enable the user to transfer his funds from one of his sources to his account on the PSP. These sources of funds should be registered by the user and available with the PSP in the registration database. The account particulars will be required by the PSP to operate the funds on behalf of the user.

When a user requires to top up the funds in the PSP account, a payment request is made using the option provided in the application. The payer and

the payee are indicated as the user. In effect, the user pays himself the sum of money that requires to be transferred to his account with the PSP.

The payment context indicates the details of the source of the funds. The source of funds can be indicated either in the preferences or chosen interactively in the application.

5.4.2 Person to Person (P2P) payments

P2P payments can be made exactly in the same manner as with other payments. However, the person who expects to receive the payment must initiate a payment request. A P2P payment cannot be directly initiated by a user intending to pay. This is an operational limitation of the protocol. The limitation is due to the fact that the details of the person that will receive the payment are necessary to originate the payment. There is no resource that can provide a mapping of the payee's name or reference to the payment details of the receiver.

However, such payments can be originated by the payer if the payee details are known by the payer, apriori. These details are entered by the payer into the application and the payment can be initiated. Such payments, like in the case of an account top-up, are initiated with the payer.

5.5 Evaluation

The evaluation of the implementation is discussed in the next chapter. The evaluation is done by estimating the total transaction time, using a typical scenario of paying at a PoS. The PoS is modelled as a smart phone with a PoS application. Therefore, both end devices are smart phones.

The evaluation is intended to estimate the real time performance of the protocol on a network. The network delays and the processing on the smart phone can impact the overall transaction delay, substantially. These are initially estimated using performance results available in literature and then followed by measuring the transaction delays on a simulated network infrastructure. On the simulated network, the performance under load is also measured.

Chapter 6
Evaluation of the UMTES Implementation

6.1 Evaluation of the Mobile Payment Solution

The mobile payment solution is evaluated for its performance in terms of the time taken for a payment to be made. The time taken for a single payment transaction is estimated. The estimation is done in two parts. The first part is done by estimating the various time components of a single payment transaction. The second part consists of estimating best case and worst case scenarios of the transaction times using results from simulation that studies the network delay components and the variation in the delays.

The estimates for a typical transaction time are then examined for the appropriateness and feasibility of UMTES as a payment protocol. This chapter presents a detail of how these estimates are arrived at and concludes by comparing the transaction times with the other similar performance measurements available in literature as well as with practical time estimates available from industry reports.
The term “user” is used to denote the Payee in the sections below. It is meant to imply the user of the smart phone in a generic sense. The term Payee will be used in the context of a payment transaction. Therefore, the two terms will be used interchangeably.

6.2 Estimating the Performance of the UMTES Implementation

In order to estimate the performance of a UMTES payment transaction, it is necessary to identify the various transaction components. Once identified, each of the estimates are either referenced from existing literature or calculated using basic references available in literature. Such an estimate of the transaction will provide a some idea of what to expect from the performance of the protocol.

6.2.1 Scenario for Estimation

For purposes of estimation of the payment transaction time, a typical payment scenario is considered. A user makes a payment at a PoS at a store. The user has a smart phone and the store has a PoS which is either another smart phone or a tablet. Therefore, it is reasonably safe to assume that the

capabilities of the smart phone and the PoS are roughly similar. Both the user's phone and the PoS are NFC capable.

The user is subscribed to a mobile network, MN1 for her voice and data services and in turn subscribed to PSP1 for payment services. Similarly, the store is subscribed to MN2 for data services and to PSP2 for payments. PSP1 and PSP2 are located in separate data centers. These data centres and the Mobile Network Operators are interconnected via a public data network, such as the Internet. The network path from the User to her PSP and from the store to its PSP are via a wireless access network which is either 3G/4G or WiFi. The network path between the two PSPs is typically on a wired network, interconnected by high speed WAN links.

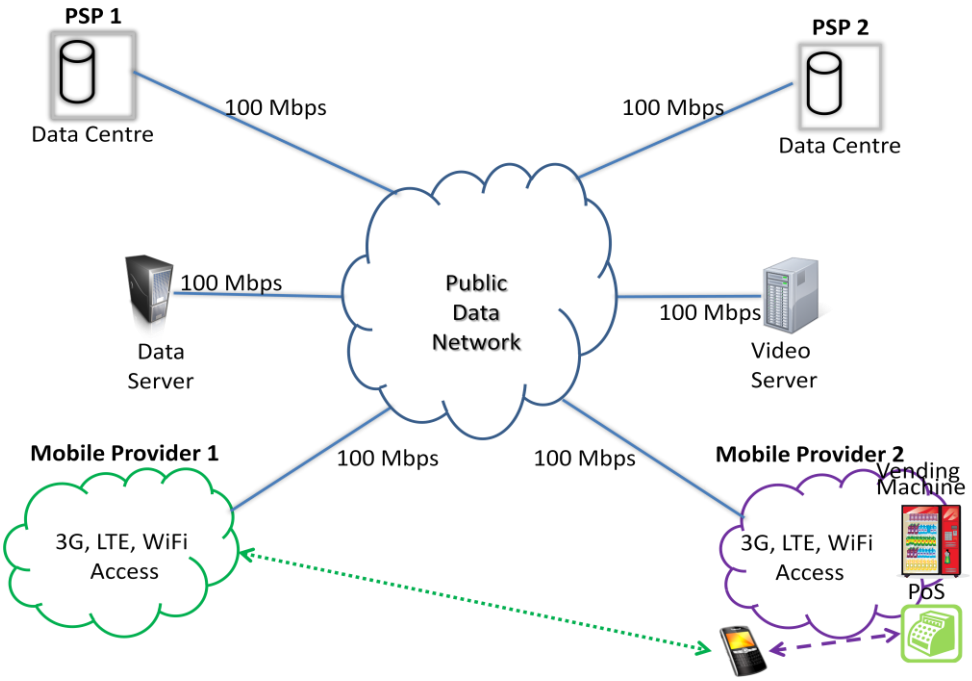


Figure 29: The Payment scenario considered for estimating the total time for a transaction

The payment scenario presented in Figure 29 shows a user smart phone at a PoS terminal. The phone is associated with its mobile provider (Mobile Provider 1) whereas the PoS is associated with its provider (Mobile Provider 2). The user smart phone interacts with the PoS to provide its identity for the PoS to charge it to make the payment (SWIP in UMTES). Each of the two PSPs, PSP1 the user's payment services provider and PSP2 the store's provider are interconnected via a public data network. Also connected to the public network are other data sources that contribute the traffic to the data network.

Notice that the network path from the smart phone to PSP1 consists of a wireless access segment and a set of wired segments to the server at PSP1.

This wireless access segment impacts the network delay when interacting with the server. The wireless access segment is in fact the primary concern of the service, apart from the computing times on the smart phone. These are two aspects that will attract focus in the course of the estimation

6.2.2 Assumptions

In order to make a fair estimate, a few assumptions are required with respect to the equipment and the network infrastructure. The assumptions are detailed below.

6.2.2.1 The smart phone and the smart phone user

The smart phone configuration consists of a touch screen based device with a hardware configuration consisting of a dual core processor at 1 GHz, 1 GB RAM, a GPU and 16 storage. The phone has a single SIM and supports both 3G and 4G (LTE) access and WiFi (802.11 a/b/g/n). The phone has a GPS, a gyroscope, light and temperature sensors. This is the minimum configuration of smart phones released in 2013 (Comparison of smartphones, 2014).

The phone runs an Android version of the OS and runs valid applications from the app store. It is not a ‘rooted’ OS and runs with the native Android security framework (Enck, W., Ongtang, M., & McDaniel, P. D. (2009)).

The smart phone user is a basic user and not a power user. This assumption impacts the speed of interaction of the user with the smart phone. The interaction time is an important factor in the time taken for the entire transaction. The user, though familiar with the phone, operates it in a non-speedy manner.

During the course of the payment, the user is stationary and is not moving around. This assumption leads to a further assumption that the association of the smart phone with the nearest provider base station is consistent and does not bounce between base stations. The impact, therefore, is a consistent receive power level on the smart phone receiver leading to fairly constant average uplink and downlink throughputs on the network.

6.2.2.2 The Mobile Network

The mobile network access by the smart phone critically impacts the speed of the transaction. There are two related concerns – coverage (access to the network) and the signal strength. UMTES is meant to be used in 4G environments.

4G technology, in general, addresses coverage issues by deploying pico cells, femto cells,micro cells and macro cells to service heterogenous coverage

requirements. It is obvious that the cell coverage areas are deployed and they are deployed appropriately in homes, malls, parking lots and so on. Each of these coverage areas have an individual base station which is uplinked to the provider network backbone. By providing good coverage across heterogeneous areas, good signal strength within the cell as well as across cell borders is ensured. This addresses both access and signal strength (bandwidth) concerns.

The network connectivity between the two mobile provider networks and the PSP infrastructure is via a public data network (refer Fig. 29). It is assumed that the public data network has a backbone network to which each of the actors in the payment are interconnected to. Each of these actors are assumed to have a full duplex 100 Mbps link with no congestion on them even at peak hours. The backbone itself is assumed to have links of at least similar bandwidth, MPLS switched , with a topology that provides multiple paths between each of the actors in a payment. The impact of these assumptions is that data forwarding between the actors, interconnected on the wired network, will happen at wire speed, with minimum delays (queuing and switching).

The network delay estimates are based completely upon the uplink and downlink bandwidth. This is almost equivalent to estimating delays on a wired network, since the wireless broadband delays are not considered. The delay variations due to location and coverage (signal strength), mobility, user density in a cell, the handset and such factors are not included in the estimate. Grogorik 2013, quotes typical delays for active connections on 3G as 100 – 500 ms and 4G as less than 100 ms. These delays are in the Radio Resource Control (RRC) layer. These are the delays that are expected to add on when the scenarios are simulated, in addition to other delays.

6.2.2.3 Other Assumptions

A few other assumptions made with respect to a payment transaction are listed here:

1. The application data is encoded using XML
2. The XML encoded data is not compressed, but encrypted
3. The computation capacity of the servers compared to that on the smart phone is very high. For compute time estimates, all compute times are estimated on the smart phone itself and not on the servers. The servers are assumed to be congestion-free and dimensioned for peak loads.

6.2.3 The Total Time of the Payment Transaction – T_{trans}

The transaction time, from a user's perspective, is the time taken to make a payment. The payment is made using her mobile device. Therefore, the time component of the transaction will include the time taken by the user for all actions pertaining to making the payment.

The time components of a payment transaction, therefore, comprise broadly of three parts, namely, the time spent by the user, the time for computation to process the data being exchanged and the time taken by the data to transit the network that interconnects the Payer and the Payee. This is represented by $T_{trans} = T_{user} + T_{compute} + T_{network}$, where T_{trans} is the total transaction time constituted by the sum of the three time components.

6.2.3.1 Time spent by the user, T_{user}

T_{user}, has two primary components – the time spent by the user interacting whit her mobile device and the time taken for the mobile device and the payee device which could be a PoS, a Virtual PoS or a remote PoS. For this estimation, we consider only a PoS. Figure 29 details the time components in a hierarchy.

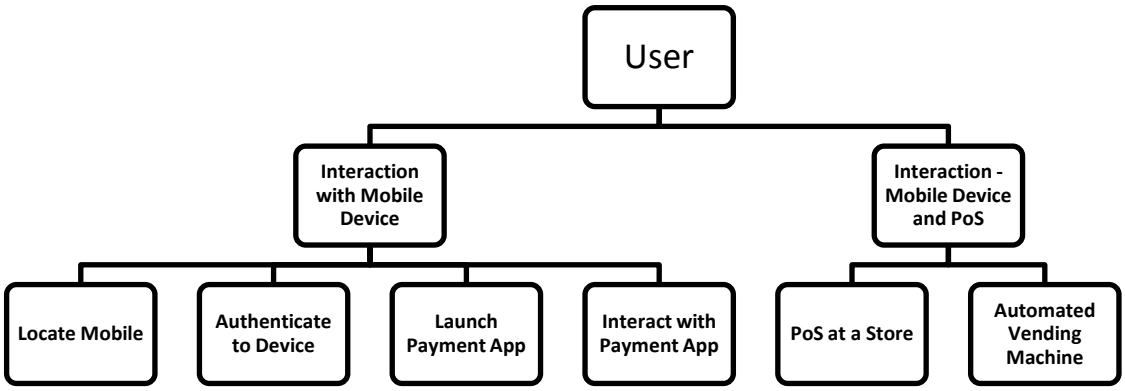


Figure 30: Time Components of the User Interaction

6.2.3.2 Time spent on computing, $T_{compute}$

$T_{compute}$, comprises of two broad components, the total compute time at the server side and the total compute time at the client side. Recall that server side implies the compute time on two servers PSP1 and PSP2 and the client side compute time includes the compute time on the Payer and Payee terminals. Assuming that the Payee uses a mobile PoS, essentially a smart

phone, the estimates for computation at the PoS are calculated similar to that on the Payer device.

Figure 31 details the time components of the computation at the clients and the servers. Apart from the applications on the server and client, UMTES and the TLS take up most of the computing requirement. In addition to this, the database accesses on the server side could contribute to the time requirement.

Most of the computation is required for the functions of encrypting, decrypting data and signing them digitally for all data exchanged. In addition to this, on the server side, the data base look up for authentication information as well as database modifications for the user account information, following the payment, have to be factored in as well. These components are not specifically shown in the figure since they are common functions to both the client and the server.

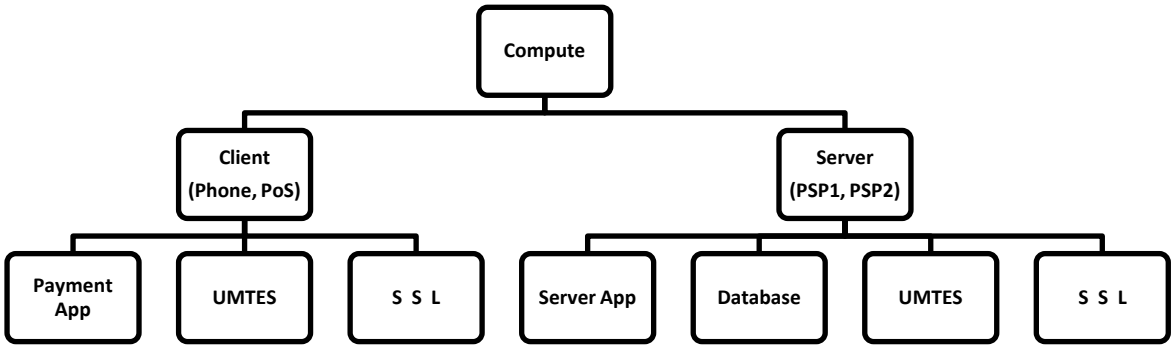


Figure 31: Time Components for Computing at the Clients and Servers

6.2.3.3 The time spent on the network, $T_{network}$

$T_{network}$, the third component of the transaction time is the time taken for data to transit the network that interconnects the clients and the servers. In this context, the time required to set up an initial connection, at the transport layer (TCP) is one primary component. The other component is the delay on the network that comprises of routing, queuing and propagation delays. Figure 32 provides a hierarchical view of the network components of the transaction time.

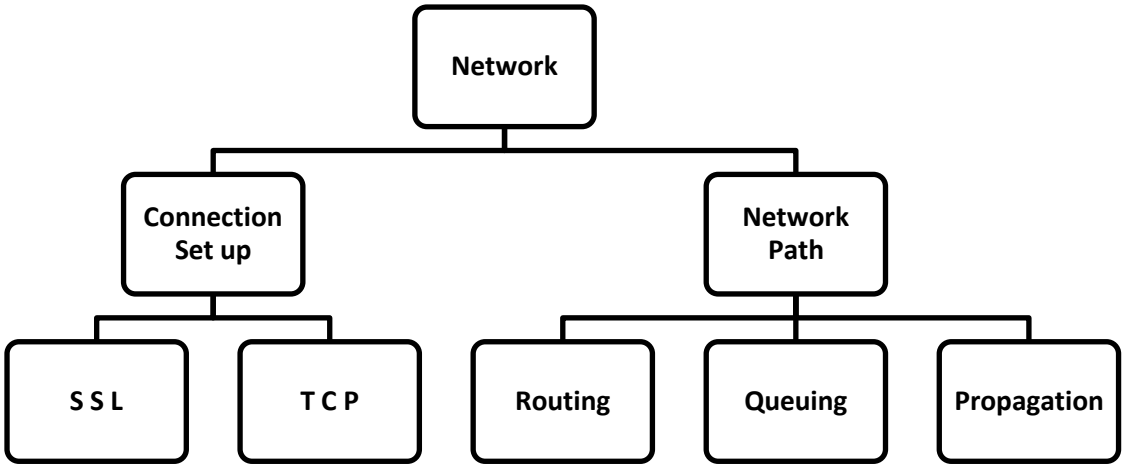


Figure 32: Time components of the Network Component

Summarising these components, they can be represented as follows:

The total transaction time is given by

$$T_{trans} = T_{user} + T_{compute} + T_{network} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

where

$$T_{user} = T_{mobile,User} + T_{mobile,PoS} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (2)$$

$$T_{compute} = T_{client} + T_{server} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (3)$$

and

$$T_{network} = T_{connection} + T_{PQR} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (4)$$

Each of the components represented in (3) and (4) are further represented as follows:

$$T_{compute} = T_{client} + T_{server} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (5)$$

where

$$T_{client} = T_{app\_c} + T_{UMTES} + T_{SSL} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (6)$$

And

$$T_{server} = T_{app\_s} + T_{UMTES} + T_{SSL} + T_{dB} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (7)$$

In (6) and (7),

$$T_{app} = t_{launch} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (8)$$

$$T_{UMTES} = T_{SSL} = \sum_{i=\{en,de,sign\}} t_i \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (9)$$

where *en = encrypt, de = decrypt, sign = keyed_hash*

$$T_{dB} = t_{auth} + t_{account} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (10)$$

where

auth = user authentication,

account = user account information access and modification

In (4),

$$T_{connection} = t_{SSL} + t_{TCP} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (11)$$

,And

$$T_{PQR} = t_{propagation} + t_{queuing} + t_{routing} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (12)$$

(1) To (12) comprehensively represent the various time components of a payment transaction.

Each of these time components will be estimated with as many available data from literature. Using these estimates, the total time for a transaction will be calculated.

6.3 Estimating the transaction time

The process of estimation is illustrated in the following sections. The process begins with the components of equation (1). The sub components of each of the primary components are estimated using references from literature. In cases where references are not available, best estimates are made and the reasoning behind making the estimates are mentioned. $T_{compute}$ is first estimated, followed by $T_{network}$ and T_{user}.

6.3.1 Estimating $T_{compute}$

The total time required for computation in the transaction is the compute time requirements on the clients (smart phone, PoS) and the servers (PSP1, PSP2) (Ref equation 3). The time components for the server and client are almost similar, but for the addition of the time component for database use on the servers.

On the server side, it is assumed that the various processes, namely the payment application, the protocol subsystem which is part of the application and the network related processes are already functional and therefore, the time required to start up these processes is not accounted into the total time required for a payment transaction.

6.3.1.1 Estimating T_{app_s} and T_{app_c}

The application processing consists of taking actions based on the protocol messages that the protocol hands over. For T_{app_s}, typically, these actions would comprise of initiating a database access or initiating a transfer for settlement or forwarding a message to the other actors. Essentially, the server application does very little processing other than routing actions to its sub-components. Therefore, the time taken by application component on the server would not have a significant impact on the total compute time on the server and hence ignored. T_{app_s}, is effectively zero.

For T_{app_c}, the application processing mostly involves user interaction and little else. Most of the other work load is taken by the protocol sub-system. The time taken for the user interaction is accounted for in the estimates of T_{user}. Therefore, this time component of $T_{compute}$is effectively ignored. In summary, both T_{app_s} and T_{app_c} are considered as nil in (6) and (7).

6.3.1.2 Estimating T_{UMTES}

Command	**Data Size in Bytes** (Command + Arguments)	Number of Arguments
REGI	34	3
ACK	32	4
INIT_REQ	108	9
INIT	19	2
ACK	16	2
AUTH	42	5
ACK	16	2
CONF	22	2
TRAN	64	7
ACK	28	3
CLOS	45	4

Table 17: UMTES - Command and Argument sizes in Bytes

T_{UMTES} involves all the actions performed by the protocol sub-system. Apart from the housekeeping activities, the major time spend is the encoding and decoding of the application data, encrypting it and decrypting it and generating a signature for the data that is to be exchanged with the server (ref. Equation 9). Similar operations are performed by SSL in order to secure the data being transported on the network. SSL takes the application data which is encoded, encrypted and signed and further encapsulates it with its own security before transporting it on the network.

In order to estimate each of the components of (9), it is necessary to know the amount of application data that requires to be exchanged. This data depends upon the protocol command and its arguments (ref. Table 17).

The application data is first encoded and then encrypted and signed. The data is encoded using XML. This causes the amount of data to increase. Using a text to XML convertor and without defining a specific schema, converting to XML showed fourteen characters used as tags per argument and the header and footer tags amount to 72 characters. This increases the data volume significantly. The data size, in Bytes, after the XML encoding is shown in Table 18.

Command	**Data Size in Bytes**	**Command Args**	**XML Encoding (72B header + 10B x # Args)** Bytes
REGI	34	3	136
ACK	32	4	144
INIT_REQ	108	9	270
INIT	19	2	111
ACK	16	2	108
AUTH	42	5	164
ACK	16	2	108
CONF	22	2	114
TRAN	64	7	206
ACK	28	3	130
CLOS	45	4	157

Table 18: Data size after encoding in XML

The XML encoding throughput is estimated as 40 Bytes per processor cycle ((Zefu Dai, Nick Ni, and Jianwen Zhu., (2010). On a 1 GHz processor, this amounts to 40 Bytes per nano second. With an average data size of 38.8 Bytes, say 40 Bytes, and a total of eleven steps to complete a transaction, the compute time for XML encoding is only 11 nano seconds at the client side and 11 nano seconds at the server side. This may not impact the total compute time, significantly.

The encoded data is now encrypted and a hash value is calculated for the encrypted data for an integrity check at the remote end. Each command data pair is encrypted on the client and decrypted upon reaching the server.

Similarly, the response, data pair sent by the server is encrypted at the server and decrypted upon receipt at the client. Therefore, for a total of eleven steps, there are eleven instances each of encryption and decryption and twenty two instances of hash generation.

The encryption is done using AES-256 with a block cipher of 16 bits and the hash is calculated using SHA-256. AES-256 is a symmetric (shared) key based encryption scheme. The time taken to encrypt or decrypt a block of data is the same (Zhao, L., Iyer, R., Makineni, S., & Bhuyan, L. (2005)). Hashes are one way functions and always perform the same steps to check data integrity.

The time taken to encrypt a data block is calculated as (0.21 x input_size_in_KB) ms. This temporal characteristic was observed on a handheld with an Intel PXA 270 processor, 624 Mhz running Windows 5.0, when estimating the performance of various encryption algorithms (Rifa-Pous, H., & Herrera-Joancomartí, J., 2011). We use this as the closest available specification to the smart phone specification mentioned in section 6.2.2.1.

AES-256 takes the input bytes, aligns them on a 16-bit boundary and then outputs the same number of bytes as the input. So, there is utmost an overhead of 15 bits (~ 2 Bytes) in cases where the input ends at one bit past the multiple of 16. This overhead decreases with the increase in input data size. The average size of the XML data in Table 18 works out to 150 Bytes. So, there is a worst case overhead of ((2/150)*100) = 1.3%. This is not significant and has no impact on the data size.

SHA-256 is used to generate a hash which is used as the signature to verify the integrity of the data sent from the sender, at the receiver side. The algorithm generates a 256 bit (32 bytes) signature. This hash value is added to the encrypted message and sent to the receiver. The computation throughput for the hash is 8.31 MBps. The compute time required for the encrypted data are calculated as ((encrypted_data/8.31) * 10^{-6}) seconds.

The various data overheads that are added to the application data that requires to be exchanged is shown in Table 19. Notice that there is an average increase of five times (500%) in the size of the application data. The column of the number of command arguments is dropped for the sake of ease.

Command	Data Size in Bytes	Command Args	XML Encoding (72Bytes header + 10Bytes x # Args)	AES-128 Encrypted Bytes (16xN)	Add SHA256 Hash (32 Bytes)	Delay for encrytpion (0.21xKB) ms + Hash (Data/8.31MBps) ms
REGI	34	3	136	144	176	0.09177704
ACK	32	4	144	144	176	0.09513704
INIT_REQ	108	9	270	272	304	0.1788633
INIT	19	2	111	112	144	0.07357548
ACK	16	2	108	112	144	0.07231548
AUTH	42	5	164	176	208	0.1112386
ACK	16	2	108	112	144	0.07231548
CONF	22	2	114	128	160	0.07868626
TRAN	64	7	206	208	240	0.13658017
ACK	28	3	130	144	176	0.08925704
CLOS	45	4	157	160	192	0.10444782

Table 19: Encoding, Encryption and Hash for the application data

The total compute delay for encryption and hashing is 0.55 ms, adding up the compute delays in the last column.

Command	Data Size in Bytes	XML Encoding (72B header + 10B x # Args)	AES-128 Encrypted Bytes (16xN)	Add SHA-256 Hash	((SSL with MAC) + (TCP + options) + IPv4 Overhead Bytes ((5+32)+(20+20) +20)	((SSL with MAC) + (TCP + options) + IPv6 Overhead Bytes ((5+32)+(20+20)+ 40)
REGI	34	136	144	176	284	304
ACK	32	144	144	176	252	304
INIT_REQ	108	270	272	304	380	432
INIT	19	111	112	144	220	272
ACK	16	108	112	144	220	272
AUTH	42	164	176	208	284	336
ACK	16	108	112	144	220	272
CONF	22	114	128	160	252	304
TRAN	64	206	208	240	316	368
ACK	28	130	144	176	252	304
CLOS	45	157	160	192	284	336

Table 20: The application data size at the network layer

Table 20 shows the size of the application data with the packet overheads at the SSL, TCP and IP layer. The SSL headers accounted for are from the SSL record protocol which has a 5 byte header with the hash of the message , 32

bytes, attached. The TCP segment header is 20 bytes with the options an additional 20 bytes. Depending upon the version of IP used, the header length varies. 20 bytes are used for IPv4 and 40 bytes are used for IPv6. For all further estimates, the IP version considered is IPv6.

6.3.1.3 Estimating T_{SSL}

The next component is the encryption and hashing time required by SSL. The three main cryptographic operations are asymmetric encryption, symmetric encryption and hashing (Zhao, L., Iyer, R., Makineni, S., & Bhuyan, L., (2005)). SSL, first opens a connection with the PSP server and negotiates a security association which involves a connection set up and a session key exchange between the two communicating end points. This is termed as the" SSL handshake" phase. The data transfer phase in SSL is governed by the SSL Record Protocol. The data transported is first compressed, then a hash value is generated and finally encrypted.

When the payment transaction starts, the SSL layer connects to the remote PSP server. The connection time largely consists of the security negotiation which requires a good deal of computation. Therefore, the time for the SSL connection phase is included in the compute time for the payment transaction, under $T_{network}$ (ref. Equation 11) .

Command	Data Size in Bytes	XML Encoding (72B header + 10B x # Args)	AES-128 Encrypted Bytes (16xN)	Add SHA-256 Hash	Delay for encrytion (0.21xKB) ms + Hash (Data/8.31MBps) ms	SSL Data Transfer - Delay for encryption (0.21xKB)ms + Hash (Data/8.31MBps) ms	Total Delay for Encryption and Hashing in ms
REGI	34	136	144	176	0.09177704	0.1297186	0.22149564
ACK	32	144	144	176	0.09513704	0.1297186	0.22485564
INIT_REQ	108	270	272	304	0.1788633	0.21428486	0.39314816
INIT	19	111	112	144	0.07357548	0.10857704	0.18215252
ACK	16	108	112	144	0.07231548	0.10857704	0.18089252
AUTH	42	164	176	208	0.1112386	0.15086017	0.26209877
ACK	16	108	112	144	0.07231548	0.10857704	0.18089252
CONF	22	114	128	160	0.07868626	0.11914782	0.19783408
TRAN	64	206	208	240	0.13658017	0.17200173	0.3085819
ACK	28	130	144	176	0.08925704	0.1297186	0.21897564
CLOS	45	157	160	192	0.10444782	0.14028939	0.24473721

Table 21: Total delay for encryption and hashes at the application and SSL layers

For the data transfer phase, the assumption made is that the compression is turned off and only the hashing and encryption functions are used. AES-128 and SHA256 are chosen for the two functions. Therefore, compute time calculations, similar to the hashing and encryption for the application data are used. A hash is first calculated on the application data (col 5, Table 20) and then the application data and the SSL hash are encrypted. Column 7 in Table 21 illustrates the compute time for encryption and hashing the data at the SSL layer. Note that the delay values are doubled (as compared to Table 16) since the compute delays at the client and server are accounted for. The compute time for encryption and hash generation for the application data is 1.104 ms ms (col 6, Table 21), the compute time for encryption and hash generation for the SSL data transport is 1.511 ms (col 7, Table 21) totalling to (1.104 + 1.511) ms = 2.614 ms.

The next estimate is the time taken for the database access and update. The Transaction Processing Council (TPC) releases the benchmarks for database performance. These benchmarks are based on specific workloads that are typical of real world applications (TPC (2014)). The TPC-E specifies a typical order-entry system with payments and this model fits with a Payer placing an order for a payment service with the PSP and effectively making a payment. The transaction rate metric is the number of new-order, payment and order-status transactions per minute. These transactions have a response time requirement of five seconds (Bernstein & Newcomer (2009)). The benchmarks released by the TPC indicate the lowest benchmark at 290,040 tpmC, which is about 48,500 transactions per second which is approximately 0.02 ms per transaction. The benchmark also specifies a guaranteed response time of 5 seconds for the specific workload request.

Table 22 summarises the compute times on the client and server. The total compute time on the server as well as the client amounts to 2.634 ms.

	T_{client}	T_{server}
T_{UMTES}	0.552 ms	0.552 ms
T_{SSL}	0.755 ms	0.755 ms
T_{dB}	N A	0.02 ms
TOTAL	1.307 ms	1.327 ms

Table 22: Compute time elements on the client and server. UMTES and SSL processing are similar. The server compute times are estimated on the client platform itself.

6.3.2 Estimating $T_{network}$

The time spent on the network comprises of two components – the time required to establish a connection and the time for which the data transits the network (ref. equation (4)). The latter comprises the propagation, queuing and routing times on the network. Each of these components are estimated separately.

Compared to the compute times, the network related time estimates will be significantly high, usually by a few orders of magnitude. The major impact is due to the propagation time on the network. In addition to this, the traffic on the network that has to be contended with, decreases the available bandwidth, causing the effective bandwidth to be, at times, significantly lower than the bandwidth of the links.

The type of links also impact the effective bandwidth. Wireless links, such as those in WiFi networks and 3G/4G networks are typically associated with lower effective bandwidth and delays when compared to wired links. In the current context, the smart phone accesses the payment service over a wireless network. Therefore, the network time or network delays as it shall be addressed as, now on, will be significant.

In a sense, $T_{connection}$ is a function of T_{PQR}. Therefore, T_{PQR} is first estimated followed by $T_{connection}$.

6.3.2.1 Estimating T_{PQR}

The propagation, queuing and routing delays are dynamic parameters of the network. Their combined impact is captured in a single network parameter, the round trip time (RTT) between the source and destination.

The network path between the client and the server comprises of both wireless and wired links. Figure 33 illustrates the network paths for the various interactions in a payment transaction. Notice that the inter-PSP interaction is on the wired segment only. In order to estimate the time taken for the network transit, the RTTs for the wired and wireless segment are measured and then the total network transit time is calculated. The smart phone user accesses the payment service via the 3G/4G network on the phone, most of the time. The bandwidth on the downlink and uplink of the 3G/4G networks are asymmetrical. That is, the bandwidth provisioned from the smart phone to the mobile provider network is less than the bandwidth provisioned from the mobile provider to the smart phone. This causes the transit times of data to

vary depending on which direction they transit, from the smart phone to the provider network or from the provider network to the smart phone.

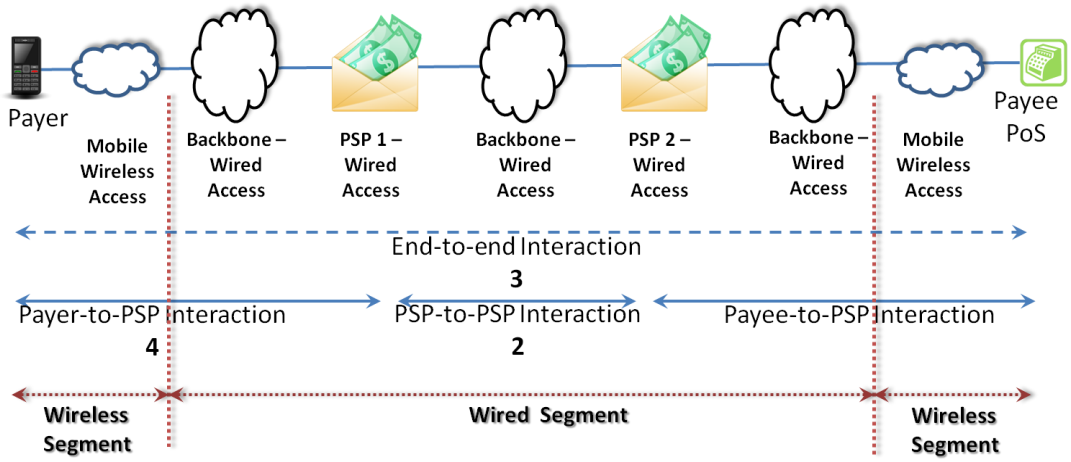


Figure 33: Wired and Wireless network segments in the path from the client to the server

In terms of the wireless access technology, three options are considered for estimates. They are Long Term Evolution (LTE) referred to as 4G, Evolved High Speed Packet Access (HSPA+) referred to as 3.5G and Enhanced High Rate Packet Data (eHRPD) referred to as 3G. The three technology options are considered to get a fair idea of how the performance of the transaction will be on current day 3Gmobile networks. Some providers in the state of transition have 3.5 G networks and a few providers have 4G networks. In the UK, five of the nine mobile network providers offer 4G access.

Chen et al (2013), Chen et al (2012b), Chen et al (2012a) and Chakraborty, A., & Das, S. (2013) provide an extensive measurement of current day 3G and 4G networks with rigorous measurements. These measurements form the basis of the network transit time estimates.

Access Technology	**Uplink Bandwidth in Mbps** *(Chen et al., 2013)*	**Downlink Bandwidth in Mbps** *(Chen et al., 2012b)*
3 G (eHRPD)	0.56	0.85
3.5 G (HSPA+)	0.91	3.47
4 G (LTE)	4.34	7.79

Table 23: Uplink and Downlink bandwidth for wireless mobile access networks

The uplink and downlink bandwidth from Table 23 are used to calculate the data transit time for the payment transaction.

Command	((SSL with MAC) + (TCP + options) + IPv6 Overhead Bytes ((5+32)+(20+20)+40)	# of Logical Hops / (Uplink or Downlink)	3G delay in ms - ((data/0.56 Mbps) U, (data/0.85 Mbps) D)	3.5G delay in ms - ((data/0.91 Mbps) U, (data/3.47 Mbps) D)	4G delay in ms - ((data/4.34 Mbps) U, (data/7.79 Mbps) D)
REGI	304	1, U	4.342857	2.672527	0.560369
ACK	304	1, D	2.861176	0.700865	0.312195
INIT_REQ	432	3, U+D+D	14.30319	5.789733	1.683605
INIT	272	1, U	3.885714	2.391209	0.501382
ACK	272	3, D+D+D	7.68	1.881268	0.837997
AUTH	336	1, U	4.8	2.953846	0.619355
ACK	272	1, D	2.56	0.627089	0.279332
CONF	304	1, U	4.342857	2.672527	0.560369
TRAN	368	1, D	3.463529	0.848415	0.37792
ACK	304	1, D	2.861176	0.700865	0.312195
CLOS	336	3, D+D+D	9.487059	2.323919	1.035173

Table 24: Network transit delays on 3G, 3.5G and 4G wireless networks

To estimate the time taken by the application data, the direction of flow is noted, since the uplink and downlink bandwidth are different. Recall that the data destined to the servers (PSPs) from the clients (smart phones) will use the uplink and the data destined to the clients from the servers will use the downlink. The time taken for transit of data is calculated as the size of the data divided by the link bandwidth. Table 24 provides the details of the data transit time on the network for each of the commands.

The transit delay on each type of wireless access network is listed in Table 21. For each type, the uplink and the downlink bandwidth are marked as “U” and “D” respectively in the column titles. The titles also indicate the transit time calculation and refer to the transit time as “Delay”.

The network transit delays for 3G, 3.5G and 4G are 60.58 ms, 23.56 ms and 7.07 ms respectively. It is reiterated here that these delay estimates are based entirely on the bandwidth and do not include the typical delays faced on the wireless access segments such as for channel access, transmit delays, link level retransmissions and so on. These additional delays are estimated using simulation.

6.3.2.2 Estimating $T_{connection}$

To transport the application data to the remote PSP server, the client has to first establish a connection to the server. There are two components in the protocol stack that are involved. First, the transport protocol, TCP establishes a connection to its peer on the server. Following this, the SSL protocol initiates a connection to its peer on the server.

Access Technology	**TWHS RTT, ms** *(Chen et al., 2012b)*	**Time for TCP TWHS (RTT x 1.5) ms**
3 G (eHRPD)	189.10	283.65
3.5 G (HSPA+)	244.31	366.47
4 G (LTE)	69.58	104.37

Table 25: TCP connection time (Three way hand shake)

SSL Hand shake- Client Command	**SSL Hand shake – Server Command**	**(Data Size + 4B handshake + 5B record) header Bytes**	**TCP with options + IPv6 Overhead Bytes (40+40)**	**(Up link or Down link)**	**3G delay in ms - ((data/0.56 Mbps) U, (data/0.85M bps) D)**	**3.5G delay in ms - ((data/0.91 Mbps) U, (data/3.47M bps) D)**	**4G delay in ms - ((data/4.34 Mbps) U, (data/7.79M bps) D)**
Hello		179	259	U	3.7	2.2769	0.4774
	Server Hello	79					
	Certificate (4 cert chain)	6004					
	Hello Done	9	6172	D	58.0894	14.229	6.338
Client key exchange		134					
Change Cipher Spec		1					
Finished		21	236	U	3.3714	2.0747	0.4350
	Change Cipher Spec	1					
	Finished	21	102	D	0.96	0.2351	0.1047
TOTAL					66.1208	18.8162	7.3555

Table 26: Network delay component of SSL Handshake

The TCP connection is initiated with a three-way handshake. There are three packets exchanged in all to establish a connection. To estimate the time taken

to establish the connection, it is necessary to know the round trip time (RTT) between the end points. The time required to open the TCP connection will be 1.5 times the RTT value. When measuring the RTT, the RTT measurement is specifically done for the TCP connection request packets which have a far smaller size than data packets (Chen, et al, 2012b; Huang et al., 2012). The RTTs for the three way handshake and the time taken for a complete three way hand shake (TWHS) is in Table 25.

Following the TCP connection set up, the SSL handshake starts. Table 26 gives the network delays in the SSL handshake phase (Freier, A., Karlton, P., & Kocher, P. (2011), Naskooskov, (2010)). The total handshake time is measured as 50.6 ms, including network latency (Shin, Y., Gupta, M., & Myers, S. (2009)), on the handheld configuration mentioned in §6.3.1.2. The measurements were done on using a WiFi access network whose RTTs are close to that of the 4G network. The equivalent time on a 3.5G network will therefore be (50.6 – 7.35 + 18.81) = 62.06 ms and for a 3G network (50.6 – 7.35 + 66.12) = 109.37 ms.

The time components of $T_{connection}$ are illustrated in Table 27. Considering the context of use as 4G, the value is 154.97 ms or ~ 155 ms.

Access Technology	t_{SSL} ms	t_{TCP} ms	$T_{connection}$ ms
3 G (eHRPD)	109.37	283.65	393.02
3.5 G (HSPA+)	62.06	366.47	428.53
4 G (LTE)	50.6	104.37	154.97

Table 27:The time spent on establishing a secure connection to the PSP servers

6.3.2.3 The $T_{network}$ estimate

The network transit time estimate for a 4G network is arrived at by the sum of T_{PQR} and $T_{connection}$. That is, (7.07 ms + 154.97 ms) = 162.04 ms.

6.3.3 Estimating T_{user}

The time taken by the user comprises of two factors – the time taken by the user with interacting with the smart phone, T_{mobile_user} and the time taken for the interaction between the smart phone and the PoS T_{mobile_PoS}.

6.3.3.1 Estimating T_{mobile_user}

The user interaction with the smart phone involves the various actions the user takes in the course of making a payment. The time taken for this interaction involves basic interactions listed in Table 28. Each of these actions were measured real time since there were no references in literature pertaining to human phone interface and the time measurement of interactions.

Action of the Payer on the Smartphone	Delay Measured/Estimated in Secs
Reach out and Pick up the phone	3
Enter a PIN to use the phone	1
Locate and Launch the Payment App	2
Swipe payer details at the PoS	3
PoS verifies payment request to be sent	2
Payment App contacts the PSP Server	1
User Authentication with Login and Password	10
Verify Payment Request details and Click to Pay	3
Minimise the payment App	1

Table 28: List of user interactions with the smart phone to make a payment

Notice that the actions are fairly basic. These actions are listed since making a mobile payment, in this context, is compared with making a conventional payment. When at the till, a user opens his wallet, counts the cash and makes a payment or uses a card to swipe it to make a payment..

The total time for the user interaction with the mobile phone to make a payment is 26 seconds. The other delays are interspersed with these actions. After the user authenticates with a login and password, the UMTES SWIPE executes with the user's ID transferring to the PoS. Following this, the payment request arrives on the smart phone. The wait for this request to arrive is accounted for in the network transit time. Once the request arrives, the payment request is verified and the user clicks to pay. Following this, the UMTES and the network transit times take over until the payment notification is received.

6.3.3.2 Estimating T_{mobile_PoS}

The interaction between the smart phone and the PoS is for the purpose of exchanging the identities of the payer and payee. Notice that both are clients and the data exchange is between the clients. This exchange is a part of the

UMTES protocol (SWIPE, ref. §5.2.4.3) and involves a NFC transfer of identity data required for the payment transaction.

The indicative throughput for the NFC transfers are about 0.1 ms/byte (Urien, (2013)). The SWIPE command and data are a total of 43 bytes and the transfer time amounts to 4.3 ms.

6.3.3.3 The T_{user} estimate

The total time for the user is the sum of the two components in § 6.3.3.1 and § 6.3.3.2 is 26s + 4.3 ms = 26.0043 s

6.3.4 The Transaction Time Estimate

The estimate of the total transaction time therefore is the total of all the components estimated so far. The total of the compute time, the network transit time and the user interaction time is 26.043 seconds.

6.3.5 Discussion

The transaction time estimates have been made entirely from measurements available in literature. In the course of estimation, some approximations and assumptions also have been made. The most important approximation is with estimating the server processing delays. The compute times for various activities on the server have been equated with the delays for similar actions on the smart phone. They have been considered as the ‘worst case’ processing delays from a server perspective.

In addition, some time elements on the server side have been assumed to be zero, for example, the time taken for database access and the database operations. Similarly, any other processing delays on the server such as process scheduling delays have not been considered. However, these delays, are expected to be of the order of milliseconds and their impact on the total transaction time should be minimal.

Table 29 lists the various estimated transaction time components. The contribution of the user interaction time is the largest component of the total transaction time at 23 seconds (rounded off). It constitutes 99.9% of the time. The next largest component of the transaction time is the network transit time.

The user component can vary depending upon the user skills such delays are acceptable since they are user dependent. The delays that accrue on the service side are the network delay and the compute delays. These delays, if perceptible to the user, will cause the user to construe the payment service as a slow service.

	$T_{compute}$ In ms	$T_{network}$ In ms	T_{user} In ms
T_{launch}	0		
T_{app_c}, T_{app_s}	0		
T_{UMTES}	1.104		
T_{SSL}	1.511		
T_{dB}	0.02		
$T_{connection}$		154.97	
T_{PQR}		7.07	
T_{mobile_user}			26000
T_{mobile_PoS}			0.43

Table 29: Transaction time components, estimated

The network time components are bound to vary, given that the access segment is a wireless access segment. Chen et al (2013) have observed a high variation in RTT measurements on the uplink and downlink on 4G mobile networks. On the uplink they observe a 50% variation and a 62% variation in the downlink RTT values. So, the worst case network time will be about 1.5 times the current value.

The sequence of events and the time taken are indicated in the Table 30.

Action of the Payer on the Smartphone	Delay Measured/Estimated in Secs
Reachout and Pick up the phone	3
Enter a PIN to use the phone	1
Locate and Launch the Payment App	2
Payment App contacts the PSP Server	1
TCP Handshake and Connect	0.056
SSL Handshake and Connect	0.104
User Authentication with Login and Password	10
Device Authentication and Registration (REGI+ACK)	0.001
SWIPE Payer details at PoS (SWIP)	3
PoS verifies payment request to be sent	2
PoS sends Payment Request; Request Arrives	0.0021
Verify Payment Request details and Click to Pay	3
UMTES protocol processing and Exchange	0.00629
Receive notification and a printed receipt from the PoS; Minimise the app	1

Table 30: The sequence of actions for making a payment and the time taken

The total time taken is 26.16 seconds for the entire transaction. Of this, the total time for network and computing components is under one second at 0.169 second.

Two assumptions made earlier could impact the total time. First, the database response time is assumed to be one transaction at 0.02 ms. However, one payment request can potentially initiate more than one database request. Apart from this, the five second response could apply. This time could add to the overall transaction time. Specifically, the database operations could dominate the total payment time.

Secondly, the assumption that the transfers between the PSP servers are equivalent to a downlink access is valid only if the PSP servers are local and interconnected, perhaps within the same data centre. If the servers are across cities, which is typically the case, the RTT increases due to the propagation delay. In Table 24, the time estimates for the TRF and ACK commands assume a downlink. These commands are exchanged between the two PSP servers which are connected on a wired network. If these servers are located across cities, then the transit times will be of the order of 30ms. A traceroute from a host in Liverpool, UK to a host in London, UK reports 28 ms RTT. This addition to the delay will not significantly change the overall transaction time. This specific issue is taken care of in the simulated scenario.

6.4 Transaction delay estimates on a simulated network

The next step in the transaction delay estimate is to simulate the network and the traffic components and measure the application delays in a realistic scenario. The network that was used for estimation earlier is simulated, the application protocol logic is encoded and simulated as a networked application. With this, the end-to-end application delays are measured. The details of the simulation scenarios are mentioned followed by the simulation details and a summary of the results. There are a number of plots that result from the various scenarios. The plots that summarise the delays are listed within the text whereas the rest are included in the Appendix.

6.4.1 Simulation Platform

The simulations were run on the network modeller and simulator, Riverbed Modeller (formerly OPNET). The modeller can simulate all components of a TCP/IP network on both wired and wireless network segments. The wired segments include LAN (Ethernet) and WAN (point-to-point) links. Wireless segments include a whole range of technologies such as Wireless LANs,

ZigBee, 6LoWPAN as well as wide area wireless technologies such as UMTS, WiMAX, and LTE. The requirements for our context are taken from wide area wired networks (point-to-point) and wireless networks (UMTS and LTE).

6.4.2 Simulating UMTES and its verification

The UMTES protocol logic was programmed in the simulator by providing the command verbs and data. The data pay load lengths were taken from column 5, Table 20. The protocol logic is executed on the payer node, the payee node, as well as the two PSP servers. The protocol data exchange between

	Phase Name	Start Phase After	Source	Destination	Source->Dest Traffic	Dest->Source Traffic	REQ/RESP Pat
INIT_REQ#1	INIT_REQ#1	Application Starts	Originating Source	PSP 2	(...)	No Response	REQ->REQ->....
INIT_REQ#2	INIT_REQ#2	Previous Phase Ends	PSP 2	PSP 1	(...)	No Response	REQ->REQ->....
INIT_REQ#3	INIT_REQ#3	Previous Phase Ends	PSP 1	PAYER	(...)	No Response	REQ->REQ->....
INIT	INIT	Previous Phase Ends	PAYER	PSP 1	(...)	No Response	REQ->REQ->....
ACK#1	ACK#1	INIT	PSP 1	PAYER	(...)	No Response	REQ->REQ->....
ACK#2	ACK#2	INIT	PSP 1	PSP 2	(...)	No Response	REQ->REQ->....
ACK#3	ACK#3	Previous Phase Ends	PSP 2	Originating Source	(...)	No Response	REQ->REQ->....
AUTH	AUTH	ACK#1	PAYER	PSP 1	(...)	No Response	REQ->REQ->....
ACK#4	ACK#4	Previous Phase Ends	PSP 1	PAYER	(...)	No Response	REQ->REQ->....
CONF	CONF	Previous Phase Ends	PAYER	PSP 1	(...)	No Response	REQ->REQ->....
TRANSFER	TRANSFER	Previous Phase Ends	PSP 1	PSP 2	(...)	No Response	REQ->REQ->....
ACK#5	ACK#5	Previous Phase Ends	PSP 2	PSP 1	(...)	No Response	REQ->REQ->....
CLOSE#1	CLOSE#1	ACK#5	PSP 1	PAYER	(...)	No Response	REQ->REQ->....
CLOSE#2	CLOSE#2	ACK#5	PSP 1	PSP 2	(...)	No Response	REQ->REQ->....
CLOSE#3	CLOSE#3	Previous Phase Ends	PSP 2	PAYEE	(...)	No Response	REQ->REQ->....

Figure 34: Command and Data Transfer logic in the application modeller

the payee and the payer occurs in the sequence defined in the protocol. Figure 34 shows the command sequence for a transaction executing in the application modeller in the simulation environment.

The protocol operation is in two distinct phases – a registration phase (referred to as REG in the course of the simulation), where the mobile node registers with the PSP server and the transaction phase (referred to as TRAN) where the payment and transfer is made. A user has to be registered in order to make a payment. Therefore, the registration process is mandatory and always executed. However, when a user needs to make a payment the registration and the transaction are executed in sequence. The payer and payee are recommended to register first and then make the payments. In the course of the simulation the delays for each of these phases is measured separately and compared with the delay for both the phases executed back-to-back. Figure 36 illustrates that the delay measurement for a (REG+TRAN) is the sum of the individual delays of REG and TRAN.

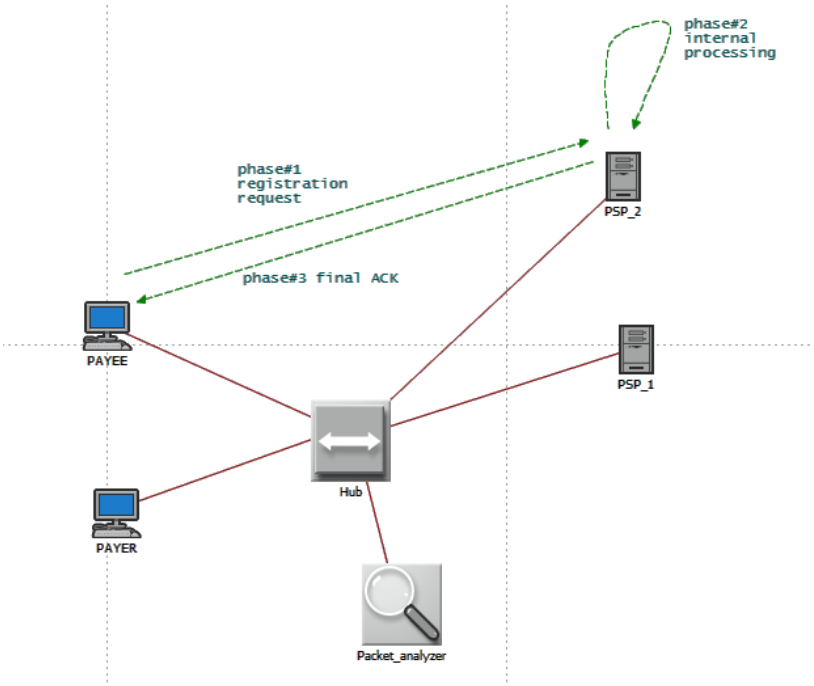


Figure 36: Simulation test bed for functional verification of the application protocol

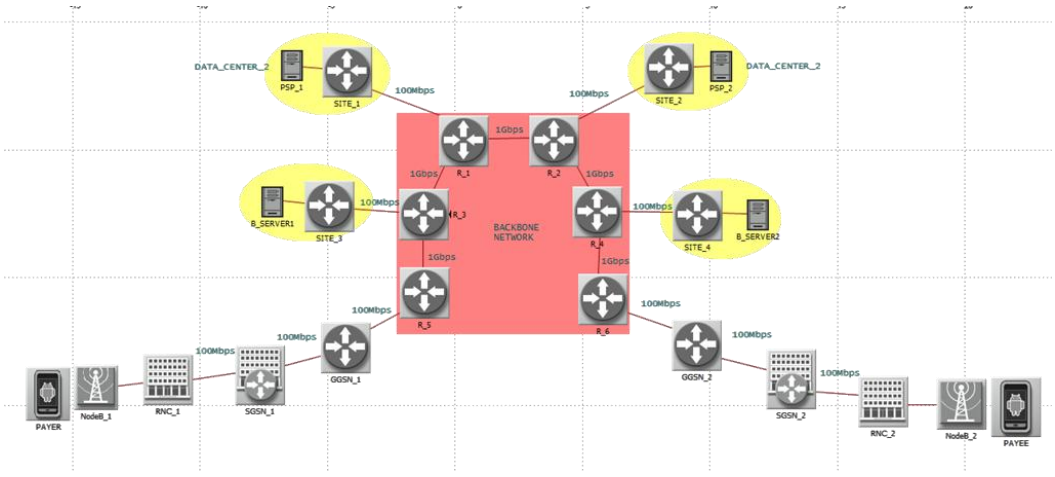


Figure 35: Network topology for the transaction delay measurements on 3G

The protocol logic was verified operationally on a wired network segment, using an Ethernet hub to interconnect the PSP servers, the payer and the payee. The protocol functions were verified from the logs on the servers as

well as the clients. In addition, a packet capture of a transaction done at the Ethernet hub was used to verify the protocol sequence, the protocol data units and the data sizes. The delay measurements indicate that the sum of the delays of the registration phase and the transaction phase is equal to the delay when both the phases are executed together. Figure 35 illustrates this measurement that is made on a wired LAN segment interconnected using an

Ethernet hub. Once the application validation is done, the network segments are configured, the mobile nodes are configured and the application is run on the end nodes to measure the transaction delays.

6.4.3 The Network Infrastructure and Topology

The network that is simulated is based on the components and topology in Fig.29. The backbone network links, each of 1 Gbps, are interconnected using core routers that switch packets at line rate. Two separate network topologies are used depending upon the wireless networks used at the edge. In the case of 3G networks at the edge, the backbone routers are of a lower capacity. The links to the background servers are 100 Mbps (ref. Fig 37). This configuration decision is made based on the simulation requirements as well as to optimise the simulation run times. The background servers are used to generate network traffic and are explained in detail in the section on simulation scenarios in § 6.4.5.

In the case of 4G wireless segments at the edge, the two servers that are used to generate background traffic are also interconnected using 1 Gbps

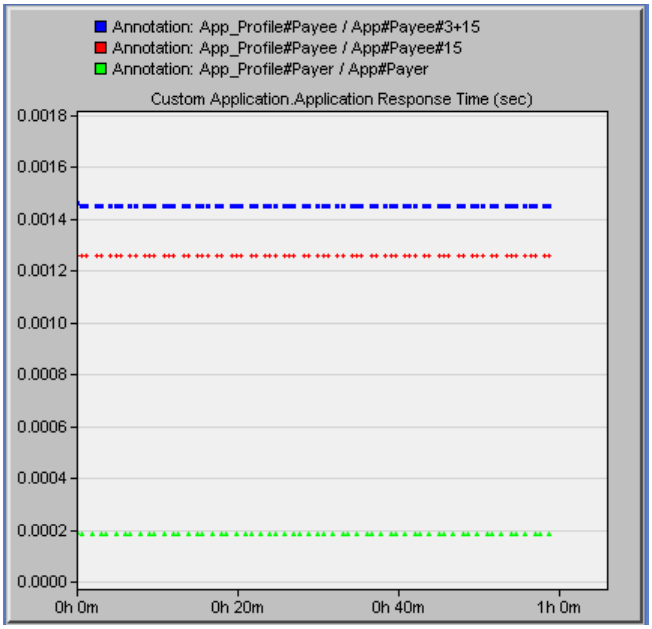


Figure 37: Delay measurements of REG (green), TRAN (red) and REG+TRAN (blue)

links to the backbone. The PSP servers use 100 Mbps links (ref. Fig 38). The wireless network segments are interconnected at either ends of the backbone. In the case of 3G wireless segment, the GGSN is connected via a 1Gbps link to the backbone (ref. Fig. 37). In case of 4G wireless segment, the EPC of the 4G network is connected to the backbone via a 1Gbps link (ref. Fig 38).

6.4.4 Simulation Scenarios

The simulations for the transaction delay estimates are done using scenarios which are designed with specific objectives. The first objective is to observe the effect of the radio access and the associated delays that would add up to the bandwidth based estimates made in §6.3. This would provide a realistic

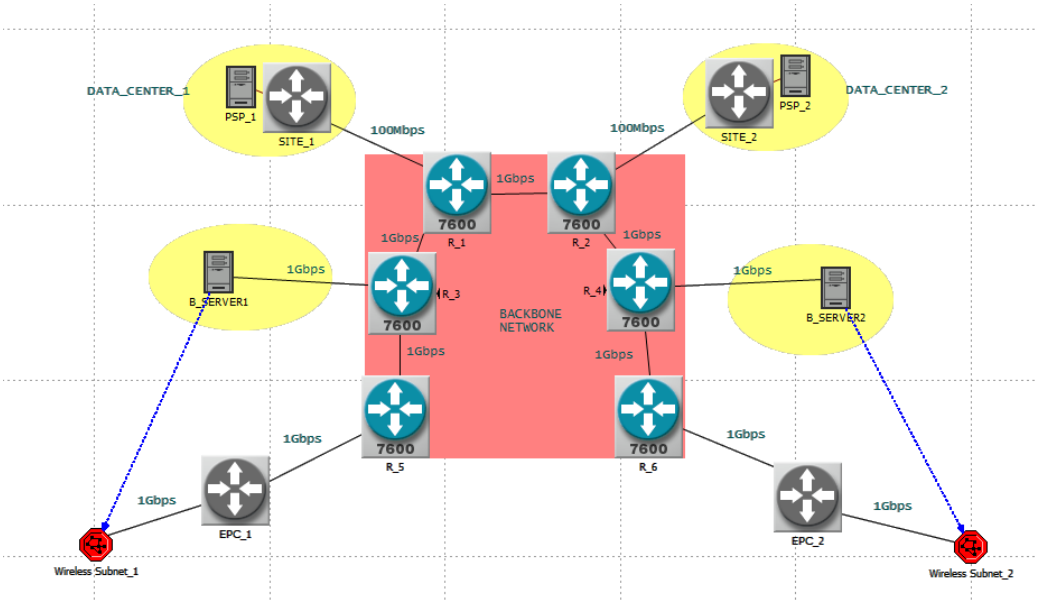


Figure 38: Network topology for the transaction delay measurements on 4G

estimate, but in an ideal condition of just the payer and payee using the network. The second objective is to simulate a realistic environment where the network has other users as well as traffic generated by them and there are a number of payer, payee pairs conducting transactions. The delays faced by these transactions is measured. The final objective is to estimate the transaction delays of a single payer, payee pair, conducting a series of transactions, when the network is under load.

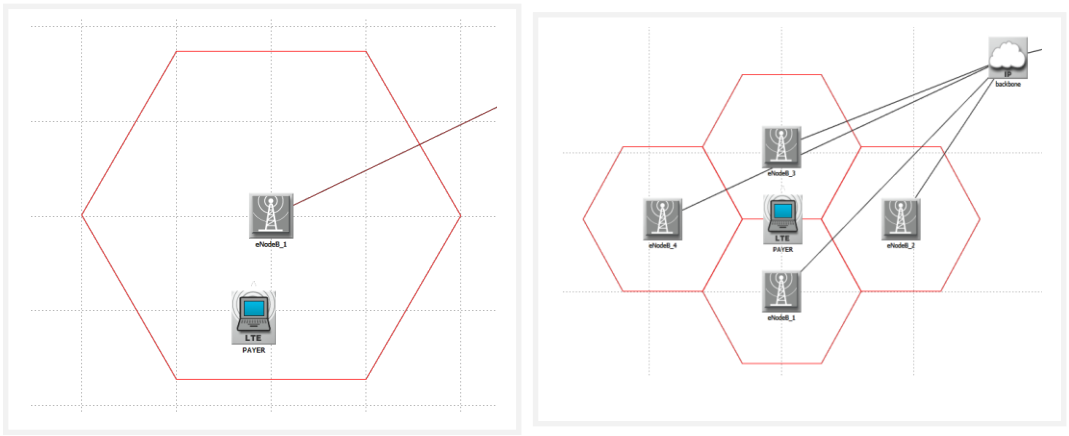


Figure 39: LTE - Macro Cell and Micro Cell configurations

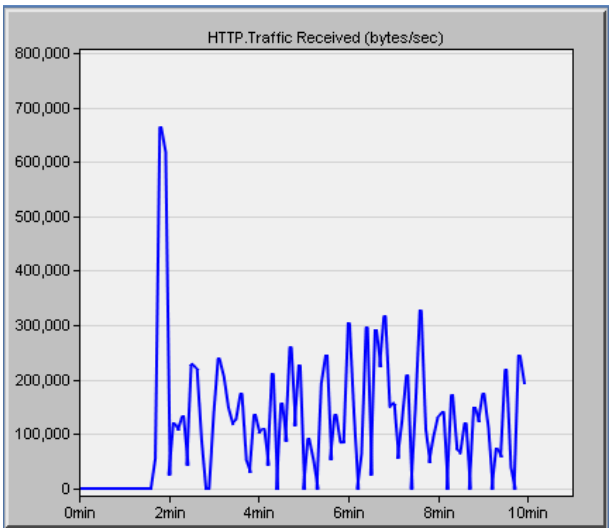


Figure 40: Http traffic generated by 20 active users in a 4G Macro Cell

In terms of the wireless access technologies, the simulations are performed with a 3G UMTS edge network, a 4G Macro Cell edge as well as a 4G micro cell edge (ref. Fig 39). While the major focus is on the 4G edge network, the 3G edge is used to provide a basis to judge whether the applications can work satisfactorily on a 3G network and the performance limitations that might come about because of the access technology.

6.4.5 Calibration of the Network

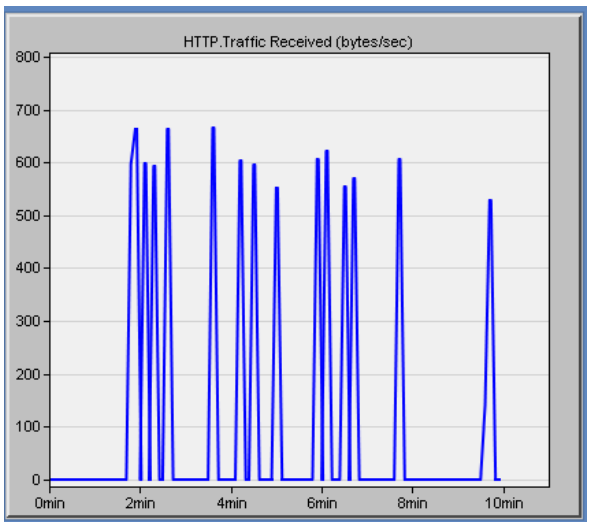


Figure 41: Http background traffic generated by ten active users on 3G

Following the configuration of a network for the simulation, the network was calibrated for end to end delays, using ICMP echo and echo_response. ICMP

packets of varied sizes were sent between various node combinations on the network and the delays were measured.

The active user profile was defined for a 3G user and a 4G user. An active 3G user is expected to access http traffic in a light browsing mode (ref. Fig. 40). This results in a low rate on-off traffic. In contrast, an active user on the high bandwidth 4G network generates heavier load – http access in a heavy browsing mode (ref. Fig 41) and a live video stream (ref. Fig 42).

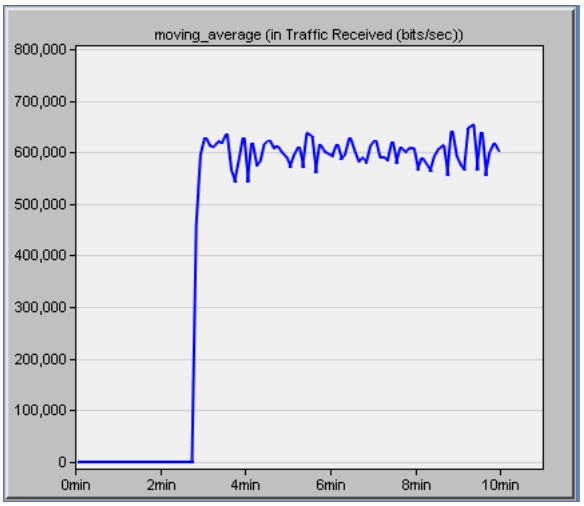


Figure 42: Video stream traffic received by one user

The ICMP based round trip time (RTT) for packets is measured with no load as well as increasing load. The number of active users were increased in steps to see the variation of the RTTs with load. Packet sizes of 512 bytes and 1024 bytes were used separately for the ICMP based RTT measurements.

	Payer to Payee		**Payer to PSP1**		**Payee to PSP2**	
	512B	**1024B**	**512B**	**1024B**	**512B**	**1024B**
No_load	1.18	1.3	1.02	1.115	1.04	1.08
10 Clients	3.428333	4.44	1.161667	2.66	2.635	2.755
20 Clients	4.341667	3.815	1.548333	1.475	3.125	3.275
30 Clients	21.015	14.895	10.595	6.055	8.035	1.235
40 Clients	0	10.405	0	8.641667	1.135	7.101667
50 Clients	0	0	8.815	8.855	1.075	1.095

Table 31: RTT values with active users and traffic, on a 3G segment

	Payer to Payee		Payer to PSP1		Payee to PSP2	
	512B	1024B	512B	1024B	512B	1024B
No_load	0.057	0.057	0.041	0.041	0.042	0.042
10 Clients	0.546	0.546	0.0424	0.0426	0.05425	0.048
20 Clients	0.064	0.0642	0.042	0.0418	0.049	0.049
30 Clients	0.0698	0.0658	0.0416	0.042	0.0532	0.0506
40 Clients	0.0638	0.0576	0.047	0.0466	0.0458	0.0484
50 Clients	0.063	0.0568	0.0456	0.0508	0.0488	0.0492
60 Clients	0.0656	0.0586	0.049	0.0432	0.0466	0.0434
70 Clients	0.0706	0.0834	0.0554	0.0536	0.0506	0.0634
75 Clients	0.0548	0.0636	0.0434	0.043	0.0528	0.0474

Table 32: RTT values with active users and traffic, on a 4G Micro Cell segment

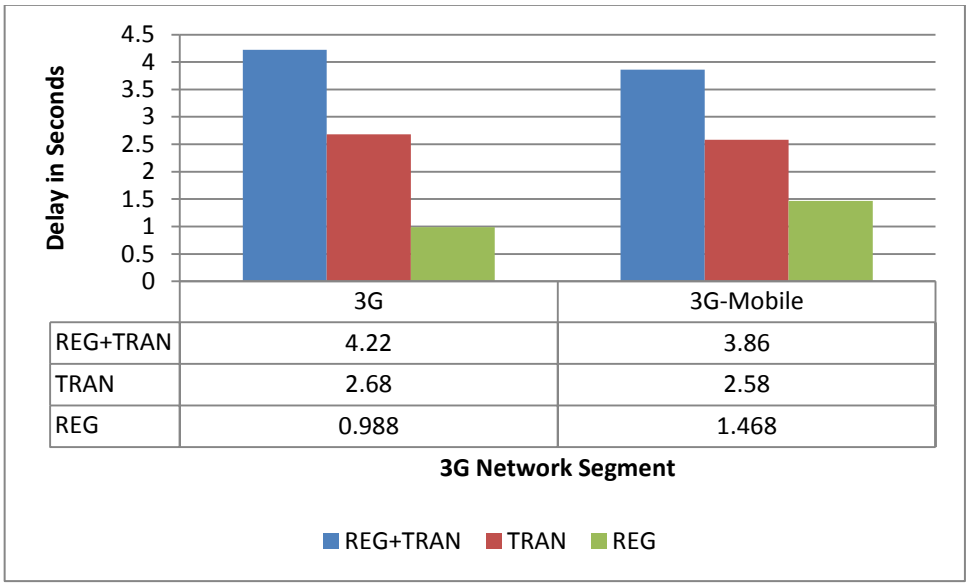


Figure 43: No Load transaction delay on the 3G network segment

On the 3G network, the delays increased very quickly when the background traffic due to the active users increased. With an increased load, there were packet drops seen on the network (zero values in Table 31).

On the 4G network segments, the delays were all less than a second with increasing background traffic. In terms of the total traffic on the downlink of the 4G network, each UE downloads 600Kbps plus 100 Kbps on-off which averages to about 650 Kbps. The load variation on the downlink is from 6.5 Mbps to 48.75 Mbps on a Micro Cell segment and 6.5 Mbps to 97.5 Mbps on a

Macro Cell segment. With this traffic, the mean RTT values for both packet sizes (512B and 1024B) from the payer/payee to their respective PSPs was 66 ms for the macro cell segment and 49 ms for the micro cell segment. The packet drops on the 4G network were less than 0.02%.

	Payer to Payee		Payer to PSP1		Payee to PSP2	
	512B	**1024B**	**512B**	**1024B**	**512B**	**1024B**
No_load	0.063	0.063	0.048	0.048	0.041	0.041
10 Clients	0.066	0.0824	0.049	0.0494	0.049	0.0654
20 Clients	0.0806	0.0808	0.059	0.0624	0.0616	0.0598
30 Clients	0.085	0.10575	0.065	0.066	0.0548	0.0714
40 Clients	0.0646	0.0754	0.0548	0.0556	0.0716	0.0566
50 Clients	0.105	0.088	0.065	0.06625	0.078	0.0628
60 Cients	0.0812	0.0976	0.062	0.0628	0.055	0.0718
70 Clients	0.0898	0.1222	0.071	0.0882	0.071	0.0718
80 Clients	0.074	0.0748	0.0548	0.0562	0.055	0.0562
90 Clients	0.0992	0.102	0.0784	0.0636	0.0644	0.0828
100 Cients	0.105	0.106	0.0712	0.0722	0.065	0.06675
110 Clients	0.09375	0.10575	0.0556	0.0728	0.0915	0.08875
120 Clients	0.1008	0.0748	0.0552	0.0564	0.0748	0.0738
150 Clients	0.1444	0.1116	0.0984	0.0668	0.0764	0.0724

Table 33: RTT Values with active users and traffic, on a 4G Macro Cell Segment

The ICMP timeouts varied based on the load. With the timeout set at 1 second, 23% time outs were recorded. However, when the timeout value was increased to 4 seconds, the timeouts decreased considerably and almost matched the packet drop value. These observations are somewhat close to the measurements made by Chen et al (2013a) where they categorise 4G networks as *not so fast, but loss free* network paths compared to WiFi access.

The maximum packet size in UMTES is 410 B and therefore, the packet sizes should experience a maximum round trip delay of 66 ms and therefore a one way delay of 33 ms, under substantial traffic load as well as user access.

6.4.5 Configuration for a simulation run

The delay measurements, from an application perspective were required for the registration phase and the transaction phase separately and the registration (REG) and transaction (TRAN) phase together, in a single session. The combined session (REG+TRAN) is expected to take much longer than the transaction phase alone, since it constitutes a longer session with most packet exchanges. This requirement was realised by measuring the REG process delays from the Payer side and the (REG+TRAN) and TRAN

delays from the Payee side. This ties in well with the protocol functional requirements that every user has to register before making a payment. In all measurements, both the wireless segments had similar conditions, namely

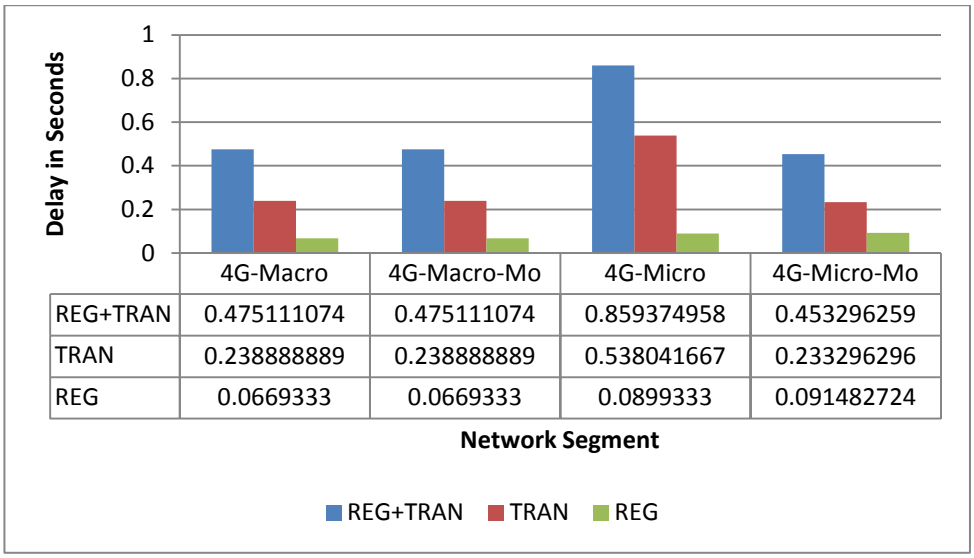


Figure 44: No Load transaction delay on the 4G Network Segments

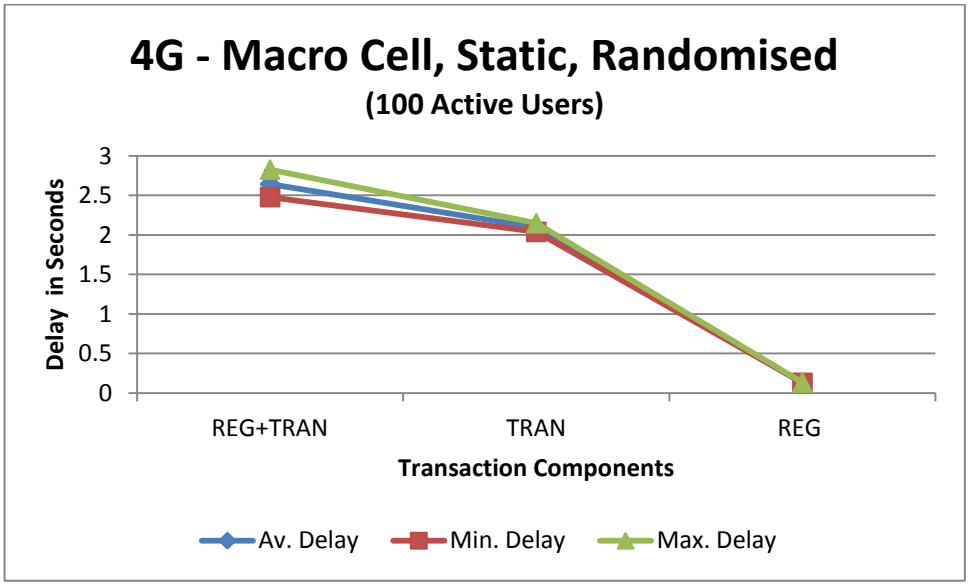


Figure 45: Transaction delay when 300 payer/payees were randomly initiated

network resources, traffic load and number of users, to ensure that the measurements made did not favour the payer or the payee.

The no-load measurements of the transaction delay for the three network configurations 3G UMTS, 4G micro cell and 4G macro cell are measured without any additional traffic on the network segments.

Fig 43 and 44 illustrate the no load delays on the 3G and 4G network segments, where the payer/payee are static and are mobile (“-Mo”). The

transaction delays on the 3G segment are close to 4 seconds. The total transaction delay, *i.e.*, REG+TRAN is 36.5% higher than the TRAN delay. The delays seem to be lesser when the payer/payee is mobile rather than when stationary. This is verified to be because of the random placement of the node, farther away from the base station. When loaded, the delays on the 3G network increases to an average of 12 seconds with a standard deviation of 12. In the case of 4G, the delays for REG+TRAN are around 475 ms except for the 4G-Micro-static case at 859 ms (due to the placement closer to the edge of the cell). Here, the REG+TRAN is almost 50 % higher than the TRAN delay.

Following these measurements, the delays for a random case were measured. For this, a sustained background load was initiated on the network and the number of payee/payer pairs transacting with each other were initiated randomly. Here again, the pairs were static and mobile.

The random initiation of the payer/payee pairs was done in the following

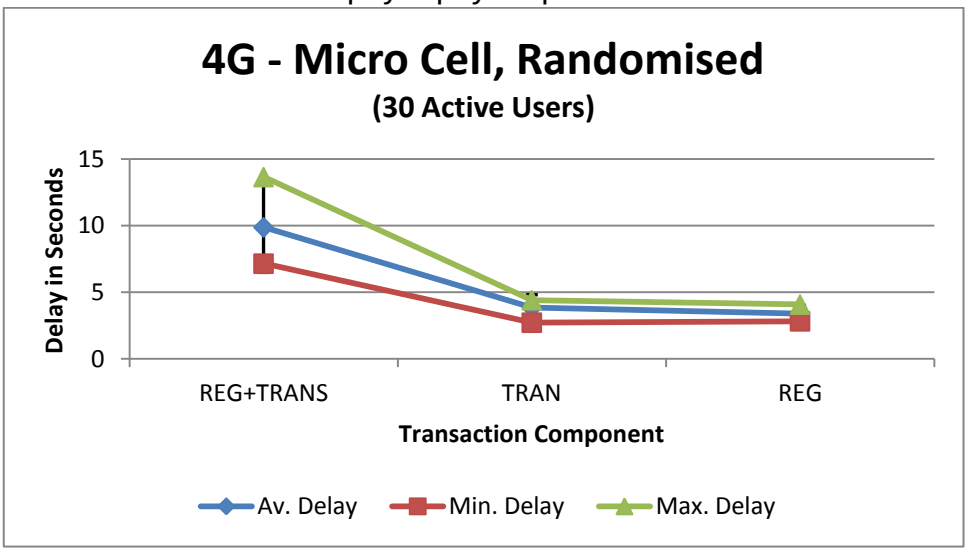


Figure 46: Transaction delay in 4G Micro cells when randomly initiated

manner. A random number between 250 to 350 was generated and an equal number of application processes were started. The process was repeated every five seconds over a five minute simulation run, giving a total of 60 invocations of the application groups of an average size of 300 payer/payee pairs. A similar randomisation was done for 4G Micro cell access with a random number range of 30 to 70 for an average application group of 50 payer/payee groups. Fig. 45 illustrates the delays for the various transaction components in a 4G macro cell where the payer/payee pairs are stationary. The REG+TRAN delays are consistent at about 2.5 seconds with a standard

deviation of 0.1745. The difference between REG+TRAN and TRAN is half a second.

When the payer/payee pairs are mobile within the macro cell the REG+TRAN delay is an average of 2.8 seconds with a standard deviation of 0.08. The difference between REG+TRAN and TRAN is 0.6 seconds.

In the case of micro cells, both the static as well as mobile case gave similar results with the REG+TRAN average delay at 3.17 seconds with a standard deviation of 0.48. The payer/payee pairs were then placed at the edge of the micro cells and the transaction delays were measured with the payer/payee nodes remaining stationary. The delays increased by a large extent with the REG+TRAN average delay at 9.87 seconds with a standard deviation of 3.37. Fig. 46 illustrates these delays. The difference between REG+TRAN and TRAN was about 6 seconds, which is a significant difference.

	Active App User Range	Inflection Point, delay	Average Delay	SD	(REG + TRAN) - TRAN	Av. Timeout %age
Micro Cell Static	0 - 70	30, 4.1 secs	6.1 secs	4.1	1.4 secs	55
Micro Cell Mobile	0 - 70	30, 4 secs	7 secs	4.3	1.8 secs	58
Macro Cell, Static	0 - 350	150, 0.9 sec	5 secs	5	2 secs	35
Macro Cell, Mobile	0 - 350	250, 1.8 secs	3.8 secs	5	1.2 secs	40

Table 34: Performance under load conditions in 4G Cells

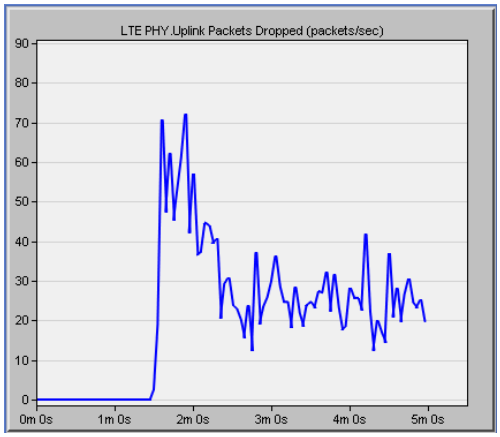


Figure 47: Packet drops on the uplink, under load

Following this, more extensive load tests were done. The performance of the protocol components were measured with increasing active user load. The traffic load was applied by increasing the number of active users in the cells. The traffic contribution per mobile node remained as earlier with 600 Kbps stream and http browsing with 100 Kbps, on-off. In the cases where the mobile nodes were stationary, the nodes were placed close to the cell edge. In the case where the nodes were mobile, the mobility path was along the cell edge in the case of macro cell and the mobility path was a crossover from one cell to the other and back, in the case of a micro cell. The micro cell user densities were varied from 10 active users to 70 active users in steps of ten and the macro cell user density was varied between 100 to 350 in steps of 50 active users. The delay for each of the transaction components were averaged over the series, after removing anomalies, other than transaction failures.

The performance under load varies with the load. Table 34 illustrates a summary of the various load tests performed. Column 3 indicates the point where the transaction delay begins to increase rapidly. In the case of a 4G micro cell, the transaction delay increases rapidly after the number of active users reaches 30, where the average delay is about 4 seconds. Recall that active users generate traffic load. The average transaction delay is between 6 to 7 seconds with a standard deviation of 4.1 to 4.3. The difference between a REG+TRAN transaction and only a TRAN transaction is 1.4 to 1.8 seconds. The average number of transactions that timed out after the inflection point is

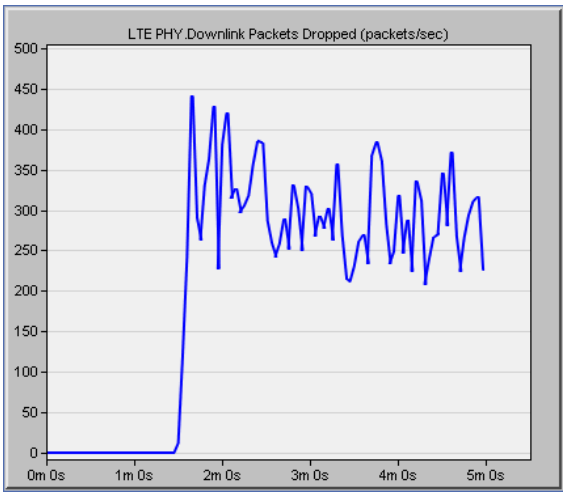


Figure 48: Packet drop rate on the downlink, under load

55 to 58%. The transaction performance for a macro cell is relatively better. Past the inflection point, the average delays are 5 and 3.5 seconds and 35 to 40 % of the transactions time out.

The standard deviation is somewhat high around 4 to 5, implying a range of ten seconds. The performance of the transaction under load is explained with reference to the packet drops on the uplink and the downlink of the 4G networks.

Fig 47 and 48 indicate the packet drop rate on the uplink and downlink that cause the transaction time outs during the load tests. The drops are due to the link buffers filling up due to the traffic load. The packets relating to the transaction arrive at these congested buffers and get dropped. If they get into the buffer without being dropped, they experience delays waiting in the service queue. It is these delays that add up to the transaction delay.

In summary, the load tests illustrate two things – that the transaction delay varies significantly with the increase in load and the average delays increase rapidly beyond the inflection point and that the difference between executing a REG and TRAN together does take more time than executing only a TRAN with the REG being done separately; the time difference is about 2 seconds. .

6.5 Comparison with other mobile payment protocols

There are a few references for payment protocol performance figures available in literature. Most of the references do not specifically term the payment protocol as a mobile payment protocol, although a mobile phone/ smart phone is used to make the payment.

Roehrs, A., da Costa, C. A., & Barbosa, J. L. V. (2012) provide measurements for the performance of their payment scheme 4IPay. However, they do not present any details in terms of the protocol data sizes and the encryption/decryption schemes they deploy. They report a total transaction time of 16.5 seconds on 3G at 144 Kbps and 22 seconds on EDGE at 88 Kbps. For phone to phone transfers, they report a time of 1.5 seconds for NFC, 3 seconds for Bluetooth and 2 seconds for WiFi based access. However, they do not report the device on which these measurements were made.

Balan et al., (2009) report for mFerio, a P2P system using asymmetric encryption, a total transaction time of 5.919 seconds. The user transaction (interaction) time is not reported as part of the transaction time. The measurements are made on a Nokia® 6131 NFC enabled mobile phone. No processor details are available.

Lukkari, J., Korhonen, J., & Ojala, T. (2004) report time of 7.19 for the ordering and payment process of which 4 is used for the payment. They do not mention the units of their measurement. It is assumed as seconds. These measurements are reported on several models of Nokia® smart phones used by the survey respondents.

Isaac, J. T., & Zeadally, S. (2013), in their implementation of PCMS, provide sufficient detail of the processes on the client side and indicate that the execution time for the payment protocol is 11.679 seconds and 1.09 seconds as the time taken to execute the merchant registration protocol. The total time for execution of the transaction is 13.58 seconds. The user interaction time is not considered in this study too. The measurements are made on a Nokia® N95 device with a 332 MHz dual CPU.

The implementation of PCMS (Isaac, J. T., & Zeadally, S. (2013)) is comparable to UMTES. The execution times are rather high compared to UMTES but that is due to the processor configuration of mobile phone used for their evaluation. The phone CPU, at 332 MHz, dual core, is far lower to a current day 1 GHz smart phone. Executing PCMS on a current day smart phone will give better results and a reduction of the payment transaction time by at least a factor of three (linearly scaling the encryption/decryption and hash generation based on the CPU speeds) and bring it closer to the UMTES transaction execution time of 169.39 ms.

Massoth, M., & Bingel, T. (2009) have compared end-to-end service times of a demo payment solution using different means of access and message the payment service, to make a payment. They demonstrate that the NFC application is the fastest and has a very little variance in the time. They observe a total transaction time of 22 seconds when the service is accessed via NFC.

In the case of UMTES, the variation in the transaction times is a result of the dynamic network conditions causing variations in RTT and consequently the network transit times. The simulation results indicate a performance range of 0.5 seconds to 1 seconds under no load conditions, 2.5 to 3 seconds when the load and the number of payer/payee pairs are increased and increases to an average of 4 seconds when the network is highly loaded with peak delays of about 7 seconds. When the payer/payee are located at the cell edge in a microcell, the delays increase to about 9.5 seconds.

The performance under normal load is considered for calculating the total transaction value. The total time spent in user actions which is part of the

payment process (ref. Table 30) is 26 seconds. The total time taken for a payment, under no load conditions will be (26+1) = 27 seconds, under increased load conditions will be (26+3) = 29 seconds to (26+4) = 30 seconds and with high loads (26+7) = 33 seconds and with high loads and at the edge of a micro cell (26+9.5) = 35.5 seconds. In the case of 3G, the total payment process amounts to (26+4) = 30 seconds and under load (26+12) = 38 seconds.

6.4 Comparison with Cash Payments

The scheme of mobile payment discussed thus far intends to be a feasible replacement for the cash payments. We compare it in terms of the total transaction time with other mobile payment mechanisms in literature.

The primary reference in literature is from the industry. The British Retail Consortium (BRC 2012), reports that the average time taken to process a cash payment at a PoS is 32 seconds, compared to 41 seconds for a card payment. The transaction time estimate of 26 seconds compares well with these observations. From the simulation results, the payment process time when using 3G vary between 30 seconds and 38 seconds and between 27 and 35.5 seconds when using a 4G network. Therefore, using mobile payments in place of cash payments, with real time settlements is feasible when compared to the metrics from BRC (2013).

In the case of the cash payment, the reduction is time is obviously due to the substitution of cash handling at the PoS by the mobile payment. However, in the case of the card transactions, the delays due to the interaction with the PoS, that is, the card swipe/s and entering the PIN are quite similar to the SWIPE and the payment request verification and clicking to pay, as part of the mobile payment transaction. Therefore, the delay is attributed to the card access network which is very often operated on a dial-up network. There are card payment devices which use data on mobile access as well.

6.5 Conclusion

This chapter dealt with a detailed evaluation of the UMTES implementation. First, an estimate of the transaction delay is made from the literature available. Following these estimates, the network delays are measured using the network simulation package. The delay measurements are based on the network configuration used for the estimates from literature.

The per command data size was considered to estimate, from literature, the total execution time of the protocol. To this, was added the network transit time. The complete transaction execution time was less than a second. The user interaction time estimate formed the bulk of the time taken. From a user perspective, once the payment request is approved, the transaction completion should be almost instantaneous. The network transit times estimated were for a 4G network. The total transaction estimated was 26 seconds. This is well below the industry observation of 32 seconds for a cash payment, at a PoS.

If the service were to be deployed on a 3G access network or a 3.5G access network, the total execution time of the transaction would be less than one second, although close. From a user perspective, the payment transaction would still be instantaneous.

The measurements from the simulation provided a more realistic estimate of the transaction delays. The delays on 3G were high at 4 – 12 seconds and those on 4G are from 1 to 8 seconds under various load conditions. The total payment process delays vary from 30 – 38 seconds for 3G and from 27 – 35 seconds for 4G.

Chapter 7
Conclusion

Mobile payments have been around for over a decade. They have not yet proliferated to the extent expected. There have been several reasons for the lack of proliferation from high learning curves for users to lack of standards to the security of paying using a mobile phone. In the meantime, two major mobile technologies will impact the proliferation – one being the transitioning of mobile network infrastructures to 4G technology which promises better coverage as well as WiFi like bandwidth to each mobile phone, and the other being the evolution of the Smart Phone. Mobile phones with multi core CPUs at 1 GHz and above, with dedicated GPUs as well as on-board sensors and scanners (bio-metric), termed as Smart Phones, have become common place.

The payments industry is also evolving. Non-banking organisations have begun providing financial services and in particular payment services. Such organisations intend to make mobile based interaction, including payments, as the preferred means of service delivery. Banks provide mobile banking services and have recently started person-to-person payments (low values) by addressing the payer and payee by their mobile phone numbers. Non-banking payment service providers, are recognised by the regulatory authorities. In addition, the European Central Bank has recognised the need and the role of non-banking payment service providers (PSP). They are termed as independent PSPs.

Independent PSPs manage the payment instruments of their customers, predominantly cards, by enabling them to have a single point of access for payment by cards. In addition, they provide a low value account based service, which is loosely termed as a wallet. Value is transferred to this account with the PSP from the primary sources of the user. The major benefit of this is an instant payment to other similar users of the same PSP.

Upon looking at industry statistics on the types of retail payments, it was found that cash transactions account for 28.93% of the total retail payments for 2012, amounting to £182 billion. By transaction volume, they accounted for 54.4% of the transactions. Essentially, all low value transactions were made with cash. The annual, average cost of cash collection to the retailer was 1.53 pence per transaction.

In this context, the motivation was to explore how the cash transactions can be converted to mobile payments and if it were feasible at all. Doing so would require that the transfer of value from the buyer to the seller must be immediate (like in a cash payment) and the costs of collection to the seller must be lower. In addition, the mobile payment mechanism must be simple, safe and secure, apart from being instantaneous. The payment service must be accessible everywhere and at all times.

This provided the motivation to set two broad objectives, with a focus on low value payments (typically, retail) – to provide a means of providing immediate transfer of value between two users on different PSPs and to ensure that the means provided remained simple, safe and secure. The immediate transfer of value will make the funds available to the user, instantly, rather than having to wait until after. Added to this, the means provided should not be too disruptive from a operational perspective, to a user. This should encourage adoption and hence proliferation of the service.

A literature review in Chapter 3 established the fact that the key impeding factors to adoption are the lack of standardised operations between the stakeholders in the emerging area of mobile payments. New market players, the independent PSPs, are a growing breed and there is a need to provide interoperable services between them before the market evolves into a near monopoly. The research goals were therefore - to evolve a service architecture upon the various stake holders in the market so that payment services, by themselves could be interoperable across all service providers, and a means for the interoperability, a protocol for enabling such a service. The protocol should support a service delivered via an application on a mobile device.

Mobile payments research has existed since just before the turn of the century and there has been substantial work in the area. The definition of mobile payments has evolved over the years and there is a reasonable consensus that a mobile device used to initiate, authorise or confirm a payment online will be termed as a mobile payment (§ 3.2.1).

The types of mobile payments is a widely studied topic. There are several ways of classifying mobile payments from different perspectives. Operationally, a hierarchical classification of mobile payments, have been proposed, where the types of payments are categorised under two categories – Remote payments and Proximity payments (§ 3.2.2).

Mobile devices have evolved in capabilities features and functions and present day mobile devices, particularly phones, are termed smart phones. They are increasingly becoming affordable. Likewise, the mobile network infrastructure is also evolving to provide high bandwidth, high throughput access to users. The focus of the work are smart phones which are becoming common place (§ 3.3.3). This adds to the design considerations of UMTES.

A look at the Mobile Payment standards and consortiums indicate an evolution in progress. Several players are introducing mobile payment based services but cater to their own subscribers. Banks are in the game with m-banking services which also provides payment services. Clearly, the user need is to have a single payment service which can manage all the payments, regardless of the payment instrument, which predominantly, is card based. The work does not include a focus on B2B payments but limits itself to P2* payments (§ 3.5.1). This impacts the design of UMTES.

Mobile payment service adoption problems have been discussed from both the buyer and seller perspectives – user operability to revenue sharing models to security. What emerges is that the user expects to have a secure, speedy and simple service, in that order (§ 3.5.2 to § 3.5.4). These requirements form the primary design requirements of UMTES.

7.1 Achievements

The work has achieved the objectives it has set out to achieve. Recall that the objectives were to provide a safe, simple and speedy mobile payment mechanism and to make the payments interoperable across PSPs so that transfer of value between them are instantaneous. The intent was to serve the cash payments segment and have these payments made using mobile devices.

UMTES is provided as a solution for interaction with PSPs as well as between PSPs. The settlement function, that transfers value between the PSPs is a part of the basic protocol. Therefore, inter-PSP value transfers are immediate and the payee will have access to the transferred funds, instantly.

UMTES is designed to be safe and speedy with minimal protocol messages which are short and carry information securely. A user always receives a payment request only via her/his own PSP and no one else. All monetary information is communicated only to the PSP and never to the payee, in any form. So, the anonymity of the cash transaction is retained. The overall

payment process mimics a card payment process with a swipe at the PoS. This is done to help faster and easier user acceptance.

UMTES is generic enough to be extendible, functionally, to accommodate cash back at a PoS, payments using cards, loyalty discounts, vouchers and other payment instruments. Most of these extensions fall into the PSP side implementations which contain the user profile and the user card information, bank access details and so on.

UMTES is extendible to accommodate remote payments too. The context of payments at PoS and/or a vending machine or a automatic dispensing machine are all considered as local payments. Remote payments include instances of the PoS being online as in an online store.

When UMTES is implemented as an Application Programming Interface (API),it can be integrated into any application. Therefore, the services can be extended to several other devices that may require to execute a payment for on-demand services, such as for Video-on-Demand on a TV or a set-top box, for other pre-paid services such as power from the smart grid on a smart meter and so on. In addition it can potentially be used as a “scheme” in a Uniform Resource Identifier (URI) which is used to indicate the resource of the payment service provider. An example would read **`umtes://psp1.co.gb/`**. This could be used in contexts of remote payment.

UMTES addresses transaction speed in two ways. First, it exchanges minimal data necessary for the transaction and secondly, it deploys symmetric key cryptography for data privacy. The application data unit sizes do not exceed the typical maximum transmission unit (MTU) of the wireless interface on the mobile device which is typically 1500 bytes. The maximum size of an IP packet with the application data is 432 bytes. So, each data exchange is only one IP packet between the end points. This helps to keep the total transit time on the network to less than a second for the whole transaction (§ 6.3.2). Using symmetric key based encryption and decryption reduces the total time taken for data privacy. This ensures that the data processing delays at the client are minimal, during the course of a transaction.

7.2 Contributions

The service architecture design in chapter 4, the protocol implementation in chapter 5 and its evaluation in chapter 6 are the major contributions of the thesis.

The service architecture design clearly identifies the functional elements of the payment service and the interactions between them. The functional elements are grouped by their service function and also reflect the stakeholder ownership. This view of the payment service, in the context of independent PSPs is the initial contribution based on which the rest of the work is developed.

The protocol implementation conforms with the scope of the service defined in the chapter. The implementation provides a framework for making a payment while keeping the identity of the payer from exposure to the payee. The payment instances illustrate the flexibility of the protocol implementation and its extendibility to adapt to various payment scenarios.

The evaluation of the implementation provides a guide to estimating the performance of a protocol. The estimate provides an idea of the performance of the solution as a precursor to a simulation study or an implementation.

Following the estimation, the protocol performance measurements are made on a simulated network. These measurements indicate the feasibility of the use of the protocol on practical networks. The network delays which form a critical component of the transaction delays are measured on the simulated network. The high load conditions that are simulated on the network provide an idea of the worst case performance of the protocol.

7.3 Limitations

While this study addresses the need for a means for mobile payments in the evolving market, there are exclusions and limitations of the solution. The limitations are both, in terms of scope and in terms of the implementation provided in this study. The exclusions and limitations are summarised as paragraphs below and they provide a lead for the future work and improvements of UMTES.

They exclusions are mentioned below:

1. This study has addressed one specific area of payments which are executed via mobile devices – retail payments. These payments are mostly in the context of low value payments. Within the focus area the protocol serves to provide the payment function. As such, it excludes the larger domain of B2B payments.
2. The model of payments is limited to an account based model causing all communication between the payer and the payee to go via the PSP. There is no direct communication between the payer and payee. The

availability of connectivity, everywhere, with 4G is the basis of the adoption of this model. Pico cells and micro cells, along with WiFi are expected to provide connectivity everywhere. P2P payments are also routed via the PSP. This is in contrast to various schemes in literature where P2P payments are performed directly from the payer to the payee without the intervention of a third party.

3. The concept of payments is limited to making a payment on a payment request. The payer decides whether to pay based on the details in the payment request, in a given context. This implies that the order information and/or details of the order are not exchanged between the payer and payee, as in the case of the SET protocol. A reference is exchanged merely for the purpose of tracking, where necessary.
4. The implementation addresses inter-PSP interoperability and low value, instant settlements. Regulation in the financial services and banking industry does not yet permit/address such direct settlements by non-banking organisations.
5. In the context of smart cities, most services are expected to be on-demand. Such services would require payments to be made online and in real time. While UMTES is capable of providing such a service, the aspects of integration into various services via service interfaces has yet to be explored.
6. In a more generic context, integrating UMTES into various smart devices that require a payment function, such as smart meters, TVs, set top boxes, etc. needs to be explored.

The implementation has a few limitation and they are mentioned in the paragraphs below.

1. The protocol implementation limits itself to exchanging identity information and payment details. The focus of the implementation is to keep the data exchange as low as possible to make real time payments with settlements, feasible. The implementation does not have the means for extending the protocol data, should there be a need to, when extending/adapting it to a larger scope of payments.
2. The number of steps involved in the protocol exchange follow a traditional “initiate-authorise-confirm” pattern. Since the origin of the payment request is verified before it reaches the payer, the whole exchange could be turned into a single-click process, rather than multiple steps. While the number of steps are more, they do not require user interaction and therefore do not delay the transaction.

3. The implementation is simplistic. Any potential error condition such as repeated time outs, data integrity errors or out-of-sequence protocol commands cause the transaction to abort. The payment transaction needs to be re-initiated with a payment request. While repeated time outs may be highly uncommon, out-of-sequence protocol commands could occur in the event of a man-in-the-middle attack or a similar attack with malicious intent. In such cases, attacks could potentially abort all payment transactions causing a denial-of-service.
4. The security scheme and elements of the security administration are left as the role of the TSM and not elaborated upon. Therefore, the details of the key exchange or key generation mechanisms are not discussed but assumed that the keys are available to perform data integrity checks.
5. TCP is used as a transport protocol for the implementation. While the protocol provides guaranteed delivery, it is primarily meant for services which have larger data payloads and protocol interactions that involve a large transport of data. The nine UMTES data exchanges are typically one packet each way with a total of thirteen packets. UDP, as a transport protocol could meet the functional needs without delay overheads such as connection establishment and memory overheads since it is a stateless protocol.
6. The choice of SSL as a protocol for end-to-end security is from an industry standpoint. Several existing secure services in the financial industry use SSL. However, IPSEC between the client and the server could serve a similar purpose. IPSEC implementations are expected to be less compute intensive when compared to SSL or TLS.

7.4 Future Work

This study has raised several issues, apart from its own focus area and limitations. They are listed here as potential for future research. Following this, additional investigations using the work in this study, are proposed.

While there is substantial research in literature on various means of implementing mobile payments and protocols, there is no strategy discussed for users to transition from their existing experience of mobile banking or card based services to an effective mobile payment solution. Such a study will enable proliferation of mobile payments as a whole, regardless of the sector of payments they address, be it P2P, P2B or B2B.

Bank accounts are the primary source of an individual's funds and the basis of eligibility for credit, that enables the credit card business. However, the banks, because of regulatory limitations, are yet unable to make immediate settlements for low value payments feasible and implement them. The impact of this is that the volume of low value payments that amount to 54.4% of the UK's retail transactions, remain high with a substantial cost of collection to the merchant. Whether it only a regulatory impediment to provide instant settlements or one related to transaction costs requires investigation.

The Banking and Financial services regulations are, although beginning to open up, not yet assistive of innovative services by new PSPs. A study on the regulatory aspects which could detail the risks of instant settlements and the limits on the value of such instant settlements would be useful.

From the perspective of the implementation and evaluation in this study, the following are proposed for future work:

A detailed cost analysis of the implementation is necessary to understand the implications and feasibility of substituting the implementation for cash payments.

A study on the acceptability of the implementation against a well known acceptability model such as the Nielsen model will illustrate the degree of acceptability of the solution. This could encourage coders to implement this mobile payment solution.

An additional simulation study of the usage scenarios using formal modelling techniques for increasing the user density (user arrivals) in the 4G cells. Such a study will be able to analyse the performance of UMTES, thoroughly. In addition to this, the performance of UMTES on different 3G access technologies such as EVDO, EDGE, HSPA. Such a study will fine grain the performance of the application protocol. Similar tests can be done to check the performance on GPRS and EGPRS to understand the feasibility of using the protocol on 2.5G network access.

Finally, a coded implementation of the UMTES would demonstrate the use of UMTES in full, its functionality, its simplicity and its speed of operation.

References

Abdel-Hamid, A.A.; Badawy, O.; Bahaa, S. (2012), PA-SET: Privacy-aware SET protocol, International Conference on Computer Theory and Applications (ICCTA), 2012, 22nd

ABEDI, Leila; NEMATBAKHSH, Mohammad Ali ABDOLMALEKI, Abbas (2012). *A Model for Context Aware Mobile Payment. J. theor. appl. electron. commer. res. [online]. 2012, vol.7, n.3, pp. 1-10. ISSN 0718-1876.*

Allee V (2011), Value Networks and the true nature of collaboration, ValueNet Works and Verna Allee Associates, http://www.valuenetworksandcollaboration.com/home/tableofcontents.html , Accessed 20/09/13

Alsedairy, T., Qi, Y., Imran, A., Imran, M. A., & Evans, B. (2013). Self Organising Cloud cells: A Resource Efficient Network Densification Strategy, http://qson.org/download/2014-ETT-Self Organising Cloud cells A Resource Efficient Network Densification Strategy.pdf

Andrews, J.G. (2013), Seven Ways that HetNets Are a Cellular Paradigm Shift, IEEE Communications Magazine, March 2013, pp 136-144

Au, Y. A., & Kauffman, R. J. (2008). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. Electronic Commerce Research and Applications, 7(2), 141-164.

Balan, R. K., Ramasubbu, N., Prakobphol, K., Christin, N., & Hong, J. (2009, June). mFerio: the design and evaluation of a peer-to-peer mobile payment system. In *Proceedings of the 7th international conference on Mobile systems, applications, and services* (pp. 291-304). ACM.

Bernstein & Newcomer (2009). Principles of Transaction Processing, ISBN 9781558606234, Morgan Kaufmann

BII Report (2012). BII REPORT: Why Mobile Commerce Is Set To Explode. Business Insider, Available from: http://www.businessinsider.com/bii-report-why-mobile-commerce-is-set-to-explode-2012-12#ixzz2LtcXEaPx[Accessed 15 April 2013].

Bollen, R. (2013), The Legal Status of Online Currencies: Are Bitcoins the Future? (May 1, 2013). Journal of Banking and Finance Law and Practice

(2013). Available at SSRN: http://ssrn.com/abstract=2285247

Bradford, A. (2003), Consumers Need Local Reasons to Pay by Mobile, Gartner. Available: http://www4.gartner.com/DisplayDocument?doc_cd=115603, Accessed 15 April 2013].

BRC (2012), Cost of Payment Collection Report 2012, British Retail Consortium, London

Brito, J., & Castillo, A. (2013). Bitcoin: A primer for policymakers. Mercatus Center at George Mason University.

Buhan, D., Cheong, Y. C. & Tan, C. (2002), Mobile Payments in M-Commerce, Telecom Media Networks. Available: http://www.capgemini.com/tme/pdf/ MobilePaymentsinMCommrce.pdf, Accessed 15 April 2013.

Canalys (2013), Mobile device market to reach 2.6 billion units by 2016, February 2013, http://www.canalys.com/newsroom/mobile-device-market-reach-26-billion-units-2016, Accessed 20/09/13

Carton, F, Hedman, J, Dennehy, D, Damsgaard, J, Tan, K and McCarthy, J, B (2012)*. "Framework for Mobile Payments Integration" The Electronic Journal Information Systems Evaluation Volume 15 Issue 1 2012, (pp14 - 25)*

Chaix, L., & Torre, D. (2011). Four models for mobile payments. University Nice Sophia-Antipolis, JEL Classification: E42, O33, February 2011.

Chaix, L; Torre, D (2012) : Which economic model for mobile payments?, 23rd European Regional Conference of the International Telecommunication Society, Vienna, Austria, 1-4 July 2012

Chaix, Laetitia; Torre, Dominique (2012) *: Which economic model for mobile payments?, 23rd European Regional Conference of the International Telecommunication Society, Vienna, Austria, 1-4 July 2012*

Chakraborty, A., & Das, S. (2013, June). Adapp: an adaptive network selection framework for smartphone applications. In *Proceeding of the 2013 workshop on Cellular networks: operations, challenges, and future design* (pp. 7-12). ACM.

Chen, Y. C., Nahum, E. M., Gibbens, R. J., & Towsley, D. (2012a) *Measuring Cellular Networks: Characterizing 3G, 4G, and Path Diversity*.

UMass Amherst Technical Report: UM-CS-2012-022.

Chen, Y. C., Nahum, E. M., Towsley, D., & Liu, C. (2013) On Uplink Measurement of Cellular Networks for Mobile Multi-Path TCP, UMass Amherst Technical Report: UM-CS-2013-027.

Chen, Y. C., Lim, Y. S., Gibbens, R. J., Nahum, E. M., Khalili, R., & Towsley, D. (2013a). A Measurement-based Study of Multipath TCP Performance over Wireless Networks. In *Proceedings of the 2013 conference on Internet measurement conference* (pp. 455-468). ACM.

Chen, Y. C., Towsley, D., Nahum, E. M., Gibbens, R. J., & Lim, Y. S. (2012b). Characterizing 4G and 3G networks: Supporting mobility with multipath TCP. *School of Computer Science, University of Massachusetts Amherst, Tech. Rep*, *22*.

Choi, Y. B., Crowgey, R. L., Price, J. M., & VanPelt, J. S. (2006). The state-of-the-art of mobile payment architecture and emerging issues. International Journal of Electronic Finance, 1 (1), 94-103.

Comparison of smartphones. (2014). In *Wikipedia, The Free Encyclopedia*. Retrieved 08:18, May 23, 2014, from http://en.wikipedia.org/w/index.php?title=Comparison_of_smartphones&oldid=609475161

CPSS (1999), RETAIL PAYMENTS IN SELECTED COUNTRIES: A COMPARATIVE STUDY, Committee for Payment and Settlement Systems, Bank for International Settlements (BIS), September 1999, http://www.bis.org/publ/cpss33.htm, Accessed 21/10/2013

Crowe M (2012), Federal Reserve Bank of Boston), Mobile Payments & Technology Landscap*e, Presentation at NCUA IS&T SME Conference, September 13, 2012, downloaded from http://www.bos.frb.org/bankinfo/payment-strategies/presentations/2012/crowe9-13-2012.pdf, Accessed 20 August, 2013*

Dahlberg, T., Mallat, N., Ondrus, J., & Zmijewska, A. (2008). Past, present and future of mobile payments research: A literature review. Electronic Commerce Research and Applications, 7 (2), 165-181.

Danzeisen, M., Braun, T., Steiner, I., & Rodellar, D. (2005, June). On the benefits of heterogeneous networking and how cellular mobile operators can help. In Parallel Processing, 2005. ICPP 2005 Workshops. International Conference Workshops on (pp. 366-371). IEEE.

Dent, A., & Dison, W. (2012). The Bank of England's Real-Time Gross

Settlement infrastructure. *Bank of England Quarterly Bulletin*, *52*(3).

Dewan, S. G., & Chen, L. (2005). Mobile Payment Adoption in the USA: A cross industry, cross-platform solution. Journal of Information Privacy & Security, 1(2), 4-28.

Duda, S., Schiessl, M. & Hess. J. M. (2002), Mobile Usability, Eye Square. Available: http://www.eye-square.de/dokumente/mobile-usability-eyesquare-english.pdf , Accessed 15 April 2013.

ECB (2013), Recommendations for the security of internet payments, European Central Bank, January 2013

Enck, W., Ongtang, M., & McDaniel, P. D. (2009). Understanding Android Security. *IEEE security & privacy*, *7*(1), 50-57.

EPC 220-08 (2010), Trusted Service Manager Service Management Requirements and Specifications, Doc: EPC 220-08, Version 1.0, January 2010, http://www.gsma.com/mobilecommerce/wp-content/uploads/2012/03/epcgsmatsmwpv1.pdf, Accessed 10/09/13

EPC 492-09 (2012), White Paper Mobile Payments, EPC 492-09, Version 4, October 2012, European Payments Council, http://www.europeanpaymentscouncil.eu/knowledge_bank_download.cfm?file=EPC492-09%20White%20Paper%20Mobile%20Payments%20-%20edition%20October%202012.pdf, Accessed 10/09/13

EPC (2013), European Payments Council. SEPA Direct Debit Transfer scheme rulebook.

ECB (2011), EUROSYSTEM OVERSIGHT POLICY FRAMEWORK, July 2011, European Central Bank, http://www.ecb.int/pub/pdf/other/ eurosystemoversightpolicyframework2011en.pdf, Accessed 26 July 2013,

F. Egger and D. Abrazhevich, (2001)*, "Security & Trust: Taking Care of the Human Factor," Electronic Payment Systems Observatory Newsletter, vol. 9, 2001*

Flatraaker, D. I., (2008). Mobile, internet and electronic payments: The key to unlocking the full potential of the internal payments market. Journal of Payments Strategy & Systems, 3(1), 60 – 70.

Freier, A., Karlton, P., & Kocher, P. (2011). The secure sockets layer (SSL) protocol version 3.0., RFC 6101, Internet Society

FSA (2013), A Review of Requirements for Firms Entering or Expanding in the Banking Sector,

http://www.bankofengland.co.uk/publications/Documents/joint/barriers.pdf, Accessed 07/11/13

Ganchev, I., & O'Droma, M. (2007). New personal IPv6 address scheme and universal CIM card for UCWW. In *Telecommunications, 2007. ITST'07. 7th International Conference on ITS* (pp. 1-6). IEEE.

Gopinath, S. (2009), Retail Payment Systems, Select Issues, BIS Papers, (Regional Seminar for Payment Systems, India, RBI & BIS), March, 2009

Gille, D (2005), A TRANSACTION COST ANALYSIS OF MICROPAYMENTS IN MOBILE COMMERCE, Journal of information and organizational sciences, Volume 29, Number 1 (2005)

Haider, F., Dianati, M., & Tafazolli, R. (2011). A simulation based study of Mobile Femtocell assisted LTE networks. In Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International (pp. 2198-2203). IEEE.

Hartmann, M. E. (2006). E-payments evolution. In Handbuch E-Money, E-Payment & M-Payment (pp. 7-18). Physica-Verlag HD.

Huang, J., Qian, F., Gerber, A., Mao, Z. M., Sen, S., & Spatscheck, O. (2012). A close examination of performance and power characteristics of 4G LTE networks. In *Proceedings of the 10th international conference on Mobile systems, applications, and services* (pp. 225-238). ACM.

Isaac, J. T., & Zeadally, S. (2013). Design, implementation, and performance analysis of a secure payment protocol in a payment gateway centric model. *Computing*, 1-25.

Isaac, J. T., & Zeadally, S. (2013). Design, implementation, and performance analysis of a secure payment protocol in a payment gateway centric model. *Computing*, 1-25.

Isaac, J.T.; Camara, J.S. (2007a), Anonymous Payment in a Client Centric Model for Digital Ecosystems, Digital EcoSystems and Technologies Conference, 2007. DEST '07. Inaugural IEEE-IES , vol., no., pp.422,427, 21-23 Feb. 2007

Isaac, J.T.; Camara, J.S. (2007b), An Anonymous Account-Based Mobile Payment Protocol for a Restricted Connectivity Scenario, Database and Expert Systems Applications, 2007. DEXA '07. 18th International Workshop on , vol., no., pp.688,692, 3-7 Sept. 2007

ISO 13616 (2007), ISO 13616-1:2007 Financial services — International bank account number (IBAN) — Part 1: Structure of the IBAN.

International Organization for Standardization

ISO 13616 (2007), ISO 13616-1:2007 Financial services — International bank account number (IBAN) — Part 1: Structure of the IBAN. International Organization for Standardization

ISO 7812 (2006), ISO/IEC 7812-1:2006 Identification cards -- Identification of issuers -- Part 1: Numbering system

ISO 7812 (2006), ISO/IEC 7812-1:2006 Identification cards -- Identification of issuers -- Part 1: Numbering system

ITU (2013), ICT Facts and Figures, The World in 2013, International Telecommunication Union, http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf, Accessed 20/09/13

Iyer et al, (2013). Small Cells, Big Challenge, IXIA, http://hetnet.ixiacom.com/

Janne Lukkari, Jani Korhonen, and Timo Ojala. (2004), "SmartRestaurant – Mobile Payments in Context-Aware Environment, in Proceedings of the 6th international conference on Electronic commerce (ICEC '04), New York, NY, USA, 2004, pp. 575-582

Jelassi, T., & Enders, A. (2005). Strategies for e-business: Creating value through electronic and mobile commerce. Financial Times/Prentice Hall.

H. Jiang, Y. Wang, K. Lee, and I. Rhee. (2012) Tackling bufferbloat in 3G/4G networks. In Proceedings of the 2012 ACM SIGCOMM conference on Internet Measurement Conference (IMC), 2012

Karnouskos, S. (2004). Mobile payment: a journey through existing procedures and standardization initiatives. Communications Surveys & Tutorials, IEEE, 6 (4), 44-66.

Kilpi, J., & Lassila, P. (2005). Statistical analysis of RTT variability in GPRS and UMTS networks (Vol. 6). Technical report, VTT and TKK, http://www. netlab. hut. fi/tutkimus/pannet/publ/rtt-report.pdf.

Kim, C., Tao, W., Shin, N., & Kim, K. S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. Electronic Commerce Research and Applications, 9 (1), 84-95.

Kountz, E. (2010): A crossroads For NFC Mobile Payments. Cambridge: Forrester, 2010

Kousaridas, A., Parissis, G., & Apostolopoulos, T. (2008). An open financial services architecture based on the use of intelligent mobile devices. Electronic Commerce Research and Applications, 7 (2), 232-246.

Kreyer, N., Pousttchi, K. & Turowski, K. (2002), Standardized Payment Procedures as Key Enabling Factor for Mobile Commerce, University of Augsburg. Available: http://www.forsip.de/download/publikationen/sipkis/wi-118.pdf [Accessed 15 April 2013].

Kreyer, N., Pousttchi, K. & Turowski, K. (2002), Standardized Payment Procedures as Key Enabling Factor for Mobile Commerce, University of Augsburg. Available: http://www.forsip.de/download/ publikationen/sipkis/wi-118.pdf, Accessed 15 April 2013.

Lim, A. S. (2005). Pre-standardisation of mobile payments: negotiations within consortia. In Mobile Business, 2005. ICMB 2005. International Conference on (pp. 392-399). IEEE.

Linck, K., Pousttchi, K., & Wiedemann, D. G. (2006). Security issues in mobile payment from the customer viewpoint.

llya Grigorik. (2013). Mobile Networks. In: llya Grigorik *High Performance Browser Networking*. California: O'Reilly Media.

LTE Small Cell v.s. WiFi User Experience, (2013), Huawei, http://www.huawei.com/ilink/en/download/HW_323974

Lukkari, J., Korhonen, J., & Ojala, T. (2004). SmartRestaurant: mobile payments in context-aware environment. In *Proceedings of the 6th international conference on Electronic commerce* (pp. 575-582). ACM.

Mallat, N. & Tuunainen, V. K.(2008). Exploring Merchant Adoption of Mobile Payment Systems: An Empirical Study. e-Service Journal 6(2), 24-57. Indiana University Press. Retrieved September 26, 2013, from Project MUSE database.

Markendahl, J., Smith, M., & Andersson, P*. (2010). Analysis of roles and position of mobile network operators in mobile payment infrastructure.*

Massoth, M., & Bingel, T. (2009). Performance of different mobile payment service concepts compared with a NFC-based solution. In *Internet and Web Applications and Services, 2009. ICIW'09. Fourth International Conference on* (pp. 205-210). IEEE.

McKitterick, D. (2003). A Web Services Framework for mobile payment

services., Master thesis in university of Dublin , September 2003.

Mellios, E., Hilton, G. S., & Nix, A. R. (2013). Ray-tracing urban picocell 3D propagation statistics for LTE heterogeneous networks. In Antennas and Propagation (EuCAP), 2013 7th European Conference on (pp. 4015-4019). IEEE.

Murugesan, R. K., & Ramadass, S. (2010). A Multipurpose global passport solution using IPv6. In *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on* (Vol. 9, pp. 405-407). IEEE.

Naskooskov, (2010) .TLS Overhead. *netsekure rng RSS*. Retrieved March 20, 2014, from http://netsekure.org/2010/03/tls-overhead/

Networld Media Group, (2013), Mobile Payments State of the Industry 2014, http://www.networldmediagroup.com/inc/sdetail/12036/15591, Accessed 21/09/13

Northstream (2002), Mobile Payments: Key Aspects for Launching Successful Service. Available: http://www.northstream.se/download/ mpayment.pdf [Accessed 15 April 2013].

Ondrus, J. (2003), Mobile Payments: A Tool Kit for a Better Understanding of the Market, University of Lausanne. Available: http://www.hec.unil.ch/jondrus/files/papers/

Ondrus, J., & Pigneur, Y. (2006). Towards a holistic analysis of mobile payments: A multiple perspectives approach. Electronic Commerce Research and Applications, 5 (3), 246-257.

Ondrus, J., & Pigneur, Y. (2006). Towards a holistic analysis of mobile payments: A multiple perspectives approach. Electronic Commerce Research and Applications, 5(3), 246–257.

Ondrus, J., & Pigneur, Y. (2006). A multi-stakeholder multi-criteria assessment framework of mobile payments: An illustration with the swiss public transportation industry. In System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on (Vol. 2, pp. 42a-42a). IEEE.

Ondrus, J., & Pigneur, Y. (2006). A systematic approach to explain the delayed deployment of mobile payments in Switzerland. In Mobile Business, 2006. ICMB'06. International Conference on (pp. 6-6). IEEE.

Parth Amin, Nadew Sikuwaru, Edward Mutafungwa, Beneyam B. Haile and Jyri Hämäläinen, (2014) Performance Study for Small Cell

Deployments in Densely Populated Informal Settlements , The Fifth Nordic Workshop on System and Network Optimization for Wireless**,** http://snow.itn.liu.se/asbtr/12-parth-SNOW_MultiRAT_Small_Cells_v2.pdf

PSUK (2013), Payment Systems in the United Kingdom*, Accessed 26 July 2013, http://www.bis.org/cpss/**pay**sys/**UnitedKingdom**Comp.pdf*

PCI-DSS (2013), PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users Version 1, February 2013, PCI Standards Council, https://www.pcisecuritystandards.org/documents/ Mobile_Payment_Security_Guidelines_Merchants_v1.pdf, Accessed 21/09/13

Piro, G., Grieco, L. A., Boggia, G., Capozzi, F., & Camarda, P. (2011). Simulating LTE cellular systems: an open-source framework. Vehicular Technology, IEEE Transactions on, 60(2), 498-513.

Poeplau, S., Fratantonio, Y., Bianchi, A., Kruegel, C., & Vigna, G. (2014). Execute this! analyzing unsafe and malicious dynamic code loading in android applications. In *NDSS* (Vol. 14, pp. 23-26).

Pousttchi, K. (2003). Conditions for acceptance and usage of mobile payment procedures

Pousttchi, K., Schiessler, M., & Wiedemann, D. G. (2009). Proposing a comprehensive framework for analysis and engineering of mobile payment business models. Information Systems and E-Business Management, 7(3), 363-393.

Pousttchi, K.; Schiessler, M.; Wiedemann, D.G (2007)., "Analyzing the Elements of the Business Model for Mobile Payment Service Provision," Management of Mobile Business, 2007. ICMB 2007. International Conference on the , vol., no., pp.44,44, 9-11 July 2007

R. Balan, N. Ramasubbu, K. Prakobphol, N. Christin, and J. Hong. (2009), mFerio: The Design and Evaluation of Peer-to-Peer Mobile Payment System," in Proceedings of the 7th international conference on Mobile systems, applications, and services (MobiSys '09), New York, NY, USA, Poland, June 2009, pp 22-25

Rahimian, V., & Habibi, J. (2008). MPaySmart: A Customer Centric Approach in Offering Efficient Mobile Payment Services. In Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE (pp. 1038-1043). IEEE.

RBI-AU (2012), Payments System Architecture, Strategic Review of Innovation in the Payments System: Conclusions,

http://www.rba.gov.au/payments-system/reforms/strategic-review-innovation/conclusions/payments-system-architecture.html, Accessed 2/10/13

Rifa-Pous, H., & Herrera-Joancomartí, J. (2011). Computational and energy costs of cryptographic algorithms on handheld devices. *Future internet*, *3*(1), 31-48.

Rochet J; Tirole J., (2006), Two-Sided Markets: A Progress Report, 35 RAND J. ECON. 645

Roehrs, A., da Costa, C. A., & Barbosa, J. L. V. (2012). A Proposal of a Mobile Payment System Based on Android. In *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on* (pp. 617-622). IEEE.

S. Chari, P. Kermani, S. Smith, and L.Tassiulas,(2000), *"Security Issues in M-Commerce: A Usage-Based Taxonomy," in E-Commerce Agents: Marketplace Solutions, Security Issues, and Supply and Demand, J. Liu and Y. Ye, Eds. Berlin: Springer, 2000, pp. 264-282.*

S. Kungpisdan, B. Srinivasan, P.D. Le. (2003), A practical framework for mobile mobile SET payment, in: Proceedings of the IADIS International ESociety Conference, Lisbon, Portugal, June 3–6

S. Kungpisdan, B. Srinivasan, P.D. Le. (2004a), Accountability logic for mobile payment protocols, in: Proceedings of the IEEE International Conference on Information Technology: Coding and Computing (ITCC), Las Vegas, NV, USA, April 5–7

S. Kungpisdan, B. Srinivasan, P.D. Le. (2004b), A secure account-based payment protocol, in: Proceedings of the IEEE International Conference on Information Technology: Coding and Computing (ITCC), Las Vegas, NV, USA, April 5–7

Seah, W., Pilakkat, S., Shankar, P., Tan, S. K., Roy, A. G. & Ng, E. (2001), The Future Mobile Payments Infrastructure- A Common Platform for Secure M-Payments, Institute for Communications Research, Systems @Work Pte. Ltd. Available: http://www.itu.int/ITU-D/pdf/4597-13.3bis-en.pdf [Accessed 15 April 2013].

Shedid, S.M. (2010), Modified SET protocol for mobile payment, Networked Computing and Advanced Information Management (NCM), Sixth International Conference on , vol., no., pp.385,389, 16-18 Aug. 2010

Shedid, S.M.; Kouta, M. (2010), Modified SET protocol for mobile payment: An empirical analysis, Software Technology and Engineering

(ICSTE), 2010 2nd International Conference on , vol.1, no., pp.V1-350,V1-355, 3-5 Oct. 2010

Shin, Y., Gupta, M., & Myers, S. (2009). A Study of the Performance of SSL on PDAs. In *INFOCOM Workshops 2009, IEEE* (pp. 1-6). IEEE.

Shneiderman, B. (2000)*, "Designing Trust into Online Experiences "Communications of the ACM, vol. 43, pp. 34-40, 2000.*

Slade, E. L., Williams, M. D., & Dwivedi, Y. K. (2013). Mobile payment adoption: Classification and review of the extant literature. *The Marketing Review*, *13*(2), 167-190.

Sundaresan, K., Arslan, M. Y., Singh, S., Rangarajan, S., & Krishnamurthy, S. V. (2013). FluidNet: a flexible cloud-based radio access network for small cells. In Proceedings of the 19th annual international conference on Mobile computing & networking (pp. 99-110). ACM.

Technavio (2012), Global Smartphones Market 2012 – 2016, June 2013, http://www.technavio.com/report/global-smartphones-market-2012-2016, Accessed 26 July 2013

TPC, (2014), TPC-E – All Results, Version 1 Results, Transaction Processing Performance Council, http://www.tpc.org/tpce/results/tpce_results.asp, Accessed 20 April 2014

Tripathi, D.M. (2011), A note on modified SET protocol for mobile payment, Internet Technology and Secured Transactions (ICITST), 2011 International Conference for , vol., no., pp.639,641, 11-14 Dec. 2011

Tripathi, D.M.; Ojha, A. (2012), LPMP: An efficient lightweight protocol for mobile payment, Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on , vol., no., pp.41,45, 30-31 March 2012

Trusted Computing Group (2011), Mobile Trusted Module 2.0 Use Cases, Version 1.0, 4 March 2011

UKPC (2012), Annual Report 2012, UK Payments Council, http://www.paymentscouncil.org.uk/files/payments_council/publications/pc-annual-review-final.pdf, Accessed 12/09/2013

UKPC (2013), Countdown starts to Mobile Payments for all, Press release, UK Payments Council, http://www.paymentscouncil.org.uk/ media_centre/ press_releases/-/page/2378/, Accessed 12/12/13

Urien, P. (2013) NFC Technologies for the Internet Of Things**,** Presentation at SMART 2013, Rome, http://www.iaria.org/ conferences2013 /filesSMART13/FUrien_Talk_smart2013.pdf, Accessed 22April 2014

Vacirca, F., Ricciato, F., & Pilz, R. (2005). Large-scale RTT measurements from an operational UMTS/GPRS network. In Wireless Internet, 2005. Proceedings. First International Conference on (pp. 190-197). IEEE.

Valcourt, E., Robert, J. M., & Beaulieu, F. (2005). Investigating mobile payment: supporting technologies, methods, and use. In Wireless And Mobile Computing, Networking And Communications, 2005. (WiMob'2005), IEEE International Conference on (Vol. 4, pp. 29-36). IEEE.

Van Bossuyt, Michaël, and Leo Van Hove.(2007), "Mobile payment models and their implications for NextGen MSPs." info 9.5 (2007): 31-43.

Vili Lehdonvirta et al.(2009), UbiPay: Minimizing Transaction Costs with Smart Mobile Payments, in Proceedings of the 6th International Conference on Mobile Technology, Application & Systems (Mobility '09), Nice, France, 2009, pp. 1:1--1:7.

Yen Choon Ching and Heinz Kreft. (2008), FairCASH: Concepts and Framework, in Proceedings of the 2008 The Second International Conference on Next Generation Mobile Applications, Services, and Technologies, Cardiff, Wales UK, 2008, pp. 269—274

Zefu Dai, Nick Ni, and Jianwen Zhu. (2010). A 1 cycle-per-byte XML parsing accelerator. In *Proceedings of the 18th annual ACM/SIGDA international symposium on Field programmable gate arrays* (FPGA '10). ACM, New York, NY, USA, 199-208. DOI=10.1145/1723112.1723148

Zhang, G., Cheng, F., & Meinel, C. (2008). Towards secure mobile payment based on SIP. In Engineering of Computer Based Systems, 2008. ECBS 2008. 15th Annual IEEE International Conference and Workshop on the (pp. 96-104). IEEE.

Zhang, G., Cheng, F., & Meinel, C. (2008). SIMPA: a SIP-based mobile payment architecture. In Computer and Information Science, 2008. ICIS 08. Seventh IEEE/ACIS International Conference on (pp. 287-292). IEEE.

Zhao, L., Iyer, R., Makineni, S., & Bhuyan, L. (2005). Anatomy and performance of SSL processing. In *Performance Analysis of Systems and*

Software, 2005. ISPASS 2005. IEEE International Symposium on (pp. 197-206). IEEE.

Appendix A
Network simulation to measure the protocol performance

A.1 Simulation Package

OPNET Modeler was used to simulate the network and the application and measure the application delays. The simulations were run on a Intel Quad Core 2 GHz CPU based system, with 16 MB RAM and 520 GB hard disk.

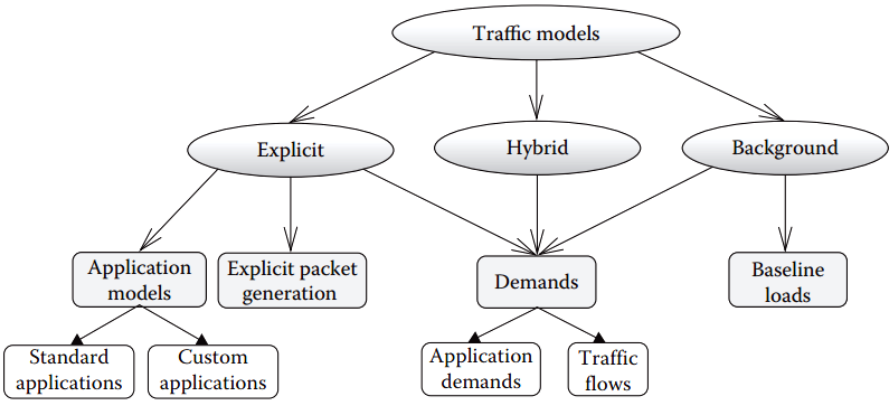
A.2 Simulation Details

A total of 56 simulations each for 3G, 4G macro cell and 4G micro cell were run and measurements were collected. The measurements were filtered for anamolies (very high instances of delay) and checked for time outs and packet drops. For every simulation run, the link occupancy of the links from the backbone network to the EPC networks were monitored to ensure that the background traffic generated by the active users were being delivered appropriately. In addition, the eNodeB links were monitored for packet drop rates. These helped to correlate the delay measurements seen by the end users on the network with the drops and traffic.

A.3 Application Configuration in OPNET

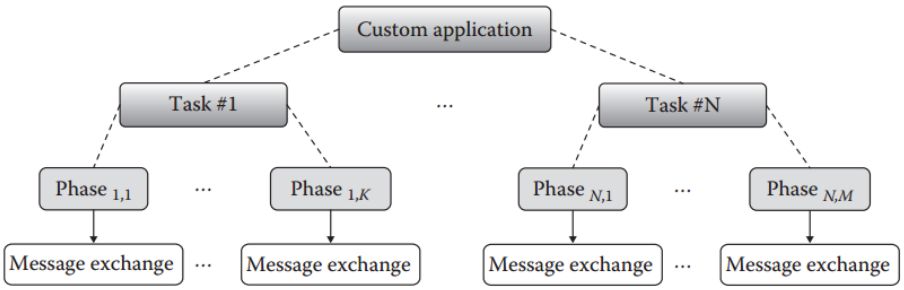
The requirement for the application is to use SSL but in OPNET SSL works only with HTTP, FTP and DATABASE application. Therefore the data type with the SSL is selected.

OPNET support different types of applications, the details of which is out of scope of this report. The figure below shows the supported applications types.



OPNET supported applications

The Standard applications have pre-defined applications e.g. FTP, HTTP, Database, Remote login etc. For custom applications a separate utility, the Task configuration Utility, is used to model the behaviour of any type of application. The custom application in OPNET supports multi-tier application with multiple phases in it to model complex applications. This is used to model the application protocol. The custom application model overview is shown in the figure below. Each application is divided into tasks and each task comprises of phases. The phases within a task are sequentially processed.



Custom application phases

The applications in OPNET are defined using the application configuration utility. These applications are then assigned to the application profile within the profile configuration utility. The profile which has a single or multiple applications in it is configured to run on the end nodes. The steps for the application definition are defined as required by the application.

The application consists of two phases.

1. Pre transaction phase
2. Transaction phase

Both the phases are configured for each client and server. Since it is a multi-tier application, it is modelled using the custom application type.

The Payer and Payee registration phases are defined. In multi-tier application each phase in application depend on the previous application phase. The pre-transaction process steps for payee are listed below:

1. Payee sends registration request to PSP 2.
2. PSP 2 takes some time in internal processing
3. PSP 2 sends an ack to Payee.

The below shows the phases inside the Task utility for the Pre transaction process for Payee’s registration.

	Phase Name	Start Phase After	Source	Destination	Source->Dest Traffic
REGISTER#1	REGISTER#1	Application Starts	Originating Source	PSP 1	(...)
internal processing#1	internal processing#1	Previous Phase Ends	PSP 1	Not Applicable	(...)
ACK	ACK	Previous Phase Ends	PSP 1	Previous Source	(...)

Steps of the Pre-transaction phase

The processing details for the registration process are:

1. Payee initializes the process with the initialization delay of 5ms (initialization time is the startup delay for that phase). This is defined in the source -> destination traffic as shown in the figure below.

Attribute	Value
Initialization Time (seconds)	constant (0.005)
Request Count	constant (1)
Interrequest Time (seconds)	exponential (1.0)
Request Packet Size (bytes)	constant (213)
Packets Per Request	constant (1)
Interpacket Time (seconds)	constant (0)
Server Job Name	Not Applicable

Payee initialization

2. Internal processing of the application data from the Payee and generating a response for PSP 2 is set as 20 ms as shown in **Error! eference source not found.** below

Attribute	Value
Initialization Time (seconds)	constant (0.02)
Request Count	constant (0)
Interrequest Time (seconds)	constant (0)
Request Packet Size (bytes)	constant (0)
Packets Per Request	constant (0)
Interpacket Time (seconds)	constant (0)
Server Job Name	Not Applicable

PSP 2 internal processing

3. PSP 2 sends the ack to the payee with the zero initialization time.

Attribute	Value
Initialization Time (seconds)	constant (0)
Request Count	constant (1)
Interrequest Time (seconds)	exponential (1.0)
Request Packet Size (bytes)	constant (213)
Packets Per Request	constant (1)
Interpacket Time (seconds)	constant (0)
Server Job Name	Not Applicable

Ack time

The Transaction phase is defined only for payee as provided in the requirements. The application is initiated from payee and then through PSP 1

and 2 to the payer and then closed at the payee. The **Error! Reference ource not found.** shows the steps involve for Transaction phases.

	Phase Name	Start Phase After	Source	Destination	Source->Dest Traffic	Dest->Source Traffic	REQ/RESP Pat
INIT_REQ#1	INIT_REQ#1	Application Starts	Originating Source	PSP 2	(...)	No Response	REQ->REQ->...
INIT_REQ#2	INIT_REQ#2	Previous Phase Ends	PSP 2	PSP 1	(...)	No Response	REQ->REQ->...
INIT_REQ#3	INIT_REQ#3	Previous Phase Ends	PSP 1	PAYER	(...)	No Response	REQ->REQ->...
INIT	INIT	Previous Phase Ends	PAYER	PSP 1	(...)	No Response	REQ->REQ->...
ACK#1	ACK#1	INIT	PSP 1	PAYER	(...)	No Response	REQ->REQ->...
ACK#2	ACK#2	INIT	PSP 1	PSP 2	(...)	No Response	REQ->REQ->...
ACK#3	ACK#3	Previous Phase Ends	PSP 2	Originating Source	(...)	No Response	REQ->REQ->...
AUTH	AUTH	ACK#1	PAYER	PSP 1	(...)	No Response	REQ->REQ->...
ACK#4	ACK#4	Previous Phase Ends	PSP 1	PAYER	(...)	No Response	REQ->REQ->...
CONF	CONF	Previous Phase Ends	PAYER	PSP 1	(...)	No Response	REQ->REQ->...
TRANSFER	TRANSFER	Previous Phase Ends	PSP 1	PSP 2	(...)	No Response	REQ->REQ->...
ACK#5	ACK#5	Previous Phase Ends	PSP 2	PSP 1	(...)	No Response	REQ->REQ->...
CLOSE#1	CLOSE#1	ACK#5	PSP 1	PAYER	(...)	No Response	REQ->REQ->...
CLOSE#2	CLOSE#2	ACK#5	PSP 1	PSP 2	(...)	No Response	REQ->REQ->...
CLOSE#3	CLOSE#3	Previous Phase Ends	PSP 2	PAYEE	(...)	No Response	REQ->REQ->...

Phases of the application transaction

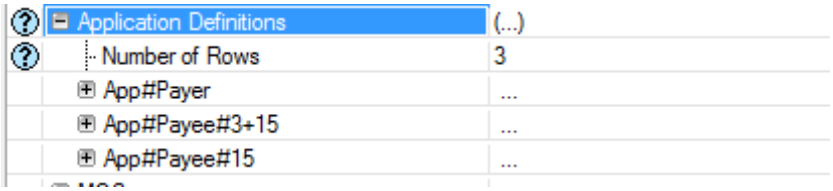
The application is started by a client with some initialization delay which is included to provide some settling time for the pre-transaction phase to successfully complete. This is set to 500 ms.

Attribute	Value
Initialization Time (seconds)	constant (0.5)
Request Count	constant (1)
Interrequest Time (seconds)	exponential (1.0)
Request Packet Size (bytes)	constant (341)
Packets Per Request	constant (1)
Interpacket Time (seconds)	constant (0)
Server Job Name	Not Applicable

Initialization time or startup delay for the transaction

The initialization time for all the remaining phases in transaction phase is zero.

Three applications are defined inside the application configuration utility. The Payer registers in pre- transaction phase and does nothing else. The payee has two phases, one is pre-transaction and the other is the transaction. First the pre-transaction phase is executed and then transaction phase starts and so on. The name of the applications defined is shown in the figure.



Application names

The functions of these applications are.

1. App#Payer is the pre-transaction process for the Payer. It has total 3 phases (steps) in it.
2. The application for payer is split in to two. App#payee#3+15 consist of pre transaction and transaction tasks. There are 3 phases for pre transaction and 15 phases for transaction. Hence it will cover the objective to measure the separate delay for pre-transaction and transaction (3+15) phases.
3. The App#Payee#15 consist of only transaction task with 15 phases, hence it will cover the objective to find the delay only for transaction process.

So with first application we can measure the delay only for pre transaction, with second application the delay combination of transaction and pre transaction while with last application the delay only for transaction process.

A.4 Results

On the payee where both pre-transaction and transaction are defined the pre-transaction process is configured to repeat after every two transaction processes. To achieve the repetition objectives the following configurations are done.

1. The Payee application repeats after every 50 sec. A single repetition consists of 1 pre-transaction and 2 transaction processes as shown in the figure. This is equivalent to the Payee registering with the PSP 2 after every two transactions made. The two applications discussed above are combined inside the single profile and the profile is configured to repeat after every 50 sec.

⊟ App_Profile#Payee	
Profile Name	App_Profile#Payee
⊟ Applications	(...)
Number of Rows	2
⊞ App#Payee#6+15	...
⊞ App#Payee#15	...
Operation Mode	Serial (Ordered)
Start Time (seconds)	constant (5)
Duration (seconds)	End of Last Application
⊟ Repeatability	(...)
Inter-repetition Time (seconds)	constant (50)
Number of Repetitions	Unlimited
Repetition Pattern	Serial

Application repitition

2. The pre-transaction phase configured for payer will repeat after every 60 sec irrespective of the app running on payee as shown in the figure.

App_Profile#Payer	
Profile Name	App_Profile#Payer
Applications	(...)
Number of Rows	1
App#Payer	
Name	App#Payer
Start Time Offset (seconds)	constant (5)
Duration (seconds)	End of Last Task
Repeatability	(...)
Inter-repetition Time (secon...	constant (60)
Number of Repetitions	Unlimited
Repetition Pattern	Serial
Operation Mode	Serial (Ordered)

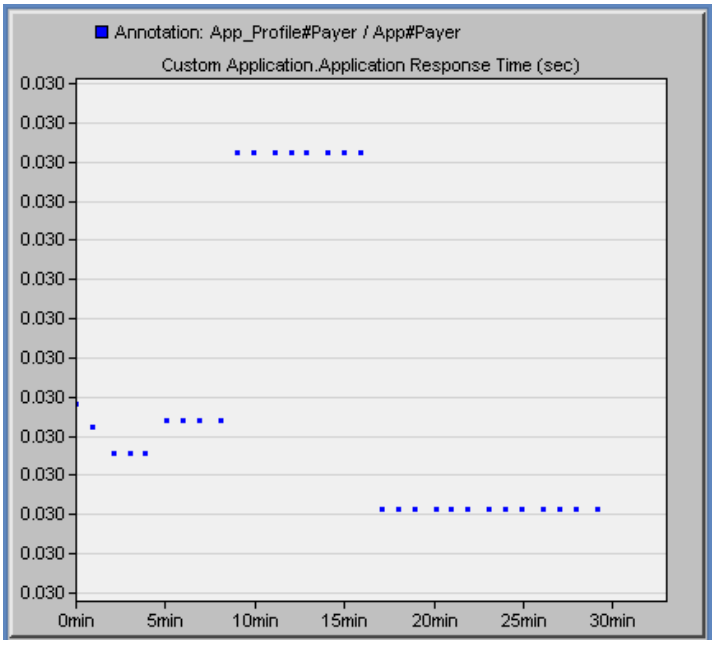
Workstation 1 application repetition

To confirm the working of repetition configuration, the application tracking delay is used. A single pre- transaction phase take about 30.1ms to complete and for payer the repetition configured is after 60sec. The simulation is run for 30 min therefore total 30 pre-transaction will be completed as shown in the figure.

Transaction Type: Custom Application			Avg=3...		
Transaction 2: App#Payer	10 sec	10 sec	30.2 ms		
Network			0.1 ms	0	0 ms
Application			30.1 ms		
Tier Pair: PAYER<->PSP_1	10 sec	10 sec	25.1 ms	0	0 ms
Message 1 (PAYER->PSP_1)	10 sec	10 sec	0.1 ms	0	0 ms
Message 2 (PSP_1->PAYER)	10 sec	10 sec	0.1 ms	0	0 ms
Transaction 5: App#Payer	70 sec	70.1 sec	30.2 ms		
Transaction 9: App#Payer	130.1 sec	130.1 sec	30.2 ms		
Transaction 13: App#Payer	190.1 sec	190.1 sec	30.2 ms		
Transaction 17: App#Payer	250.1 sec	250.2 sec	30.2 ms		
Transaction 21: App#Payer	310.2 sec	310.2 sec	30.2 ms		
Transaction 25: App#Payer	370.2 sec	370.2 sec	30.2 ms		
Transaction 29: App#Payer	430.2 sec	430.2 sec	30.2 ms		
Transaction 33: App#Payer	490.2 sec	490.3 sec	30.2 ms		
Transaction 37: App#Payer	550.3 sec	550.3 sec	30.2 ms		
Transaction 41: App#Payer	610.3 sec	610.3 sec	30.2 ms		
Transaction 45: App#Payer	670.3 sec	670.4 sec	30.2 ms		
Transaction 49: App#Payer	730.4 sec	730.4 sec	30.2 ms		
Transaction 53: App#Payer	790.4 sec	790.4 sec	30.2 ms		
Transaction 57: App#Payer	850.4 sec	850.5 sec	30.2 ms		
Transaction 61: App#Payer	910.5 sec	910.5 sec	30.2 ms		
Transaction 65: App#Payer	970.5 sec	970.5 sec	30.2 ms		
Transaction 69: App#Payer	1030.5 sec	1030.5 ...	30.2 ms		
Transaction 73: App#Payer	1090.5 sec	1090.6 ...	30.2 ms		
Transaction 77: App#Payer	1150.6 sec	1150.6 ...	30.2 ms		

The pre-transaction for the Payer repeats every 60 seconds

The figure below shows the application response time for payer, it can be seen that there are total about 30 dots which represent 30 repetition of the pre transaction phase. The performance is consistent at 30.2ms.



Application response time for Payer.

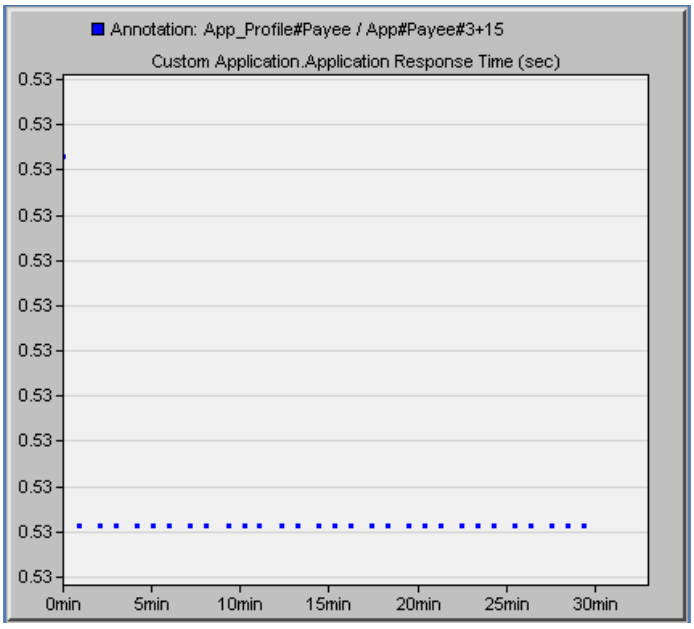
X-axis is simulation run time, Y-axis is Payer registration delay in sec

For Payee it can be seen that the average time for single repetition (1 pre-transaction and 2 transaction is more than 1 minute, 30ms for pre transaction and 1 sec for two transaction) and there is additional 50 sec gap to start the next repetition. The **Error! Reference source not found.** shows the pplication tracking delay for payee. It can be seen from the figure the app#payee#3+15 repeats two times, out of which one is pre transaction and second is transaction and then app#payee#15 which is the transaction case and the process repeat again. The application response time for these both applications is shown in the figures below.

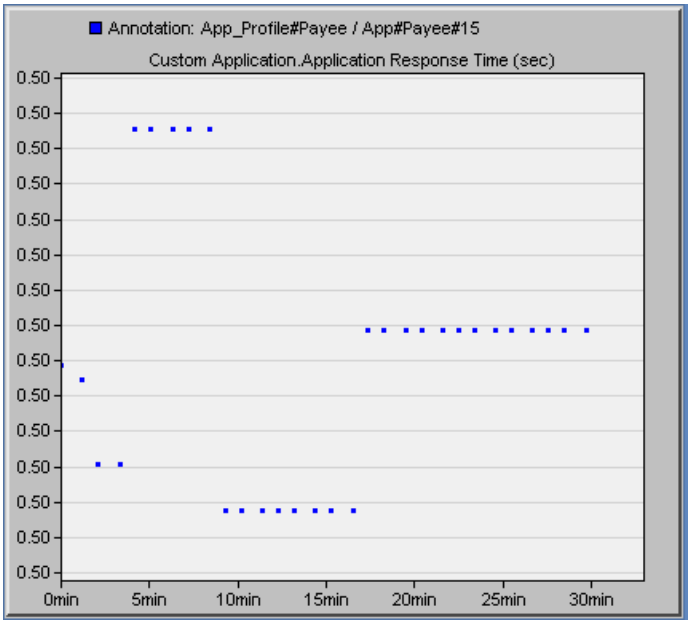
Notice that the execution time is reported as 500.4ms and the network delay is reported as 0.8ms totalling to 501.3ms.

Client: PAYEE		Avg=3...		
Transaction Type: Custom Application		Avg=3...		
Transaction 1: App#Payee#3+15	10 sec	10 sec	30.2 ms	
Network			0.1 ms	0	0 ms
Application			30.1 ms		
Tier Pair: PAYEE<->PSP_2	10 sec	10 sec	25.1 ms	0	0 ms
Message 1 (PAYEE->PSP_2)	10 sec	10 sec	0.1 ms	0	0 ms
Message 2 (PSP_2->PAYEE)	10 sec	10 sec	0.1 ms	0	0 ms
Transaction 3: App#Payee#3+15	10 sec	10.5 sec	501.3 ...		
Network			0.8 ms	0	0 ms
Application			500.4 ...		
Tier Pair: PAYEE<->PSP_2	10.5 sec	10.5 sec	1.2 ms	0	0 ms
Tier Pair: PSP_2<->PSP_1	10.5 sec	10.5 sec	1 ms	0	0 ms
Tier Pair: PSP_1<->PAYER	10.5 sec	10.5 sec	0.9 ms	0	0 ms
Transaction 4: App#Payee#15	15.5 sec	16 sec	501.3 ...		
Network			0.8 ms	0	0 ms
Application			500.4 ...		
Tier Pair: PAYEE<->PSP_2	16 sec	16 sec	1.2 ms	0	0 ms
Tier Pair: PSP_2<->PSP_1	16 sec	16 sec	1 ms	0	0 ms
Tier Pair: PSP_1<->PAYER	16 sec	16 sec	0.9 ms	0	0 ms
Transaction 6: App#Payee#3+15	71 sec	71.1 sec	30.2 ms		
Transaction 7: App#Payee#3+15	71.1 sec	71.6 sec	501.3 ...		
Transaction 8: App#Payee#15	76.6 sec	77.1 sec	501.3 ...		
Transaction 10: App#Payee#3+15	132.1 sec	132.1 sec	30.2 ms		
Transaction 11: App#Payee#3+15	132.1 sec	132.6 sec	501.3 ...		
Transaction 12: App#Payee#15	137.6 sec	138.1 sec	501.3 ...		
Transaction 14: App#Payee#3+15	193.1 sec	193.1 sec	30.2 ms		

Payee App tracking delay



Payee App with pre-registration and transaction - completion time

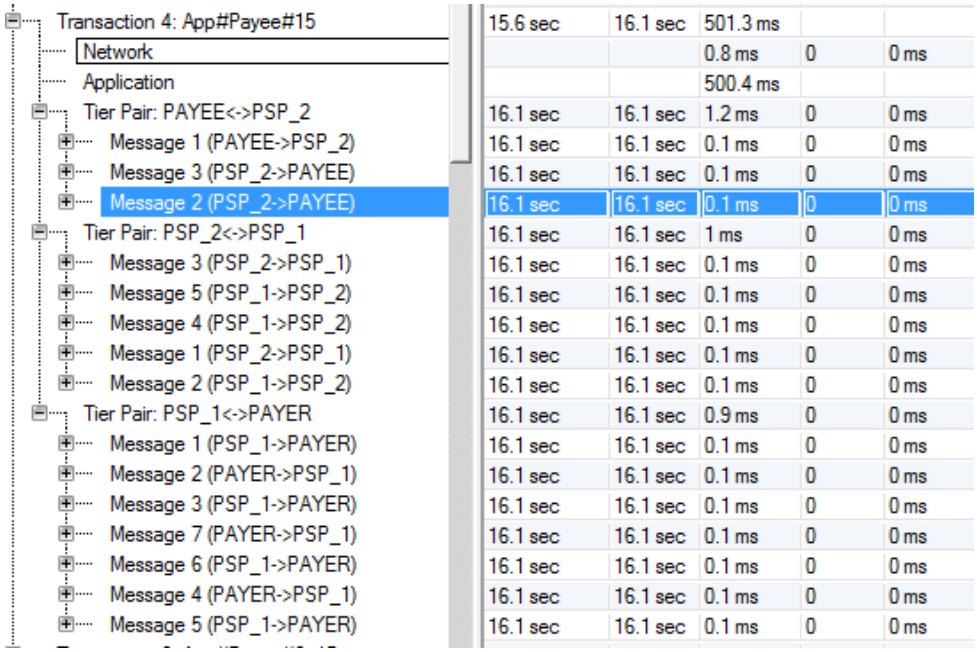


15 Payee App with transaction - completion time

Completion time is the time taken for all the tasks in the Custom Application to complete. Since there are only 6 tasks in pre transaction phase for Payer, its response time is only 50ms while for Payee there are 6 phases in pre-transaction and 15 phases in transaction task and the response time is 0.501 second. The response time also include the initialization time for all the phases inside a single task, therefore this time is greater.

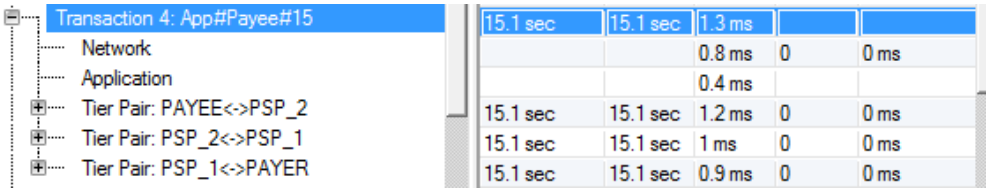
The Packet network delay is the Network delay experienced by Request and Response packets. It is completely different thing from the application response time or task response time. Packet network delay is included inside the application response with additional delays of initialization time, inter request wait time etc. The delay experiences by a packet using the network part include this delay. The packet network delay for payer is shown in the figure. The packet network delay for Payee is shown in the figures above. The variation in the graph is due to nanosecond delay difference in different application repetition as can be seen in the graph the y-axis is constant at 56 microsecond and 62 microsecond.

The transaction phase takes 500ms for completion, so for the complete cycle of 1 pre-transaction and two transactions for payee, the completion time is more than 1 sec. Let’s explore the reason for 500ms. The application tracking delay will help to track the delay. The snap shot is taken from the application tracking delay for transaction process of 15 phases as shown in the figure below



The Payee transaction cycle

The figure shows the total completion time of 501.3ms, out of which 0.8ms is the network propagation time for the 15 messages send and 500.4ms is the application delay. Out of 500.4ms delay 500ms is the initialization time delay introduce when the first message send from the payee as explained above the back off time, else all other message is completed in a duration of about 0.1ms. The difference in sum of delays and total delay of 501.3ms is due to the fact that OPNET take average of these, but our calculation is approximately the same.



The Payee transaction cycle without the 500ms initialisation delay

If the initial 500ms delay is removed this delay will become very less as shown for the case with zero back off time below. The delay reduces to 1.3ms for the transaction phase completion as the start up delay is zero.

The application is successfully programmed and simulated for a simple wired network with the following objectives achieved.

1. The custom application is defined with data size of including the SSL overhead.
2. The custom application consists of transaction and pre-transaction processes. There are total 3 commands or phases in pre-transaction and 15 in transaction.

3. There are total 3 applications define to separately observed the measurements for each. One application consists of combination of transaction and pre-transaction, 2nd application consists of only transaction and 3rd application consists of only pre-transaction.
4. Payer is configured to run only pre-transaction process with the repetition of every 60 second
5. Payee performs both transaction and pre transaction with the repetition of 50 sec. A single repetition for payee means one pre-transaction and two consecutive transactions.
6. From result it has been found that pre-transaction process takes 30ms to complete which include initialize time of each phase and network delay

It has been found that transaction process takes 501.3ms to complete including 500ms of initialization time of the first phase.

A.5 Network Design

There are 3 types of network designs to be calibrate, which are 3G, 4G macro and 4G micro cell. The network is configured using the parameters listed below.

1. Path loss model for LTE macro cell is modified to UMa-Los/NLos(ITU-R M2135).
2. Path loss model for LTE micro cell is modified to UMi-Los/NLos(ITU-R M2135).
3. 3G network radio access network is modified to have a single hexagonal cell with radius of 1km.
4. All the links in the network are OC24 (1244.16Mbps) except the PSP-1 and PSP-2 data center links. Previously only core links were OC24 and other links were OC3.
5. The backbone network routers are cisco 7609 routers as the to support the switching rate for more than 200 active users.
6. The background servers are connected directly to the backbone router.
7. The background users application is modified to run at 100 second of simulation while the transaction application run at 150 sec. The traffic should build up and be stable i the 50 secs of simulation run time.
8. The transaction app is configured to repeat after every 5 second so it is expected to have continuous transaction after 150sec and if the number of transactions are less, it implies that due to congestion at the LTE access network, data has been dropped.

The following steps are performed for 3G network configuration

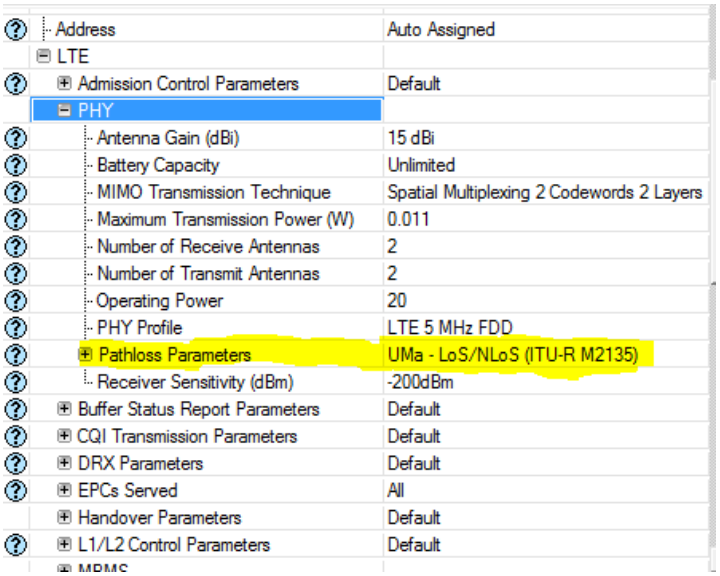
1. Deployed the radio access network using deploy wireless utility, it doesn’t support UMTS feature. Therefore other type is selected during

the configuration and the UMTS network elements are manually entered.

2. Mobility is configured automatically which can be verified and modified from the mobility configuration node. The speed, area of mobility, pause time and mobility start time can be modified.
3. Left side of operator network have GGSN id 1, SGSN id 1 and RNC id 1.
4. Right Side of operator network have GGSN id 2, SGSN id 2 and RNC id 2.
5. All the data type is background and uplink and downlink bandwidth for the UE is set as the default for background data type. The data rate for background was increased 600kbps for uplink and 1.8Mbps for downlink but RB allocation error was receiving, which stopped at 256kbps for uplink and downlink. The reason for this can be UMTS allocate data in a round robin fashion from 4 QoS classes and for a single class all of the data rate can't be assigned.
6. The models that are used from the UMTS library which support sonnet links connectivity are umts_wkstn_adv, umts_node_b_slip_adv, umts_rnc_ethernet2_atm2_slip2_adv, umts_sgsn_ethernet_atm_slip9_adv, umts_ggsn_ethernet2_slip8_adv.
7. Ping traffic is configured for calibration using IP_PING flow from the object palette. The IP attribute node is required to model the ping traffic behaviour..

The following steps are performed for 4G network configuration.

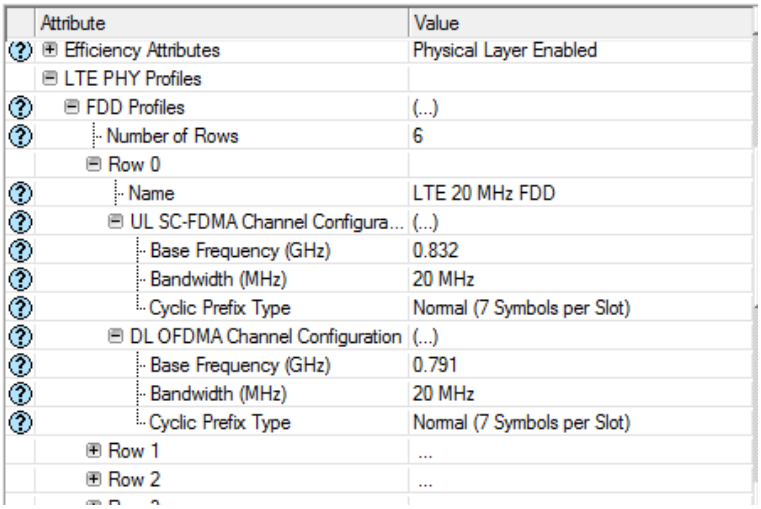
1. Radio access is deployed using wireless wizard discussed in the 3G network. LTE network is available for configuration in wireless wizard as shown in the figure below.
2. Path loss model is configured from the LTE attributes of EnodeB and UE present under the physical configurations as shown in the



Address	Auto Assigned
LTE	
Admission Control Parameters	Default
PHY	
Antenna Gain (dBi)	15 dBi
Battery Capacity	Unlimited
MIMO Transmission Technique	Spatial Multiplexing 2 Codewords 2 Layers
Maximum Transmission Power (W)	0.011
Number of Receive Antennas	2
Number of Transmit Antennas	2
Operating Power	20
PHY Profile	LTE 5 MHz FDD
Pathloss Parameters	UMa - LoS/NLoS (ITU-R M2135)
Receiver Sensitivity (dBm)	-200dBm
Buffer Status Report Parameters	Default
CQI Transmission Parameters	Default
DRX Parameters	Default
EPCs Served	All
Handover Parameters	Default
L1/L2 Control Parameters	Default

Path loss model

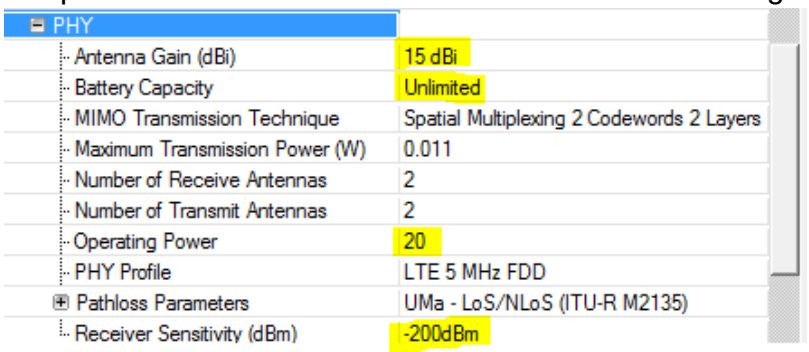
3. The physical profile of 5 MHz is configured to use with the base frequencies of as shown in the



Attribute	Value
Efficiency Attributes	Physical Layer Enabled
LTE PHY Profiles	
FDD Profiles	(...)
Number of Rows	6
Row 0	
Name	LTE 20 MHz FDD
UL SC-FDMA Channel Configura...	(...)
Base Frequency (GHz)	0.832
Bandwidth (MHz)	20 MHz
Cyclic Prefix Type	Normal (7 Symbols per Slot)
DL OFDMA Channel Configuration	(...)
Base Frequency (GHz)	0.791
Bandwidth (MHz)	20 MHz
Cyclic Prefix Type	Normal (7 Symbols per Slot)
Row 1	...
Row 2	...

Physical profile

4. Configured power for enodeB and UE is shown in the below figures.



PHY	
Antenna Gain (dBi)	15 dBi
Battery Capacity	Unlimited
MIMO Transmission Technique	Spatial Multiplexing 2 Codewords 2 Layers
Maximum Transmission Power (W)	0.011
Number of Receive Antennas	2
Number of Transmit Antennas	2
Operating Power	20
PHY Profile	LTE 5 MHz FDD
Pathloss Parameters	UMa - LoS/NLoS (ITU-R M2135)
Receiver Sensitivity (dBm)	-200dBm

Power for enodeB

PHY	
Antenna Gain (dBi)	-1 dBi
Battery Capacity	5.0
Downlink MIMO Transmission Tech...	Use Serving eNodeB Setting
Maximum Transmission Power (W)	0.005
Modulation and Coding Scheme Ind...	9
Multipath Channel Model (Downlink)	LTE OFDMA ITU Pedestrian B
Multipath Channel Model (Uplink)	LTE SCFDMA ITU Pedestrian B
Number of Receive Antennas	2
Number of Transmit Antennas	1
Pathloss Parameters	UMa - LoS/NLoS (ITU-R M2135)
Receiver Sensitivity (dBm)	-200dBm

Power for UE

5. Mobility configurations are the same as discussed in 3G.
6. Ping traffic is defined the same way as discussed in 3G.
7. The LTE nodes used with sonnet link support are lte_enodeb_4ethernet_4atm_4slip_adv and lte_access_gw_atm8_ethernet8_slip8_adv.
8. IP addressing is set to default IPV4.

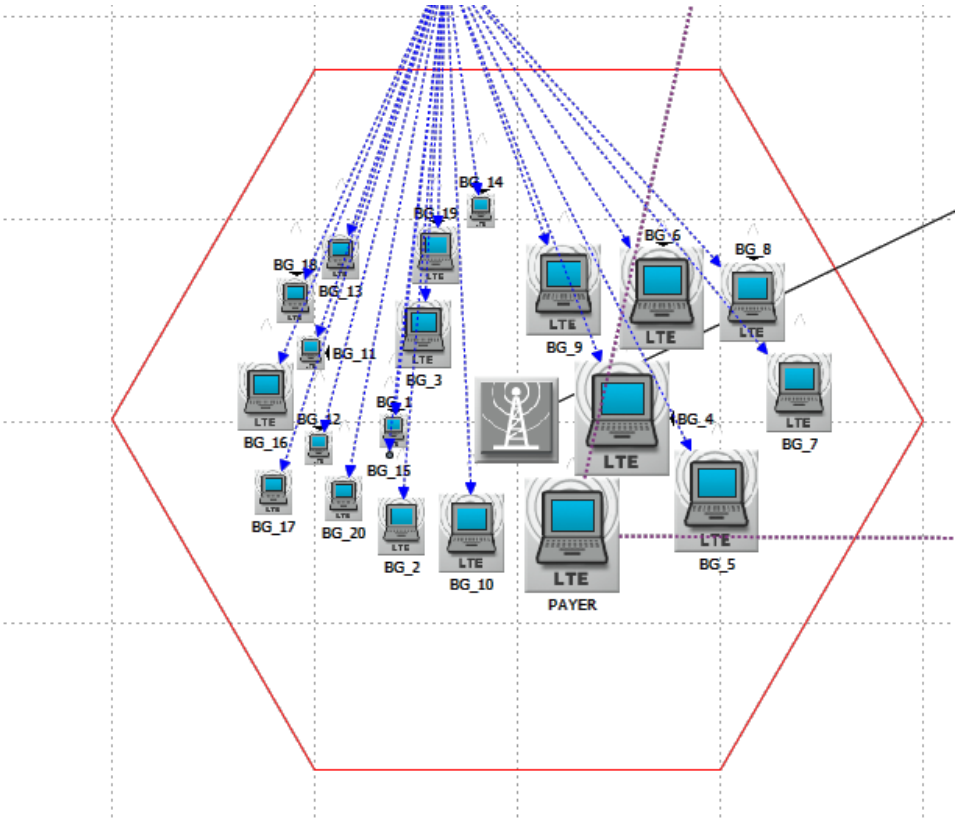
A.5.1 4G micro cell configuration

4G micro cell configurations are the same as discussed for 4G macro cell with difference in path loss model and power as shown in the figures below.

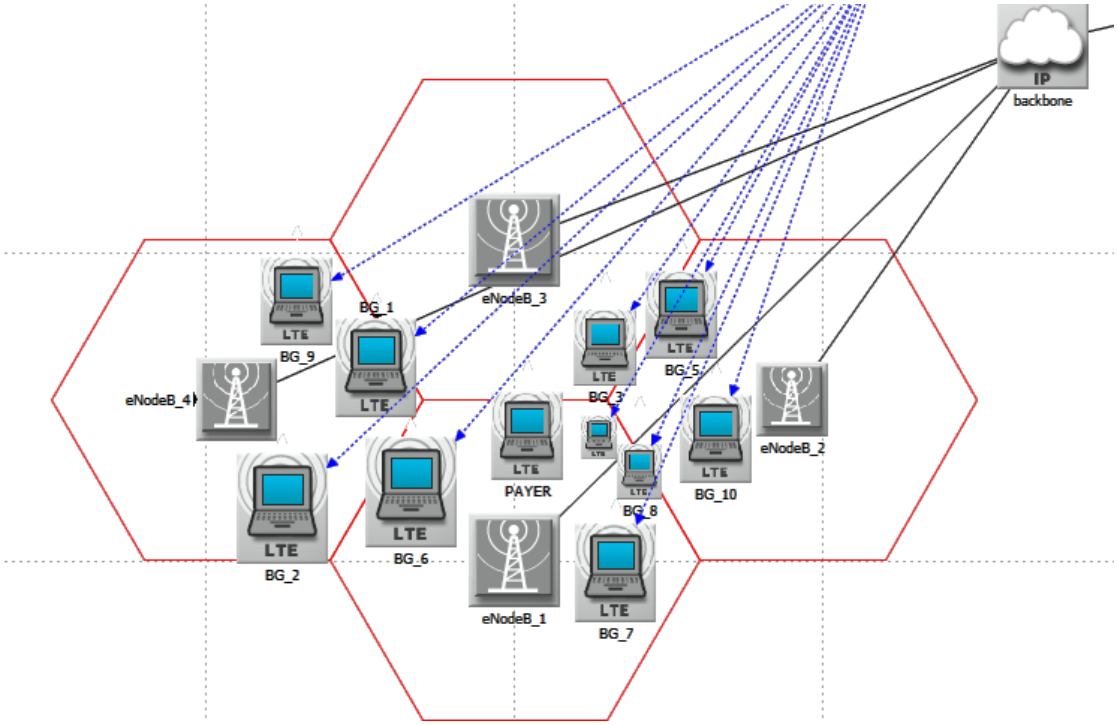
PHY	
Antenna Gain (dBi)	15 dBi
Battery Capacity	Unlimited
MIMO Transmission Technique	Spatial Multiplexing 2 Codewords 2 Layers
Maximum Transmission Power (W)	0.0032
Number of Receive Antennas	2
Number of Transmit Antennas	2
Operating Power	20
PHY Profile	LTE 5 MHz FDD
Pathloss Parameters	UMi - LoS/NLoS (ITU-R M2135)
Receiver Sensitivity (dBm)	-200dBm

enodeB power

PHY	
Antenna Gain (dBi)	-1 dBi
Battery Capacity	5.0
Downlink MIMO Transmission Tech...	Use Serving eNodeB Setting
Maximum Transmission Power (W)	0.0015
Modulation and Coding Scheme Ind...	9
Multipath Channel Model (Downlink)	LTE OFDMA ITU Pedestrian B
Multipath Channel Model (Uplink)	LTE SCFDMA ITU Pedestrian B
Number of Receive Antennas	2
Number of Transmit Antennas	1
Pathloss Parameters	UMi - LoS/NLoS (ITU-R M2135)
Receiver Sensitivity (dBm)	-200dBm



Traffic Flows in the 4G Macro Cell

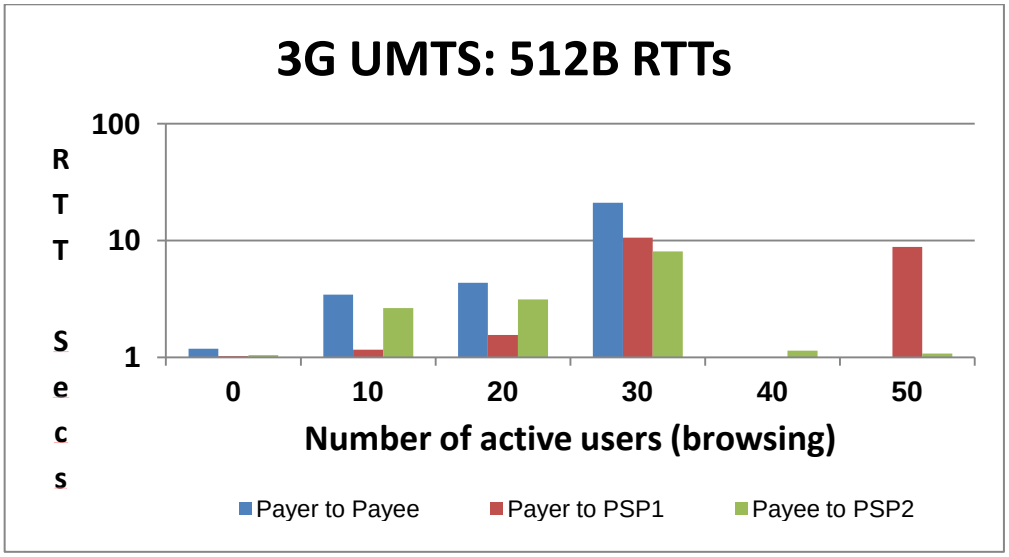


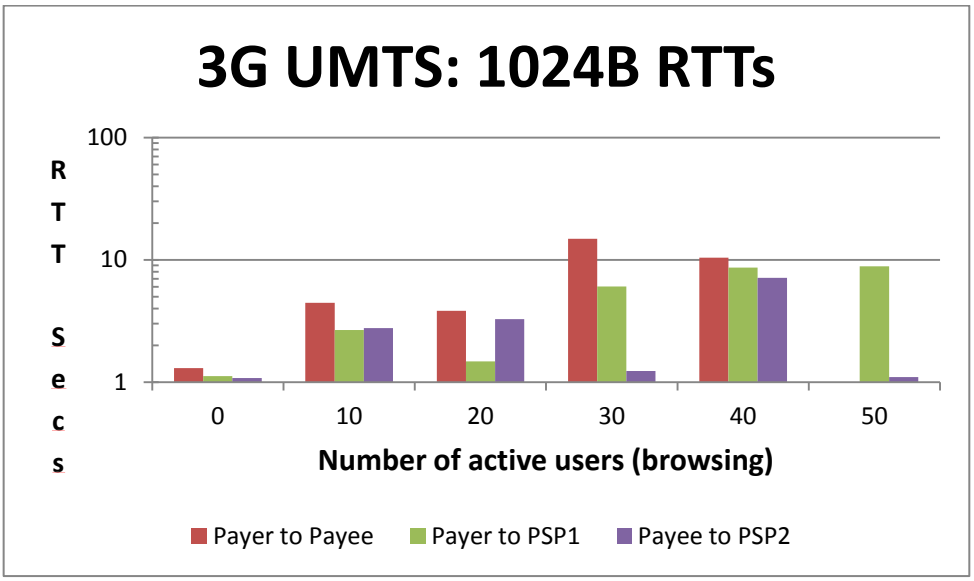
Payer inside a four micro cell 4G network

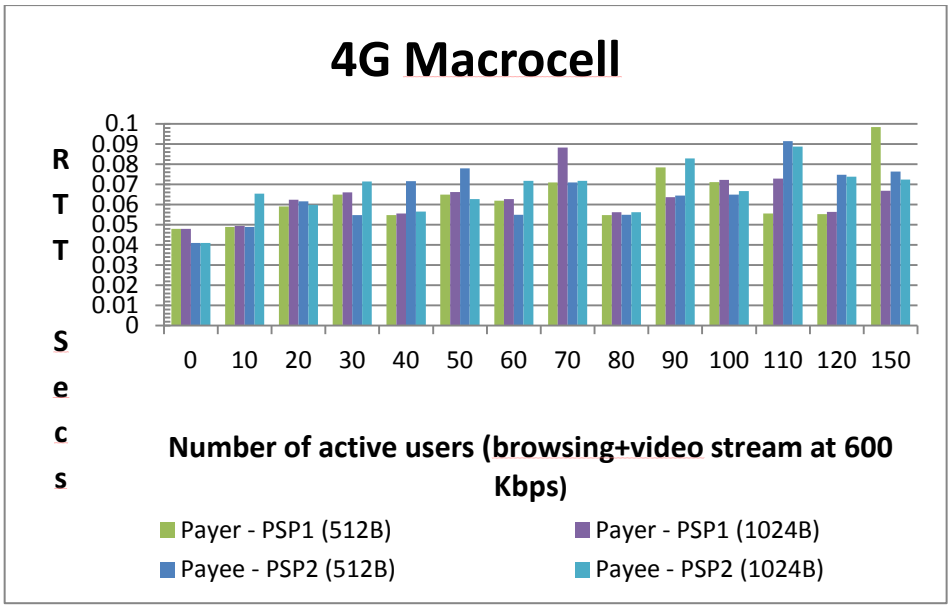
Appendix B
Delay measurement plots from the network simulation runs

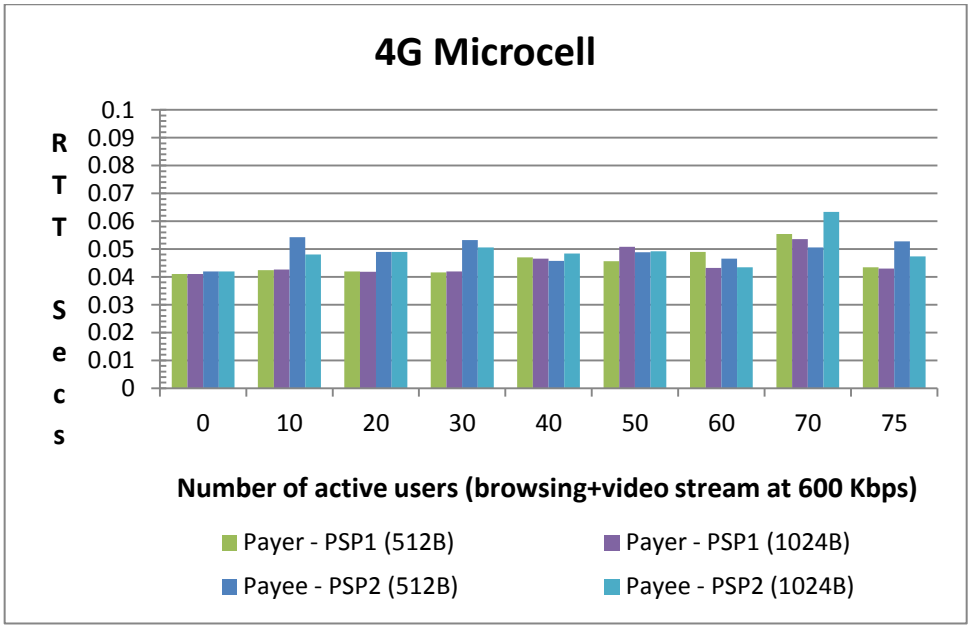
The plots included here are those plotted directly from the raw data which contains the anomalies. The plots for reference are included in the main text in Chapter 6. These plots are included here for reference and in place of the raw data tables.

B.1 RTT Plots



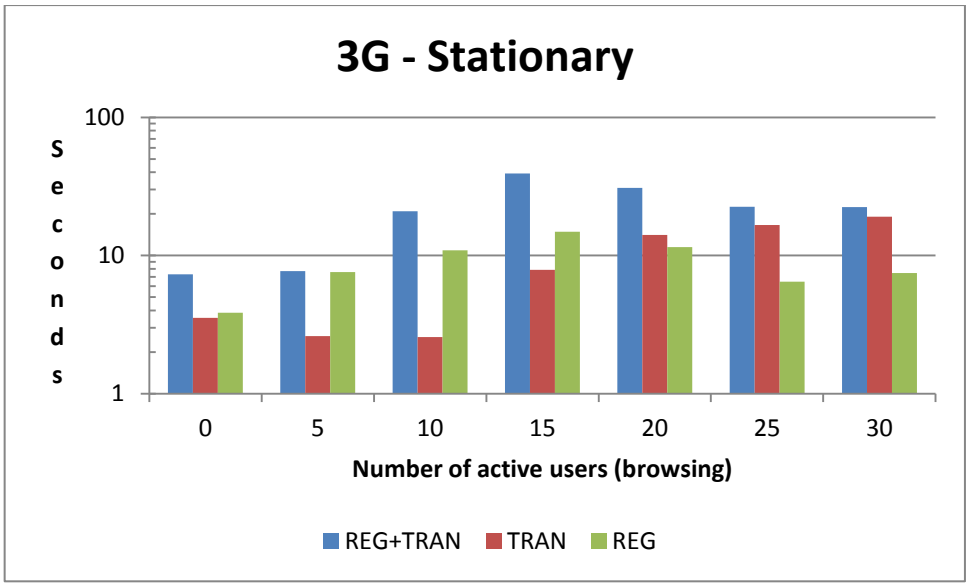


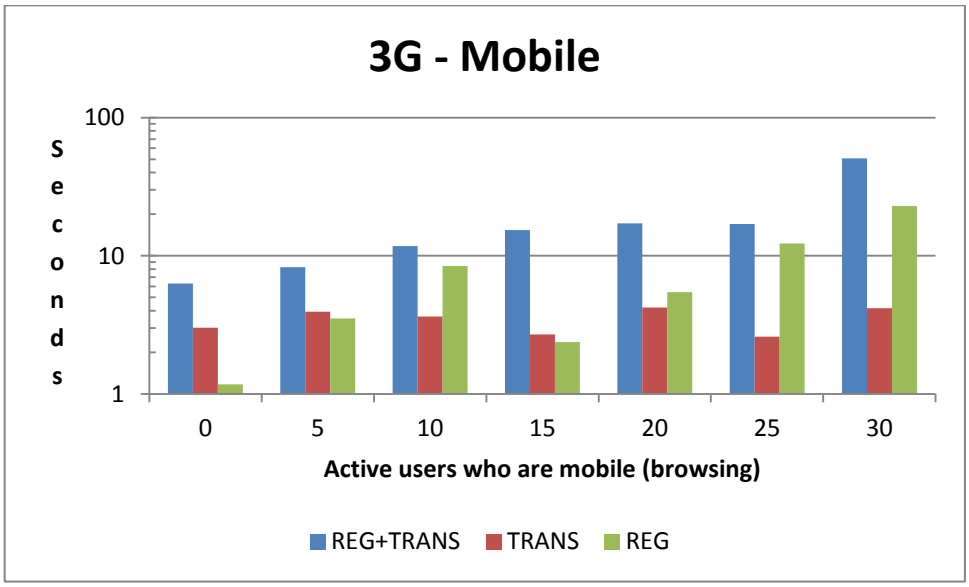


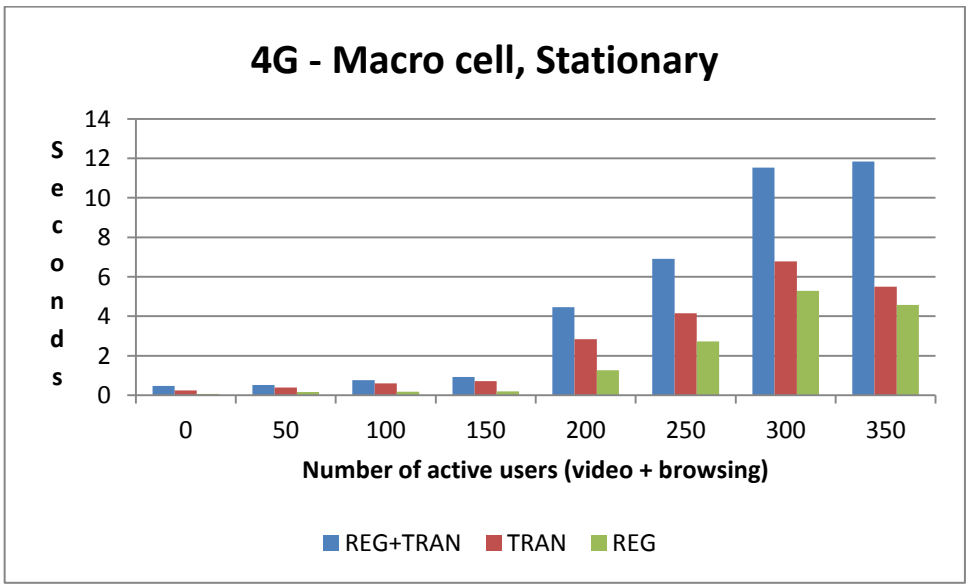


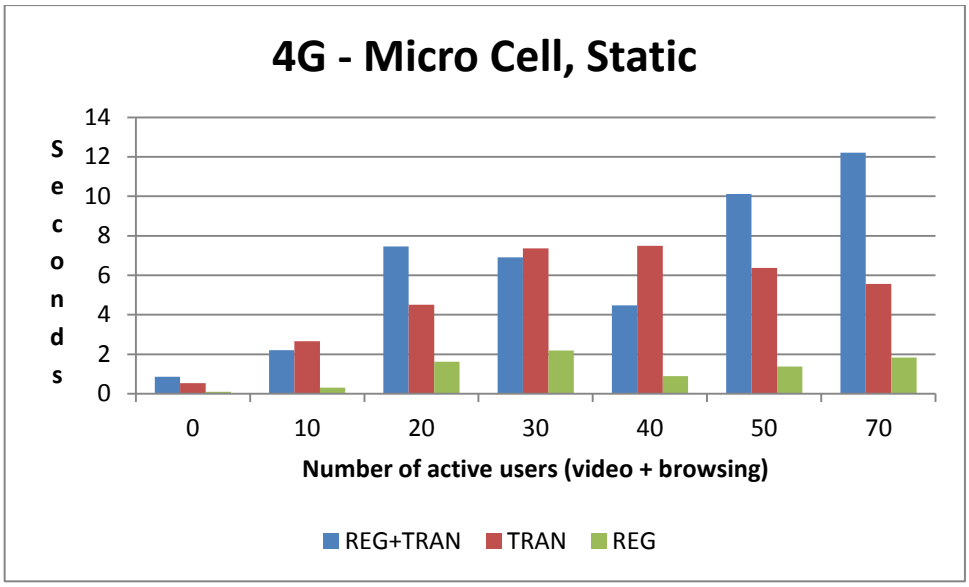
Transaction Delay Plots

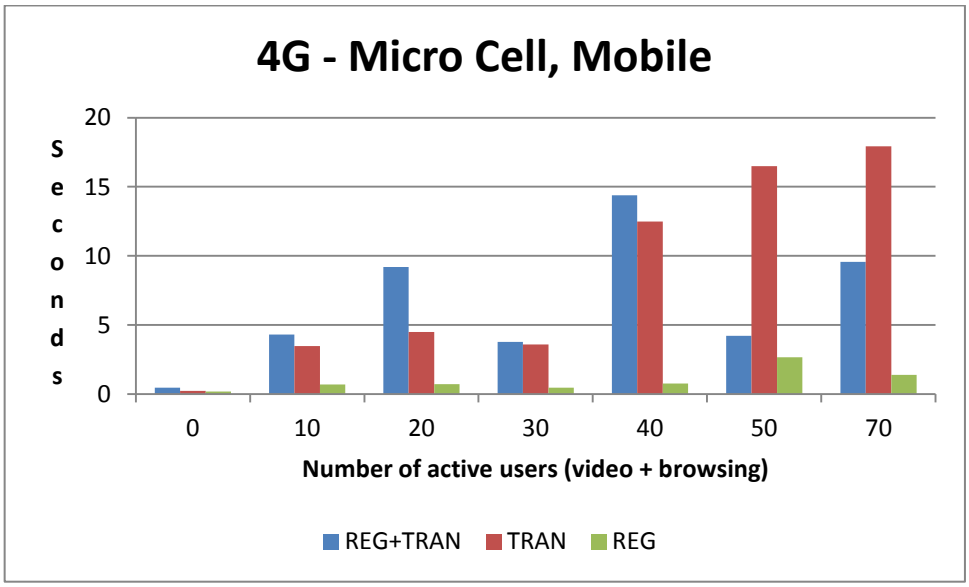
These delay plots are for a transaction between a payer and payee, with other active users in the cell generating traffic.

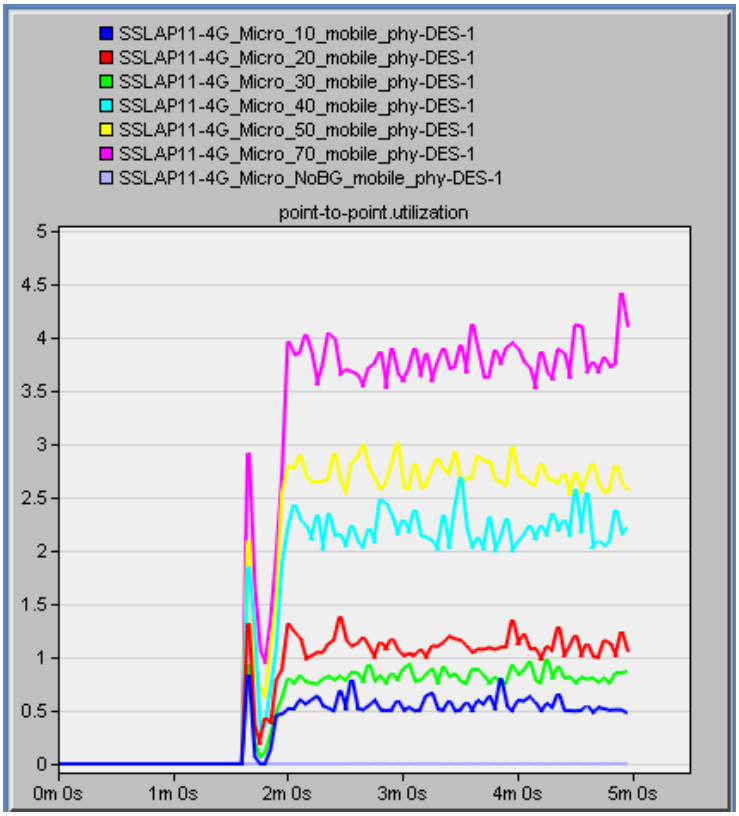

3G - Stationary
Seconds
100
10
1
0
5
10
15
20
25
30
Number of active users (browsing)
REG+TRAN
TRAN
REG


3G - Mobile
Seconds
100
10
1
0
5
10
15
20
25
30
Active users who are mobile (browsing)
REG+TRANS
TRANS
REG

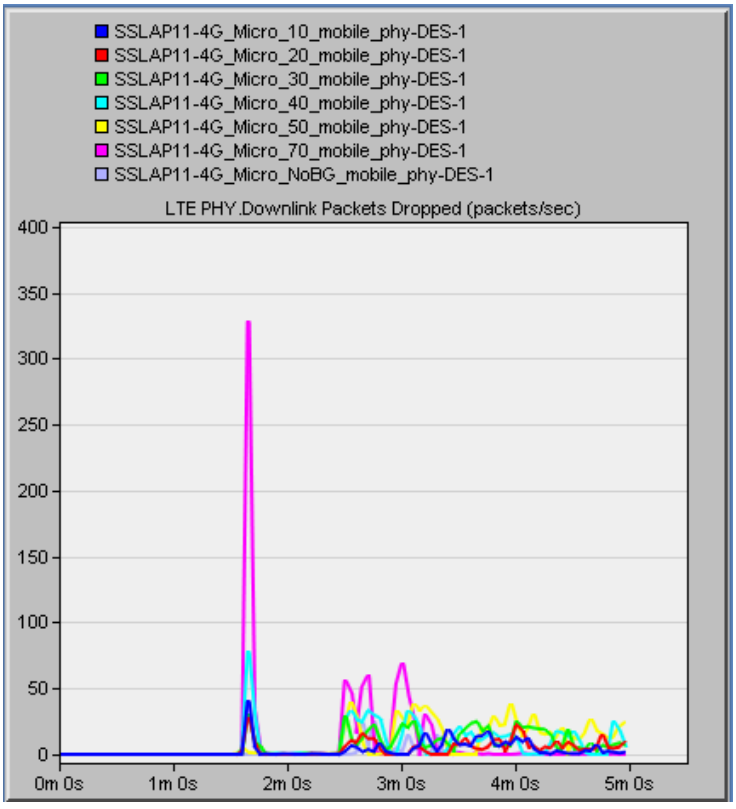

4G - Macro cell, Stationary
Seconds
14
12
10
8
6
4
2
0
0
50
100
150
200
250
300
350
Number of active users (video + browsing)
REG+TRAN
TRAN
REG


4G - Micro Cell, Static
Seconds
14
12
10
8
6
4
2
0
0
10
20
30
40
50
70
Number of active users (video + browsing)
REG+TRAN
TRAN
REG

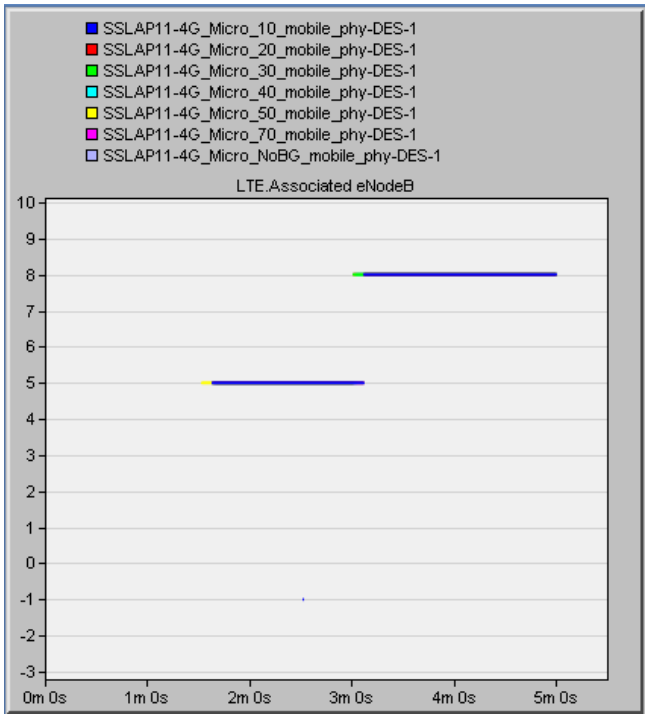

4G - Micro Cell, Mobile
Seconds
20
15
10
5
0
0
10
20
30
40
50
70
Number of active users (video + browsing)
REG+TRAN
TRAN
REG



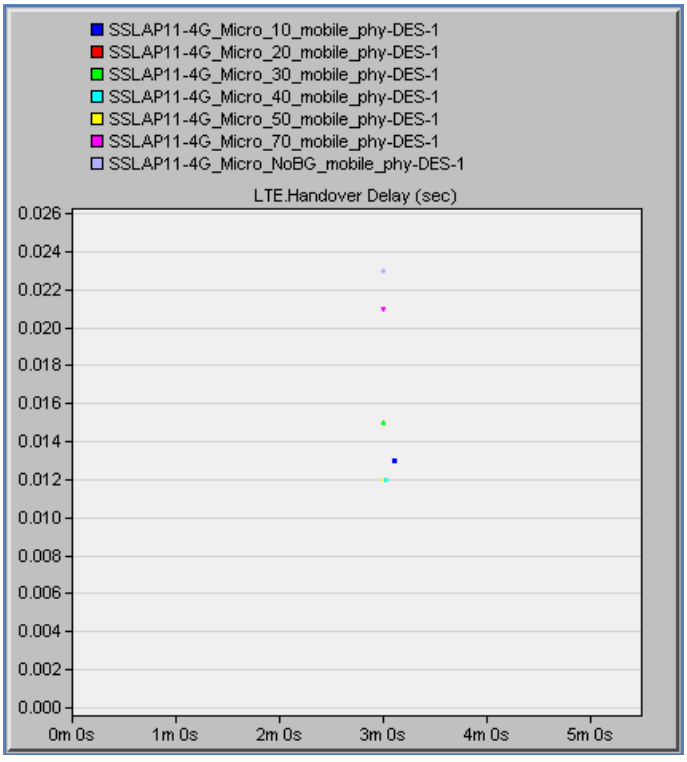
Link occupancy graph for the 4G Micro Cell load delay plot



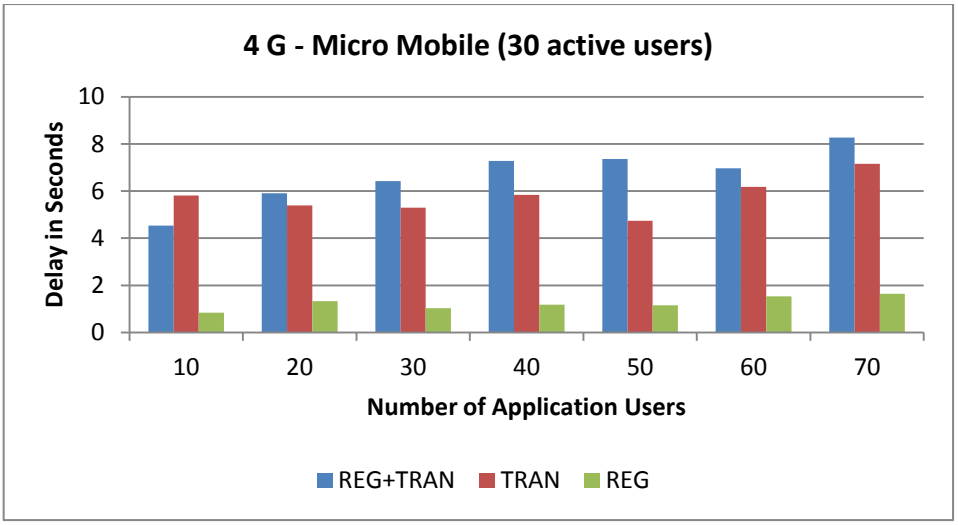
Packet drops at the radio layer

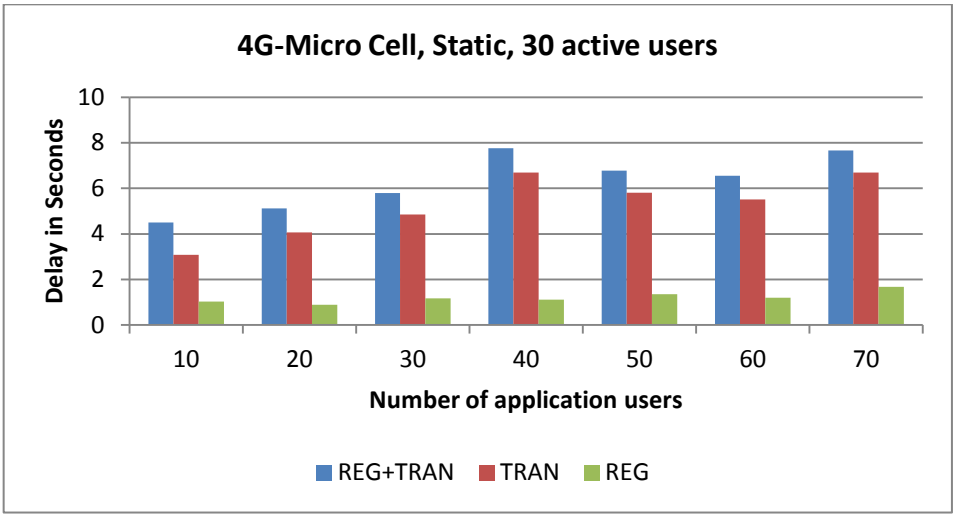


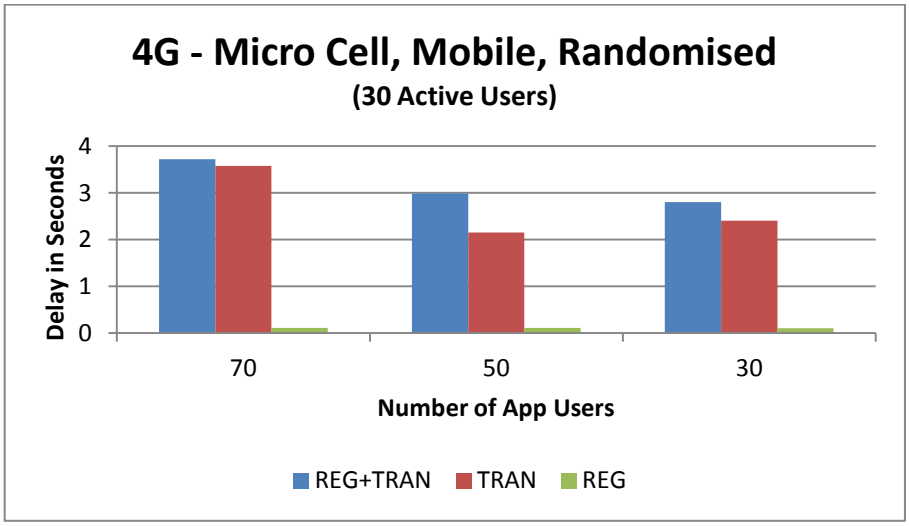
Handovers in the micro cell mobility case

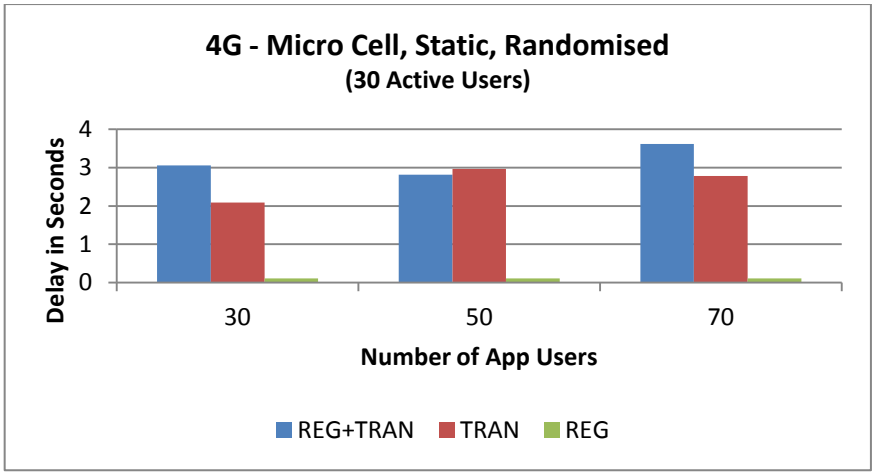


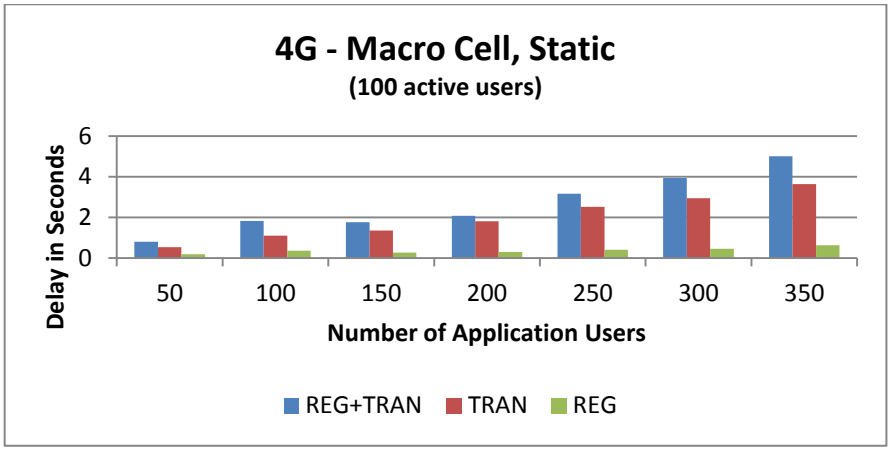
Hand over delay in micro cell mobility case

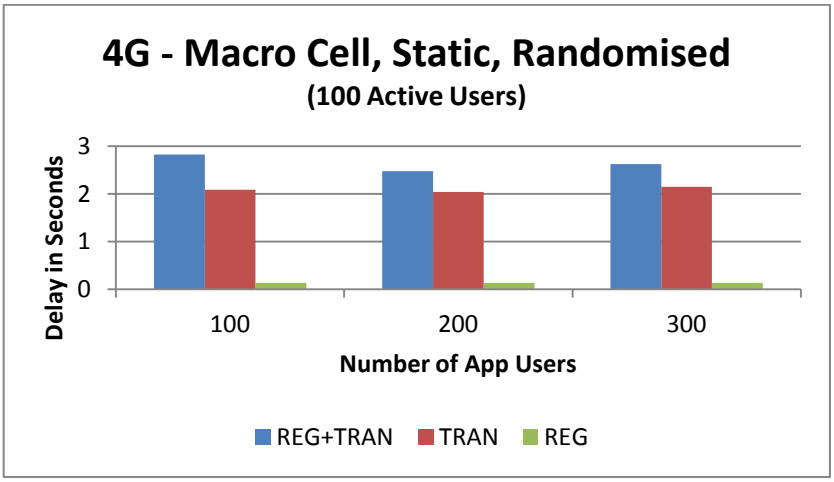

4 G - Micro Mobile (30 active users)
Delay in Seconds
10
8
6
4
2
0
10
20
30
40
50
60
70
Number of Application Users
REG+TRAN
TRAN
REG

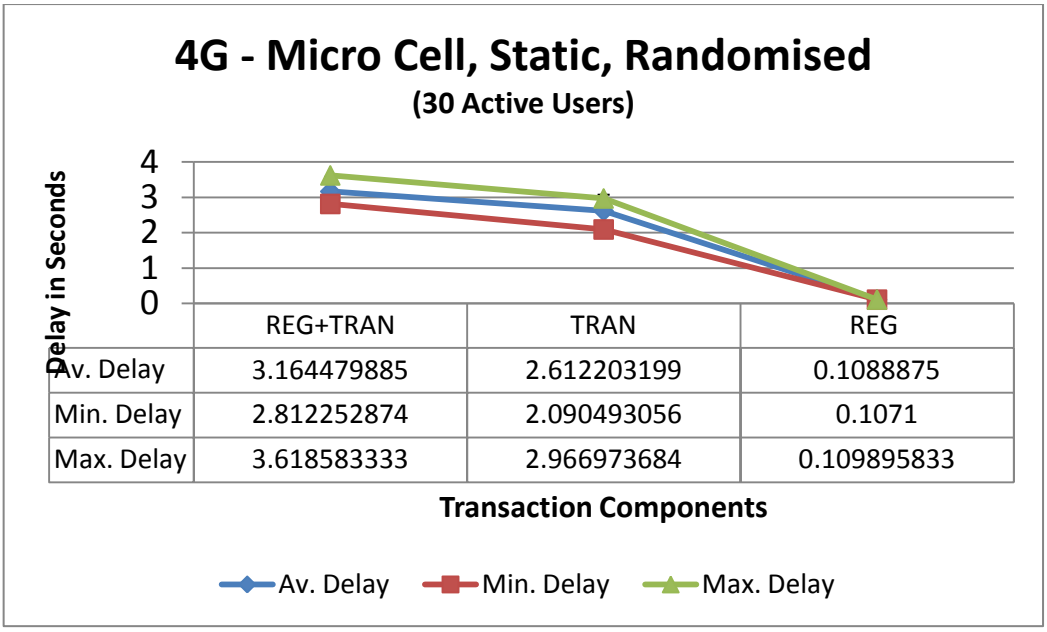

4G-Micro Cell, Static, 30 active users
Delay in Seconds
10
8
6
4
2
0
10
20
30
40
50
60
70
Number of application users
REG+TRAN
TRAN
REG

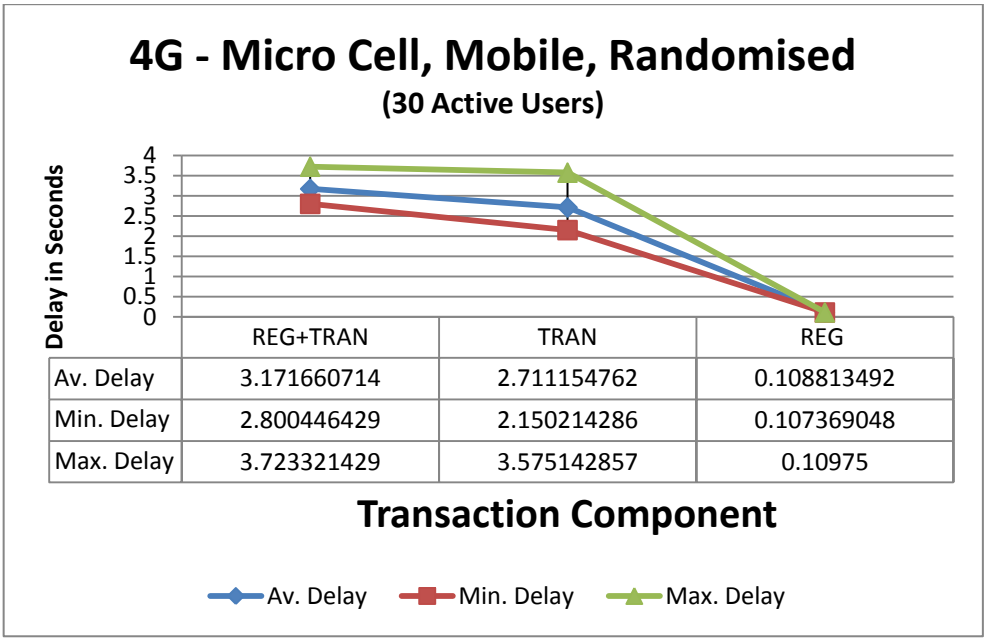

4G - Micro Cell, Mobile, Randomised
(30 Active Users)
Delay in Seconds
4
3
2
1
0
70
50
30
Number of App Users
REG+TRAN
TRAN
REG

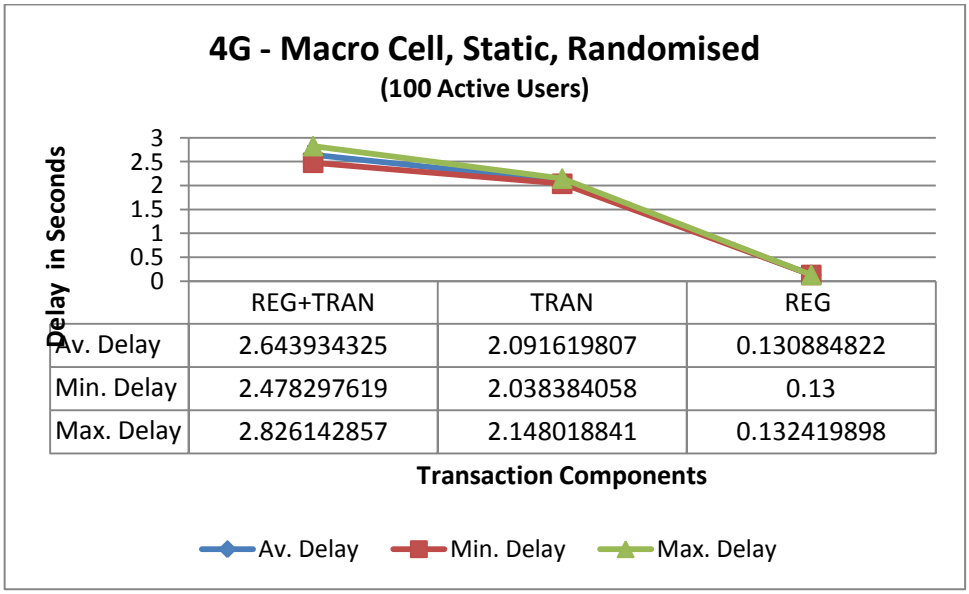

4G - Micro Cell, Static, Randomised
(30 Active Users)
Delay in Seconds
0
1
2
3
4
30
50
70
Number of App Users
REG+TRAN
TRAN
REG

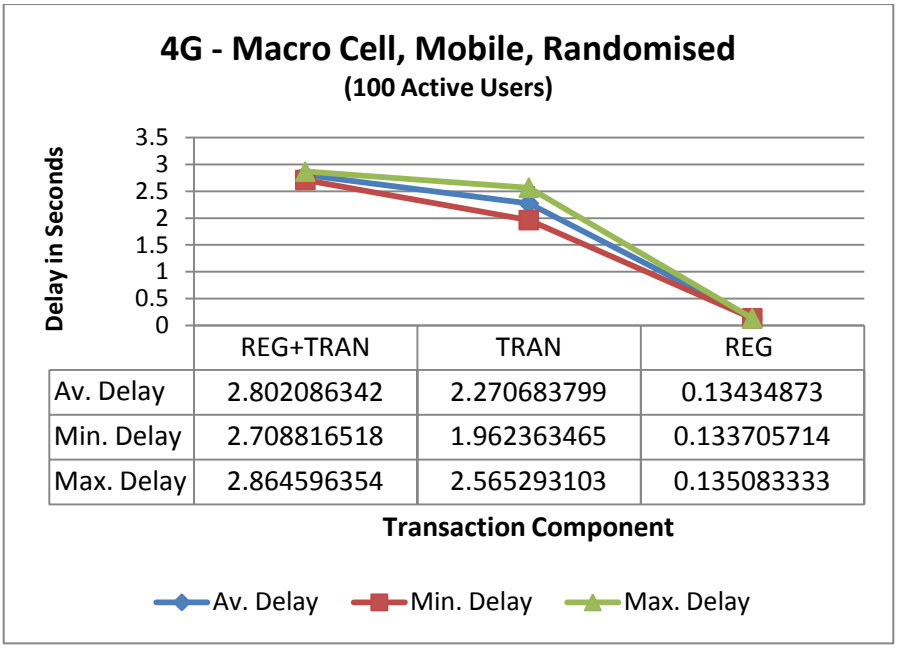

4G - Macro Cell, Static
(100 active users)
Delay in Seconds
0
2
4
6
50
100
150
200
250
300
350
Number of Application Users
REG+TRAN
TRAN
REG

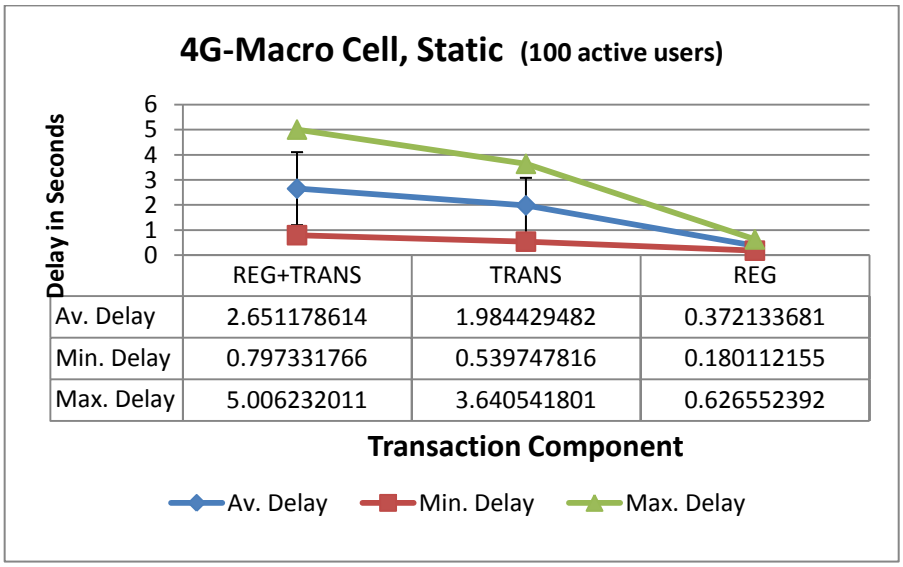

4G - Macro Cell, Static, Randomised
(100 Active Users)
Delay in Seconds
0
1
2
3
100
200
300
Number of App Users
REG+TRAN
TRAN
REG

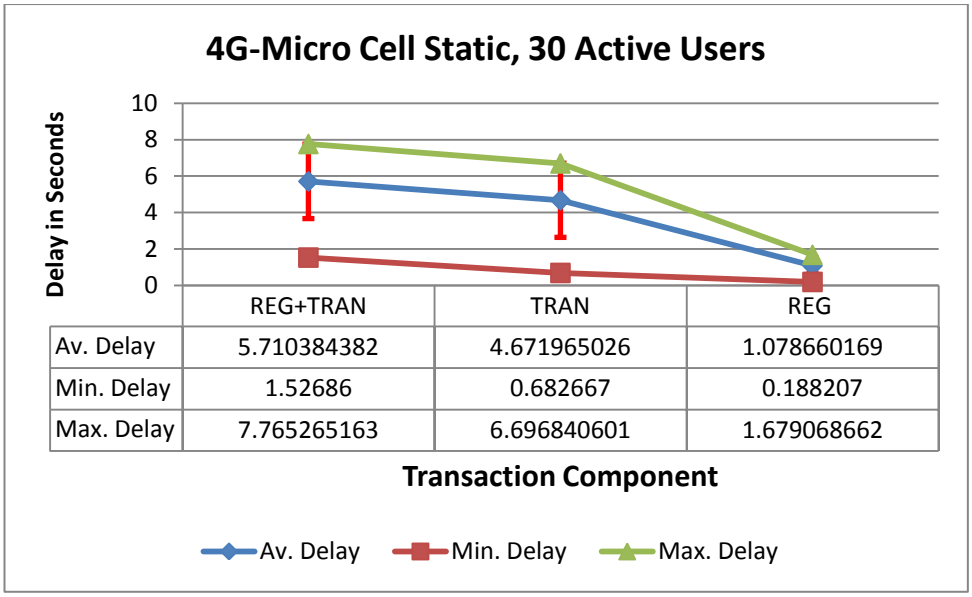

4G - Micro Cell, Static, Randomised
(30 Active Users)
Delay in Seconds
4
3
2
1
0
REG+TRAN
TRAN
REG
Av. Delay
3.164479885
2.612203199
0.1088875
Min. Delay
2.812252874
2.090493056
0.1071
Max. Delay
3.618583333
2.966973684
0.109895833
Transaction Components
Av. Delay
Min. Delay
Max. Delay


4G - Micro Cell, Mobile, Randomised
(30 Active Users)
Delay in Seconds
4
3.5
3
2.5
2
1.5
1
0.5
0
REG+TRAN
TRAN
REG
Av. Delay
3.171660714
2.711154762
0.108813492
Min. Delay
2.800446429
2.150214286
0.107369048
Max. Delay
3.723321429
3.575142857
0.10975
Transaction Component
Av. Delay
Min. Delay
Max. Delay

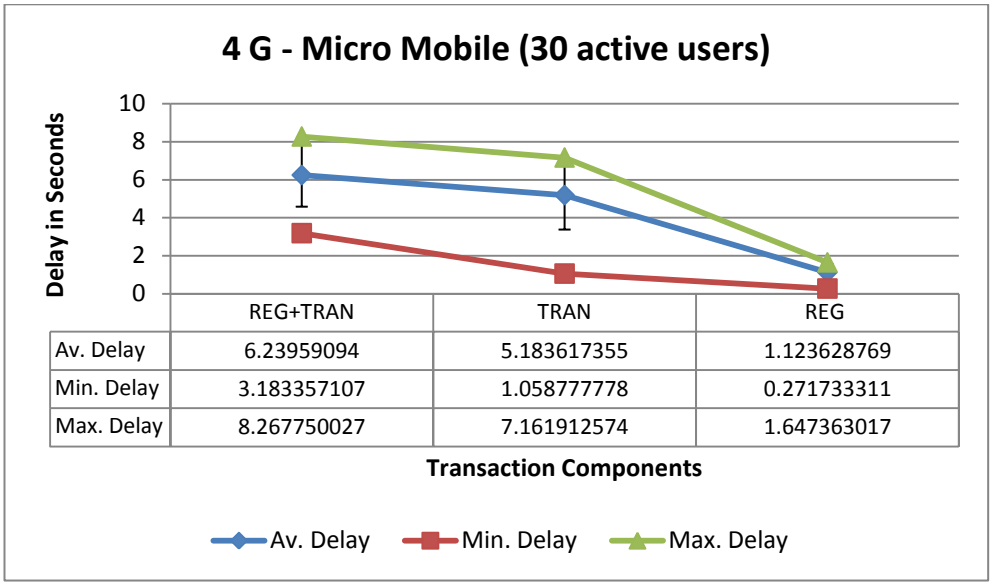

4G - Macro Cell, Static, Randomised
(100 Active Users)
Delay in Seconds
3
2.5
2
1.5
1
0.5
0
REG+TRAN
TRAN
REG
Av. Delay
2.643934325
2.091619807
0.130884822
Min. Delay
2.478297619
2.038384058
0.13
Max. Delay
2.826142857
2.148018841
0.132419898
Transaction Components
Av. Delay
Min. Delay
Max. Delay


4G - Macro Cell, Mobile, Randomised
(100 Active Users)
Delay in Seconds
3.5
3
2.5
2
1.5
1
0.5
0
REG+TRAN
TRAN
REG
Av. Delay
2.802086342
2.270683799
0.13434873
Min. Delay
2.708816518
1.962363465
0.133705714
Max. Delay
2.864596354
2.565293103
0.135083333
Transaction Component
Av. Delay
Min. Delay
Max. Delay

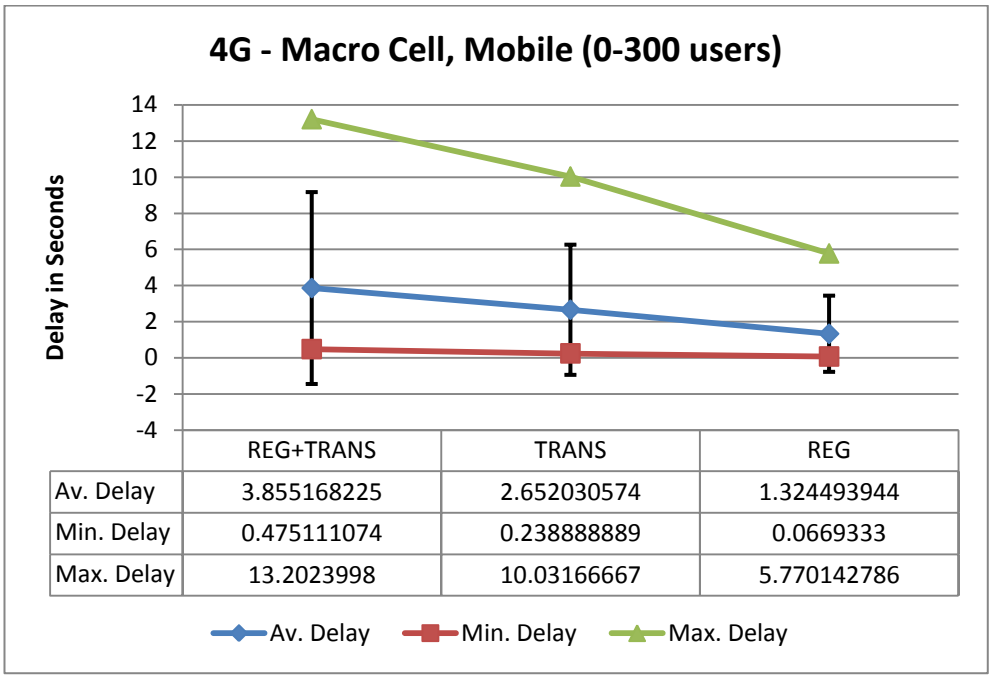

4G-Macro Cell, Static (100 active users)
Delay in Seconds
6
5
4
3
2
1
0
REG+TRANS
TRANS
REG
Av. Delay
2.651178614
1.984429482
0.372133681
Min. Delay
0.797331766
0.539747816
0.180112155
Max. Delay
5.006232011
3.640541801
0.626552392
Transaction Component
Av. Delay
Min. Delay
Max. Delay



	REG+TRAN	TRAN	REG
Av. Delay	5.710384382	4.671965026	1.078660169
Min. Delay	1.52686	0.682667	0.188207
Max. Delay	7.765265163	6.696840601	1.679068662

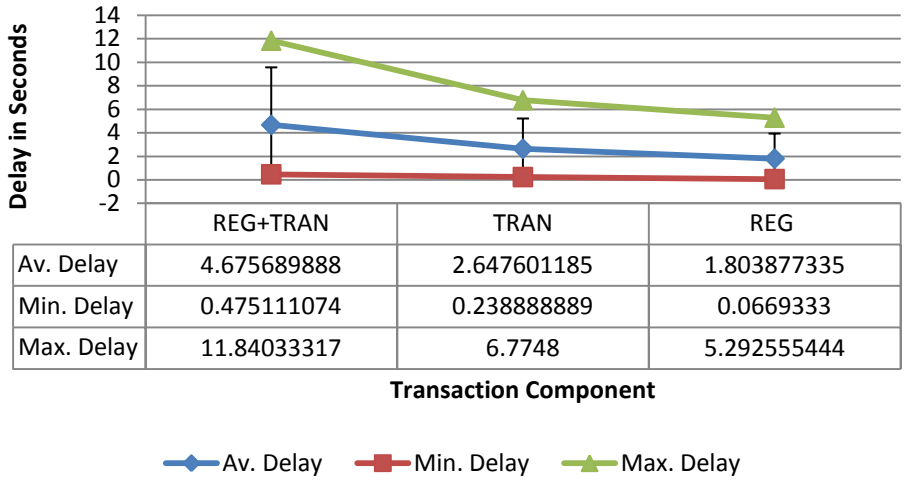


	REG+TRAN	TRAN	REG
Av. Delay	6.23959094	5.183617355	1.123628769
Min. Delay	3.183357107	1.058777778	0.271733311
Max. Delay	8.267750027	7.161912574	1.647363017



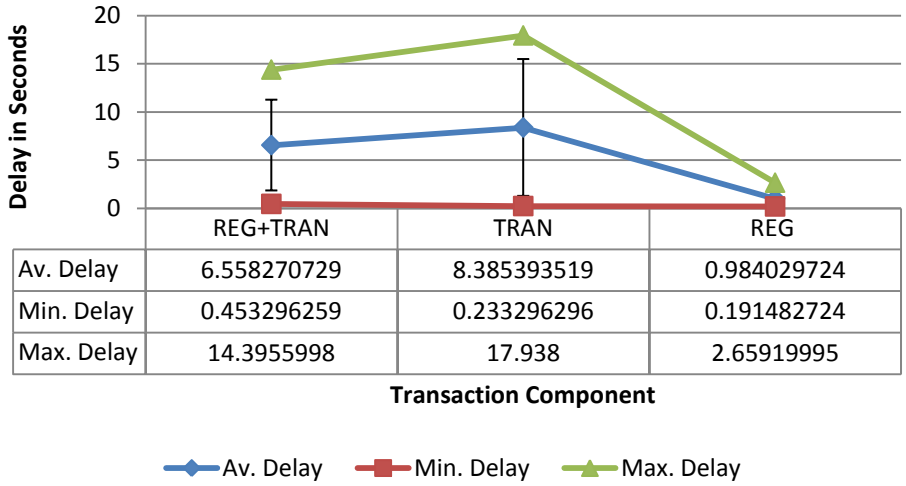
	REG+TRANS	TRANS	REG
Av. Delay	3.855168225	2.652030574	1.324493944
Min. Delay	0.475111074	0.238888889	0.0669333
Max. Delay	13.2023998	10.03166667	5.770142786

4G - Macro Cell, Static (0-350 users)



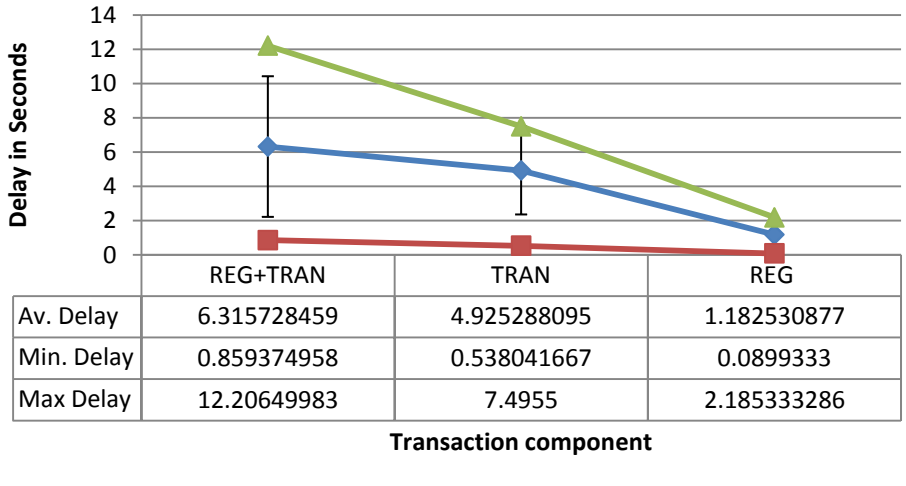
	REG+TRAN	TRAN	REG
Av. Delay	4.675689888	2.647601185	1.803877335
Min. Delay	0.475111074	0.238888889	0.0669333
Max. Delay	11.84033317	6.7748	5.292555444

4G - Micro Cell, Mobile (0-70 users)

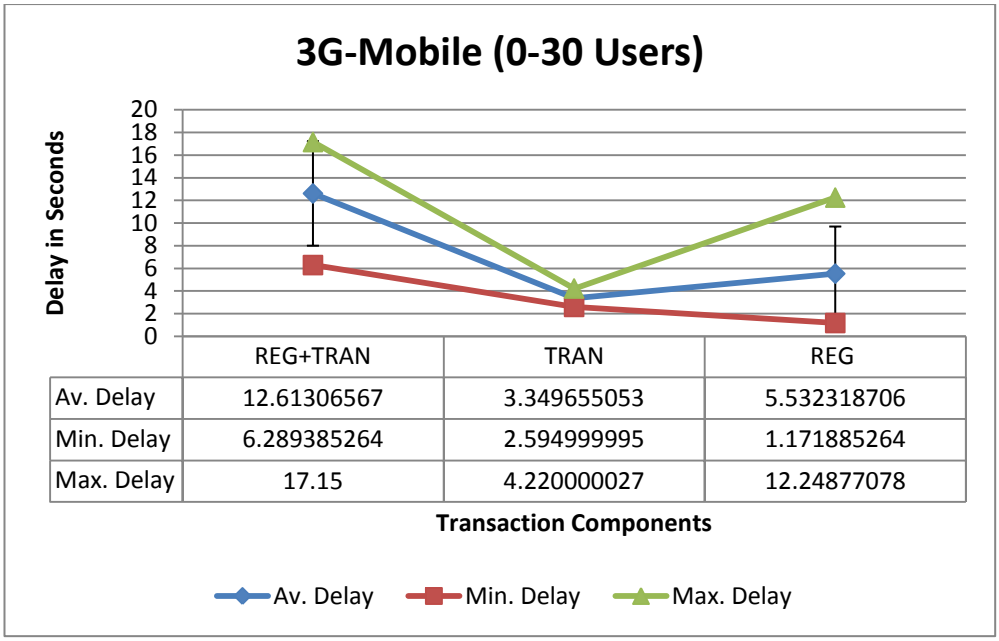


	REG+TRAN	TRAN	REG
Av. Delay	6.558270729	8.385393519	0.984029724
Min. Delay	0.453296259	0.233296296	0.191482724
Max. Delay	14.3955998	17.938	2.65919995

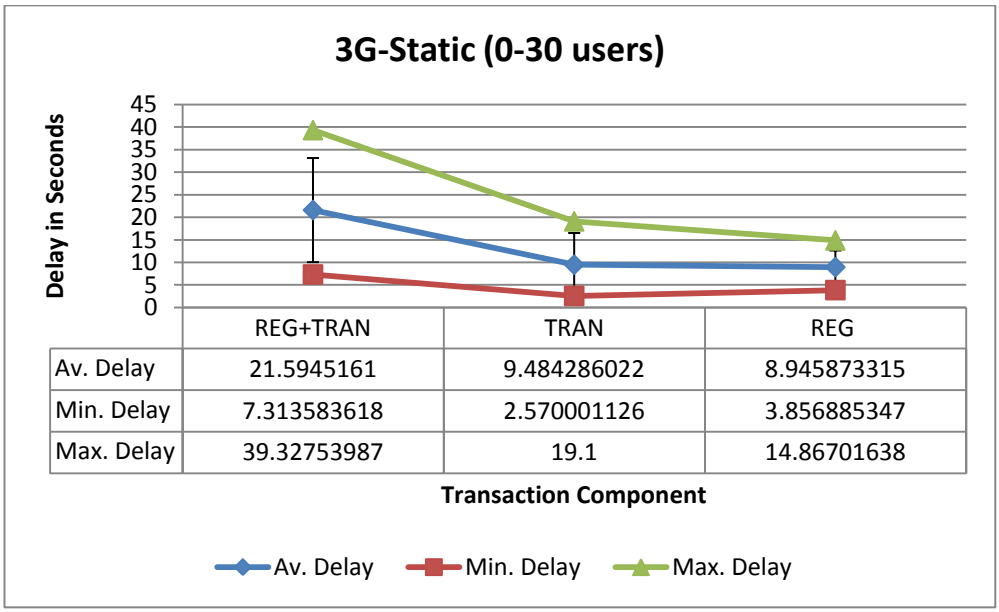
4G - Micro Cell, Static (0-70 users)



	REG+TRAN	TRAN	REG
Av. Delay	6.315728459	4.925288095	1.182530877
Min. Delay	0.859374958	0.538041667	0.0899333
Max Delay	12.20649983	7.4955	2.185333286



	REG+TRAN	TRAN	REG
Av. Delay	12.61306567	3.349655053	5.532318706
Min. Delay	6.289385264	2.594999995	1.171885264
Max. Delay	17.15	4.220000027	12.24877078



	REG+TRAN	TRAN	REG
Av. Delay	21.5945161	9.484286022	8.945873315
Min. Delay	7.313583618	2.570001126	3.856885347
Max. Delay	39.32753987	19.1	14.86701638