1-1-2011

A secure multiparty micropayment protocol for internet access over WLAN mesh networks

Nitish Biswas
Ryerson University

A SECURE MULTIPARTY MICROPAYMENT PROTOCOL FOR INTERNET ACCESS OVER WLAN MESH NETWORKS

by

Nitish Biswas

B. Sc. Engg.(EEE), Bangladesh Institute of Technology, Rajshahi, Bangladesh, 1988

M. Sc. Engg.(Computer), Bangladesh University of Engineering and Technology, 2001

A Thesis

presented to the School of Graduate Studies at

Ryerson University

in partial fulfillment of the

requirements for the degree of

Master of Applied Science

in the Program of Computer Networks

Department of Electrical and Computer Engineering

Toronto, Ontario, Canada, 2011

Author's Declaration

I hereby declare that I am the sole author of this thesis.

I authorise Ryerson University to lend this thesis to other institutions or individuals for the purpose of scholarly research.

Author's signature: _____

I further authorise Ryerson University to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

Author's signature: _____

Ryerson University needs the signatures from all the persons using or photocopying this thesis. Please sign below with address and date.

Abstract

A Secure Multiparty Micropayment Protocol
for Internet Access over WLAN Mesh Networks
© Nitish Biswas, 2011

Master of Applied Science
Computer Networks Program
Department of Electrical and Computer Engineering
Ryerson University

Presently, multi-hop WLAN mesh networks have become an alternative to wired networks for last-mile user access enabling numerous internet-based services. Thus, we have proposed MMPay, a secure multiparty micropayment protocol for internet access over WLAN mesh networks, enabling: a secure network access anywhere and anytime according to user desire; seamless user roaming across the independent operator's networks; and lightweight real-time payments to all involved parties that eliminate huge user trust relationships, online remote user authentications and mutual roaming agreements among the participating parties.

The incontestable MMPay scheme has been devised from existing micropayment schemes emulating their good attributes and eliminating security vulnerabilities and difficulties, which includes: hash-chain based variable length payment instrument, user's payment certificate at smartcard, shared and mixed signature scheme, and an efficient redemption approach. The OPNET-simulation results show that the pricing contract response-times are little lengthy but have no effect on data communication; payments and hand-offs are efficient; and the scheme has no effect on data communication ETE-delay and throughput. Thus, the scheme is secure, efficient and lightweight, and will be a practical solution for future small to large-scale WLAN mesh networks enabling faster hand-off.

Acknowledgement

I would like to express my sincere gratitude and profound indebtedness to my supervisor Dr. Cungang Yang for his constant guidance, helpful advice, knowledge sharing and endless patience throughout the progress of this work.

I gratefully acknowledge the kind support, valuable advice and encouragement of Dr. Bobby Ma not only during the course of this work but also throughout the program duration. His vast knowledge, experience and generosity were a privilege for me. I also would like to thank him and his staffs for providing a nice research environment and financial support.

I would like to covey sincere thanks to my defence committee and other reviewers for their efforts to review my work and insightful advice extended to me.

I would like to thanks Mr. Arseny Taranenko, Dr. Amir Esmailpour and Ms Xiaoli Li for their technical support and guidance. Thanks to all my classmates for their extended support during this difficult emotional time. Special thanks to all who have supported me during the progress of my work and the program.

Finally, I would like to express my hearty gratitude to my parents, family members and friends, especially Mr. Abul Akanda along with his family members for their never ending caring support, advice and encouragement to achieve this goal. I remember the grace of the almighty God allowing me to do this work.

to my family and friends

Contents

List of Tables

List of Figures

List of Abbreviations

ACL:	Access Control List
AES:	Advance Encryption Standard
AODV:	Ad-hoc On-demand Distance Vector routing
AP:	Access Point
AWPP:	Adaptive Wireless Path Protocol
BSS:	Basic Service Set
B:	Financial Broker
CA:	Certificate Authority
CDR:	Call Detail Record
DES:	Data Encryption Standard
DoS:	Denial-of-Service
DSL:	Digital Subscriber Link
DSSS:	Direct Sequence Spread Spectrum
EAP:	Extensible Authentication Protocol
EOIP:	Ethernet over IP
ETE:	End-to-end
FHSS:	Frequency Hopping Spread Spectrum
FSM:	Finite State Machine
GSM:	The Global System for Mobile Communications
H:	Hash Function
HMAC:	Hash Message Authentication Code
HWMP:	Hybrid Wireless Mesh Protocol
IEEE:	Institute of Electrical & Electronic Engineers
IMEI:	International Mobile Equipment Identity
IMSI:	International Mobile Subscriber Identity (IMSI)
ISP:	Internet Service Provider
LAN:	Local Area Network
MAC:	Medium Access Control/ Message Authentication Code
MAN:	Metropolitan Area Network

MANET:	Mobile Ad-hoc Network
MP:	Mesh Point
MPP:	Mesh Point Portal
MS/MU:	Mobile Station/ Mobile User
MSP:	Private Mesh Network Service Provider
NO:	Network Operator
OFDM:	Orthogonal Frequency Division Multiplexing
OPNET:	Optimized Network Engineering Tools
OLSR:	Optimised Link State Routing
PKI:	Public Key Infrastructure
pMAP:	Private standalone Mesh Access Point
PMK:	Primary Master Key
POS:	Point-of-sale
QoS:	Quality-of-Service
rMS:	Relay Mobile Station
SHA:	Secure Hash Algorithm
SP:	Service Provider
SSL/TLS:	Secure Socket Layer/ Transport Layer Security
TAP:	The Transferred Account Procedure
TID:	Transaction identifier of the pricing contract
TIPHON:	Telecommunications and Internet protocol harmonization over networks
TTP:	Trusted Third Party
TMK:	Temporal Master Key
UOBT:	Unbalanced One-way Binary Tree
VSAP:	Value Added Service Provider
WISP:	Wireless Internet Service Provider
WiMAX:	Worldwide Interoperability for Microwave Access
WMN:	Wireless Mesh Network
WPA:	WiFi-Protect Access

Chapter 1: Introduction

1.1 General

The Internet has become the main medium for social networking, communication, education, business, gaming, and entertainment. Customers access internet service mainly through fixed landlines and have a strong legal trust relationship with the service provider. Throughout the last decade, the vast development and deployment of wireless mobile networks such as 3G UMTS [HALSV02, LC01], WiMAX [WiM04], and WiFi [WiFi97], wireless networks have become the alternative to wired networks for last-mile connections. The wireless LAN mesh, WiMAX and their integration provide the opportunity to deploy a wireless metropolitan area network (WMAN) to access the internet over a mesh network and enable network access anytime and anywhere.

A huge number of value-added services, such as mobile internet applications, have developed along with e-commerce and m-commerce to satisfy user-interests. Different payment protocol schemes have been proposed and deployed to support e-commerce and m-commerce for session-based applications and event-based applications. In event-based applications, the user's payment is reflected by one time events, such as traditional macro-payment. But a session-based application consists of three phases: session-setup, communication, and session-end; users are charged during communication, based on either time spent or data volume transferred. In session-based applications, users can make payments using different micropayment protocol schemes. Micropayment schemes allow multiple payments in a payment transaction for a session-based application during the communication session.

Most of the present micropayment schemes are designed for single vendor payment, and non-repudiation is not considered. As the internet service access over a wireless mesh network may involve multiple parties in a transaction, they all have to be paid for their services in real-time to avoid unnecessary trust relationships among them. The present study is an effort to find a new variant of a micropayment protocol scheme to pay multiple parties simultaneously in a session; thus, a user can choose any available service provider for internet access anywhere and anytime.

1.2 WLAN Mesh Network for Internet Access

A wireless LAN (WLAN) mesh network is a multi-hop wireless network which emulates the bridge functionalities, where WLAN devices have relay functions that communicate directly with each other instead of communicating via the base station. In a WLAN mesh network congestion control, routing, QoS and security features are implemented in the MAC layer. WLAN mesh devices are of three types: Mesh Portal (MPP), Mesh Point (MP) and Mesh Access Point (MAP). The MPP is equipped with a gateway function and also provides transparent bridging functions. A mesh provides a high speed of 600Mbit/s over a shorter distance and provides a single broad-cast domain like the Ethernet Bridge. MAP provides the connection to legacy WLAN mobile stations (MS) having no WLAN mesh functionality. Mesh devices contain multiple radio interfaces and use separate channels for MP(s) and user-stations. The WLAN mesh (IEEE 802.11s) is designed for small-to-medium scale networks with a maximum of 32 MP(s) (MAP included), but multiple mesh networks can be connected through transparent bridges of the MPP to expand the network scale [ATYY06]. Presently a high-end MPP can communicate with 499 MP(s) and MAP(s), and thus a wireless LAN mesh network may contain thousands of MAP(s) to form a metro wireless mesh network.

The deployment of WLAN mesh technology by different vendors, its clean wall, easy, and cost-effective implementation approach have attracted small-to-large organizations to implement network services over the mesh. Currently most offices, educational institutions, health centres, public stations, marketplaces, and recreational centres deploy wireless mesh networks for user accesses acting as internet hotspots. They also provide different network services over WLAN mesh networks. Users get network access through their WLAN mesh interfaces or through legacy WiFi interfaces within the range of wireless mesh networks. Development of WiMAX mesh network technologies and its integration with WiFi provide further opportunities to deploy heterogeneous wireless mesh networks for client access. It is expected that in the near future, high-speed wireless internet service providers (WISP) with a WLAN mesh network will emerge in metro areas and be combined with WiMAX in rural areas. Different private value-added mesh network service providers (MSP) are also expected to emerge to further extend the coverage of WISP services.

Most of the user mobile stations are capable of communicating using one or more wireless technologies, and they are roamed frequently to different service providers and to access the network services. Thus, anytime and anywhere, a user can get access to a WISP network directly through other mesh user stations, through multiple independent private MAP(s), or through multiple private small network service providers over wireless mesh networks.

1.3 Multi-Party Micropayment for Internet Access over Wireless Mesh Network

The remarkable growth of the internet has brought with it the need to perform commercial transactions over the public internet and mobile network, thereby enabling electronic commerce (e-commerce) and mobile commerce (m-commerce). With the development of the internet and e-commerce, millions of value-added service providers (VSAP) have emerged to provide different network applications for user interests. Most of the services are small valued, real-time, and need multiple transactions. In order to pay for these VSAP(s) over the internet, different micropayment schemes are proposed with online and offline validation of the payment instrument, suitable for single-vendor transactions. Micropayment schemes allow multiple small payments as low as one tenth of a cent in real-time in a single transaction with lightweight cryptography like a hash chain.

With the evolution of wireless and mobile communication technologies, customers can access network services anywhere and anytime and can use internet services. Customers need a strong trust relationship with the home service provider to ensure payments and need predefined mutual roaming agreements between serving service providers and the customer‘s home service provider to roam anywhere. However, due to the requirement of strong legal binding, customers are not allowed to choose from the pool of available competitive local service providers. To overcome these difficulties, unnecessary trust relationships, roaming agreements, and multi-party payment clearance, Peirce [Pei00] first proposed a multi-party micropayment protocol for mobile communication to pay all involved parties in real-time as described below in Chapter 3. In the protocol scheme, RSA public-key certificates are used at service providers and brokers, but the customer is considered as the least trusted entity without public-key certificates, as customers are millions in number. However, other variants of

multi-party micropayment schemes for mesh ad-hoc network, a public-key certificate for a group of users and for a single user are proposed in tamper-resistant client smartcard devices.

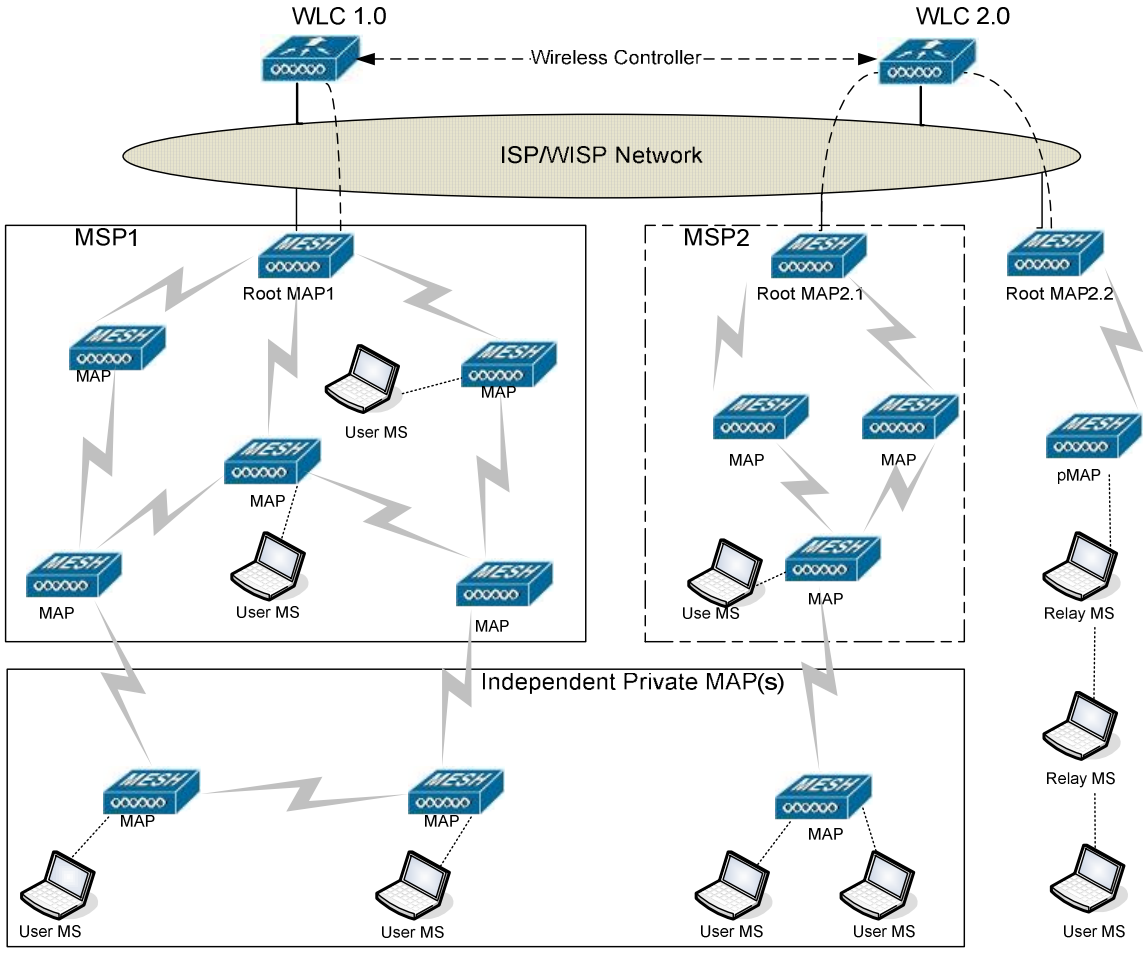


Figure 1-1 Internet Access over Wireless LAN Mesh Network

Internet access over a wireless mesh network also involves multiple entities, and they all provide network access service. It is considered that the service providers, beyond the local ISP/WISP, will be taken care of and remunerated by the ISP. But in local access the user mobile device may reach the ISP through multiple relay MS(s), through multiple pMAP(s) and private MSP(s) as shown in Figure 1-1. The internet access over the mesh may involve multiple service providers, and they have to be paid for their services. The customer mobile devices are insecure and move to access the internet from any ISP at any time, which leads to proposing a new variant of a multi-party micropayment protocol scheme to pay all involved entities in real-time to avoid an unnecessary and infeasible trust relationships among them. The protocol scheme is suitable for both the multi-vendor and single-vendor environment, and it is expected to solve the problem of identity theft, non-repudiation and fraud in e-commerce

as customer public-key certificates are used. The ongoing development of public-key cryptography mainly short signature scheme and identity based crypto, their deployment in smartcard devices and their hierarchical certificate deployment approach demand to use public-key digital certificates in micropayment schemes.

In the new proposed protocol scheme as described below in Chapter 4, all the participating entities in a transaction must register with a financial broker to obtain their pseudo identities and public-key digital certificates. All the financial brokers must have public-key digital certificates from the central CA and have CA authorities for their clients. The broker also provides the users with tamper resistant client smartcards for key generation, for maintaining certificate account balance, and for signing the first pricing contract. Users purchase payment certificates from their brokers or from any other online brokers using an existing macro-payment system. A payment certificate contains a user public-key along with other financial information and has a short expiry date to prevent unlimited use of the fund in case of a smartcard compromise. When a user first enters in a new WISP/ISP region, s/he signs the pricing contract that includes the first payment hash chain, an authentication chain, a hand-off secret, all involved parties' identities with their charges in the transaction, and a transaction identity. In case of a hand-off, ISP/WISP signs a new hand-off pricing contract including new parties; but the contract includes the last spent hash value of the existing payment hash chain and a new hand-off secret. The user smartcard releases payment hashes for an ongoing transaction and maintains the payment certificate balance. In the protocol scheme, the ISP/WISP alone is responsible for fixing the charges of a transaction and for redeeming payment hashes to a broker. Offline, only the redeeming broker verifies the pricing contracts and payment hashes, and compiles payment reports for all the participating entities according to the pricing contracts. All other brokers update their client accounts and broker accounts accordingly and clear inter-broker accounts periodically.

1.4 Motivation of Work

In recent years, wireless networks have become widely acceptable as an alternative to wired networks for connecting end user devices. Standardization of wireless technologies and their decreasing costs enable their success in the mass-market, specially increasing development of

wireless technologies, their security features. In addition, their easy and faster clean wall and cost effective deployment approach attracts all small and large network operators and value-added service providers to implement these technologies for customer services. The private and small service providers are inter-connected to reach wired internet service providers (ISP). A multi-hop wireless network topology is a mesh network, and presently most of the offices, public stations, market places, and recreational centres are internet hotspots. They provide different services through different wireless technologies like Wireless IEEE 802.11, Bluetooth, Infrared, Home RF, Wireless Mesh, and WiMax. User mobile devices are capable of communicating using one or more wireless technologies. Users roam frequently to different service providers in order to access the services. Thus, a user can be connected to an ISP directly, through other users, or through multiple private small network service providers. To obtain quality services, no one can expect free services from intermediate entities who are forwarding the network traffic among the ISP and users. Thus, all involved parties should be paid to cooperate with each other and for relaying network traffic.

A traditional billing system is credit based and needs a strong legal binding among customers and their service providers to ensure payments. This system has been used for about 120 years and works well in monopolistic environments with a small number of trusted service providers provides a limited number of services [Pei00]. And a user can roam to another service provider only when service providers have mutual roaming agreements to ensure their payments. However, for millions of VSAP(s) and cooperative network service providers, it is impossible to have mutual roaming agreements among all providers.

In a wireless environment, the internet access over multiple independent users and small service providers involves multiple parties. To pay multiple parties, either the user has to establish a trust relationship with all the involved parties or the user's home service provider must have roaming agreements with all of them, and then the roaming user needs to be authenticated by all the serving entities. All involved entities must have their own billing and accounting systems, and most of the time the values of their services are less than the costs of billing and accounting services. Thus, these roaming agreements are not only impossible; but also unrealistic in multiparty transactions. These difficulties motivate the use of multiparty micropayments to make a payment to multiple participating parties in real-time. The real-time

payment schemes avoid unnecessary user trust relationships and mutual service agreements among participating parties and the user service provider, and eliminate the huge trust assumptions, security risks, and overheads of billing and accounting systems.

Presently, most of the private wireless internet service providers such as internet hotspots, educational institutes, recreational centres, shopping malls, and public places, provide free internet access to user WiFi devices and realise their costs of services from other corners of their business. They provide the basic service without the premium services. To obtain quality premium services they must be paid for their services. Due to standardization of the wireless mesh network (802.11s) and WiMAX network (802.16), their integration and their cost-effective deployment approach, it is expected that high speed Wireless Metropolitan Area Networks (WMAN) will emerge in the near future. In a WMAN, movement of a user mobile station (MS) will cause a hand-off and a lengthy user authentication to multiple parties through the distance user home service provider; it may cause the end of ongoing sessions. The growth of WMAN(s) and different independent WMAN(s) operated by different operators in the same region will provide the user's opportunity to choosing any operator anywhere and anytime. The usage of any real-time payment protocol only enables this opportunity for the users, which motivates us to compile a new variant of a multiparty micropayment protocol scheme.

Present credit based billings need costly billing and accounting systems.They store different usage data information as CDR(s) at different levels of communication devices. The billing and accounting cost is estimated to be about €5.00 to €10.00 per user per month [Eng98] and the system requires storing the CDR(s) data for years to resolve disputes. It is expected that the monthly wireless usage bill to an independent service provider is less than the cost of accounting and billing. Credit based billing also suffers from non-repudiation as users do not take part in the billing process, and every years service providers loose about 3% to 5% of their total revenue due to fraud [Sey98, ES97]. In post-paid billing systems, there is no guarantee of full payment by the users, which requires engaging a third party bill collection agency. In 2000, Peirce [Pei00] first proposed a multiparty micropayment protocol to overcome the shortcomings of post-paid payment systems for mobile communication. In his scheme, users are the least trusted entities as they are billions in number. The protocol scheme

allows making payment to all involved parties in a call in real-time. He proposed the financial broker-signed hash chain as a payment instrument. A single payment hash from the commitment chain provides different values to different service providers involved in a call according to the enforcer signed dynamic pricing contract. He also extended the scheme to access ad-hoc networks and called it "Mobile Ad-Hoc Network Payment", where he proposed to use a user smartcard as an enforcer like a real enforcer on behalf of a financial broker with whom the user has accounts. He proposed a digital certificate for the smartcard enforcer for a group of 100 users instead of every user. Tewari and O'Mahony [TM01] proposed "Multiparty Micropayments for Ad Hoc Networks", which eliminates the trusted third party (the enforcer) signed price contract; they proposed public-key digital certificates for all users, and the users have to carry multiple payment commitments for data transfer over the ad-hoc networks. These works motivate us to search for a payment scheme for internet access over wireless mesh networks where all participating entities must have public-key digital certificates for achieving real non-repudiation. To get internet access from many available service providers using an existing micropayment scheme, users have to carry multiple payment instruments and one instrument must include one of the current service providers along the path. These two conditions are impossible for a huge number of service providers. Otherwise, users can carry a single chain with a common trusted third party (TTP) enforcer who will authenticate users and endorse payments; but the TTP may not be in the communication path. Then, the distance online communications are required. Alternatively, users can purchase payment commitment chain from financial broker at the time of authentication using an existing macro-payment system but Zhu [ZWM04] mentioned that the cost of each macro-payment is at least 20 cents using a credit card. Thus, usages less than 20 cents have no worth to service providers.

We are in a digital age and all the entities should have public-key digital certificates for their identities. Because of the emergence of e-commerce along with value-added services and independent internet service providers using wireless mesh networks, customers also need digital certificates having matching key pairs for pursuing various internet services with localised and offline user authentication and with real non-repudiation. Presently, many countries provide digital identities to their citizens mainly for security reasons. It is our opinion that this security vulnerability is due to corruption and the corruption itself is based on unauthorized and untraced monetary transactions. Thus, all the monetary transactions must be

authentic and traceable through non-repudiation for achieving accountability and transparency. Presently mesh network devices support both the private share-key authentication and public-key authentication for clients and for service providers. The share-key authentication scheme needs mutual knowledge about clients and service providers in advance and with the scheme non-repudiation is not possible. These factors motivate us to choose public-key user authentication in the new scheme.

In first world countries, most people use credit cards for shopping, bill payments and many other financial transactions that make their daily life dynamic, secure and comfortable. But identity theft and credit card fraud are the problems in e-commerce and in electronic payment systems. In 2008, McMaster University of Canada released a report on "Measuring Identity Theft in Canada". This report indicated that about 6% of Canadian adults, or almost 7 million people, were the victims of some kind of identity theft and spent over 20 million hours and $150 million to resolve the problems. And in more than the half of these unauthorised purchases credit cards were used. Other types of credit card frauds in Canada are also reported by Shane Gross in "Online Shopping" in March 2009 as:

- 37% of all lost funds are through fake credit cards, criminals skim information from magnetic strip of the cards;
- 23% of all card frauds are through stolen cards;
- 10% of all losses are through the card information obtained through telemarketing and deceptive internet sites;
- 4% of all losses are through identity theft unauthorized credit cards;
- It costs only $1 to purchase your credit card number online.

Shane Gross also cited US statistics of 2008 from "trustedid.com" indicating that there are over 10 million identity theft victims in the US; an identity is stolen in every four seconds, $8000 on the average it costs to restore one identity, and a victim spends 600 hours on average. He also cited US Federal Trade Commission 2007 statistics indicating identity thefts that has already cost consumers over $5 billions and 21% of consumers fear to conduct online transactions for this reason. Credit card fraud is somewhat limited through the use of tamper resistant chip cards and user authentication through the user password. But the identity theft can only totally be prevented using a client digital public-key certificate, which will make a user's identity public but will have no value without a user-signed authentication message.

The use of chip cards for client authentication mainly in payments is increasing. Thus, the chip card capacity and security features are increasing. Presently, most of the chip cards can handle multiple cryptographic functions, such as RSA, DSA, DES, AES, SHA, and the bilinear pairing function. These factors also have motivated us to use the client smartcard with a digital public-key certificate in our proposed protocol scheme.

1.5 Objective and outline of thesis

The thesis work is an endeavour to devise a secure multiparty micropayment protocol for internet access over WLAN mesh networks. The study includes investigation of existing multiparty micropayment protocol schemes; devise a new protocol scheme and finally a simulation of the novel protocol scheme in OPNET environment.

The thesis comprises six chapters. Chapter 1, the introduction, includes an overview of multiparty micropayment for internet access over WLAN mesh networks and gives the motivation of the work. Chapter 2 presents the overview of the wireless mesh technology, the existing billing systems for communication based services, existing electronic micropayment techniques, and emerging problems in billing and accounting systems. On the other hand, Chapter 3 presents existing multiparty micropayment schemes with their abilities and difficulties. In Chapter 4, we have proposed the new multiparty micropayment protocol scheme, MMPay. Security analysis and performance analysis are also presented there. Finally protocol optimizations are carried out according to the performance bottleneck. Chapter 5 presents the protocol simulation results and the results analysis. Simulation of sub-protocols has been performed in OPNET. In Chapter 6 we have concluded that the MMPay scheme is secure, lightweight and efficient.

1.6 Summary of contributions

The main contributions of the research work are:

(1) We have proposed a secure multiparty micropayment protocol for internet access over multi-hop wireless WLAN mesh networks.

(2) We have simulated the protocol scheme in OPNET as custom applications for performance analysis.

The MMPay has been designed as a secure and lightweight protocol scheme contributing the following aspects:

- We have proposed a user prepaid payment certificate for seamless user roaming across independent WLAN mesh networks increasing service provider's confidence in payments, and reducing the purchasing cost of a payment instrument.
- We have proposed multiple payment hash chains for a communication session without security vulnerability for reducing payment hash generation costs and storage costs at the user smartcard.
- We have proposed a hand-off secret to make payments unique for a communication session.
- We have proposed a data-transfer-credit-balance for service continuation with previous session balance at hand-off which also enables accurate accounting.
- We have proposed the signature of intra-domain hand-off pricing contract using keyed hash supporting fast mobility and without any security vulnerability.
- We have proposed an inter-domain mobility group for faster user authentication at inter-domain hand-off, supporting fast mobility.
- We have proposed single point payment redemption and an aggregation of redemption message by the ISP; that will reduce the payment redemption cost significantly.
- We have proposed user smartcards for the use of inexpensive user devices and universal devices, which will also prevent overspending by the users.

Chapter 2: Preliminaries

2.1 Introduction

From the beginning of human civilization, people have been getting services, providing services, and exchanging goods for fulfilment of their needs; money becomes an effective exchanging media for these activities. Money is a token having certain monetary value of an actual asset and issued by a trusted authority. Accumulation of goods or services in a transaction has certain value, accounting and valuation of this transaction is billing or invoicing. Transfer of money from one party to another for such a bill is a payment. Over the years, money has evolved to make payment systems efficient and secure. Modern payment systems are either account based or token based and money as a payment instrument includes cash, checks, payment cards, and other payment commitments.

Now in the information age and due to the emergence of the global internet system, different types of electronic communication based services are also emerging. Accounting and billing for these services, different automated electronic billing systems and payment systems have been proposed and implemented. The advancement of wireless technologies during the last few years, the wireless mesh network (WMN) as an access network for internet service along with value added services, its billing and payment systems appear as greater issues.

2.2 Wireless Mesh Network as Access Network

In recent years, wireless networks have become widely accepted as an alternative to wired networks for connecting end users for backhaul to internet access. Wireless networks bridge the distance among the base stations, the internet gateways, and the end-user devices. A WMN has no generalized definition or architecture but it is a special form of MANET. However, WMN(s) are multi-hop wireless networks having mesh routers or WLAN mesh points (MP) and mesh clients, where mesh routers have minimal mobility and formed WMN(s) backbone [AWW05]. A WMN is dynamically self-organized, self-healed, and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves (creating, in effect, an ad hoc network). This feature brings many advantages to

WMN(s) such as low up-front cost, easy network maintenance, robustness, and reliable service coverage. The general WMN(s) are characterised as follows:

(a) All nodes in WMN are wireless with limited transmission range and rate.

(b) Multi-hop wireless network, which provides extended coverage range, redundant routes, and non-line-of-sight (NLOS) connectivity among the mesh clients.

(c) Support for ad hoc networking, and capability of self-forming, self-healing, and self-organization. WMN(s) enhance network performance, because of flexible network architecture, easy deployment and configuration, fault tolerance, and mesh connectivity, i.e., multipoint-to-multipoint communications. Due to these features, WMN(s) have low upfront investment requirement, and the network can grow gradually as needed.

(d) Mobility depends on the type of mesh nodes. Mesh routers usually have minimal mobility, while mesh clients can be stationary or mobile.

(e) Multiple types of network access. WMN(s) provide backhaul access to the Internet, peer-to-peer (P2P) communications, and access to other wireless networks providing services to end-users.

(f) Dependence of power-consumption constraints on the type of mesh nodes. Mesh routers usually do not have strict constraints on power consumption. However, mesh clients may require power efficient protocols.

(g) Compatibility and interoperability with existing wireless networks.

(h) WMN(s) infrastructure consists of a wireless backbone with mesh routers. The wireless backbone provides large coverage, connectivity, and robustness in the wireless domain. However, the connectivity in ad hoc networks depends on the individual contributions of end-users which may not be reliable.

(i) WMN(s) provide integrated service by supporting conventional clients that use the same radio technologies having access point capability.

(j) Mesh routers in WMN(s) provide dedicated routing, have multiple radios and have multiple bridging capabilities.

2.2.1 Wireless Mesh Network Architecture

WMN(s) consist of two types of nodes: mesh router and mesh client. Figure 2-1 depicts the generalized architecture of wireless mesh networks [ZGWWMR07]. At the top level, there

are backbone mesh routers with gateways connected to wire internet, at mid level there are backbone mesh routers with or without gateway and at the bottom level there are user devices and the mesh clients. The mesh clients are of two types. First group, having routing enable mesh clients, forms mobile ad-hoc network (MANET) to extend the reach of internet access. Second group, having non-routing mesh clients, is connected to the access point (AP) to access network services.

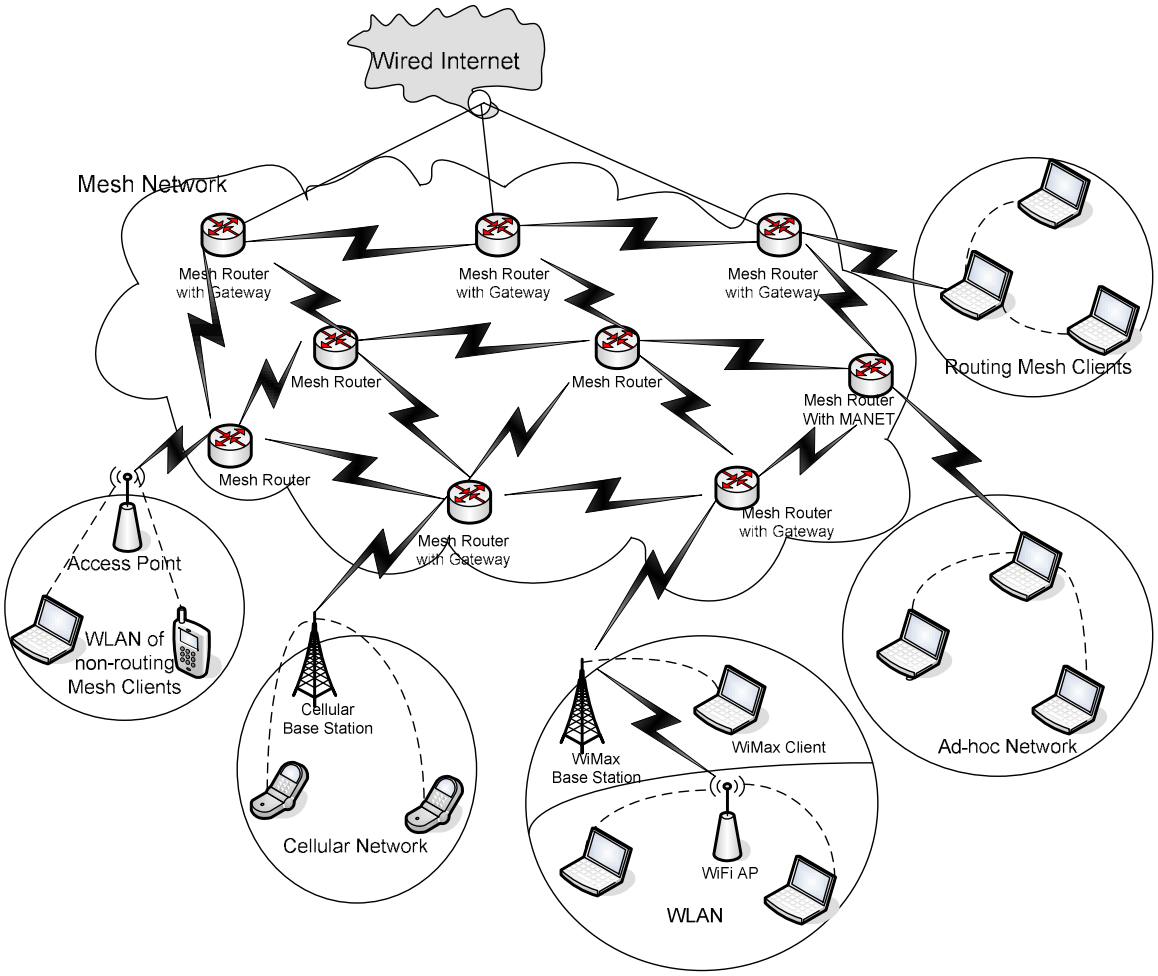


Figure 2-1 Wireless Mesh Network Architecture

Mesh Router:

Wireless mesh router contains additional routing functions to support mesh networking and gateway/repeater functions as in a conventional wireless router. For flexible mesh networking, a mesh router is usually equipped with multiple wireless interfaces built on either the same or different wireless access technologies. Compared with a conventional wireless router, a wireless mesh router can achieve the same coverage with much lower transmission power

through multi-hop communications. The medium access control (MAC) protocol in a mesh router is enhanced with better scalability in a multi-hop mesh environment and reactive routing protocols are embedded here. Wireless routers are usually built based on dedicated and compact computer systems. Enhanced security features are deployed using IEEE 802.1X standard and equipped with supplicant and enforcer functionality. In IEEE 802.11s technology, mesh point portal (MPP) is the backbone mesh router with gateway function. Mesh point (MP) is a repeater, mesh access point (MAP) is for the user access and MANET access.

Mesh client:

Mesh clients have the same wireless technology with or without routing functionality. They can be a laptop/desktop PC/ pocket PC/ PDA/ IP phone/ RFID reader. They may also have functionality to access AP or MANET nodes.

Mesh Architectures:

The architecture of WMN(s) can be classified into three main groups based on the functionality of the nodes:

(1) Infrastructure/Backbone WMN(s):

This type of WMN(s) includes mesh routers forming an infrastructure for clients that connect to them. The WMN infrastructure/backbone can be built using various types of radio technologies, mostly used IEEE 802.11 technologies. With gateway functionality, mesh routers can be connected to the Internet. Infrastructure/Backbone WMN(s) are the most commonly used types. Typically, two types of radios are used in the routers, i.e., for backbone communication and for user communication, respectively. In community usage, mesh routers are placed at the top of the roof for client access from the building and from the road, and backbone access to other routers placed on other sides normally over long range directional antenna.

(2) Client WMN(s):

Like MANET, client WMN provides peer-to-peer network connections among client devices. Client nodes constitute the actual multi-hop wireless network to perform routing and configuration functionalities as well as providing end-user applications to customers. Hence, a

mesh router is not required here. In Client WMN(s), a packet destined to a node in the network hops through multiple nodes to reach the destination. A client WMN is usually formed using single type radio interface.

(3) Hybrid WMN(s):

This architecture is the combination of infrastructure and client meshing as basic architecture shown in Figure 2.2-1. Mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients. While the infrastructure provides connectivity to other networks such as the Internet, Wi-Fi, WiMAX, cellular, and sensor networks; the routing capabilities of clients provide improved connectivity and coverage inside the WMN.

2.2.2 Security Features in WMN(s) Architecture

The wireless mesh networking has appeared as a new and promising wireless networking environment for the next generation wireless networks. It facilitates quick and easy extension of local area networks into a large-scale wide area networks. There are a great number of potential application scenarios for wireless mesh networks ranging from home and community networks to high speed MAN(s) as described in [AWW05]. In near future, heterogeneous WMN(s) are expected to be used and security is considered as the most critical issue there. Several survey of security requirement in wireless mesh network has been done as in [Ger06, RK08].

(1) Security Objectivise in Wireless Mesh Networks

To ensure the security of WMN(s), the following are the major objectives:

- **Confidentiality:** Certain information is only accessible to those who have been authorized to access it.
- **Integrity:** It provides guarantee of non alteration of transmitted messages.
- **Authenticity:** It provides assurance that participants in communication are genuine and not impersonators.
- **Non-repudiation:** It ensures that the sender and the receiver of a message cannot deny their transactions.

- **Authorization:** It is a process in which an entity is issued a credential by the trusted certificate authority. It is generally used to assign different access rights to different level of users.
- **Anonymity:** It allows user identity private and hidden to other communication parties.

(2) Security Attacks in Wireless Mesh Networks

The major attacks are briefly described as follows:

- **Denial-of-Service (DoS) attack:** The DoS or distributed DoS (DDoS) is to flood any central resource so that it can not perform.
- **Impersonate attack:** It is a serious attack in WMN(s). A malicious nodes as man-in-middle can get the authority of a valid special privileged node and can change the network configuration.
- **Routing table overflow attack:** An attacker attempts to create huge number of routes to nonexistent nodes and to prevent new routes from being created or to overwhelm the protocol implementation. This attack could also lead to a resource exhaustion or DoS attack.
- **Wormhole attack:** An attacker receives packets at one location in the network and tunnels them selectively to other colluding nodes and then resent the packets in the network again.
- **Black-hole/sink-hole attack:** A malicious node uses the routing protocol to advertize itself as having the shortest path to the node and then drops the received packet.
- **Byzantine attack:** An invalid operation of the network initiated by malicious nodes where the presence of compromised nodes and the compromised routing are not detected.
- **Location disclosure attack:** This attack reveals something about the structure of the network or the locations of nodes such as which other nodes are adjacent to the target, or the physical location of a node.

(3) Wireless Mesh Networks Security Mechanism

The IEEE 802.11i security mechanisms and the associated WiFi-Protect Access (WPA2) profiles provide the basic building blocks for 802.11-based security for mesh networking and for typical client access. The 802.11 security framework uses the 802.1X port-based access control mechanisms to prevent unauthorized wireless access. The client is the supplicant that requests authentication from an authentication server through authenticator. The Extensible Authentication Protocol (EAP) is a flexible protocol used to carry arbitrary authentication information, and rides on top of 802.1X and RADIUS. Authentication methods are based on TLS/SSL technologies where a secure tunnel and network-to-client authentication can be performed using a digital certificate (X.509v3), and clients can authenticate using either their own client certificate (EAP-TLS) or provide a username and password authentication exchange inside the secure TLS tunnel (EAP-PEAP or EAP-TTLS). Upon successful client authentication, keying material is generated and distributed to enable encryption and integrity checking. The integrity checking prevents both message tampering and ensures an authenticated client cannot be impersonated. The WPA2 profile adds AES encryption and key management. The standard of WPA2/802.11i security mechanisms are summarized below [Ger06]:

- Standardization activities for security will focus on inter-AP security controls, where client access uses standard WPA2/802.11i authentication and encryption.
- Standardization on security between mesh access points is still being finalized within the standard. However, link-by-link security mechanism will be based on 802.11i, with a security architecture based on 802.1X authentication.
- Mesh APs may have supplicant, authentication and authentication server roles.
- EAP 4-way handshakes must occur between all mesh routing peers, where centralized 802.1X authentication is supported. However, means of communicating between authentication server and remote mesh AP is presently not within the scope of the standard.
- The 802.11r standard for client mobility influences the security architecture by enabling a hierarchical key distribution scheme to improve mesh route maintenance.

(4) Security Features in Wireless WLAN Mesh Products

There are different wireless mesh networking products having different architectures and capabilities. All products offer multiple SSID policies with WPA2-compliant client access. However, their security features vary greatly. Detailed security features of Cisco 1500 Series Mesh AP(s) are described in [Ger06] as they are introduced at March 2005. The Cisco Lightweight Mesh Access Point extends the lightweight AP model to the multi-hopping mesh architecture. The mesh access points connect and authenticate to a Cisco WLAN controller using a proprietary Adaptive Wireless Path Protocol (AWPP). The followings outline some of the product highlights:

- 802.11i compliant station access on the first hop
- Lightweight architecture uses LWAPP with shared key or X.509v3 authentication between AP and WLAN controller
- Multiple SSID and VLAN mappings with different security policies
- Certificates pre-provisioned with a digital-certificate-based trust relationship between AP and controller, where access granted by MAC address ACL tied to digital certificate
- Extensive packet filtering capabilities

2.2.3 Application of WMN(s) for Internet Access

WMN(s) have clear advantage over other wireless networks like cellular, standard IEEE 802.11 WLAN, ad-hoc network, sensor network for implementing localized broadband network solution along with backhaul internet access. These applications motivate the research and advancement of WMN(s). The main applications are as follows:

- Broadband home networking
- Community and neighbourhood networking
- Enterprise networking
- Metropolitan area networking
- Public place and transportation system networking
- Health and medical systems networking
- Building automation
- Security surveillance systems networking

- Emergency systems networking

These WMN(s) applications along with their own internet access system, as a group can share the internet access with others and can extend the range of coverage area. These make the internet access system reliable, robust, redundant, and cost effective.

2.3 WiMAX as Access Network

WiMAX (Worldwide Interoperability for Microwave Access) is a telecommunication protocol that provides fixed and mobile Internet access. The current WiMAX revision provides up to 40 Mbit/s with the IEEE 802.16m update expected to offer up to 1 Gbit/s fixed speeds. The forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL". WiMAX covers long range up to 50 KM but like other wireless technology its speed is decreased with the distance covered. With IEEE 802.16e standard it can cover mobility up to 70 KM/hours.

Main components of WiMAX mesh are base station (BS) and subscriber station (SS), the client mobile device. BS provides the access service to the SS(s) using scheduling algorithm, gateway to internet, and backhaul to cellular network. SS(s) communicate to BS and can form ad-hoc network for peer-to-peer communication over user nodes.

Wireless access techniques are continuously expanding their transmission bandwidth, coverage and quality of service support in recent years. Present success of Wireless Local Area Networks (governed by the IEEE 802.11 standards), integration of WiMAX with WiFi technologies has been proposed [LLCC09]. Traditionally, WiFi hotspots are connected to the Internet through a wired connection (e.g., Ethernet), and therefore have high deployment costs, particularly in remote rural or suburban areas with low population densities. Therefore, it has been suggested that the evolving family of WiMAX-based Wireless Metropolitan Area Network (WMAN) technologies represent a promising solution for providing WLAN hotspots with backhaul support [NH07] and having reduced backhaul cost. Using a WiMAX-based backbone network to connect WiFi hotspots to the Internet not only avoids the requirement for a costly wired infrastructure but also makes the provision of wide range of heterogeneous wireless mesh network topology.

2.4 Accounting and Billing for Communication Services

All network service providers must be remunerated for the use of their resources for services provided. Recording of usage of resources to render services is accounting and billing is a process of applying tariffs to the usages details to generate invoice for payment. Peirce [Pei00] made a study for the billing methods and he mentioned in general that the existing billing systems collect usage details in form of Call Detail Records (CDR) and send them to the billing server. The contents of CDR vary depending on vendor, services, and billing rates.

2.4.1 Fixed Telecommunication Billing:

Like early manual telephone exchange of late nineteen century, current automatic exchange records call details (CDR) using automatic message accounting system. The size of a CDR can range from 20 bytes to several hundred bytes. Normally two or more records are created for the same call, an originating record, and terminating and trunk record. CDR(s) are stored at local exchange and periodically sent to remote centralized billing system, but they are sent immediately for hot billing. Billing software extracts required billing information from CDR(s) and calculates calling cost applying appropriate tariff based on call distance, call duration, time of day, subscriber type, QoS etc. CDR is the only proof of a call and a sophisticated duplication scheme is used to prevent the loss. However there is no authenticity of these records as they are created by network operator only. Thus CDR(s) can be denied by customers or falsified by the network operator.

Along with CDR the raw switching data are stored for settlement of customer dispute. These huge customer CDR(s) are required to store at least for a year or longer. CDR is standardised by European Telecommunications Standard Institute (ETSI) for billing and statistical purpose. The critical fields for billing are the source of a call, destination of a call, time and duration, routing points, and service information.

2.4.2 Credit based Mobile Telecommunication Billing:

Mobile networks consist of a large number of independent network operators, spanning many different geographic areas and countries. Mobile users roam frequently between operators who have arranged a bilateral roaming agreement. Unlike fixed telecommunication system, billing

in mobile systems have a roaming leg, an originating leg, and a terminating leg. In telecommunication, a calling party normally bears all the cost but in the case of calling to a roamer, a roamer bears the cost of a roaming leg and terminating leg. Multiple CDR(s) or toll tickets can be generated for different legs that include the originating, terminating, and roaming call components. The Global System for Mobile Communications (GSM) uses 17 different types of toll tickets and the one for a mobile originated call contains 55 possible fields [ETSI99c]. The International Mobile Subscriber Identity (IMSI) identifies the source of a mobile originated call. In addition to regular CDR, the toll ticket contains location area, cell ID, radio channel allocation and international mobile equipment identity (IMEI).

The visited network operator provides services to roamers without subscriber contracts or credit authorisations but authenticates the roamers with their home network operator. In GSM the CDR(s) of roamers are transferred from the visited network back to the home network using TAP, the Transferred Account Procedure. The Cellular Inter-carrier Billing Exchange Record (CIBER) is used for roamer billing by operators of CDMA, US TDMA and analogue AMPS networks. Each network operator may have to exchange CDR(s) and payments with a huge numbers of other network operators. The GSM Association has introduced a wholesale tariff among GSM operators for roaming services, called the Inter-Operator Tariff (IOT).

2.4.3 Prepayment Mobile Telecommunication Billing:

In this billing scheme, a strong legal binding agreement with a customer is not required and users pay in advance for a desired service. Calls are cut-off in near real-time when the pre-paid amount has been used up. The coin-operated payphone was one of the first pre-paid solutions for the telephone network. Prepayment in a mobile system is complicated as users receive call and roam. The majority of pre-paid mobile solutions are based on temporary accounts, maintained at the home location. Prepaid international roaming imposes additional difficulties because the prepaid account at home location must be decremented in real-time as calls are made. The Customised Applications for Mobile network Enhanced Logic (CAMEL) allows home NO(s) to provide operator specific services to their roaming subscribers. When a roaming user initiates a call, the CAMEL process in their home network is contacted by the visited network for further instructions. CAMEL sends charging mechanism, call limit and

CDR format to visited network. For real-time prepaid roaming CAMEL is contacted online at before, during and after every call. Charging mechanism for prepayment scheme is relatively simple and thus simple CDR format is used for billing and the statistical purposes.

2.4.4 Mobile Data Billing:

Currently mobile and internet are integrated networks and millions of mobile users use internet service from their mobile phones. Initially data communications were provided by the Short Message Service (SMS) over voice channel in GSM. Presently, the General Packet Radio Service (GPRS) and the Enhanced Data Rates for GSM Evolution (EDGE) are used in GSM for shared packet switched service. CDMA uses the High Speed Packet Access service HSPA for data communication. Considering the wireless bandwidth and mobile device screen size and capability, a lightweight wireless application protocol (WAP) suit has been designed. Thus a WAP gateway is required at NO side to translate. Billing for the use of the radio resources takes place as before using TAP.

In GPRS billing, three different CDR(s) are introduced. They record usage information at different positions of the network. The mobility management CDR (M-CDR) containing location and identity information is generated at Serving GPRS Support Node (SGSN) when the GPRS user first attaches to the network. The SGSN CDR (S-CDR) and the GGSN CDR (G-CDR) are created at the start of a GPRS session. The S-CDR records the radio network usage including the QoS, while the G-CDR remembers the external IP network usage and optionally external IP. Mobile data increases the number, size, and complexity of CDR(s) that records every change during a session to allow accurate billing. CDR(s) are transferred reliably to a common charging gateway for billing using the GPRS Tunnel Protocol (GTP) over UDP/TCP.

2.4.5 Internet Usage Billing:

The Internet forms the central part of 3G and 4G networks and thousands of application providers and content providers are providing their value added services over IP. Different CDR(s) are used for different IP traffic, applications and services. Service Detail Records (SDRs) are used to record the reservation and usage of network transport services for different

networks like IP, ATM etc. The Contract Negotiation and Charging in ATM Networks (CANCAN) ACTS project [CAN98] defined the format and contents of a SDR specifically for ATM. The SUSIE project [SUSI99] defined the SDR for internet service with best-effort (IntServ) and internet service with quality of services (QoS) as Premium IP Service (DiffServ) as A Premium IP Network Accounting Record (PIP-NAR). SUISE also proposed SDR and charging scheme for Multi-Protocol Label Switching (MPLS) usages. SUISE estimated the cost for SDR processing in real-time for hot billing is 2.17 cents [SUSI00].

The IPDR organisation, an industry consortium set up in 1999, has defined a generic common usage record format, the IPDR for recording any type of IP resource usage generated by routers, bandwidth managers, gateways, roaming access servers, application servers and e-commerce transactions. The Network Data Management–Usage (NDM-U) [IPDR00] document defines the initial structure of an IPDR in XML. The IPDR contents and fields are not fixed, called usage attributes, are defined as XML elements for different services. For example, there are 38 fields defined for a VoIP service that are completely different from those defined for an e-mail service. Presence of huge numbers of IPRD(s) make billing process complex. Jalda [Bog00] proposed an alternative to generating detailed CDR(s), where a provider calculates the charges in real-time and sends a simple charge request to the billing host. In Jalda at the start of a session with a content provider the user digitally signs a contract authorising a payment up to a specified amount for that provider. The signed contract is passed to a central independent billing server through the provider with whom the user has an account. As the user utilises resources the provider sends multiple charge requests instead of a CDR to the billing server over secured SSL.

The Open Settlement Protocol (OSP) [ETSI00d], proposed by TIPHON, defines how inter-domain usage, pricing, and authorisation information is exchanged between Internet telephony operators. The OSP defines a CDR format, a Usage Detail element for IP telephony. There are fields to allow the billing unit to be in seconds, packets, or bytes, and several different address types, including e-mail, IP addresses, H.323 identifiers [ITU99a], or E.164 telephone numbers [ITU97b]. The OSP adds digital signatures to CDR(s), preventing tampering during the clearing process.

2.4.6 Content based Billing and non-Repudiation:

In 3G and 4G architecture a large number of competing Value-Added-Service-Providers (VSAP) are providing on-line contents and services. Content based billing (CBB) service information is recorded at WAP-gateway as WAP-CDR and content supplier web-server as web-CDR according to 3GPP standards. CDR(s) contain OSI Layer-3 to OSI Layer-7 information for duration, volume and content based billing. The Content Based Billing (CBB) allows service providers to bill for application-based (IP) and content based services, and to generate additional revenue by differentiating their service charges.

There is a security risk to generate CDR(s) by the VSAP(s) and thus the non-repudiation is required for services and billing. The Advanced Security for Personal Communications Technologies (ASPECT) proposed an incontestable charging procedure, designed to allow small payments for value-added services [HP98, MPMH+98, HHMM+98]. The ASPECT approach is to break a call into two chargeable components. The first component is the basic charge for bearer services, the transport of call data, provided by the network operator which is handled using traditional billing. The second chargeable component is the premium rate charge for use of services provided by a VASP. The ASPECT solution allows the mobile user to make many small payments directly to the VASP, as the services are provided. Each payment token can only be generated by the user as a proof that s/he agrees to pay the VASP a small fixed amount. At the end of the day, the VASP forwards the payment proof to the user's NO, who then bills the user in the traditional fashion. But this approach still does not provide non-repudiation of NO bill and does not guarantee of payment by the user. Presently most of the content billing is revenue sharing approach where content usage bill is generated at user NO based on WAP-CDR(s) and VSAP(s) are paid based on billed to customer NO which is generated at VSAP based on WEB-CDR(s).

2.5 Electronic Payment Systems

The providers of goods or services must be remunerated for the cost of their resources usages, and the respective costs are determined in billing systems in form of invoices. Payments against the invoices are the real remunerations for their services or goods. Electronic payment is the transfer of monetary value in form of electronic means from one party to another over

internet. There are mainly two electronic payment models: traditional macro-payment and micro-payment. The traditional payment model allows only one payment in a payment transaction which has been widely adopted in the event based applications. On the other hand micro-payment allows multiple small valued payments and suitable for the session based applications.

The examples of traditional macro-payment model include the credit card platforms [BGHH+00, And98, SET97, LM94] and the electronic cash platforms [BBCM+94, MN93, CMS96]. The Secure Sockets Layer (SSL) [FKK96], and its successor, Transport Layer Security (TLS) [DA99] and a WAP version of TLS, the WTLS [WAP99a], are used to encrypt all messages, including the payment card details, sent between the payer and the payee over the World Wide Web. SSL uses X.509 public certificate mainly for vendor authentication. Robust cryptography of macro-payment requires heavy calculations and message transactions and thus it needs minimal fee about 20 cents per payment transaction [ZWM04], therefore is not suitable for charging smaller amounts.

A micro-payment scheme, with lightweight cryptography, is an electronic payment system designed to allow efficient and frequent payments of small amounts, as little as a tenth of a cent. For these it uses minimum CPU computation, message communication and relaxes security requirements, which is acceptable due to the small amounts involved. The majority of micropayment systems are designed to pay information goods over the internet at a peer-to-peer transaction and they need communication with trusted third party at the beginning of a payment. It has two payment models, the notational payment model and the token based payment model. In notational model, users transfer the payment message enabling the value of the payment and the payment orders and such systems include Millicent [Man95], Micro-iKP [Bel95], NetBill [ST95], and SVP [SV97]. In the token model, the transaction mainly exchanges payment tokens. The token represents coins or bank notes; PayWord and MicroMint [RS96] are payment systems of such type.

With the growth of wireless and mobile technology m-commerce has become popular. As most of the transaction involves multiple parties, in 2000 Peirce [Pei00] proposed first multi-party micro-payment protocol and its variants in his PhD thesis. Later in 2001 Zhu

[ZWM04] also proposed similar micropayment protocol for multiple vendors, those are detailed in Chapter 3. Pierce studied all existing micropayment schemes and classified them into different categories according to cryptographic technique used are public-key, secrete sharing, hash chain, hash collision and sequence, and probability. He concluded hash chain based schemes are the best suited to a scenario with computational lightweight user devices with small storage and limited bandwidth, and vendors who have to process a large number of payments per second. He also introduced one of the NO as an enforcer who signs pricing contract and keeps user balance limiting the usage of RSA certificate. Some of the potential micropayment schemes are descried here:

In 1996, the first group of micropayment schemes were Pederson's phone ticks [Ped96], PayWord [RS96], NetCard [AMS96], and iKP micropayments [HSW96]. They were independently proposed using hash chains [Lam81]. On the first payment to a new vendor, the user signs a commitment to that vendor with a new hash chain. Vendor identity in the payment commitment prevents it being redeemed by other vendors. A broker, or trusted third party, is introduced to aggregate micropayments to many different vendors. Actual monetary value is claimed by redeeming the highest spent hash token, along with the commitment, at a broker with whom the user has an account. The average cost per payment is (n hashes + 1 signature)/z, where z number of payment has been made using n hashes. The cost is the same as the cost of public-key based schemes when only single payment is made and schemes have same issue of PKI implementation.

Mini-Pay [HY97] and NetCents [PHS98] are pure public-key based micropayment schemes. In Mini-Pay customers buy daily credit limit from their brokers and spend it to any vendor singing with his RSA private-key provided by the broker. However, in case of customer software compromise, there is a possibility of overspending but traceable by the broker. On the other hand in NetCents, vendor specific credit certificate is used and vendor can transfer the balance to other vendors, and here there is no chance of over spending but at the beginning of a transaction with a new vendor an on-line communication with the broker is needed. These public-key based schemes require PKI implementation, which makes it unsuitable to implement.

Rivest and Shamir's MicroMint [RS96] is the first micropayment scheme using the idea of hash collisions. Broker issued payment tokens are defined as k-way hash function collisions, and no public key cryptography is used. Wheeler proposed the extensions [Whe96b] to MicroMint which reduce the storage and communications cost. Wheeler also proposed payment transactions using bets [Whe96a], a probability scheme, where an on-line coin flip [Blu82] between the payer and payee is used to decide whether the payment is actually made or not.

SubScrip [FW96] is a customer-vendor share-secrete micropayment scheme, where a shared secret in the form of an account ID is used to authenticate the user to the account. At first a macro-payment is required to setup temporary customer account to the vendor. With each purchase the amount is deducted from the account value upon presentation of the account ID. As the secret account ID is sent in the clear across the network, a new secret account ID is issued after every purchase to prevent an eavesdropper spending the change. Author has proposed to encrypt the new secrete ID using user public-key which eliminates the saving of use of share-secrete.

Millicent [Man95, GMA+95] is the first share-secrete micropayment scheme using a broker as payment aggregator. A user gets user-broker share secrete and a vendor gets vendor-broker share secrete from the broker. Then for secure mode, the scheme uses customer-vendor share secrete. At first customer purchases bank script and then purchases vendor script using the bank script. The vendor script contains authentication MAC using vendor-broker secrete. A user purchases electronic means from a vendor and makes micropayments using a vendor script. The vendor issues change for remaining values and includes an authentication code using special customer master-secrete. The keyed hash is used as message authentication code (MAC).

PayFair [YLH99] micropayment scheme provides user fairness combining share-secrete and hash chains. Like Millicent customer and the vendor share secretes with a trusted third party broker. These secrets are used to generate keyed hashes (MAC) to protect all communication with the broker. A customer withdraws bank encrypted token with serial number and it is specific to the customer. The customer uses the bank token as a hash chain root (W_{n+1}) and

produces a payment hash chain (W_n, …,W_1,W_0). To purchase web contents, the customer sends hash anchor (W_0), token serial number, and authentication MAC using customer-broker secrete to the vendor. The vendor verifies the hash anchor with the broker on-line. The broker regenerate token from token serial number, verify the user authentication using customer created MAC, bind the token with the vendor, send authentication to the vendor and place money to vendor accounts. Now the customer can make micropayment transactions using hash like PayWorld [RS96]. The vendor keeps the account for the customer and stores the highest spent hash value. Upon full spending of the customer token or upon expiry the vendor consolidate payments with the broker. In 2000, Peirce [Pei00] proposed improvement of PayFair and called it PayFairer. In PayFairer scheme, users generate hash chains for a particular vendor and send hash anchors to the broker for commitment. The broker commits it using self secrete which includes vendor-id, hash anchor, and length and it is then sent to the customer encrypted with vendor-broker share secrete. Hash root never leaves the customer's machine. The vendor knows that the chain has been committed by the broker because it is encrypted with his shared secret. The user makes payments releasing hash values like regular hash chain schemes. In this scheme no on-line communication is required and the broker does not require storing the commitments.

In 1997, J. Stern and S. Vaudenay proposed Small Value Payments (SVP) [SV97] scheme. The scheme uses the universal secret broker key (K_B). The universal broker secrete is presented in all vendor's tamper-resistant devices. A user withdraws a token that is certified with an authentication hash of user identity, token, and K_B. The user-broker transaction is secured by user-broker share secrete. Every time the token is spent by the user, it is freshly authenticated to the vendor smart card using a challenge-response protocol. The user sends a token, a user identity, and a random number. The vendor smart card sends a challenging random number. The user then sends a payment transaction containing authentication hash of user identity, vendor identity, value, user random, vendor random, and token authentication hash. As a vendor share the K_B with a broker, there is a possibility that the vendor can regenerate the token authentication hash and can validate the payment transaction authentication hash for excess value.

In 2003, Kim and Lee [KL03] proposed a micro-payment scheme that supports multiple merchants. This is an improvement of PayWord [RS96] scheme. The scheme is divided into three phases: certificate issuing phase, payment phase, and redemption phase. At certificate issuing phase the certificate broker issues a special hash chain along with a regular payment hash chain, where each hash value of the special chain is specific to a particular vendor. Using these hash values user can mark a portion of a hash chain specific to a particular vendor and uses a single hash chain to pay multiple vendors.

In 2004 Z. Yang, W. Lang, and Y. Tan [YLT04] proposed a new fair micropayment system based on hash chain. This is a share-secrete scheme like PayFairer [Pei00], where users (U) and merchants (M) have accounts with a broker (B) and they share secretes with the broker. Before purchasing electronic contents or service from a merchant, a user withdraws a payment hash chain from the broker. The hash chain is specific to the merchant, user, and an order along with a one time user-merchant session key. The broker also transfers payment information to the merchant along with the hash anchor (W_0) and user-merchant session key for authentication purpose. The user then transfers the order-information along with required payment hashes encrypted by user-merchant session key. The merchant can verify the payment and provide the ordered contents or services to the user. The merchant redeems the highest spent hash from the broker, after verification, the broker adds money to the merchant's account. Author also proposed the technique of using same payment chain to multiple merchants; basically that is withdrawing multiple chains for multiple merchants with a single user-broker transaction.

In 2006, Xiaoling Dai, Oluwatomi Ayoade and John Grundy proposed Off-line Micro-payment Protocol for Multiple Vendors in Mobile Commerce, Mobile-NetPay [DAG06]. It is an improved version of their protocol NetPay [DL99] according to the idea of Zhu's multiparty micropayment protocol [ZWM04]. In this protocol mobile users (MU) have accounts with a broker (B). A MU sends request for n payment hashes to B and gets payment hashes (W_1, W_2, …, W_n) with a electronic coin identity (ID_C) through a secure channel. The broker deducts MU accounts, creates a signed touch stone, $T=(ID_C, W_0)Sig_B$, and creates a record for the coin $\{ID_C, W_0, n, W_{n+1}\}$. To purchase downloadable content from a Vendor (V) the user sends the coin identity, encrypted payment hashes according to content price, broker

identity with port or last vendor identity with port, and MU's NO identity. The vendor transmits the coin identity to broker or to the last vendor for verification of last spent payment hash index. The broker sends T and signed current index, I={ID_B, 1}Sig_B but the last vendor sends T and vendor signed current index, I ={ID_V, i}Sig_V, where i=current unspent index of the payment hash. The vendor checks the validity of payment hashes from W_0, W_0 =$Hash^m(W_m)$ and provides the content to the user. After the transaction, the vendor sends T and current I to MU's NO. At the end of the day or at a predefined time the vendor sends payment hashes with coin identity to the broker, upon verification of payment hashes the broker deposits a specified amount to the vendor's accounts and returns an acknowledgement with an account balance statement.

In 2007, Phone Lin, Hung-Yueh Chen, Yuguang Fang, Jeu-Yih Jeng, and Fang-Sun Lu proposed "A Secure Mobile Electronic Payment Architecture Platform for Wireless Mobile Networks" [LCFJL08] based on ID-based cryptography (IBC) [BF01]. The general IBC concept was proposed by Shamir [Sha85] in 1984 as parallel cryptography of RSA. In IBC, each user owns public and public key pairs; both are driven from user identity information and other parameters. In general, a central authority generates parameters and keys for users. Parameters are placed in a public site and keys are transferred to user devices using a secure channel. Using these key pairs and random parameter, users can generate mutual share-secrets to other users or vendors who have key pairs from the same central authority. Three hash techniques (H_1, H_2, H_3) and the Bilinear Pairing function (ê) are used for key generation, where public key ($k_{pub,u}$) = H_1(User Identity); user private key ($k_{pri,u}$) =S.$k_{pub,u}$; S is a secrete random number; user side user-operator share key $k_{u\text{-}o}$=H_2(ê($R_{u\text{-}o}$.$k_{pub,o}$,$k_{pri,u}$)); operator side user-operator share key $k_{u\text{-}o}$=H_2(ê($R_{u\text{-}o}$.$k_{pub,u}$, $k_{pri,o}$)); $R_{u\text{-}o}$ is public random parameter chosen by the user; H3 is SHA or MD5 and used for payment token generation.

The scheme uses this share key generation technique and based on these author proposed a share-secrete micropayment system like the new fair micropayment scheme [YLT04]. Here the mobile network operator (O) is acting as the central authority and payment aggregator. User (U) and the content provider (P) have accounts with O and they get identities, keys and public parameters from O. The protocol comprises of there phases as withdrawal, payment and deposit. In the withdrawal phase, the user withdraws token T_N having value N from O for P

for a particular order-information. The user encrypts the messages by k_{u-o} and sends along with $R_{u-o}.k_{pub,u}$. The operator decrypts and authenticates the message and generates tokens (T_{N+1}, T_N, …, T_0). S/he transfers T_N, T_0 and it's unique serial number S_N to the user. S/he also sends S_N along with order-information (OI) and $R_{o-p}.k_{pub,o}$ to the provider (P). In payment phase the user sends an encrypted message containing S_N and required payment tokens, and along with $R_{u-p}.k_{pub,u}$ but does not send user identity. The provider verifies the payment with T_0 from the data base and delivers electronic contents to the user for a valid payment. In the deposit phase, the provider sends encrypted highest spent pay token T_J and an index J along with token serial S_N to the operator. The operator queries database for user identity, provider's identity, T_0 and share secrete. Then s/he decrypts the deposit message and verifies the payment token hashing T_N. For valid payment tokens s/he deposits value to P's accounts and deducts U's accounts.

In 2009, Hong Wang, Jialin Ma, and Jing Sun proposed a new prepaid micropayment scheme [WMS09] based on the idea of PayWord [RS96] but they used multiple hash chains having different unit values. Both the vendor (V) and customer (C) have accounts with a trusted broker (B) who is responsible for payment aggregation. The scheme comprises registration, transaction, redemption, and revocation sub-protocols. In registration, customers and vendors register with the broker and get public-key certificates. In a transaction, the customer creates multiple hash chains for different unit values like 1/10 cent, 1 cent, 10 cents, 1 dollar, 10 dollars etc. Then those are sent to the broker for signed commitment. A payment commitment contains user identity, unit value, hash anchor (W_0), chain length, total value, expiry, and the broker signature. For purchasing, the user browses the vendor site and sends signed order list. The vendor in reply sends signed transaction identity along with price, order list, user identity, and date. According to vendor signed total price the user compiles signed payment using multiple hash chains, for example to pay the amount of $43.231, s/he uses 5 hash chains. S/he pays 4 hashes from 10 dollars, 3 hashes from 1 dollar, 2 hashes from 10 cents, 3 hashes from 1 cent and 1 hash from 1/10 cent chain. For paying 4 dollars s/he will use {(1 dollar, 1) (W_4, 4)}, where 1 dollar is the unit value of hash, 1 is starting hash index of the chain, W_4 is maximum spent hash value, and 4 is the index of maximum spent hash value. S/he signs the payment containing vendor identity, transaction identity and payments chain values. In redemption, the vendor sends customer signed payments and commitments at a predefined time. The broker

checks the database and updates the vendor accounts. Any double spending and overspending are detected by the broker and the customer is responsible for these. In revocation, the customer redeems expired and unused commitment from the broker.

2.6 Emerging problems for billing and payments

The evolution of mobile networks enables service deployment and content delivery by independent providers through the heterogeneous network infrastructure of fixed and mobile operators. Communication billing is moving forward form circuit-switched voice and best-effort data domain into the realm of large-scale packet networks with variable QoS and an ever-growing plethora of applications and contents. Thus the new usage records are defined in form of CDR(s) for new services for every segment of the network usage. This leads to a large numbers of CDR(s) being generated and stored at different segments of inter-network for a single call. For example, a mobile user is buying contents from a remote VSAP, this will generate S-CDR, M-CRD, G-CDR and WAP-CDR at a mobile network operator, WEB-CRD at a content provider and a number of IPDR(s) will be generated at different ISP(s) through them the VSAP is connected. If the user is in roaming then the visited network will verify user authentication and the credit-limit with the user home network using online AAA protocol and will send related CDR(s) to the home network. All the involved parties require to store and maintain these CDR(s) records for years for the use in disputes. They need to process bills separately and to make inter operator settlement and clearing.

The huge number of CRD(s) maintenance and multi-staged billings does not guarantee the payment from customers. The presence of a huge number of independent service providers makes the scenario father complex as their CDR(s) may not be authentic at the absence of non-repudiation. For authentic pricing and usage records, VSAP(s) must have an agreement with a trusted Network Operator or a trusted third party for their billing and payment that adds further cost for their services to customers. A central Charging, Accounting and Billing (CAB) [KKA02] service has been proposed for 4G networks. The CAB can be under the administrative domain of one of the involved players or may be belong to an independent trusted third party, CAB provides charging, billing and accounting functions. All the involved parties (NO, WLAN, VSAP) register their charges to CAB and send usage CDR(s) to CAB

through a CAB-Gateway. Using this concept Bango Inc. has been providing billing and accounting services for electronic contents over the globe including 120 countries. They provide multiple payment methods including payments through carrier billings. In the year 2011, Bango Inc. extends their billing services to Canada to cover 20 million cell phone users to buy electronic contents from different VSAP(s) through Bango and pay through their carrier bill.

The CDR approach of billing has been in use for over 120 years and working fine in monopolistic environments with a small number of trusted NO(s) providing a limited number of services. This credit based approach needs strong legal binding with their customers for ensuring payments. Currently, a huge number of independent NO(s) and VSAP(s) are operating and providing millions of services and thus, the trust relationship model is no longer adequate. The fixed tariff of traditional CDR based billing scheme does not allow dynamic charging according to real-time network condition and does not provide customer option to choose alternate access network for service in real-time. The billing system with the huge number of services and charges is very complex and costly. The cost of billing software and system is about several billions of dollars and it has recurring cost for handling, paper, postage, payment processing, and clearing, is about €5.00 to €10.00 per billing transaction [Eng98]. The customers are billions in number but they do not take part in billing process and thus, the billing suffer from non-repudiation and NO(s) loose about 3% to 5% of their total revenue due to fraud [Sey98, ES97]. The U.S. Federal Trade Commission has highlighted the widespread problem of fraudulent billing [FTC98]. However, this is only one of many aspects of telecommunications fraud [Col99a, Col99b, Col00, ES97], which costs the industry an estimated €12 billions annually. The telecom watchdog agency reported that wireless carriers were the target of 52 percent of the 3,747 complaints it received in the 2009-2010 monitoring period, up from 38 percent in 2008-2009 [CP10]. According to the AP, October 3, 2010 – Verizon Wireless could pay out up to $90 million in refunds to cell phone customers who were improperly charged for inadvertent Web access or data usage over the past several years. The post-paid unlimited credit based billing system leads the fraud and there is no guarantee of a full payment by the user. The service provider then bounds to engage a third party to collect the outstanding, which incurs more cost to customers. Overall, the multiple CRD(s), complex rate, and the complex billing scheme lead around 20% of revenue leakages [TCS].

Chapter 3: Existing Multiparty Micropayment Protocols

3.1 Introduction

In network communication, a typical service involves multiple parties to transmit network traffic for delivering desired services. The involved parties must be remunerated for their part of service. Presently users are connected to trusted single service provider for network communication services and they make payments to single point for most of the services response to a periodic billing. The service provider in turn makes payments to other related service providers for their part of communication services. All the services are credit based and billed after services relying on trust relationships and mutual service agreements which are vulnerable to non repudiation.

Present development of communications and wireless technologies are allowing private and small service providers to grow very fast. Now users roam frequently to different service providers. The serving service providers must have mutual service agreements to ensure their remunerations for their services authenticating users from their home locations. As the service and payment relies on trust and a contract agreement between a user and his local service provider, user cannot access services at his wish. The current billing methods with their implicit trust relationships become drastically inadequate in such environments. To overcome these situations, Peirce [Pei00] in his Ph. D thesis first proposed ***multi-party micropayment protocol*** for mobile communication. He mentioned it is more secure and efficient to pay everyone involved in a call for their services. The real-time payment eliminates the huge trust assumptions, security risks, and overheads of billing. Such payments for network services will be ongoing and repetitive small amounts.

Peirce also extended the protocol scheme for Mobile Ad-Hoc Network Payments. Tewari and O'Mahony [TM01] proposed "Multiparty Micropayments for Ad Hoc Networks", which eliminates the trusted third party "the Enforcer" signed pricing contract. In 2001, Zhu independently presented Micropayment Scheme for Multiple-Vendor in M-Commerce [ZWM04]. Zhang and Fang [ZF07] in their paper "A secure authentication and billing

architecture for wireless mesh networks" proposed a micropayment protocol using identity based signature scheme for network access over mobile ad-hoc networks.

3.2 Multi-Party Micropayment for Mobile Communication by Peirce

Peirce [Pei00] proposed the first ***multi-party micropayment protocol*** for mobile communication as a flexible protocol usable with any multi-party service model. He proposed the protocol scheme to overcome the shortcomings of current CDR billing and online payment verification of macro-payment schemes. He introduced a financial broker-signed hash chain as a payment token in his scheme using secure hash function like SHA1 [NIST93]. He mentioned the scheme would ensure to remove unnecessary trust from the system; reduce the online communications overhead of contacting a home location; eliminate fraud due to CDR tempering and falsification; provide fair dynamic charging; remove user trust and accountability; remove needs for mutual roaming agreements; and allow real-time payments to all involved entities getting service anywhere by anyone who holds valid payment tokens.

3.2.1 Peirce Protocol Scheme

A user attaches to the network through an access network operator (NO), either over a mobile wireless link or from a fixed terminal. The user makes calls or sends data packets through the access NO for which s/he pays in real-time. Tariffs are dynamically set by each party at the start of a call. The connection may pass through one or more other network operators before reaching the destination user or VASP. The user releases a stream of micropayment tokens into the network to pay all the SP(s) as the call proceeds. The same payment token is worth a different amount to each entity as defined at call setup. Hash chain based payment tokens are purchased by the user from one of several online brokers. The tokens are spent through a designated SP, called the enforcer, who prevents overspending and cheating by the user or the other SP(s). Cheating by the enforcer itself will be detected after the fact. After the call, payment tokens can be efficiently redeemed by each SP at their chosen but defined broker. Only the final token received needs to be redeemed as the other tokens can be derived from this. Unspent tokens can be spent on a different call to a different destination, but through the

same enforcer to prevent double spending. Over dated unspent or partially spent tokens may later be refunded by the issuing broker.

The protocol scheme comprises of 5 (five) components: Payment Chain Purchase, Pricing Contract, Enforcer Endorsement Chain, Releasing Payment throughout a Service, and Multiple Broker Clearing for Redeeming Payment.

Payment Chain Purchase:

A mobile user purchases prepaid tokens, the payment hash chain, from a third party broker, using an existing macro-payment system indicating any SP as the enforcer. The user generates a payment hash chain of length N, having hash anchor P_0, from the hash root P_N by repeatedly applying a one way hash function, such as SHA1 [NIST93]. The broker commits the hash chain by digitally signing the payment chain commitment, $Comm_P = \{P_0, Length, Chain\_value, Enforcer, Expiry\}Sig_{Broker}$. As the payment commitment includes the enforcer, the user spends the commitment through enforcer and the enforcer keeps record of the commitment value being spent and endorses the payment. The enforcer prevents the chance of over spending and double spending of the payment chain by the user. Figure 3-1 depicts payment chain purchasing.

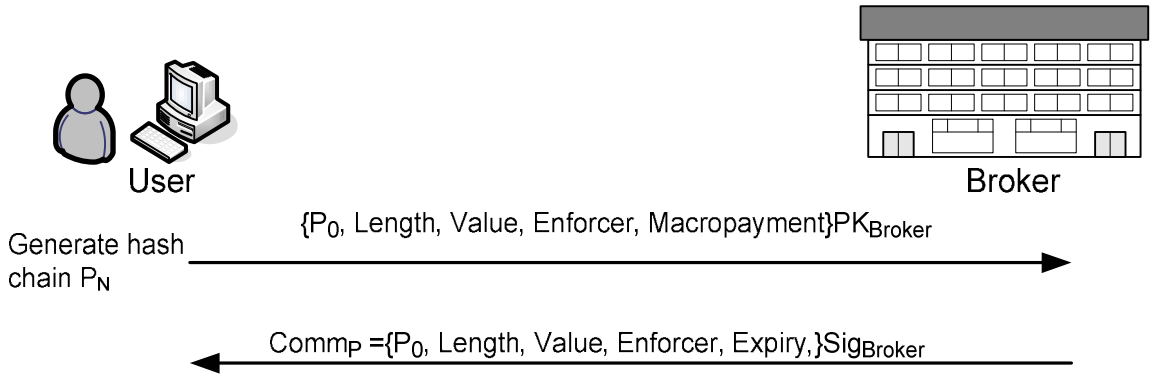


Figure 3-1 Payment Chain Purchase

The payment chain purchasing needs a macro-payment and public-key encryption if the user deals with an unknown broker. But a user who has an account with the broker, shared secret can be used for authentication and integrity like HMAC or for symmetric key encryption.

Pricing Contract:

To make a call the mobile user must have a payment chain commitment for any one of the NO(s) or VASP(s) involved in the call. Figures 3-2 shows "Constructing a Pricing Contract" and the local network operator, SP1, is the enforcer. The user sends the call request details, unspent payment hash value just next of the last spent hash and the payment chain commitment to the enforcer. An enforcer signed pricing contract is then generated by the SP(s) involved in the call. Its purpose is to allow verifiable dynamic tariffs, fix the starting hash in the payment chain, create a record of the call, and link a single payment commitment to multiple SP(s) for the call. *Pricing Contract = {TID, SP, Charge, Comm$_P$, P$_{start}$, Start, P_value, Comm$_E$, R_Broker}Sig$_{Enf}$,* where TID is the transaction identifier of the pricing contract, partly generated by each SP to prevent replay attack. Charge includes tariff and rate for each SP which allows dynamic charging. P_{start} is the staring payment hash for the current contract and Start indicates the position of P_{start} in the payment hash chain. P_value is the value of a single payment hash for this particular service. $Comm_E$ is an endorsement chain commitment hash anchor E_0 signed by the enforcer along with pricing contract, which prevent over spending and double spending of payment commitment. R_broker is the broker fixed by each SP through him SP will redeem payment hashes for this service.

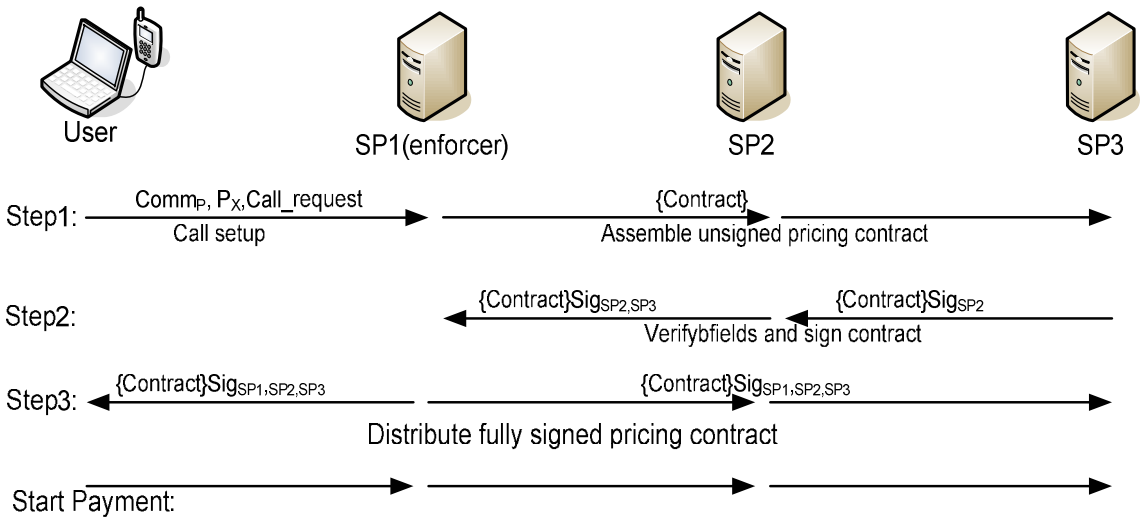


Figure 3-2 Constructing a Pricing Contract

The enforcer is responsible for ensuring that the pricing contract is constructed correctly using a three-way handshake protocol, as shown in Figure 3-2. The pricing contract may be signed by all the involved SP(s) as shown in figure and the user has to verify all the signatures. But

the mobile device has limited processing and storage capacity and the Enforcer is the most trusted entity in the contract, thus Peirce proposed to omit the SP(s)'s signatures from the contract. A new contract may be required to compile and sign during mid-call to reflect any change of tariff and to cope with handover.

Enforcer Endorsement Chain:

The enforcer, identified in the payment chain commitment, is given the role of preventing double spending of payment hashes and all the payment hashes must pass through him to keep record of account balance. The enforcement hash is attached to the payment hash to authenticate the payment which provides the opportunity of spending remaining unused hashes of a payment chain commitment to a new call or service. Enforcer uses a unique hash chain to a call and includes hash anchor E_0 to the pricing contract and signs the pricing contract. As endorsement hash is attached to payment hash, SP(s) cannot claim excess value even if the payment chain commitment for two different calls/services to the same SP.

Releasing Payments throughout a Service:

Payment is an ongoing process during the call or service. A user releases payments hash at a regular interval as set in the pricing contract and SP(s) provide contracted services for valid payment hashes. If the user does not get desired service, s/he ends the call by not realising any more payment hashes. The enforcer keeps a record of how much of a payment chain has been spent and prevents *double spending* of payment hashes. Figure 3-3 shows user payments through a service. At first NO verifies the payment validity by performing one hash function on it to obtain the previous payment hash, and then the NO forwards the payment hash and his own endorsement hash to the other SP(s). Each SP independently verifies both the payment hash and the endorsement hash. The hash function is one way, and thus payment hashes cannot be forged. The knowledge of the payment hash is the proof of payment by the user. The user releases next unspent payment hash starting from the payment chain. The enforcer verifies that the payment validity, adds the enforcer hash value and forward to other SP(s). Each SP independently verifies both the payment hash and the endorsement hash. Since the hash function is one way, payment hashes cannot be forged, and knowledge of the payment hash is proof of payment. All the SP(s) store the highest spent payment hash, enforcement hash, and pricing contact for redemption.

Redeem payment Hashes and Multiple Brokers Clearing:

At the end of the day, each SP will redeem the highest spent payment hash obtained from the call with their preferred broker identified in the pricing contract. The broker will only accept a payment hash from an SP if a corresponding endorsement hash and pricing contract accompany it. Redeeming broker gets his identity and SP's payment portion from the attached pricing contract, and update SP's accounts accordingly. Periodically the redeeming broker will clear the payment hashes in bulk with the payment commitment issuing broker; for this there should be private networks for the brokers.

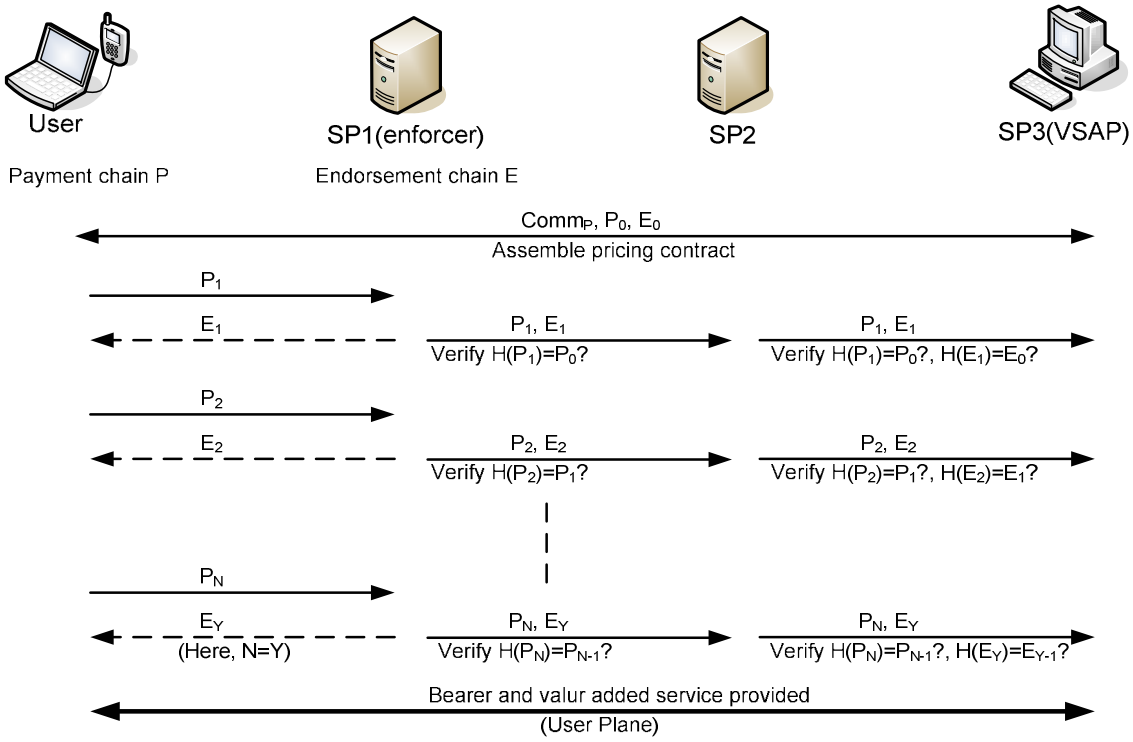


Figure 3-3 User pays all SP(s) with same Payment Hash

3.2.2 Analysis of M Peirce Protocol Scheme

Peirce [Pei00] made an analysis of the protocol scheme and mentioned the computationally expensive components of this protocol are assembling pricing contract and redeeming payment hash. But the main component of the protocol, the payment process is very efficient and only needs to compute and comparison of two hashes at each participating SP. He also made an analysis for security vulnerability and claims that the protocol scheme is secure assuming the digital signatures cannot be forged, hash chains cannot be inverted, and an

encrypted message requires the correct secret key to decrypt. According to his analysis the security claims are summarised as follows:

(1) An outside attacker fraud as man-in-the-middle is not possible as the payment chain root never leaves the user device; only one user is allowed to use a payment hash chain concurrently. The pricing contract includes every involved SP(s), and redeeming needs a valid endorsement hash along with pricing contracts.
(2) User cannot over spend or double spend the payment chain as it must be spent through the enforcer who keeps the accounts balance of a payment commitment chain.
(3) Non-enforcer SP(s) cannot obtain extra values or other SP's values as participating SP(s) identities are include in the pricing contract and redemption process needs enforcer generated endorsement hash.
(4) Enforcer frauds are detectable as s/he signs the pricing contract and distributes it to others, but an undetectable stealing is limited to a singe hash value.
(5) The financial broker cannot fraud as the amount owed to each SP by the broker can be proved to an independent third party.
(6) Denial-of-Service attack is not possible as request of new pricing contract is requires an unspent hash. However, eavesdroppers can only get one hash and that can be use once for signing a false pricing contract. And eavesdropper cannot invalidate the payment hash as enforcer informs the user regarding unauthorised usage of the last payment hash value for a new price contract request.

The original protocol scheme is designed to access communication service from anywhere, but the presence of an enforcer in the payment commitment chain limits the user access. Users have to carry multiple payment chains and it is impossible when service providers are not limited. Also the payment redemption by every involved SP(s) in a call to their brokers makes the scheme costly and the redemption cost may override the actual value of service from micropayment. Peirce made the protocol simulation in LAN environment using JAVA with Pentium-II 233 MHz as user machine and 400 MHz as SP machine. The simulation results shows that user needs only 0.01049 ms for next token generation as array lookup from cached chain, but it takes approximately 5 ms to a generate payment hash from a cached root of distance 50. The time taken by each SP(s) for verification payment and endorsement is very

little and it is 0.0844 ms. Payment redemption cost for 10c for 3 SP(s) is approximately 1673 ms including communication time, but processing time at each broker is 234 ms with a 400MHz machine. The simulation result indicate the use of long payment commitment chain needs more user storage or it will introduce more delay for next payment token generation. Also the storage of payment tokens in an inexpensive user device introduces security vulnerability.

3.3 Mobile Ad-Hoc Network Payments by Peirce

A mobile ad-hoc network is group of mobile hosts act as router to others, which connect to each other to form a multi-hop wireless network topology [CM99, CMC99]. As they move, the routes between nodes may change dynamically over time and routes are determined by underlying routing protocols (normally reactive protocol). An ad-hoc network may be connected to fixed network through one or more nodes. As mobile nodes have energy constrain, they may not relay a stranger's traffic free. Thus Peirce proposed a variant of his multi-party micropayment protocol for mobile ad-hoc network to pay all the participating nodes in real-time. His work is for inspiring intermediate nodes to relay other user traffic by getting them paid. He assumed that nodes only relay best-effort traffic.

3.3.1 Mobile Ad-Hoc Network Payment Protocol

In the multi-party micropayment scheme, user must have payment chain commitment which must be spent through the enforcer. Mobile ad-hoc network routes are changed frequently and any node selected as enforcer will be changed, thus the author proposed universal smart card enforcer as described in Section 3.3.2. As all the nodes in the call route are normal user and less trusted. He proposed to remove non-enforcer signature form the pricing contract as part of performance optimization. For redeeming payment hashes, participating nodes account identities to their brokers and charges must be included in pricing contract as in user-to-user payment scheme. For a fixed network connection, the node is a regular SP and his signature is required in the pricing contract. Thus the author proposed separate contracts for mobile ad-hoc network access and fixed network access using a separate payment chain. The mobile ad-hoc network payment protocol architecture is shown in Figure 3-4.

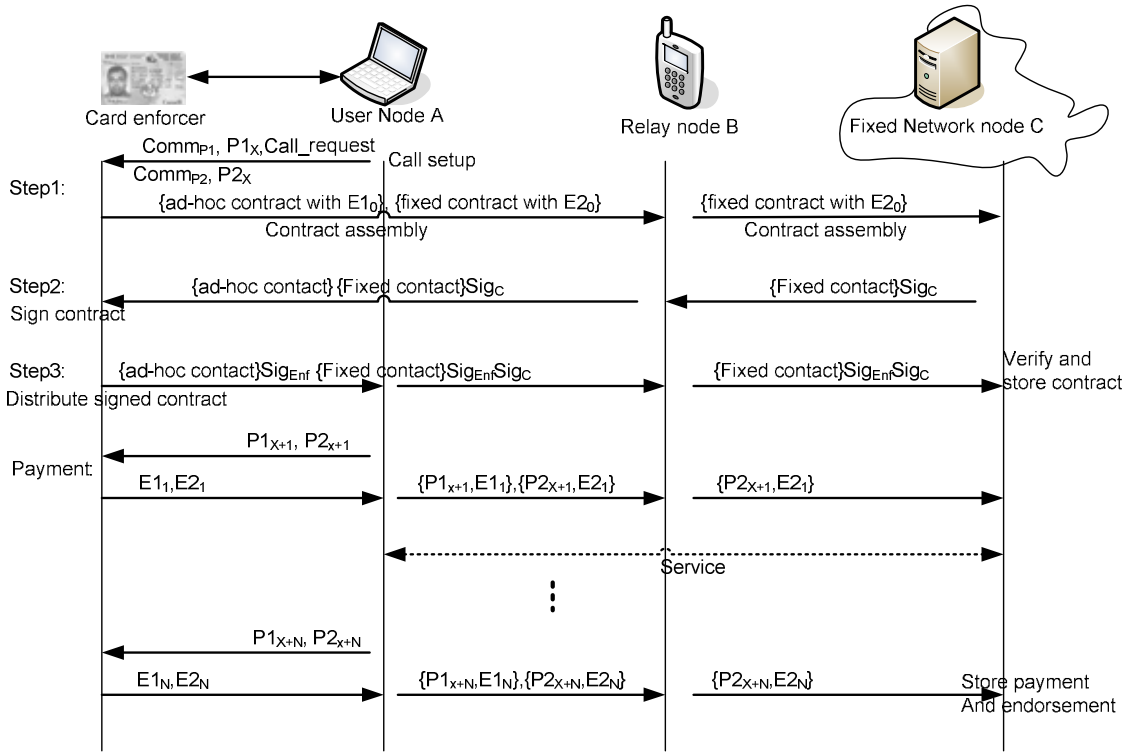


Figure 3-4 Mobile Ad-Hoc Network Payment Protocol

A new ad-hoc pricing contact is required when the call route is changed, but the same payment chain can be used. As the ad-hoc pricing contract is only signed by the user smart card enforcer, the contract assembling cost is relatively less than for basic multi-party micropayment scheme in which all participating parties sign the contract. To avoid frequent call route change, the author suggested that, the mobile device should be mobility-aware and the underlying routing protocol should take care about frequent mobility in case of route selection. Using this idea, the number of new inter-call ad-hoc pricing contract can be minimized.

3.3.2 The Smart Card is the Enforcer

Main idea of multi-party micropayment is not to involve unnecessary parties as an enforcer. Thus enforcer entity is proposed to be resided on the smart card. Enforcer became a program on the smart card and that cannot be tampered. It assumes the same trust and characteristics of a real enforcer, having private key with matching digital certificate. It will keep the balance of a user payment commitment, sign the pricing certificate, and provide endorsement hash like real enforcer. Since this enforcer is local to the user, it can be present in any call route.

Therefore a single payment chain assigned to the card enforcer can be spent at multiple SP(s), which provides the offline flexibility needed for local payments. The local VSAP does not require a digital certificate and it only needs to have an account to the broker. As smart card is not temper proof and all users use it, there could be a possibility to forge the private key. However, Peirce [Pei00] proposed a digital certificate for a group of 100 users.

3.3.3 Mobile Ad-Hoc Network Payment Protocol Analysis

In this protocol the enforcer is a smart card which assumes the same trust as real enforcer. But all the users or a group of users use the smart card enforcer having same private key and public key with matching digital certificate. Smart card is tamper resistance but not tamper proof. If any user breaks the card security and gets access to the private key then s/he can double spend his/her own payment hashes and also other payment hashes from the same group. The security vulnerability can be reduced with short validity of the digital certificate. For downlink traffic from fixed network or VSAP should have some charges, but author does not indicate in this regard. However it can be done through new pricing contract or including separate charge and payment chain in the pricing contract.

3.4 Multiparty Micropayments for Ad-Hoc Network by Tewari and O'Mahony

In an infrastructure less ad-hoc network environment, mobile nodes under individual control may not cooperate each other to relay network traffic. However, it is envisaged that in near future the ad-hoc network will have a great role in everyday life and it will complement existing mobile and fixed communication networks by extending the reach of fixed network to the user. Tewari and O'Mahony proposed a variant of multiparty micropayments where each involved node will be paid at real-time while forwarding packets and that may motivate the mobile nodes to cooperate to relay network traffic. In the protocol scheme, authors remove the involvement of the trusted third party (TTP) and the long-live pricing contract which bind all participating node in the call route, unlike other micropayment schemes. They also remove the drawback of virtual currency system nuglets [BH01]. In the scheme all the participating nodes are paid separately using separate hash chain, which is mentioned as very efficient in ad-hoc network, where handover or route change are occurred frequently.

3.4.1 Multiparty Micropayments for Ad-Hoc Network Protocol

The payment scheme has proposed employing micropayment technology, the hash chain, which allows each of the nodes involved packet forwarding to be paid in real-time. Here involved parties are source user mobile nodes in a ad-hoc network, packet relaying device mobile nodes in ad-hoc network or ISP nodes in fixed network, destination mobile node in ad-hoc network or a VSAP in fixed network, and a broker to whom all parties have accounts. Protocol components are broker commitment as the payment hash chain endorsement, charge assembly, endorsement distribution, and payment for packet forwarding, route change management, and redeeming payment token. The protocol has been designed to address the issues of payment for relaying nodes in ad-hoc network and must achieve some goals as off-line payment verification, use of lightweight cryptography, minimize system fraud and flexibility of route selection by the user. In this protocol all involved parties must have private-keys and matching digital certificates to authenticate their participations.

Purchasing Broker Commitment:

The user must have an account to the broker. The broker supplies each account holder with a smart card, which is loaded with private key, matching digital certificate for user identity, and broker certificate. User generates a set of hash anchors using unbalanced one-way binary tree (UOBT) [YHH99] and in a single message which is signed by user private key and encrypted by broker public key, then the user sends these anchors along with sub-chain length and value of a single hash of a sub-chain and macro-payment details to buy prepaid payment tokens, the broker commitments. The UOBT root never leaves secure hardwire module of user device. The broker generates and signs a set of secret payment endorsement, the broker commitments, along with endorsement value (random number) correspond to each anchor send by the user and a signed user receipt. These payment endorsements are encrypted by the user public key and they can be decrypted by the user smart card at the endorsement distribution phase. The purchase of payment chains and broker commitment are shown in Figure 3-5. The broker signed payment endorsement consists of an anchor value PX_0, the endorsement value, the length of hash chain, the value of a single hash, user identity, expiry date, and broker signature. The receipt contains all anchors as, $Receipt = \{A, (P1_0, P2_0, \ldots, PX_0), Length, Value, Expiry\}Sig_{Broker.}$

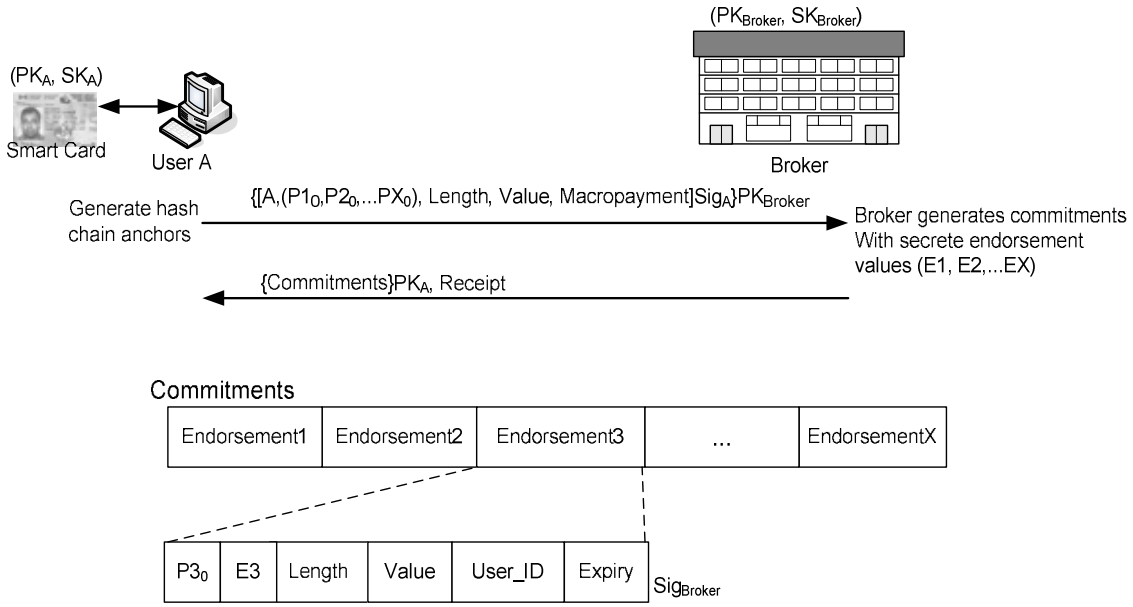


Figure 3-5 Purchase of payment chain and broker commitment

Charge Assembly and Endorsement Distribution:

A call setup from a source user node to a remote destination is mainly for assembly of charges and collection of relaying node user identity, thus the user can pay them at the time of packet forwarding. Users identify the routes to the destination using an underlying reactive or proactive protocol and then subsequently query nodes along one or multiple routes sending charge requests. The intermediate nodes, the relay nodes, add their identity and charges signed by their private key to the charge reply message along with their digital certificate return to the user. The user selects the best route and distributes secured payment endorsements encrypted with the public key of relay nodes from its smart card to the smart cards of the participating nodes along the route. The protocol transactions are shown in Figure 3-6. Each node along the path is now ready to accept payment token for forwarding user packets. Since this signalling is crucial for packet forwarding; author suggested using a reliable protocol like TCP for transmitting endorsements. Alternatively UDP can be used; endorsements may transmit three times along with first three data packets.

Making Payments:

For forwarding each packet or sequence of packets, the user attached multiple payment hash tokens one for each relay node. As shown in protocol transaction, charge of node B is 1 hash token but charge of C is 2 hash tokens. As all the endorsements have same length, two

endorsements ($P2_0$, $P3_0$) are transmitted for node C. In case of a payment only a single payment token is sent from $P2_0$ as $P2_2$ is twice up of previous token $P2_0$. Intermediate relay nodes store the highest payment hash token along with secrete endorse for redeeming the value. Payment tokens are sent in plain text as it has no value to other without corresponding secrete endorsement.

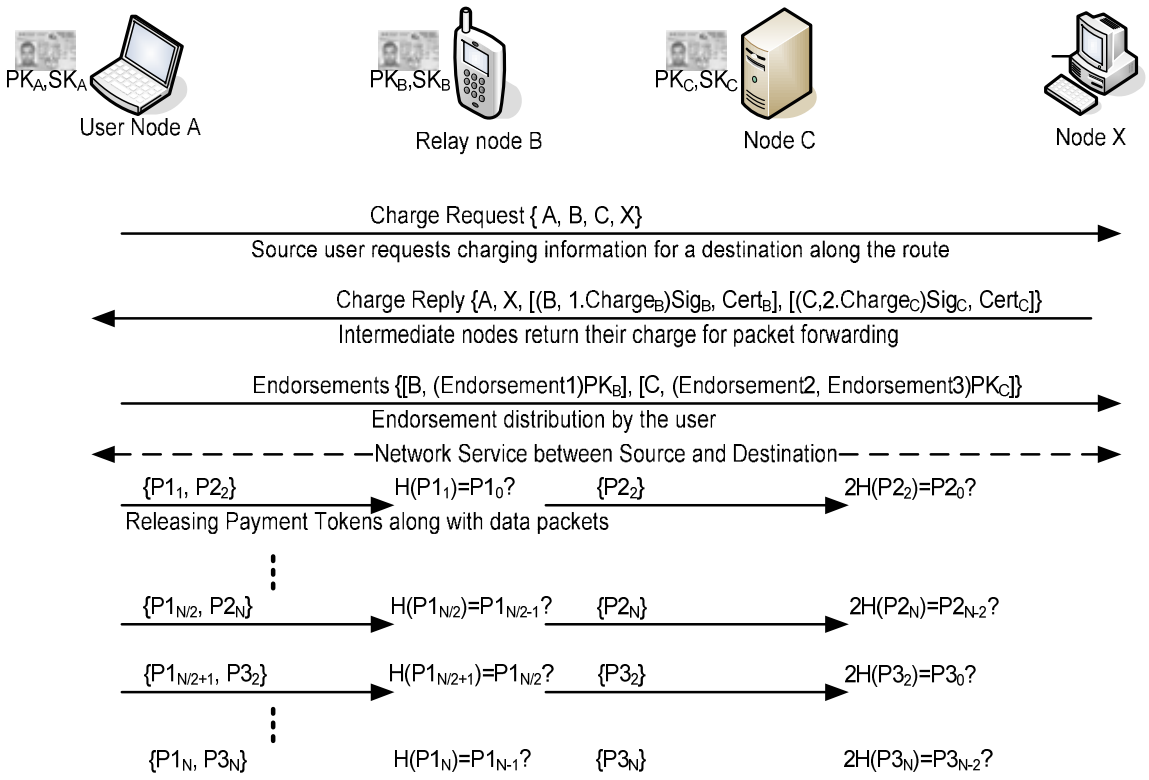


Figure 3-6 Ad-Hoc Network Protocol Transactions

Redeeming Tokens and Broker Clearing:

Periodically a node will contact with its broker and deposit payment tokens that it has collected for data forwarding. The smart card of the node encrypts the collected secure endorsement with broker public key and it will sign the highest payment token along with encrypted endorsement and user identity for sending to broker. The broker verifies the redeeming message, credits the account of the node and issues a receipt for the same. At a later date after expiry date of a payment endorsement, the broker will also reimburse the user for the remainder of the unspent hash value. The proposed scheme hash has only one broker but it may have multiple brokers, then offline broker clearing is required for redeeming tokens.

Route Change Management:

In ad-hoc network topology change will occur frequently, this will result in a route change toward destination node. However all the nodes along the path must be paid for data forwarding and new nodes must have endorsements for payment verification. Now in this scheme, after new charge assembly, new endorsements form UOBT will transfer to the new nodes and other will still use previous endorsement for payment verification

3.4.2 Ad-Hoc Network Protocol Analysis

This protocol scheme is claimed efficient for paying multiparty in real-time and it uses hash chains as payment instruments; this allows off-line verification of payment instruments. Asymmetric key algorithm is only used at call setup. Online TTP verification and long-lived pricing contract involving all parties are eliminated that makes efficient for route change management. UOBT is used for efficient storage of multiple hash chains. However a trusted hardware device is used at user, if one of the tamper resistant devices compromises, the scheme will suffer from a limited amount of fraud. Unlimited usage of a chain is limited by expiry date.

Exclusion of enforcer and pricing contracts is required to buy a fixed valued payment chain having fixed value to a singe hash. This will cause the user to carry a huge number of payment chains of different lengths and values. Sometimes it is impossible for roaming users to make a proper combination of endorsements for a payment. As in this scheme small valued chain say 10x10 UOBT is used, if a singe hash has value of one-tenth cent, then value of one chain is only one cent. It is obvious that the value of such a chain will be overridden by the communication cost and processing cost for purchasing broker commitments and redeeming tokens. The decryption of payment commitments at every relay nodes using their private key makes the system expensive and that is against the protocol goal.

3.5 Zhu Multiple-Vendors Micropayment Scheme in M-Commerce

At the emergence of wireless and mobile network, m-commerce introduces the mobile networks to e-commerce. Under m-commerce, users are now buying every kind of information

ranging from daily news and journal papers to movies on the Internet through wireless networks using mobile handheld devices. These commodities, services, or information items on the Internet have low values, ranging from cents to several dollars, and it needs frequent small payments in real time with the services. Thus the author introduced the multiple-vendor micropayment scheme for m-commerce [ZWM04].

3.5.1 Zhu Protocol Scheme

In the protocol scheme, a mobile user (MU) is attached to Internet through the access (NO) for basic network connectivity service, and they use verity of services from other VSAP(s) in Internet connected to user access NO through other SP(s). The other player of the scheme is a broker for micropayment aggregation among the entities. In the scheme, a user makes a payment in real-time to all participating parties for their services. Hash chain is used as a payment instrument thus SP(s) can verify the payment off-line. The scheme comprises of four components as: (1) Payment Chain Purchase, (2) Pricing Contract, (3) Payment Processes, and (4) Redeeming Payment Hashes. Protocol components are described as follows:

Payment Chain Purchase:

A mobile user purchases prepaid tokens and the payment hash chain, from a third party broker, using an existing macro-payment system indicating his connected NO. The user generates a payment hash chain of length N, having hash anchor P_0, from the hash root P_N. The broker commits the hash chain by digitally signing the payment chain commitment, $Comm_P = \{P_0, Length, Chain\_value, NO, Expiry\}sig_{Broker.}$ As the payment commitment includes NO, the user spends the commitment through NO and NO keeps record of the commitment value being spent and endorse the payment. NO prevents the chance of over spending and double spending of the payment chain by the user.

Pricing Contract:

A mobile user sends the request details, such as destination, service type, Quality of Service (QoS) requirements, and the payment chain commitment to the NO for his desired service from a particular VSAP. Then a signed pricing contract is compiled by the SP(s) involved in

the service including VSAP. The pricing contract is to allow flexible dynamic tariffs; fix the starting hash in the payment chain; decide the value for a single payment hash for the service; create a record of the service; and link a single payment commitment to pay multiple SP(s) for the service. *Pricing Contract = {TID, SP, Charge, $Comm_P$, P_{start}, Start, P_value, $Comm_E$, R_Broker}$Sig_{SP(s)}$,* where TID is the transaction identifier of the pricing contract, party generated by each SP to prevent replay attack. Charge includes tariff and rates for each SP. P_{start} is the staring payment hash for the current contract and Start indicates the position of P_{start} in the payment hash chain. P_value is the value of a single payment hash for this particular service. $Comm_E$ is an endorsement chain commitment that is a hash chain created and signed by the NO for each pricing contract, which prevents over spending and double spending of a payment commitment. The $Comm_E$ is $\{E_0\}sig_{NO}$. R_broker is the broker fixed by each SP through whom they will redeem payment hashes for this service.

Payment Processes:

Payment is an ongoing process, with the user releasing payment hashes at regular intervals. Interval might be time duration or data volume or both for the service. In return for a valid payment, the SP(s) continue to provide agreed service. The payment process is depicted in Figure 3-7. If the user does not get the agreed service, s/he can terminate ongoing contract by not releasing any more payment hashes. The cost of per unit service transaction is the sum of the tariff rate of all SP(s) and it is P_value as agreed in pricing contract. At first NO verifies the payment validity by performing one hash function on it to obtain the previous payment hash, and then the NO forwards the payment hash and his own endorsement hash to the other SP(s). Each SP independently verifies both the payment hash and the endorsement hash. The hash function is one way, and thus payment hashes cannot be forged. The knowledge of the payment hash is the proof of a payment by the user.

Redeeming Payment Hashes:

At the end of the day or predefined interval, each SP will redeem the highest spent payment hash for the service provided with their preferred broker identified in the pricing contract. The broker will only accept a payment hash from an identified SP if a corresponding endorsement hash and signed pricing contract accompany it. The broker knows how much to pay each SP from the contents of the pricing contract.

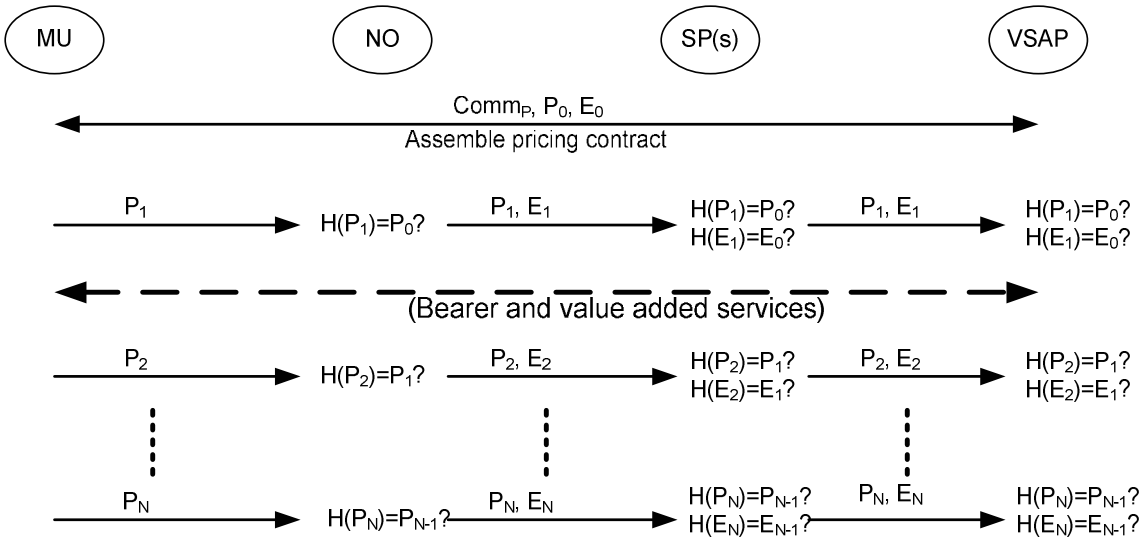


Figure 3-7 Zhu Multi-vendor Micropayment Process

3.5.2 Zhu Protocol Analysis

The Zhu multiple-vendor micropayment protocol is actually a variant of multi-party micropayment protocol by Peirce [Pei00]. Thus the computationally expensive component of this protocol is assembling pricing contract and redeeming payment hash. In the protocol scheme, user access network operator (NO) used as fixed enforcer as NO is considered as fixed to a mobile user. The main component of the protocol, the payment process is very efficient and only needs to compute and comparison of two hashes at each participating SP. The security feature of this protocol is like multi-party micropayment protocol presented by M Peirce and accordingly outside-attacker, user, SP(s) and NO frauds are prevented but the fraud by NO as enforcer is limited to a single payment hash only. Broker fraud is detectable by the third-party audit.

3.6 Zhang-Fang Micropayment Protocol Scheme for Wireless Mesh Networks

Wireless mesh networks WMN(s) are gaining growing interest as promising technology for ubiquitous high-speed network access. The improvement of wireless technology features and integration with WiMAX technology, it is envisaged that the future large-scale WMN will consist of huge number of WMN domains, each administered by independent operator. Unlike cellular network WMN may be on a community or on a large-scale as metro, thus the number

of WMN(s) is expected to be larger. Users desire single-sign-on (SSO) and seamless roaming across the WMN domains, which demands mutual authentication between user and WMN domain for secure network access and payment. Authors propose a secure authentication and billing architecture, called UPASS, for wireless mesh networks [ZF07]. UPASS features a novel user-broker-operator trust model builds upon the convention certificate based cryptography (CBC) and the emerging ID-based cryptography (IBC).

3.6.1 Zhang-Fang Protocol Scheme

In the protocol scheme, a mobile user (MU) is attached to a WMN domain wireless mesh router directly of through multi-hop ad-hoc mesh network. For access the network user and domain router will authenticate each-other and user has to pay all the involved entities for their services in real-time. The serving mesh router will provide network access and backhaul internet service for these it should be paid for both the services. As UPASS is credit based and uses user-broker-operator trust model builds upon the convention certificate based cryptography and the emerging ID-based cryptography, the other payers are central certificate authority (CA) who provides domain certificate and signed the IBC public parameters for WMN domain operators, brokers who provide user credit as ID-based certificate for network access and responsible for micropayment aggregation among the entities, domain operator who administers domain routers and provides ID-based certificate for the routers and the associated users after successful authentication. The scheme comprises two phases as entity authentication and billing.

3.6.1.1 Entity authentication

UPASS uses hybrid trust model combination of CBC and IBC. The scheme consists of number of IBC trust domains maintain by each WMN domain operator and broker. Every WMN domains and brokers periodically generate ID-based public parameters, register it with the CA as certificate and place it to a public place for public use. Users resister with their broker for private-key (U-key) and ID-based certificate which acts as credit card for network access, called U-pass. U-pass:= {U-NAI, expiry-date, other-terms as credit-limit}, where user network access identity (U-NAI): = user-id@broker-domain. All the WMN domain router register with their domain and obtain R-pass:= {R-NAI, expiry-date) and R-key. Entity

authentication comprises inter-domain and intra-domain user-router authentication and user-user authentication.

Inter-domain User-Router authentication:

When a user first enter into a new domain, it gets router (R1) broadcasted beacon message which contain R1-pass, router-timestamp (t1) encrypted by router private-key (R1-key), charges, and domain public parameters. User verifies the router identity using WMN-domain public-parameters and R1-pass, then unicasts U-pass and encrypted time-stamp (t2) to the router. Router verifies user-identity using U-pass and user's broker-domain public parameters. For genuine user, router contracts the domain administrators for user temporary identity {U-Pass, U-key}. After successful mutual authentication they derive share-key using IBC share-key equation using Bilinear Pairing Function (ê) as $K_{U,R1} = \hat{e}(\underline{U\text{-}key}, H_1(R1\text{-}pass)) = \hat{e}(H_1(\underline{U\text{-}pass}), R1\text{-}key) = K_{R1,U.}$

Intra-domain User-Router authentication:

Intra-domain authentication occurs when user moves from coverage area of current service router (R1) to target router (R2) in the same WMN-domain. User gets R2 broadcasted beacon message which contain R2-pass, router-timestamp (t1) encrypted by router private-key (R2-key), charges, and domain public parameters. User verifies the router identity using WMN-domain public-parameters and R2-pass. As R2 is in the same domain, user generate share-key ($K_{U,R2}$) and then s/he computes MIC using $K_{U,R2}$ from t1, user-timestamp(t2), and R2-pass. User sends the message to R2 along with U-pass and t2. R2 verifies user U-pass expiry and then generate share-key ($K_{R2,U}$) and verifies the MIC. After successful authentication R2 acknowledges the user.

User-User authentication:

User-User authentication is required when a user is attached to router over ad-hoc network. Initially users are associated each-other without authentication only for authentication message forwarding. After successful authentication of both the users with the router in the same domain, they get temporary credential from domain administrator as (U1-pass, U1-key) and U2-pass, U2-key). Then they can authenticate each-other using challenge-handshake protocol

and can compute share-key $K_{U1,U2} = K_{U2,U1}$ for secure hop-by-hop communication and ensuring payments.

3.6.1.2 Billing

After successful authentication users can access network service through uplink path and directly from a router as a downlink path. Users have to pay in real-time using a micropayment scheme. In the scheme a hash chain is used as a micropayment token. For network access authors consider there are two rates λ for uplink and downlink for router and γ for each relay nodes for uplink data forwarding. If there are n nodes for uplink then uplink rate is $R_{up} = \lambda + n\gamma$ but downlink rate is λ. The billing scheme comprises 3 components as (1) payment structures, (2) making payment (3) redemption of payment structures.

Payment structures:

For the billing process authors design a payment structure using multiple-hash-chains. Making payment from user (U1) to the WMN router (R1), the payment structures are defined using $D_{U1->R1} := \{R1\text{-}NAI, expiry\text{-}date, L, a_1, t, m\}$ as $\{S_{R1\text{-}key}(D_{U1->R1}), (a_m), (w_{1,t}), (w_{2,t}), \ldots, (w_{m,t})\}$, where expiry-date is the date up to this R1 can redeem the payment structure, m is length of authentication hash and the number of payment hash chains, t is the length of each payment chain, a_1 is the first authentication hash derived from random secrete a_m as $a_1=h^{m-1}(a_m)$ and L is value of each payment hash. All the payment hash chains $\{w_{i,j}\}$, where $m \geq i \geq 1$ and $t \geq j \geq 1$, are generated from random numbers by U1. Before the start of a communication session or during the authentication phase, user U1 sends the signed commitment $\{S_{R1\text{-}key}(D_{U1->R1}\}$ of the payment structures to R1. R1 sends acknowledgement to U1. U1 generates only singe payment chain $\{w_{1,t}\}$ for making a payment, and after full spending of the current payment chain, user generates the next chain and sends a triplet $\{a_2, w_{2,1}, h_{a2}(w_{2,1})\}$ as next authentication hash, the payment hash anchor, and MIC of hash anchor using next authentication hash to the router R1. R1 accept the triplet upon verifying MIC as the knowledge of a_2 is the proof that the payment hash chain $\{w_{2,t}\}$ is generated by U1.

Making Payments:

In this scheme user only makes payments to the router. And router makes payment to all the associated relay nodes for their services using the similar scheme maintained by the router.

Relay nodes add MIC of data packet using node-router share-key as proof of their participation. For making payment user maintains debt counter DC_{U1} for R1 and similarly router R1 maintains a profit counter PC_{U1} for U1. DC_{U1} is updated by λ units for one unit data received and by R_{up} units for one unit data sent. Similarly PC_{U1} is updated by λ units for one unit data sent and by R_{up} unit for one unit data received from U1. User sends payment hash when DC_{U1} reach a threshold $\square_{R1}$, as $DC_{U1} \geq \square_{R1.}$ If the user has sufficient payment hash chain, say in chain 2 having starting unspent hash of index 5, then s/he can make payment using $\{w_{2,j}, j\}$ such that $t \geq j \geq 5$ and $(j-5+1)L \geq \square_{R1}$. User and router make decrement of their debt counter and profit counter respectively by (j-5+1)L units. R1 stores payment hash $\{w_{2,j}, j\}$ for redemption.

Redemption of payment structures:

All the collected payment structures should be redeemed from the user's broker before expiry dates. At the end of the day or a predefined time every routers report all the stored payment records to the domain operator and the operator compiles these according to the user's broker and sends them in bulk to the respective brokers as: [$SR1\text{-}key(D_{U1->R1}), a_k, \{w_{i,1}, h_{ai}(w_{i,l}), w_{i,ki}, k_i \mid 1 \geq i \geq k\}$]. The broker verifies user signature for the payment structure commitment, verifies expiry date, verifies $a_1 = h^{k-1}(a_k)$ and stores $a_1, a_2, \ldots, a_k$, verifies MICs of payment chain anchors, and verifies payment hash as $w_{i,1}=h^{ki-1}(w_{i,ki}) \mid 1 \geq i \geq k$. After successful verification broker update WMN operator account balance. If operator has no account with the user's broker, s/he can redeem payment records to his/her own broker. Then the operator's broker clears inter-broker accounts depositing payment records to the user's broker. Similarly relay users can redeem their payment structure with their broker or with operator's broker.

3.6.1 Zhang-Fang billing Scheme analysis

In the billing scheme the commitment of payment structure is user-router specific thus there is no chance of double-spending and double-redemption. The nice feature of the billing scheme is that new signed commitment of payment structures is not required after route change in ad-hoc network portion as all the relay nodes are paid by the associated router. The usage of payment structures only one payment chain in generated but in total multiple chains are used which will reduced the payment chain storage cost and computation cost of next payment hash

generation. But the scheme is vulnerable to security risks from the second payment chain. All the payment chains are authenticated by MIC, thus the unspent portion of the payment hashes may be claimed by the corrupt routers by changing the payment hash as authenticated hashes are known to him or user may deny his last payment chain. All the relay nodes are paid by the associated WMN router and for the verification of relay nodes participation, relay nodes add MIC and their identities, and if there are 3 nodes then about excess 78 bytes are requited to transmit along with every data packets. The router also required extra processing load as it needs to run extra process for all the relay nodes with each packet received but these will not reduce the processing load of relay nodes as they also run billing protocol with the router for their remunerations.

3.7 Abilities and difficulties of existing multipart micropayments

All the existing schemes have some good abilities and difficulties with security vulnerability.

Good abilities:

(1) All the schemes use fault-tolerant and lightweight crypto based payment instrument, the hash chain, which makes the scheme efficient for ongoing payments.

(2) Most of the schemes need one/two public-key based signatures for a particular communication session.

(3) Peirce introduced temper resistance smartcard as enforced at user device and Tewari-D'Mohany introduced temper resistance smartcard for user to carry payment tokens and to encrypt payment endorsements which enables user access anytime and anywhere.

(4) Zhang-Fang use IBC certificate for local authentication and credit certificate with private-key making payment also enables user access to any party.

(5) At hand-off Tewari-D'Mohany eliminates pricing contract involving all parties and releases payment endorsement only to the new nodes at hand-off for achieving fast hand-off.

(6) Zhang-Fang use multiple hash chains a payment structure as payment commitment for efficient payment chain generation and next payment token generation.

(7) Zhang-Fang proposed single point payment at wireless router and in turn router makes payment to the local ad-hoc network relay nodes which elements most of the costly hand-off pricing contracts signing for seamless roaming.

Difficulties:

(1) All the schemes proposed redeeming payment tokens by all the participating parties, those make the redemption process more costly.

(2) Peirce's basic scheme and Zhu's scheme are for single enforcer and enforcer must be in the communication path.

(3) Peirce and Tewari-D'Mohany use small valued and small length payment commitment chains those make the scheme costly for payment commitment purchasing.

(4) In Peirce's scheme, the compromise of smartcard makes the scheme vulnerable as most of the nodes use the same private-key.

(5) At hand-off signing of price and decryption of payment endorsement at relay node's smartcard make the Tewari-D'Mohany's scheme infeasible.

(6) Releases of multiple small valued payment tokens for a single payment as tokens are prefixed make the Tewari-D'Mohany's scheme costly.

(7) In the entire schemes except Zhang-Fang the partially spent payment chains will be discarded at the hand-off.

(8) In Zhang-Fang scheme the next payment chain is signed by HMAC, where the corrupted router may claim full chain for a partially spent payment chain. Also the user may deny last payment chain, those make the scheme vulnerable.

(9) In Zhang-Fang scheme for payment of relay nodes, relay nodes must include the data hash with every data packet which makes the scheme computationally costly and router has to run multiple processes with every data-packet received. Also the routers have to maintain multiple hash chains for payment and have to make frequent payments to the relay nodes which will degrade the performance of the routers otherwise all the routers need heavyweight costly systems with huge upfront investment costs.

Chapter 4: A Secure Multiparty Micropayment Protocol for Internet Access over WLAN Mesh Networks

4.1 Introduction

A mobile user can access networks and can enjoy backhaul internet services directly from an ISP/WISP, through other users, or through multiple private small network service providers using different wireless technologies. Users will roam frequently to different service providers for internet access and they have to pay all the involved entities for their services; additionally relaying entities must also be paid. The payment should be in real-time to avoid unnecessary user trust and mutual service agreements among the participating parties. Real-time payments eliminate the huge trust assumptions, security risks, and the overheads of billing.

Peirce [Pei00] in his Ph .D thesis first proposed ***multi-party micropayment protocol for mobile communication*** and also extended the protocol scheme for Mobile Ad-Hoc Network Payments. Different authors also proposed multiparty micropayment protocol schemes for Mobile Ad-Hoc Networks as presented above in Chapter 3. But the recent emergence of high-speed multi-hop WLAN Mesh technology (IEEE 802.11s), its deployment, and integration with WiMAX technology encourages different small entrepreneurs to deploy WLAN mesh networks as an access network. These access networks demand a new variant of multiparty micropayment protocol for internet access over WLAN mesh network for seamless user roaming across the networks, easy authentication, and an efficient micropayment. In this section we propose a novel multiparty micropayment (MMPay) protocol scheme for internet access over multi-hop WLAN mesh networks as a variant of Peirce's [Pei00] protocol scheme.

Peirce proposed, the end user should not have a digital certificate, but from it's variants for ad-hoc network it is now obvious that a user must have a digital certificate with matching key-pairs for localized offline user authentication and non-repudiation. In our proposed protocol scheme, users have public-key digital certificates for their identities and have payment certificates making payments to multiple vendors in a single transaction or multiple transactions. The existing multiparty micropayment schemes have some security

vulnerabilities and usages of small valued broker signed payment commitment chains make them costly for chain purchasing and payment redeeming. In our scheme these are addressed.

Internet access service comprises two-way communications, and ISP/WISP provides two types of services: basic network access service and backhaul internet services. The basic service includes network access service and connectivity service to locally connected nodes. If the ISP provides both the internet service and connectivity service to locally connected nodes, the internet service provided will be considered as a value-added service, and the user will pay separately to the ISP with separate session with ISP gateway. However, we do not consider intra-domain data communication in our protocol scheme and it is assumed internet service charges are included in ISP's network access service charges. It is also assumed that the user device is cheap and not fully capable to protect user private key. Thus, we propose a client smartcard as a secure device that will generate and store private key and provide trusted protocol accounting services, for network access and for other value added services.

4.2 Protocol Goals

The protocol goals are set to overcome the shortcomings of current CDR billing, macro payment online payment verification, and the difficulties of existing multiparty micropayment schemes. These goals will ensure to remove unnecessary trust and mutual agreements from the system, and reduce the online communications and processing overheads.

1. Real-time payment to all parties from any location:

A user's mobile device should be able to pay all the involved parties providing services in real-time, regardless of its current location. Users will carry prepaid payment certificates from financial brokers.

2. Cryptography for off-line payment verification:

Any entity accepting the payment should be able to verify its validity off-line efficiently, without the need to contact a third party. Each payee should be guaranteed for their payments. Thus the following cryptographies are used in the scheme:

(1) ISP/WISP and Brokers must have CBC certificates for their identities and public parameters. They may have domain certificate for short signature scheme or for IBC scheme depending on implementation.
(2) MSP and pMAP must have CBC based certificates or domain certificates from their brokers depending on implementation.
(3) Users must have CBC based or domain based prepaid payment certificates.
(4) Users must have account identity to their prime brokers.
(5) SHA1 [NIST93] based hash chain is used as the payment instrument.
(6) 1024 bits RSA is used for CBC.

3. User accountability

In the wireless mesh environment user devices may participate in network traffic relaying and roam frequently across the networks. Thus selection of a fixed enforcer for fixing value of a payment hash is nearly impossible. For peaceful and corruption free environment, monetary transactions should be transparent. All involved parties must have client identities and matching certificates from their brokers.

4. Remove need for roaming agreements

The mobile user will pay all involve parties for their services in real-time, no bilateral roaming agreements are necessary among the home SP(s) and foreign SP(s).

5. Dynamic charging

Both the ISP/WISP and VASP(s) should be able to dynamically price their services on per request basis. The relay nodes are extending the reach of an ISP, thus, their charges will be fixed by the ISP. The need for the dynamic charging for integrated Internet services is highlighted by Stiller et al. [SFPW98].

6. Multiple brokers

Users should able to purchase prepaid payment certificates for any online broker who have payment aggregation capability. If necessary a payment token should be redeemable and verifiable at any broker to whom the participating party has an account and who trusts the issuing broker, without need to contact directly to the issuing broker.

7. Portability of monetary value

The payment certificates along with protocol accounting software are stored on a secure client smartcard that allows them to be used in the universal system. The smartcard should be password protected.

8. Minimize system fraud

The effort for stealing value from the system must be far greater than the reward gains. Post-fact detection must identify the culprits.

9. Minimize payment instrument cost

The purchasing and redeeming cost of a payment instrument must be far less than its value.

10. Flexible in route selection in mesh

A user node should able to choose the most optimal route to it destination. At route change toward destination the user should able to setup the path efficiently for forwarding traffic and making payments.

4.3 Protocol Scheme

A user are attached directly to the internet service provider (ISP) access network through a WLAN mesh network, or over multiple private WLAN mesh service providers (MSP). The high level model of the scheme, its players and their interactions are shown in Figure 4-1. In the scheme participating parties are financial broker (B), individual user mobile station (MS), private standalone WLAN mesh access point (pMAP), private WLAN mesh network service provider (MSP), internet service provider (ISP), wireless internet service provider (WISP) and value added service provider (VSAP). The brokers are interconnected to form a private network. Other players have accounts to their respective brokers and have client identities from their brokers. The user purchases internet contents or access the internet through ISP/WISP for which s/he pays in real-time.

In general, in the wireless LAN mesh (802.11s) environment, a user is connected to an ISP through pMAP(s) and a MSP, but in rural area users may be connected through multiple relay user mobile stations (rMS) and a MSP. The MSP can provide services independently and acts

as a Wireless ISP (WISP). A small MSP can act as an associate of an ISP to extend the ISP networks. A Service Provider (SP) is any entity who provides a service during the communication sessions and includes rMS, pMAP, MSP, ISP, NO and VASP. The tariffs need to be set dynamically for a communication session to pay all the involved entities that are identified in the session pricing contract. In the protocol scheme after session establishment, the user releases a stream of micropayment tokens/ hashes into the network to pay all the SP(s) as the session proceeds. The same payment token is worth a different amount to every entity as fixed at the start-up of the session in the form of a pricing contract. Payment tokens are generated by the user device against a payment certificate purchased by the user from one of the several online brokers.

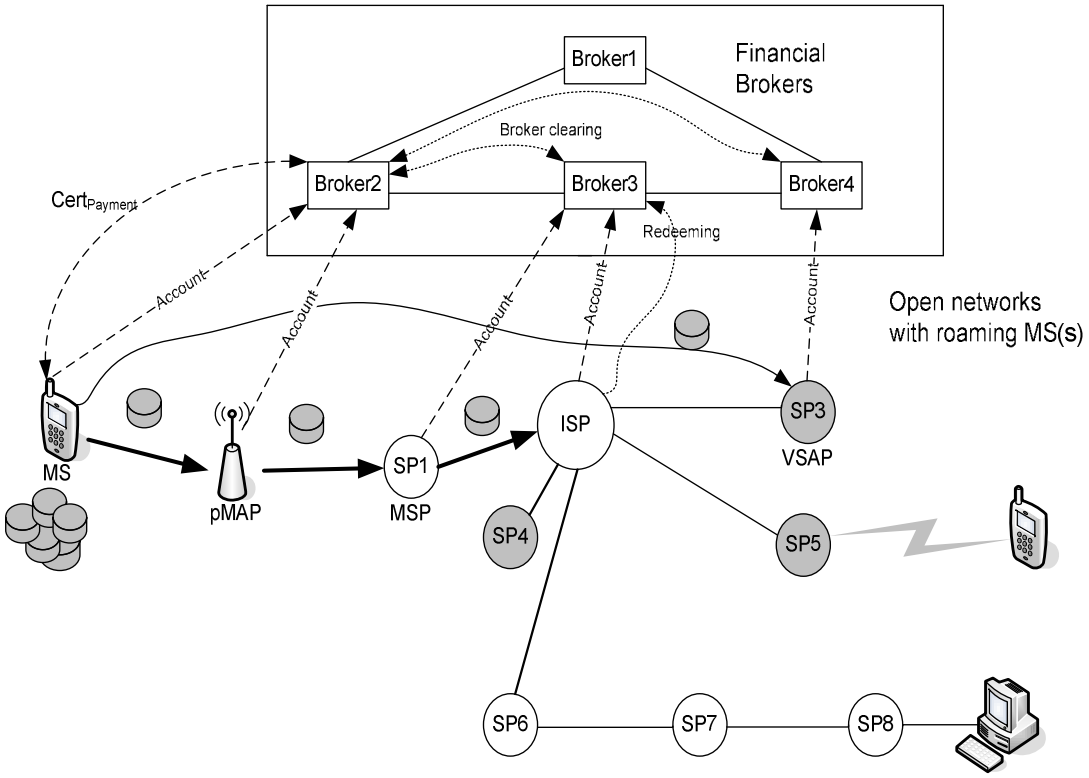


Figure 4-1 Protocol System Model

After the call, the collected payment tokens can be efficiently redeemed by the ISP/WISP for all the SP(s) as all the other SP(s) are extending the ISP/WISP networks. At a delayed time every SP can verify their payments at their brokers. Only the final payment token received from a payment chain needs to be redeemed along with the pricing contract and a user payment certificate. Associate MSP(s) have fixed wireless devices and they must have an agreement

with the ISP for their charges according to their coverage area. Charges of rMS(s) and pMAP(s) are fixed by the ISP dynamically during a session. Main components of the protocol scheme are client registration, payment certificate purchase, pricing contract agreement, ongoing payment, redeeming payment hash, payment certificate and broker clearing, and mid-call and hand-off management.

4.3.1 Client registration

All the users and service providers (SP, MSP, WISP/ISP, and VASP) must register to one of the trusted brokers, who have the capability of payment aggregation and the certificate authority. The broker will physically verify the client national identity according to country rules and regulations and will provide a pseudo identity certificate and will maintain client accounts for the service providers. The broker provides a client card for the user MS(s) containing user identity, share-key, broker certificate, CA root certificate, the initial prepaid payment certificate, and payment software in form of a temper resistance smartcard, which will provide protocol accounting service by generating the payment chains, signing the pricing contracts, and releasing the payment hashes. The format of a client identity certificate is $Cert_{Client}$= *{Client-identity, Broker, Client, Public-key, Expiry}*Sig_{Broker}. When a short signature or IBC scheme has been implemented, the ISP/WISP and brokers register their domain along with public parameters. Then the users, MSP, VSAP and pMAP get domain certificates instead of CBC certificates from their respective home domains. For ease of protocol analysis we use CBC certificate for all the entities.

4.3.2 Payment certificate purchase

A mobile user will purchase prepaid payment certificates from his broker or from any online third-party broker, using an existing macro-payment system. The user sends a purchase message containing the certificate amount, new public-key and macro-payment details signed by user private-key along with a user existing payment certificate. The broker after verifying the user authentication and user accounts or a macro-payment, issues the broker signed payment certificate. The payment certificate ($Cert_{Payment}$) contains Certificate-identity (C_ID), issuing Broker, Value, user Public-key (PK_{User}) and the expiry date. This payment certificate must be spent through the user client smartcard. $Cert_{Payment}$= *{C_ID, Broker, Value,* PK_{User},

Expiry}Sig$_{Broker}$. Figure 4-2 depicts a payment certificate purchasing mechanism from a third-party broker.

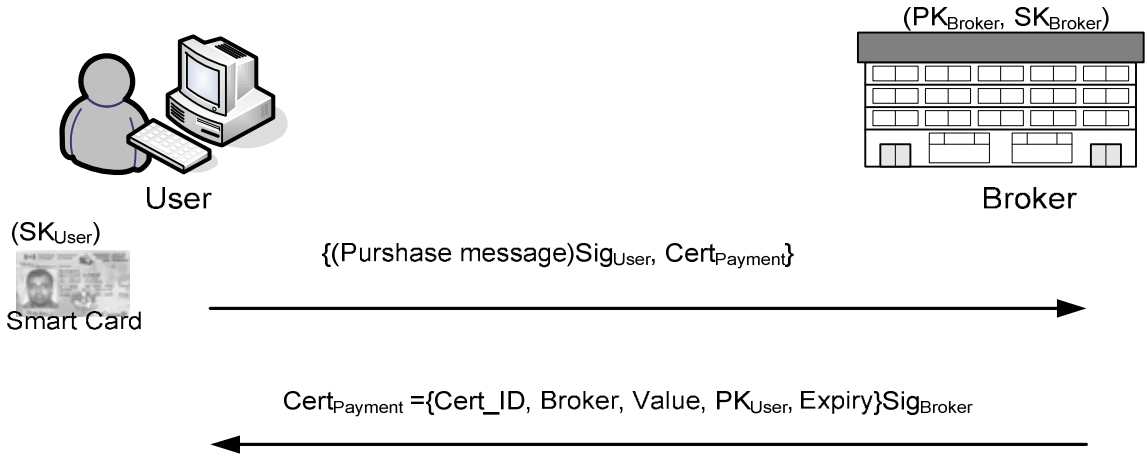


Figure 4-2 Payment certificate purchasing from third-party broker

4.3.3 Pricing contract agreement

To obtain network access and to enjoy internet services the mobile user must have a valid payment certificate. A user joins the wireless network without authentication or showing his credential but for sending or receiving information s/he must establish a communication session in form of a pricing contract and release payment hashes. In a WLAN mesh environment, users associate with the ISP gateway and maintain primary master keys (PMK) and share-keys. Both the user and ISP authenticate their messages using keyed-hashes (HMAC). Users have to establish different sessions for standard best-effort services and premium services. In internet service the up-link and down-link service charges are different, thus users have to pay separately for up-link and the down link. In a session of a WLAN mesh environment, there may involve pMAP(s) and a MSP between the users and ISP, and every one must be paid for their part of service. The pMAP(s) and MSP are extending the ISP network and their service rates are fixed by the ISP or by the neighbour ISP after a hand-off. Figure 4-3 depicts a pricing contract construction using the three-way handshake protocol. The user is responsible for ensuring that the pricing contract is constructed correctly. In case of the ISP gateway has down-link information to the user, but there is no established session to the user, then the ISP optionally sends a pricing contract request message to the user. In step-1: user having uplink or downlink data, the user sends the pricing request message to multiple

paths along with transaction identity for a session to the ISP through intermediate pMAP(s) and a MSP.

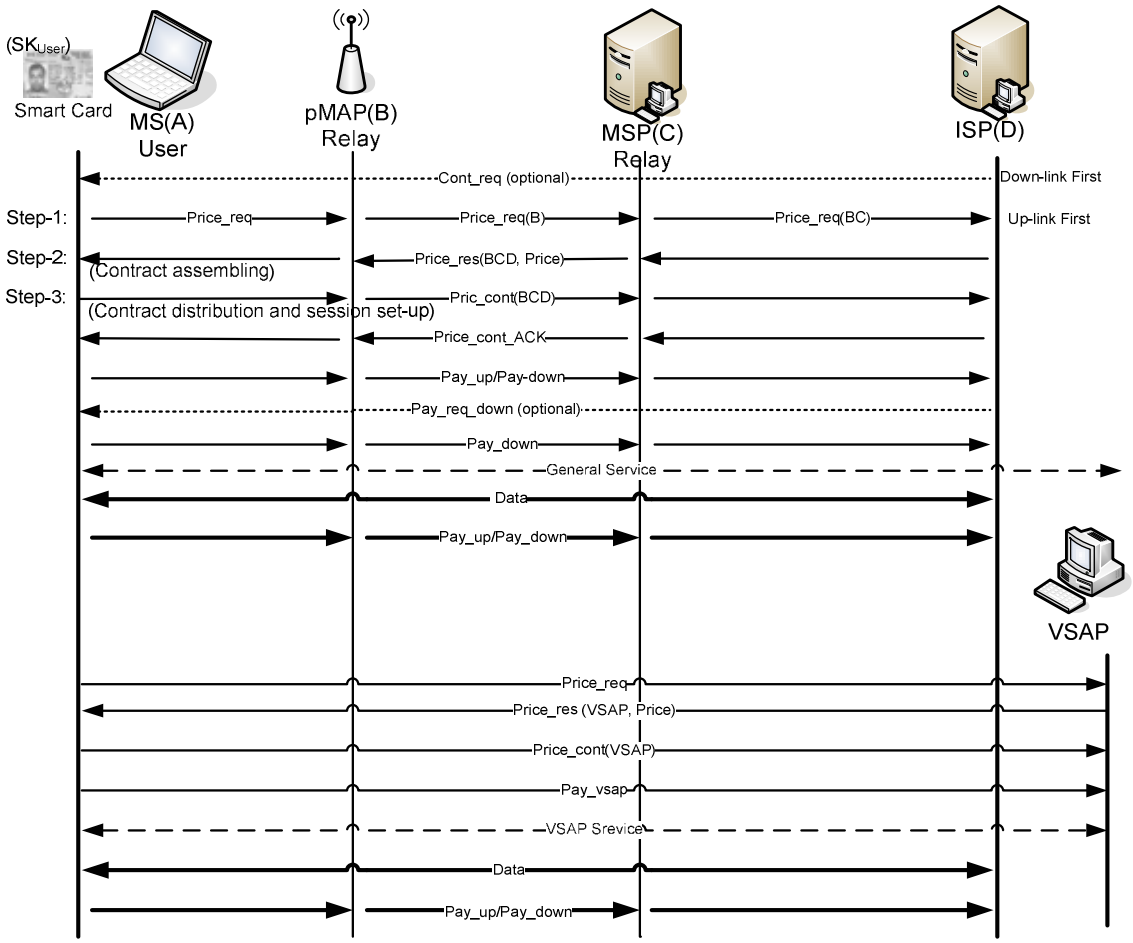


Figure 4-3 Construction of a pricing contract

The MSP and pMAP(s) add their identities and transaction identities to the message and forward it to the next. The ISP queries for current pricing rates; adds a transaction identity and pre-signed or share-key signed current pricing rates to the price response message. In step-2: the ISP returns the price response message to the user using best root through intermediate the MSP and pMAP(s). The MSP and pMAP(s) verify price rates and their part of the message. The user verifies the pricing rates and assembles the pricing contract. In step-3: the user sends the contract to the client smartcard for signing. The user smartcard verifies the balance of current payment certificate; creates two payment chains for uplink and downlink; includes hash anchors ($P1_0$, $P2_0$), and signed the pricing contract. The user distributes the pricing

contract to the ISP through pMAP(s) and the MSP. All the intermediate participants in the route verify the pricing contract, establish a communication session, and forward it to the next. The ISP verifies the contract, payment certificate, establishes a session and acknowledges it to the user. In next steps: upon receiving acknowledgement, the user releases the first payment hash for uplink or for the both-ways. The user may release payment hash along with the session data.

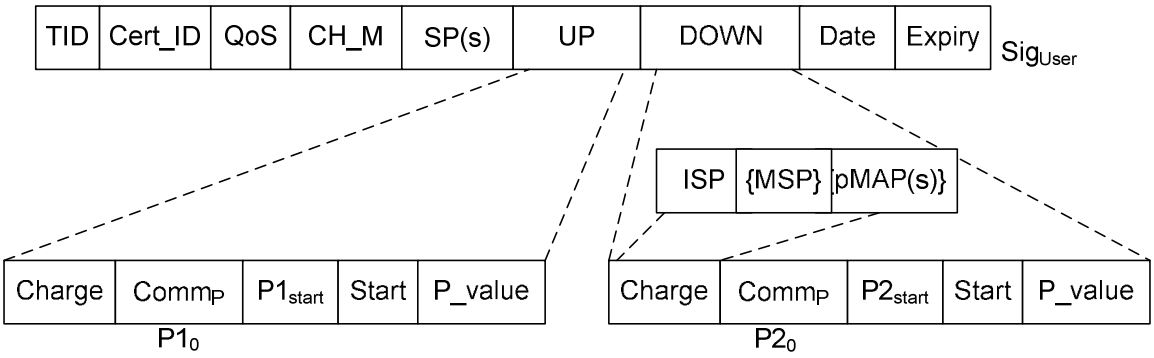


Figure 4-4 Content of a pricing contract

A new pricing contract is required to compile and sign during the mid-session to reflect any change of tariff and to cope with a hand-off. For value added services, the user directly contract with VSAP(s), signs a pricing contract, releases payment hashes, and receives the services. Also for any electronic content purchasing from a VSAP, the user releases multiple payment hashes and the value of a single payment hash must be the permissible amount according to the micropayment systems. The pricing contract sub-protocol has been modeled as follows:

1.0 Start of protocol

2.0 User checks for routes to ISP and compiles messege1: Price_req

2.1 User forwards message1 along with HMAC to ISP/ISP2 through relay service provider nodes

2.2 Relay nodes add their node identity to the message1

3.0 ISP/ISP2 verifies message1 and compiles message2: Price_res

3.1 ISP/ISP2 forwards message2 along with HMAC to user

4.0 User verifies the message2, complies and signs message3: Price_cont

4.1 User forwards message3 to ISP/ISP2 through relay service provider nodes

4.2 Relay nodes verify message3 and establish session; forward message3 to the next

5.0 ISP/ISP2 verifies message3, establishes session, and compiles message4:
Price_cont_ACK
5.1 ISP/ISP2 forwards message4 to user
6.0 User verifies message4 and is ready for payment and data transfer
7.0 End of protocol

A signed pricing contract is shown in Figure 4-4. Its purpose is to allow verifiable dynamic tariffs, fix the starting hash in the payment chain, create a record of the session, and link a single payment commitment to multiple SP(s) for the session. The charging mechanism and service tariff rate will vary according to the service requested, current network load, and time of the day amongst other things. The pricing contract describes the tariff rate and charging mechanism, such as per second, per data unit, or QoS type. The pricing contract fields are described as follows:

- TID: Transaction identifier for the contract, partly generated by every SP.
- Cert_ID: User Payment Certificate identity (C_ID)
- QoS: Transaction type or QoS type.
- CH_M: Charging mechanism, such as per second or per data unit or full.
- SP(s): The identity of the ISP, MSP(s), and pMAP(s)
- UP: Uplink contact information
- DOWN: Downlink contract information
- Date: Date of the pricing contract
- Expiry: Expiry date of the pricing contract (2 days)
- Sig_{User}: Contract signed by the user using user private-key
- Charge: Tariff rate for each the ISP, MSP and pMAP(s) for uplink or the downlink.
- $Comm_P$. Hash anchors of payment chains for uplink or the downlink.
- PX_{Start}. Starting payment hashes from the chain for uplink or the downlink. For a new payment chain this will be $P1_0$ or $P2_0$. For a partially spent chain this will be the last spent hash value.
- Start. Position of P_{Start} in the payment chain.
- P_value. The value per payment hash for the transaction for uplink or the downlink.

4.3.4 Ongoing Payment

The payment is an ongoing process during the session or service. A user maintains an account for the transaction session and at a payment threshold the user smartcard generates a payment hash for the next payment. User and the ISP also synchronize the data transfer for proper accounting, as the WLAN mesh may not confirm the end-to-end data transfer. The user smart

card keeps a record of how much has been spent, updates certificate balance to prevent overspending. The user device optionally generates a session payment secrete from the payment hash and releases it along with the payment hash at a regular interval, and SP(s) provide the contracted service for a valid payment hash. If the user does not get the desired service, s/he ends the session by not realising any more payment hashes. Figure 4-5 depicts a user making payments through a session for uplink data. At every interval, the user releases a payment hash, where the payment starts with $P1_1$ from a new payment chain. The ISP, MSP and pMAP(s) independently verify that the payment is valid by performing one hash function on it to obtain the previous payment hash; in this case the starting hash is $P1_0$. Since the hash function is one way, payment hashes cannot be forged, and knowledge of the payment hash is proof of the payment. The downlink payment is similar as uplink as depicted in Figure 4-3, only an optional payment request may make by the ISP if downlink information arrive before the payment. They forward the valid payment hash to the next. The ISP verifies the payment hash, the session payment secrete and optionally acknowledges the payment to the user as shown as dotted lines. Only the ISP/WISP redeems the highest payment hash $P1_N$, and all the other SP(s) will be paid according to the pricing contract.

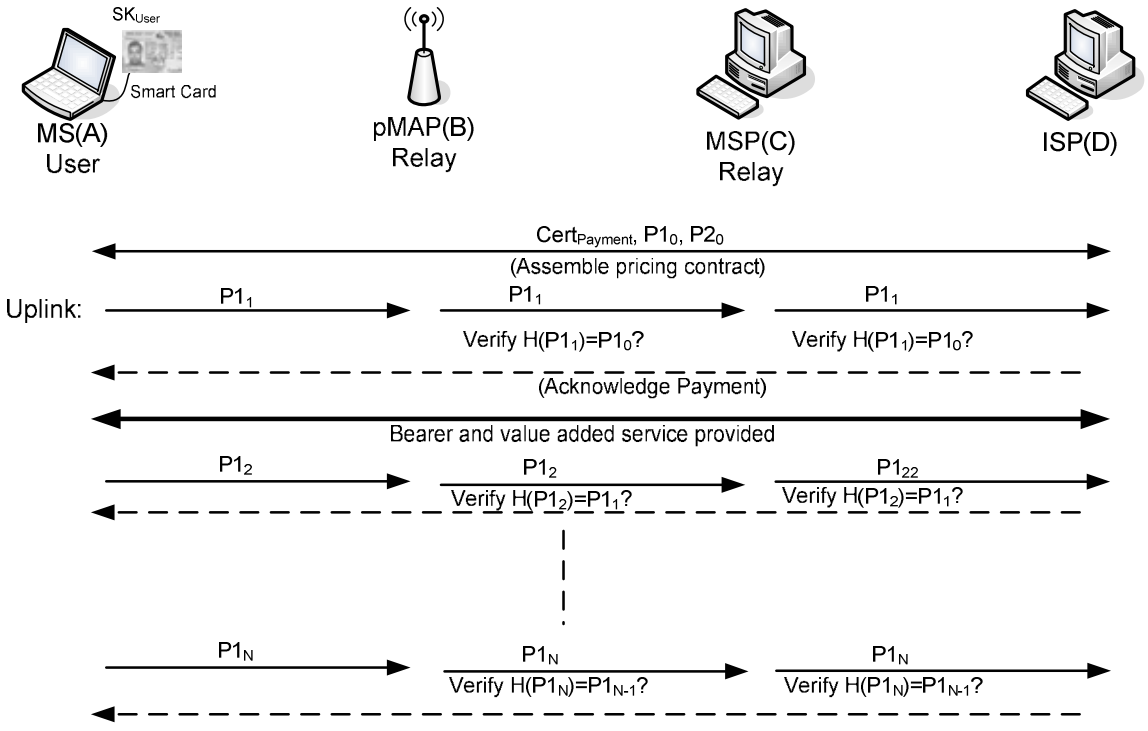


Figure 4-5 User pays all SP(s) with same payment hash for uplink

The ongoing payment sub-protocol has been modeled as follows:

1.0 Start of protocol

2.0 For a payment threshold, user generates the next payment hash, updates the certificate balance, generates the session payment secrete from the payment hash and compiles messege1: Pay

2.1 User updates session status and forwards message1 to ISP/ISP2 through relay service provider nodes

2.2 Relay nodes verify the payment hash, update session status and forward messag1 to the next

3.0 The end entity (ISP/ISP2) verifies the payment hash and the session payment secrete, updates session status and compiles message2: Pay_ACK

3.1 ISP/ISP2 forwards message2 to user

4.0 User verifies message2 and continues data transfer

5.0 End of protocol

4.3.5 Redeeming payment hashes, payment certificate and multiple broker clearing

End of the day in a suitable time or a predefined time interval, only the ISP/WISP/VASP will redeem the highest spent payment hash obtained from a communication session with the payment certificate issuing broker or from its own broker. The broker will only accept a payment hash from an ISP/WISP/VASP if a corresponding user payment certificate and the pricing contract accompany it. The ISP groups the messages chronologically according to the user payment certificate and attaches a user payment certificate for a group. In a batch process, the broker verifies the pricing contract and finds SP(s) identities and their payment portions from the attached pricing contract. A SP amount is SP's charge*(X-Start) and the user amount is P_value*(X-Start) for deduction. The broker can verify the payment hash by doing (X-Start) number of hashes on P_X and comparing that with the starting hash as included in the pricing contract. Then the broker compiles a clearing payment message for every SP's broker and for the user certificate issuing broker along with their payment reports and transfers the batch message to all the related brokers. Upon getting clearing payment message SP(s) brokers will update SP(s) accounts and payment certificate issuing broker accounts. Periodically brokers

will clear the inter-broker payment through a common payment gateway or a common bank or through inter-bank money transfers. The certificate issuing broker updates the user certificate balance and stores all the payment records for future verification in case of any dispute. All the other SP(s) and MS(s) can verify their payment at their brokers. A user also redeems his payment certificate balance from the issuing broker after the expiry. The payment certificate issuing broker verifies the certificate expiry and transfers the certificate balance to the user home broker, and in turn the user home broker updates the user accounts balance.

4.3.6 Mid-call and hand-off management

In the protocol scheme, the ISP and MSP, pMAP(s) wireless devices are fixed but the user-MS(s) move their positions. These will result the route change toward the ISP. However, all the service providers along the path must be paid for the new session and all the new providers along the path must have the new pricing contract. Also with during the time passes, the price rate may be changed at every 60 minutes. Thus, with the new rates, a new pricing contract must be signed for the transaction session. In case of route change and the price rate change the user smartcard signs a new pricing contract using the current payment hash chain and distributes it along the new path. But in case of spending of the current payment chain to a threshold, the user smartcard generates a new payment chain and signs the new pricing contract. Practically, the intra-domain hand-off in the same MSP will happen frequently, there the physical path toward the ISP will change but the payment path will not change. Then the new pricing contract signing is not required but the new serving MAP of a MSP will have to collect the payment records of the current pricing contract from the old serving MAP, or from a central AAA server. The hand-off and mid-call management process has been modeled as follows:

1.0 Start of management process

2.0 User checks for hand-off or end of payment chain or change of price

3.0 In case of end of payment chain or change of price

3.1 Call sub-protocol: Pricing contract agreement starting after message2

4.0 In case of hand-off

4.1 User checks for the change of the accounting path

4.2 In case of accounting path change

4.2.1 Call sub-protocol: Pricing contract agreement with exiting payment chains

4.3 In case of physical path change

4.3.1 User requests to the ISP to distribute the old pricing contract along with session status

5.0 End of management process

4.4 Security analysis of the protocol scheme

We have examined the proposed payment scheme for possible attack and it is secure against attacks. We use 160 bits SHA1 as hash chain for payment instrument, 1024 bits RSA algorithm for digital signature and a temper resistance smartcard at a user node. As the digital signatures cannot be forged, hash chains cannot be inverted, and an encrypted message needs the correct secrete key to decrypt, so we consider our scheme is secure. This scheme is a variant of multi-party micropayment protocol of Peirce [Pei00]. Thus, we have made an analysis of the protocol for security vulnerability on attack is based on writing a number of claims and proving each claim to be correct. The claims are described in 5 (five) groups as follows:

4.4.1 Outside attacker fraud as man-in-the-middle-attacker

(1) An attacker cannot obtain value during a payment certificate purchase from a broker:

As the user signed purchase request send to a broker, an eavesdropper can not able to get value from the micropayment information. Even if the attacker observes the payment certificate and macro-payment information; s/he can not use it with out the knowledge of the user's private RSA key which is secured in a smartcard.

(2) An attacker cannot redeem value from a paid session, even if all the payment messages are observed:

Redeeming value requires a valid pricing contract signed by the user, and the pricing contract includes involved parties, as the eavesdropper identity is not included in the contract, s/he will not get any value even if s/he observe all the messages. The redemption is only permitted to the ISP or the VSAP.

(3) An attacker cannot impersonate a value holder to obtain a free service:

In the protocol scheme, the pricing contract is signed by the user smartcard, thus having knowledge of the last payment hash and the user payment certificate; the eavesdropper cannot use it for getting a free service. Also all the pricing contract sub-protocol messages are authenticated by HMAC using the ISP-user share-key.

(4) An attacker cannot impersonate a valid SP during a communication session:

The route from the user to an ISP is determined by the under laying routing protocol. If the attacker is not in the route, s/he will be identified by other connected MSP(s) and MS(s) along the route or by the ISP to whom all relay service provider must be registered, as well as all the node-to-node messages are encrypted in the wireless LAN mesh environment.

4.4.2 User Fraud

(1) A user cannot spend more than the total value or double spend of a payment chain and cannot be obtained a chargeable service for free:

The total value along with the certificate identity specified in the broker-signed payment certificate must only be spent through the user smartcard. The smartcard maintains the account balance and it is not possible to overspend or double spend without compromising the smartcard. The broker also records the total amount redeemed against a payment certificate, thus any overspend is detectable by the broker and the user is only responsible for the overspending and double spending. SP(s) provide a service only after getting a fresh pricing contract which includes timestamp or TID. Thus, the user can not obtain a chargeable service for free; s/he must release payment hashes obtaining the service.

(2) Colluding with any party gains no additional value or services:

The user smartcard is responsible for contact signing and any overspending is detectable by the broker. The ISP(s) and VSAP can only redeem the payment hashes along with the user signed pricing contact and a corresponding user payment certificate. Thus, colluding with SP(s), the user can not gain additional value or extra service because for all cases, the user accounts will be deducted.

(3) Limited anonymity is provided:

The user's actual identity is not specified in the user account-identity, and only the pseudo certificate identity is included in the user payment certificate.

4.4.3 SP Fraud

(1) An SP cannot obtain more value than paid by a user:

An ISP for all the other SP(s) only can redeem payment hashes along with pricing contacts and user payment certificates. The user signed pricing contract defines the payment hash value for the participating SP(s) for a communication session.

(2) An SP cannot obtain value belonging to another SP:

The participating SP(s) identities are specified in pricing contracts and thus, they cannot obtain others value without the signature forgery of the pricing contract.

(3) Pricing contracts cannot be replayed at session setup without detection:

The pricing contract contains TID as fresh nonce from all the participating SP(s) or user timestamp and signed by the user. Any attempt of reusing an old contract will be detected.

(4) An extra value cannot be obtained by collusion:

The relaying SP(s) can not redeem the payment hashes and can not obtain an extra value by collusion with others. But an ISP can obtain a higher payment hash from a separate pricing contract that includes the same payment chain. The ISP is considered a trusted entity and the payment inquiry from other SP(s) will detect the ISP fraud. Usage of a new payment chain for the new pricing contract will prevent this situation in case of dispute.

(5) Stealing value by the SP(s) is limited to a single payment hash:

Upon getting a payment hash SP(s) may close the session and a session may be closed due to a hand-off or mid-call rate-change, thus the maximum value of a singe hash may be lost by the user. To overcome this situation the part of the first unit of the hand-off session may be offered free of charge like many other services offered now a days, then in average nobody will loose any value.

4.4.4 Broker Fraud

(1) The amount owed to every SP by the broker can be proved to an independent third party:

The values of the payment hash to the participating SP(s) are identified in the signed pricing contract. Therefore, any party can verify the amount owed to a specific SP. The inter-broker payment clearing massages also provide the proof of owed amounts. However, the brokers are the most trusted entities in the scheme.

4.4.5 Denial-of-Service Attacks

A denial-of-service (DoS) attack is an attempt to deprive legitimate users of system access. In the protocol scheme, the signing of a pricing contract is the most computationally expensive event. The user signs the pricing contract, which already limits the DoS attacks. The contract replay as a DoS attack is limited as all relay pMAP(s) and MSP include their transaction identities in the contract or current timestamp is included in the user signed pricing contract. The blocking of a payment hash by intermediate relay pMAP(s) may cause frequent new pricing contract signing by the user but implementation of protocol at the MAC layer or at the network layer will limit user access to block payment hashes. As well, there will be a change in route if a number of predefined times of loss connections occur, which in turn limits the attacks. Most of the time, a route change will not affect the accounting path and thus, a new pricing contract signing is not required. The routes are monitored by the ISP gateway controller and an affected root will be blocked temporarily in case of frequent loss of connection. In the protocol scheme, the ISP-user transactions are synchronised periodically which will detect and prevent the blocking of transactions.

4.5 Performance estimates and assumptions

The theoretical performance of the scheme in terms of computation, storage, and communication has been examined like other multi-part micropayment schemes. The computation cost has been measured in terms of the number of hash computations. It has been assumed there are four SP(s) involved in an average; there are two pMAP(s), a MSP and an ISP. 1024 bits RSA and the 160 bits SHA1 have been used as crypto functions for the estimation. An average general field size is 16 bytes, and sizes of the other protocol fields have been assumed as below in Table 4-1:

Object	Details	Size(bytes)
SP/ Broker(B)	URL/ Name of SP/ Broker	16
Date	Expiry Date (Expiry)	2
Time	Time stamp	12
SP/User/Broker Identity	Coded Identity	4
Client account identity	B:Client (SP/User): B_ID, SP_ID, U_ID	8
Certificate identity	Certificate Identity (C_ID=B:Certificate No.)	16
Hash	SHA1 (P_0, P_1, etc.)	20
RSA Private Key (d)	Private Key (SK_{SP})	128
RSA Public Key (e, n)	Public Key (PK_{SP})	134
RSA Signature	Signed by any entity (Sig_{SP})	128
SP Public Certificate	{ SP_ID, B, SP, PK_{SP}, Expiry, Sig_{Broker}} for SP	304
Len	Chain Length	2
TID	Transaction ID party generated by an entity	4
QoS	Best-effort, Premium services	2
CH_M	Charge mechanism (unit of service)	2
Charge	Tariff Rate	2
Value	Monetary Value	2
Payment Certificate	{C_ID,B,Value,PK_{User}, Expiry, $Sig_{Broker.}$}	298
General protocol fields	Field not defined	16
Price rate/ Signed price rate (premium, BE)	ISP, MSP, and pMAP rates for up/down with QoS, CH_M and time of validity	36/176

Table 4-1 Size of basic protocol fields

According to basic protocol fields, the size of a partial pricing contract as a pricing request, a contract summary, and a signed pricing contract are estimates as follows in Table 4-2:

Object	Content	Size of content	Total
Price request:			
User MS to pMAP(1)	Price_req, TID	16+4	20
pMAP(1) to pMAP(2)	Price_req, 2TID, SP_ID	16+2*4+8	32
pMAP(2) to MSP	Price_req, 3TID, 2SP_ID	16+3*4+2*8	44
MSP to ISP	Price_req, 4TID, 3SP_ID	16+4*4+3*8	56
Price replay from ISP to user MS			
Trough all relay entity	Price_rep, 5TID, 4SP_ID, Price rate	16+5*4+4*8+24	92
Fully signed contract from use MS to ISP			
Trough all relay entity	Full TID, Cert_ID, QoS, CH_M, SP(s)_ID, UP and Down (Charge, PX_0, PX_{start}, Start, P_value), 2Date, Sig_{User}	5*4+16+2+2+4*8 +2*(6+20+20+2+2) +2*2+128	304
Contract summary			
MS, pMAP(s) and MSP	TID(s), SP(s), Up/Down { Charge, PX_0, PX_{start}, Start, X P_value},2Date	20+32+2*{6+20+20 +2+2+2)+4	150

Table 4-2 Size of Multi-Party Micropayment Components

4.5.1 Storage costs

The storage requirement for user MS, pMAP(s), MSP and the ISP has been calculated in terms of bytes. Mainly two types of storages; they are certificate storage and the payment material storage. It has been considered that there are three concurrent payment sessions run at user MS, two for uplink and the downlink internet access and one for a VASP service. As it has been assumed at every 60 minutes a new pricing contract will be signed and thus, the average payment hash chain length has been assumed 300. Optionally we can store one hash value per 30 hashes then the storage requirement is 200 bytes (10*20) for a singe chain, or we can calculate one payment hash value at the cost of 149.5 hashes in an average. Thus, the storage estimations are as follows:

Entity	Contains	Content size	Total
Certificate storage (bytes)			
User MS	$Cert_{Broker}$, SK_{User}, $Cert_{Payment}$	304+128+298	730
SP (ISP/ MSP/ VASP/pMAP)	$Cert_{Broker}$, $Cert_{SP}$, SK_{SP}, $Cert_{Root}$	3*304+128	1040
Payment Materials(bytes):			
User MS	C_ID, Value, 2*(5TID, $P1_0$, $P1_X$, X, P_value, $P2_0$, $P2_Y$, Y, P_value), Part of VASP contract	16+2+2*{20+2*(20+20+2+2)}+{8+20+20+2+2}	286
	Optionally hash storage, 4 chains	4*200	800
	Optionally contract sum./contract	150/304	304
pMAP(s) and MSP	{TID, $P1_0$, $P1_X$, X, P_value, $P2_0$, $P2_Y$, Y, P_value}	{20+2*(20+2)}	64
	Optionally contract/ contract sum.	150/304	304
ISP	{TID, $P1_0$, $P1_X$, X, P_value, $P2_0$, $P2_Y$, Y, P_value}, Pricing contact	{20+2*(20+2)}+304	368
	Payment Certificate per user basis	298	298

Table 4-3 Storage estimation for the protocol scheme

From values presented in Table 4-3, it is clear that the storage costs of the scheme are acceptable according to the present capacity of a mobile device. The user needs to store under 2Kbytes in total and only 286 bytes for 3 ongoing concurrent sessions, which are suitable for a device with limited storage like a smartcard. A user can calculate the payment hash value at a faster rate at the cost of 400 bytes per session. User and the relay stations can optionally store the contract summary or signed contract for verification purpose. The cost of a contract summary is only 150 bytes and a user stores it in the mobile device for daily payment verification. Thus, a user or a relaying service provider can store 7084 contract summaries

using only 1 Mbytes of storage, which is enough for a relay MS(s). The storage of payment materials is 64 bytes during a communication session bytes and is only 44 bytes after the session. Thus, the payment storage for pMAP(s) and MSP along with the contract summary is 194 but it is 348 bytes for an ISP. The ISP also needs to store the user payment certificate once per user. However, the payment records will be stored no longer than a day.

4.5.2 Communication costs

The runtime storage and communication costs for a session involve session establishment in form of a pricing contract and the payments. The pricing contract compilation and signing, and making the first payment is the first phase of commutation. The ongoing payments are the other phases. The commutation costs are estimated in Table 4-4.

Entity	Contains	Content size	Total
Communication for first payment (bytes)			
User MS -> pMAP1	{TID, Price_req}, {Signed contract, $Cert_{Payment}$}, {TIDs, PX_Y}	20+{304+298}+40	662
pMAP1-> pMAP2	{2TID, SP_ID, Price_req}, {Signed contract, $Cert_{Payment}$}, {TIDs, PX_Y}	32+{304+298}+40	674
pMAP2 -> MSP	{3TID, 2SP_ID, Price_req}, {Signed contract, $Cert_{Payment}$}, {TIDs, PX_Y}	44+{304+298}+40	686
MSP->ISP	{4TID, 3SP_ID, Price_req}, {Signed contract, $Cert_{Payment}$}, {TIDs, PX_Y}	56+{304+298}+40	698
ISP---> User through MSP and pMAP(s)	{5TID, 4SP_ID, Price_res, Price rate}, { TIDs, Cont._ACK}	{20+32+16+36/176} + {20+16}	140/ 280
Communication for ongoing payments (bytes) for all entity			
User --->ISP through pMAP(s) and MSP	{TIDs, PX_Y, Y}/ {TIDs, $P1_X$, X, $P2_Y$, Y}	{20+20+2}/64	42/64

Table 4-4 Runtime storage and communication estimations

The runtime and communication cost at the session set-up is a little high as the 3-way hand-shake is required. The maximum message size is only 602 bytes between a pair of entities at the pricing contract distribution phase along with a user payment certificate. However, if a user can send a payment certificate along with the pricing request then the

maximum size of the message will be only 354 bytes between MSP and the ISP; the payment certificate distribution is required once when the user signs the pricing contract. Thus, the maximum message size is only 354 bytes, which is quite reasonable in the wireless LAN mesh environment.

4.5.3 Computation costs

The hash function is the basic component in cryptography and we have used SHA1 in our scheme. The computation cost of SHA1 has been considered as the unit cost. The equivalent number of SHA1 hash computations for RSA signature verification and signature generation are 238 and 2910 respectively [Pei00]. Thus, the computation costs in terms of hash unit for different entities in the scheme has been estimated for the pricing contract compilation, contract signing and making the first payment, and then for the ongoing payments as shown in Table 4-5.

Entity	Contains	Content size	Total
Computation cost for first payment (#hashes):			
User MS	Verify $\{Sig_{ISP}\}$, Generate $\{P1_0, P2_0,$ signing contract $\}, \{P1_1, P2_1,$ secret$\}$	238 + {2*300+ 2910} +{2*14.5+2}	3779
MSP/pMAP	Verify $[\{Cert_{Payment}, Sig_{User}\}, \{P1_1, P2_1\}]$	2*238+2	478
ISP	Verify $[\{Cert_{Payment}, Sig_{User}\}, \{P1_1, P2_1,$ secret$\}]$	2*238+2+2	480
Ongoing Payments(# hashes)			
User MS	(n-1)/2 hashes to get $P1_X$ or $P2_Y$, Secrete	(30-1)/2+1	15.5
MSP/pMAP	Verify $\{P1_X$ or $P2_Y\}$	1	1
ISP	Verify $\{P1_X$ or $P2_Y$, secrete$\}$	1+1	2

Table 4-5 Computation costs for the scheme

The computation costs, for the protocol scheme at different entities as shown in Table 4-5, has been estimated considering hash generation, hash verification, signature generation, and signature verification. But there are also other costs, such as message compilation, data comparison, session setup and the session end. However, these costs are negligible compare to the hash computation cost. According to the cost table, the computation cost at the user MS is very high as 1024 bits RSA signature generation, signature verification, hash chain generation are done at the user smartcard but it is only one time for a communication session. The pricing contract and session establishment cost for the other entities are relatively low compared to the existing protocol schemes, which will be beneficial for cooperative relay pMAP(s) and the loaded MSP to serve more users. The ongoing payment costs are also low, which will make the

scheme efficient. In the protocol scheme, the user MS is a weak device and the user smartcard is the weakest component, this introduces the computational bottleneck to the scheme. We are hopeful as the smartcard technology is advancing every day and presently, a medium smartcard can generate 1024 bits RSA signature at 41 milliseconds (ms) and can verify it at 5 ms. Researchers are working hard for improving the smartcard crypto capabilities, speed, and data rate. Now most of the smartcard contains crypto modules along with the 2048 bits RSA signature scheme. Different groups also working for combining multiple smartcards in a USB smart device and in the near future we will get the suitable smartcard device at an affordable price.

4.5.4 Performance estimation for financial broker

The financial brokers are the most trusted entities in the protocol scheme. They should have large and secure computing systems with huge storage capacity and communication facility. In proposed scheme, the work load of a broker is similar to other micro payment protocol schemes and will therefore minimize some of the costs. In the existing multi-party protocol schemes, users purchase multiple payment hash chains and all the payment commitment chains are signed by the broker, but in our scheme a user purchases a payment certificate weekly or bi-weekly, which will reduce the computation and communication costs of payment chain purchasing about 1000 times. In case of redemption, we propose only the ISP/WISP/VASP can redeem the payments along with the pricing contracts, but in the existing schemes all the SP(s) redeem payments with their brokers. We expect, this will reduce the communication, computation and storage costs about 4 times as we have considered 4 SP(s) will participate in a session. But in the protocol scheme, redeeming broker will transmit the user accounts update information to the other brokers and in tern all the brokers will update their client accounts. All the other corners are similar to other multiparty micropayment schemes, where all the related brokers will communicate with the payment certificate issuing broker for payment aggregation and the inter broker clearance. In our protocol scheme, all the users have digital certificates in the form of payment certificates, thus the brokers have to maintain the certificates as a certificate authority and an updated certificate revocation list to a public place.

4.6 Optimisations of the protocol scheme

The theoretical performance estimation of the scheme shows that the user smartcard devices are the performance bottleneck as they have to sign the pricing contracts and to release the payment hashes. A midrange smartcard can sign at the cost of 41 ms, thus, it may not be a problem for an initial session set-up but it is a big problem for a hand-off situation. To improve the situation we have proposed a share contract signing approach, where the user will sign the initial pricing contact and the ISP will sign the subsequent hand-off pricing contracts. In the scheme, all the relaying entities are extending the network of an ISP/WISP and the ISP is trusted to them. The relaying entities may not require verifying the signatures of the pricing contracts and storing them. The MSP is the biggest relay service provider in the proposed scheme and only the root MAP(s) of the MSP or the MAP(s), who are connected to the ISP only are responsible for protocol accountings, but they are already loaded for the high volume of data transfer. All the MAP(s) of a MSP may share the accounting loads and thus, we have proposed following optimisations of the protocol scheme.

(1) A relay entity need not verify the signatures on the pricing contracts:

To ensure the payment, the relay entity needs to verify: his price, user signature on the pricing contract, and the user payment certificate. But in the wireless communication all the peer-to-peer messages are encrypted and the pricing contract is verified by the ISP. We assume that without the valid pricing contract the ISP will not provide any service. As a trusted entity and for his business s/he must verify the pricing contract and the user payment certificate. If any discrimination occurs then the relay entity can resume the verification.

(2) A relay entity need not store the pricing contract for the payments:

In the scheme ISP/WISP/VSAP is only responsible for the redemption of payment hashes for all the entities participated in a communication session and the ISP is trusted. Thus, the relay entity needs not to store the full pricing contracts, but s/he can store the summary contracts for the verification of payments. If any discrimination occurs then the relay entity can resume storing the pricing contracts.

(3) The ISP/WISP can sign the pricing contract at hand-off and mid-call situations:

The user payment certificate must be spent through the user smartcard, which keeps a record of certificate balance. The user will sign the pricing contract: when a user enters into an ISP for the first time, a user having a new session at an inter-domain hand-off, and at the full spending of a payment instrument. But a new pricing contract as a hand-off pricing can be signed by the ISP at a hand-off or a mid-call tariff rate change situation. The starting point of the payment chain in the new hand-off pricing contract will be the last spent payment hash. For this purpose, we have introduced the new hand-off secrete hash values to make the pricing contract and payments unique along the path instead of payment secretes, and the first hand-off secrete hash value H_0 will be included in the user signed pricing contract, where H_0=h(P_0, session-secrete) and session-secrete=h(current-contract, ISP-user share-secrete). At the hand-off or mid-call situation user or the ISP will include the new series of hand-off secrete hash, but for the payment for a session user will release the next hand-off secrete as H_1=h(P_1, session-secrete) along with the next payment hash. The ISP can verify H_1 as a trusted entity but all the relaying entities will store the last hand-off hash along with the last spent payment hash as the proof of a payment as a payment triplet {P_X, H_X, X}. The ISP will sign and distribute the new hand-off pricing contract and the user will verify and store the new hand-off pricing contract if the value of a payment hash is changed, and releases payment triplets for the session. The new pricing contract will need to include a data-transfer-credit-balance (DCB) field of size 6 bytes. The optimised hand-off pricing contract sub-protocol has been modeled as follows:

1.0 Start of protocol

2.0 User checks for routes to ISP/ISP2 and compiles messege1: Hoff_cont_req

2.1 User forwards message1 along with HMAC to ISP/ISP2 through the relay service provides

2.2 A relay provider add its identity to the message1 and forwards to the next

3.0 ISP/ISP2 verifies message, generates session-secrete, hand-off secrete hash, calculates data-transfer-credit-balance, compiles and signs message2: Hoff_cont

3.1 ISP/ISP2 forwards message2 to user through relay service provider nodes

3.2 A relay provider verifies message2; establish session and forward message2 to the next

4.0 User verifies message2 and is ready for payment and data transfer; optionally sends ACK with session data or with next payment

5.0 End of protocol

(4) For a session a single payment hash chin can be used for both the uplink and downlink traffic:

In a multiparty payment scenario, all the relaying entities are extending the ISP/WISP service connection and their tariff rates should be fixed by the ISP at the certain ratios of ISP tariff rates. And the uplink tariff rate is multiple of the downlink tariff rate. One unit of price rate for the down link service can be fixed, and then the rate for the uplink service can be calculated from a multiplying ratio included in the pricing contract. Using this single unit rate, total cost for the uplink and downlink services can be calculated as:

*Total cost = previous cost + (up/downlink data * unit rate * link ratio)*

*= {previous data + (up/downlink data * link ratio)}* unit rate*

= calculated data unit rate*

As the tariff rate is fixed in the pricing contract and the payment hashes are released for the number of unit of service is provided, thus using a single payment hash chain for calculated data or the service, the total cost of service for uplink and the downlink can be determined. 1000 as default ratio for the downlink service can be used and an uplink ratio relative to downlink can be included in the pricing contract.

(5) Multiple sessions for multiple QoS(s) are not required, only one session can be sufficient for all the QoS(s) and the payment can be made using single payment chain:

The WLAN mesh devices can prioritise four different classes of services. These are voice, video, best-effort and back ground. Using the same concept of usage of a singe hash chain for uplink and the downlink, using a basic unit price rate for the best-effort downlink service, the other rates for different classes of services can be calculated from their multiplying ratios. The wireless data packet contains the QoS value, thus the total cost of data transfer for all the services can be calculated as follows:

Total cost = previous cost + (up/downlink data unit rate * link ratio* QoS ratio)*

*= {previous data + (up/downlink data * link raio* QoS ratio)}* unit rate*

*= calculated data * unit rate*

1000 as default ratio for downlink and best-effort service, and the other ratios for the different QoS(s) can be included in the pricing contract. Then using only a single payment hash chain, the payment can be made for all the services in a transaction session.

(6) *All the Mesh Access Points (MAP) can share the payment protocol load instead of bearing the load by the MAP(s) connected to the WISP:*

All the MAP(s) in a MSP except the root Access Point (RAP) have the similar capability. But the root AP (RAP) is highly loaded as it relays a huge number of traffic and communicates with the Wireless LAN Controller (WLC). A MAP connected to the ISP/WISP may not be RAP, and then it is better to share the payment protocol load among all the MAP(s) in the MSP. During the session establishment phase all the MAP(s) along the path have the payment protocol capability and should verify the price request for the MSP identity; in case there is no MSP identity in the request message, it will add the MSP identity. It also verifies the signed pricing contract and sets up the session if it has added the MSP identity other wise it will add the user Mac-address in the session database without the session identity for incoming and outgoing traffic to relay traffic. At the payment and data transfer it will verify the session database using Mac-address, for established sessions it will do all the protocol calculations and relay the traffic.

(7) *The pricing contract sub-protocol contains 4 (four*) messages *but the first two messages, the price-request and price-response can be embedded to the user association activities:*

All the wireless LAN mesh users maintain share-key and PMK with the ISP/WISP gateway. Thus at the time of association a user can request for price and the accounting path signed by HMAC using the ISP-user share-key. The ISP/WISP can send the share-key signed price response to the user through the associated MAP. The message may reach directly to the user only through the neighbour MAP then the relaying service providers may not able to add their part of pricing contract transaction identity (TID) preventing replay attacks. The pricing contract contains the current-time, and using a predefined time-window the relaying service providers can verify the contract freshness preventing the replay attack. The omission of full TID(s) will reduce the pricing contract size about 16 bytes and only the user part of TID(s) can be used as a unique session identity. From these

16 bytes, 10 bytes along with date field will be required for current-time and 6 bytes can be used for the data-transfer-credit-balance field.

(8) *A small length payment chain can be used and at the full spending of the payment chain a new pricing contract with a new payment chain can be signed by the ISP:*

In wireless communication frequent hand-off occurs due to user movement and as a result signing of new hand-off pricing contracts are required. This leads to usage of a small length payment chain, that will reduced the payment chain computation and storage cost at the user smartcard device. For this purpose, we have introduced a new payment authentication chain having a small length to authenticate the new payment chain. The first hash value A_0 of the authentication chain as hash anchor will be included in the user signed pricing contract, then the first payment after new chain will be a payment quadrant $\{A_1, P1_1, H_1, 1\}$ but the subsequent payment is a payment triplet $\{P1_2, H_2, 2\}$.

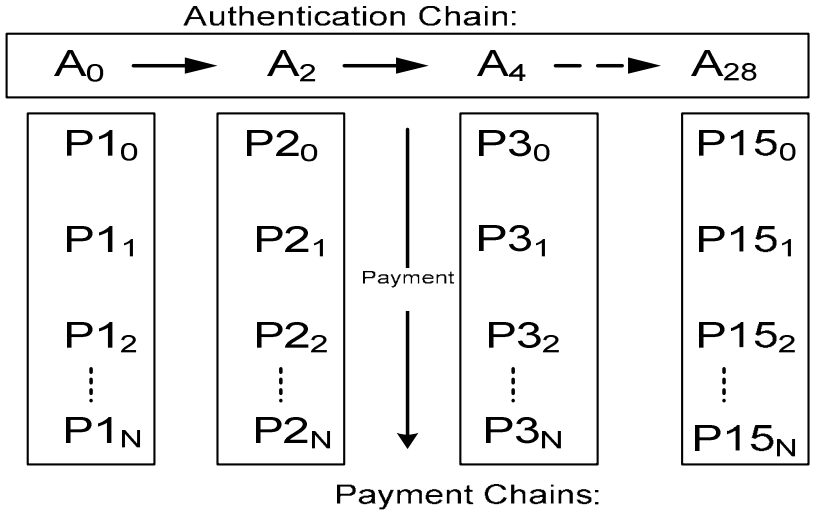


Figure 4-6 Construction of payment chains with authentication chain

At the full spending or spending to a threshold of the current payment chain $\{P1_I | N \geq I \geq 0\}$ at the hand-off, a newly user generated payment chain $\{P2_I | N \geq I \geq 0\}$ authenticated by the next authenticating hash A_2 will be transferred to the ISP for signing a new hand-off pricing contract, where $A_1 = h(A_2)$. The knowledge of A_2 is the proof that the payment chain has been generated by the user, and then the ISP signs the new hand-off pricing contract including the new payment chain. As the ISP signed pricing contract will be distributed along the path including the user, s/he can not alter the hand-off contract

gaining excess values from the payments. Then the first payment after the new hand-off contract is a payment quadrant $\{A_3, P2_1, H_1, 1\}$. The release of A_3 is the authentication of the new payment chain by the user, and s/he can never deny it. The construction of payment chains are depicted in Figure 4-6. The payment structure will allow making 15*300=4500 payments but the user needs to store only a payment chain of length 300 and an authentication chain of length 29 for an ISP.

(9) *The intra-domain hand-off contract and the hand-off contract for the change of charges can be signed by the ISP using the share-secrets:*

The ISP/WISP is the most trusted entity in WMN domain and it is assumed that s/he will not cheat a small amount for the business reputation. In general, the ISP domain administrator and AAA devices are secure, trusted, and auditable. In case of frequent hand-offs, the hand-off pricing contract will be signed by the HMAC(s) using all the participating entity's share-secret. According to our assumption in an average there are only pMAP2, pMAP1 and MSP between ISP and user, thus only 3 HMAC(s) are required for signing the hand-off pricing contract, which will significantly improve the performance of the protocol scheme. In case of the change of charges, the hand-off pricing contract will be signed by 3 HMAC(s), where the SP(s)'s charges will be changed but the value of the singe payment hash will be unchanged. The user can verify the hand-off pricing using the hand-off secrete hash as it has been derived from the ISP-uses share-key. The value of a single payment hash is already defined in the last public-key pricing contract or the hand-off pricing contract. Using the new charges, the data-transfer-credit-balance will be calculated, but the payment will be made using the value of a single payment hash as identified in the last public-key signed contract as follows:

```
t_charge:=isp_charge+msp_charge+pmap1_charge+pmap2_charge
cal_data:= (up_or_downlink_data * link_raio* QoS_ratio)
DCB :=  DCB – cal_data
if DCB ≤ threshold
    make a payment
    DCB: = DCB + {(unit_data_volume*p_value)/t_charge}
endif
```

The new hand-off pricing contract is signed using HMAC by the ISP, these can be altered by involved entities in the session for gaining value but all parties agreed to trust ISP for the payment and s/he is trusted for his business interest thus his judgement is final regarding the payment. However, the cheating of relaying entities can be detected as the pricing contract, the payment triplet and the payment quadrant contain hand-off secrete hashes those are unknown to all the relaying entities but every body along the path store them. The ISP cheating is also detectable as user-ISP shared-key is embedded in the public-signed contract if form of hand-off secrete. At the time of auditing and payment redemption, the ISP will provide the user-ISP share-key to the broker verifying the hand-off pricing contacts. In case of any dispute, signing will be resumed using public-key. Alternately, the ISP can periodically authenticate the HMAC(s) at a certain threshold along the path at a hand-off. The format of HMAC(s) authentication message is depicted in Figure 4-7, and the size is about 246 bytes in an average. All the SP(s) along the path can verify their stored HMAC(s) and it will ensure their payments.

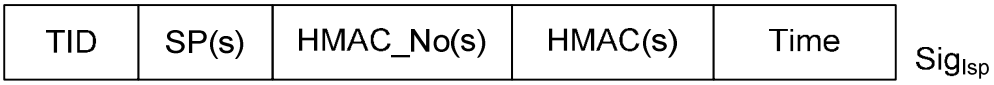


Figure 4-7 HMAC(s) authentication message format

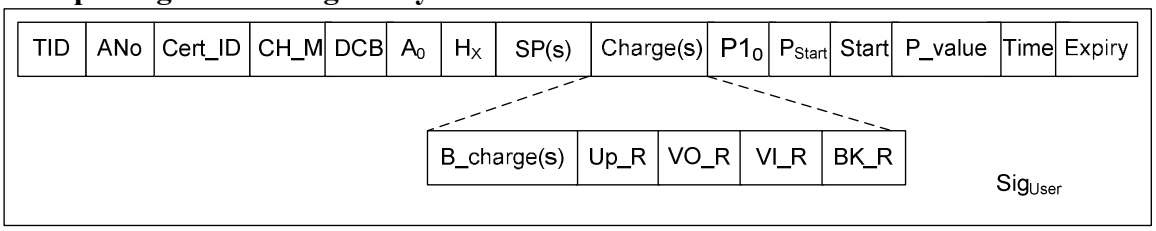
(10) The first pricing contact can be signed by the ISP:

The user smartcard signs the first pricing contract against a trusted broker signed payment certificate. In turn the ISP signs subsequent hand-off pricing contracts including the payment chain embedded in the user signed pricing contract. Thus, the ISP can sign the first pricing contract like a hand-off if the user smartcard provides a signed payment commitment. The payment commitment should include the user payment certificate identity, a payment authentication hash anchor, the first payment chain hash anchor, the ISP identity, the value of a single hash, current timestamp and the expiry date. The ISP signed pricing contact will eliminate the user's payment certificate verification cost at relaying service providers {MSP(s) and pMAP(s)}. This optimisation will be effective: when a large WISP will provide IBC/short-signature based for its associated service providers and MAP(s), and the network access charges are nearly constant at a certain period of time.

4.6.1 Performance Estimation of the optimise scheme

According to proposed optimisation the format of the signed pricing contract will be changed. The pricing contract contains charging mechanism, base service tariff rate, uplink ratio, QoS ratio for voice traffic, QoS ratio for video traffic, QoS ratio for back ground traffic, hand-off secrete hash, authentication hash, and a single payment chain. The charging mechanism and service tariff rate and ratios will vary according to current network load, and time of the day amongst other things. Figure 4-8 depicts optimised pricing contracts.

First pricing contract signed by the user:



Subsequent hand-off pricing contract signed by the ISP:

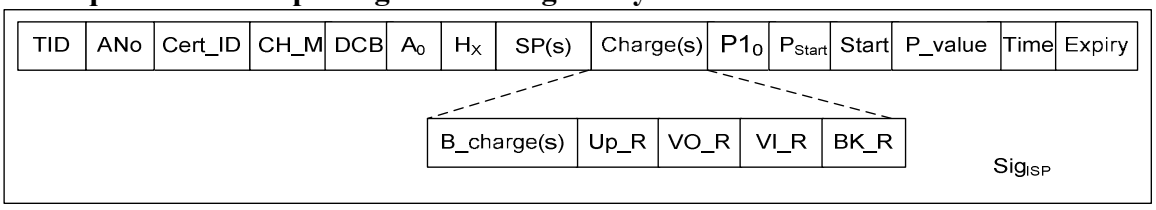


Figure 4-8 Pricing contract and hand-off contract for the optimised scheme

The pricing contract fields are described for 4 SP(s) as follows:

- TID: Transaction identifier for the contract generated by the user, 4 bytes
- ANo: Position of payment chain authentication hash value (A_0), 2 bytes
- Cert_ID: Payment certificate identity (C_ID), 16 bytes
- CH_M: Charging mechanism, such as per data unit, 2 bytes
- DCB: Data-transfer-credit-balance, 6 bytes
- H_0/H_X: hand-off secrete hash value, 20 bytes
- A_0: Payment chain authentication hash value, 20 bytes
- SP(s): The identity of ISP, MSP(s), and pMAP(s); 4*8=32 bytes
- Charge(s): Charges for all SP(s) and pricing ratios
- B_charge(s): Base charges for Downlink best-effort service for all SP(s), 4*2=8 bytes
- UP_R: Uplink service charge ratio, 2 bytes
- VO_R: Voice traffic service charge ratio, 2 bytes
- VI_R: Video tariff service charge ratio, 2 bytes
- BK_R: Back ground tariff service charge ratio, 2 bytes
- $P1_0$: Hash anchors of first payment chain, 20 bytes
- P_{Start}. Starting payment hash from the chain, 20 bytes

- Start: Position of P_{Start} in the payment chain, 2 bytes
- P_value. The value of single payment hash for the transaction, 2 bytes
- Time: Date and time of the pricing contract, 12 bytes
- Expiry: Expiry date of the pricing contract (2 days)
- Sig_{User}: First contract signed by the user, user signature, 128 bytes
- Sig_{ISP}: Hand-off contract signed by the ISP, ISP signature, 128 bytes

The size of the optimised pricing contract is also (166+128), 304 bytes. In the optimised scheme, the cost of storage, communication and computation will be reduced. If there are 5 hand-off(s) and 2 sessions per user, then the internet access cost reductions are as follows:

Storage Costs:

In the original scheme the entities along the path store 12 pricing contracts or contract summaries, but only 6 contracts or contract summaries are required in the optimised scheme and the hand-off contract size is only (304-128+60)= 236 bytes. Thus, the contract storage cost is reduced to half. The payment hash chain storage cost is reduced to quarter as the single payment hash chain has been used for uplink, downlink, and all the QoS(s) services. The pricing contract and payment hash storage cost for the MAP(s) of a MSP will be further reduced as a distributive approach has been used. The hand-off pricing contracts are signed by the ISP, thus the ISP need not to store the public-key signatures of the hand-off pricing contracts. The value of the single payment hash will not be changed in most of the hand-off contracts, and those are not required to store in the user devices.

Communication Costs:

The commutation cost of the optimised scheme will be reduced as the hand-off pricing contracts are signed by the ISP; the partial contract along with pricing rate from the ISP is not required to transfer to the user. As the hand-off pricing contract is signed by the ISP, a user payment certificate is not required to distribute with the hand-off contract request. The communication cost will be further reduced at least to half as one pricing contract is signed for all the QoS(s) services. Also the ISP can combine all the hand-off pricing contracts and can sign the combine one for the redemption. Thus, only one combined signature is required to transfer over communication channel to the financial broker instead of all the signatures at redemption.

Computation Costs and Timing:

In the optimised scheme one payment hash chain of length 300 is required for both the uplink and downlink services instead of two payment hash chains of length 300. But an extra hand-off secrete hash is required along with a payment hash. As a small length payment chain has been used, the next payment hash calculation cost will be reduced. Single pricing contract is signed for all QoS services, thus the signing cost is reduces to half in average and one hash chain is used instead of 4 hash chains. The user only signs the first pricing contract, the ISP signs the rests and then some are signed using HMAC(s), thus the overall signing time will be reduced as ISP maintains a large computing system.

In the optimised scheme the computation load of a financial broker will also be reduced significantly. The hand-off pricing contracts are signed by the ISP, and thus ISP can combine all the hand-off pricing contracts without signature and can sign it for the redemption. Thus, the broker needs to verify only the combined signature for a group of hand-off pricing contracts.

4.7 Summarization of protocol scheme

The proposed multiparty micropayment (MMPay) protocol scheme has been designed for internet access over wireless WLAN mesh networks as a variant of Peirce's [Pei00] protocol scheme, but it is assumed to be suitable for ubiquitous use. The summary of the scheme after optimization is detailed as follows:

Cryptography:

Cryptography has been chosen for efficient offline verification of the payment instrument. In the protocol scheme, the 160 bits SHA1 [NIST93] is used for hash function, the hash chain [Lam81] is for the payment instrument, and the 1024 bits RSA is for CBC for the public-key signature. Short signature and IBC are also considered for the intra-domain authentication.

Participating parties in the scheme:

CA provides PKI infrastructure, the digital certificates for the brokers and WMN domain operators. S/he also certifies their domain public parameters for IBC and short-signature schemes. The Finical brokers are the payment aggregators; they provide the client

account-identity, prepaid payment certificate for the user, and digital public-key certificate for others as a certificate authority. The ISP/WISP provides internet access and mesh network access service as a domain operator. MSP and the pMAP(s) extend the ISP mesh for network access. Users MS(s) enjoy the services and also optionally extend the ISP mesh networks. VSAP provides internet based value added services for the users.

Payment certificate:

In our scheme, the prepaid payment certificate is used as a payment commitment which can be purchased weekly or bi-weekly. Thus, the payment certificate purchasing cost is reduced significantly. Usage of prepaid certificate provides the opportunity to grow the business and provides guarantee for payments.

Smartcard:

The user devices contain a secure and tamper registrant smartcard to protect user private-key and to provide protocol accounting service. The smartcard is provided by the user home broker at the time of registration. The usage of a smartcard provides the opportunity of using inexpensive user devices and universal devices for ubiquitous payments. The payment certificate in the smartcard also provides the opportunity of seamless user roaming across the networks and internet access anywhere and anytime.

Pricing contract:

The pricing contract is signed by the user smartcard once s/he enters in a new WMN domain. The WMN domain controllers maintain associated user profile along with a share-key and a PMK, and thus all the protocol messages are authenticated by keyed-hash (HMAC) to prevent DoS attacks. The first two messages of this sub-protocol are for pricing and path setting as a MSP may use distributed approach for protocol implementation mentioned in the protocol optimization section. This part is the most costly and time consuming part in the whole protocol scheme and used only once for a particular WMN domain, but have no effect for user network access as the communication start after successful a pricing contract agreement and distribution of the first payment token. For VSAP services users have to sign and maintain separate pricing contracts implemented separately but using the same smartcard accounting application.

Payment:

The payment is an ongoing process during the communication session and users have to release payments in a regular interval according to the pricing contract. This is the most critical but efficient process of the scheme as hash chain has been used as the payment instrument. A user releases payment triplet $\{H_X, P_X, X\}$ to make a payment, where only 15 hashes for users, 1 hash for relay service providers and 2 hashes for ISP are required for making and verifying a payment. For the payment process variable length multiple hash chains have been proposed but only a small length authentication chain and a payment chain of length of about 300 has been generated for an ongoing session, which reduces the user payment storage cost and next payment token generation cost as well. Also the inclusion of hand-off secret hash provides unique payment tokens for a session although the same payment chain has been used for different sessions.

Hand-off pricing contract:

In the wireless networks, the hand-off is common and frequent in a fast mobile environment; thus, the efficient hand-off management is a great challenge in the protocol design. In our scheme, the hand-off pricing contracts are signed by the ISP/WISP. The intra-domain hand-off pricing contracts for user movement are signed using HMAC(s) along with a periodical authentication of HMAC(s) option, which makes the scheme further efficient and provides a scope to implement the protocol scheme in a fast mobile environment though the communication range of the MAP(s) are limited. Unlike the pricing contract, in hand-off, only two messages are required which reduces the communication cost and timing. With the inclusion of an authentication chain, the scheme provides the scope of signing the hand-off pricing contract by the ISP using a new payment hash chain without any security vulnerability. The usage of different values for the charge component and a single payment hash provides the opportunity to store only selected number of hand-off pricing contracts at the user devices where value of a payment hash is changed or a new payment hash chain is included in the contract. The proposal of inter-domain mobility group enables the scope to maintain the profiles for neighbour ISP(s) and inter-connection over EOIP tunnels for the fast hand-off and uninterrupted internet service for hand-off users through inter-domain connections.

Redemption of payment tokens:

The payment token redemption process is computationally expensive in all the existing micropayment protocol schemes. In our scheme, as all the relaying service providers (MSP and pMAP) are extending the ISP/WISP wireless networks, the ISP/WISP is responsible for the payment redemption for all of them. Because the ISP/WISP signs the hand-off pricing contract, s/he compiles all the pricing contacts, hand-off pricing contract and payment tokens together, and puts a single signature for all of them discarding all of his/her signatures. These will significantly reduce the payment token redemption communication costs and the broker end computation costs as s/he will verify only one signature instead of a group of signatures. Also the single point redemption further reduces the broker end computation costs and overall communication overheads.

4.8 The comparative performance estimation of MMPay scheme

The MMPay scheme has been devised as a variant of Peirce's multiparty micropayment scheme for mobile ad-hoc networks. Thus, a comparative performance of MMPay with Peirce's mobile ad-hoc networks scheme is detailed as follows:

Security: The MMPay scheme is more secure as all the protocol messages are authenticated and the public-key digital certificates are provided for each user instead of a group of users.

Storage: The certificate storage cost is similar for both schemes, but the ongoing storage cost will be far less than for Peirce's scheme, as: it uses multiple payment hash chains; hand-off contracts are signed by ISP mostly using HMAC(s); a single pricing contract is signed for all the uplink, downlink and QoS(s); users do not store HMAC-signed hand-off contracts; and the ISP compiles a payment report discarding all its own signatures for redemptions.

Communication and computation: The computation and communication costs are similar for the user-signed first pricing contact. However, in all the other cases, MMPay costs are far less than these at Peirce's, as: a single pricing contract for QoS(s)/downlink/uplink session, single point redemption, multiple payment hash chains, ISP-signed hand-off contracts and weekly/bi-weekly payment certificates are used. Furthermore, the ISP compiles the payment reports discarding all its own signatures for redemptions.

Chapter 5: Protocol Simulations in Opnet Modeler and Results

5.1 Introduction

The new protocol is best to simulate and to examine in a network simulator environment. The Optimized Network Engineering Tools (OPNET) is a very powerful network simulator for cost, performance and availability analysis. Opnet is also well accepted by the Network Protocol Designers for new protocol designs and performance analysis. In order to analyze the performance of the proposed protocol scheme, we have deployed the protocol scheme as custom application in Opnet Modeler 14.5, in the wireless ad-hoc mesh network environment. We have considered the response-time and latency, data communication throughput, and ETE delay as protocol performance indicators as they are used in billing protocol simulation [CCG09].

5.2 Opnet Modeler

Opnet modeler comprises mainly of three domains called network model, node model and the process model. Node model specifies the objects in a network domain and the process model specifies objects in the node domain [SP03, Opnet]. Figure 5-1 depicts the Opnet models hierarchy.

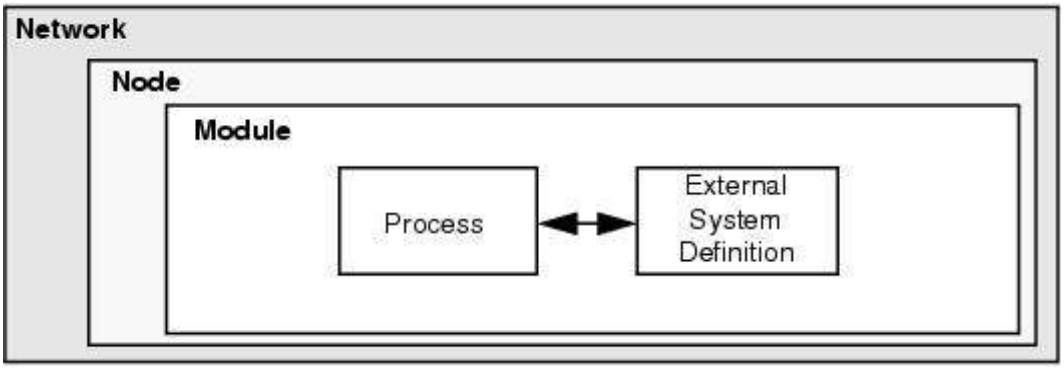


Figure 5-1 Hierarchical levels of Opnet models

Network Model:

The network model defines the Opnet project that contains a network topology, devices, network nodes, links, traffic flows, applications, and other network objects. Simulation work is

done at the network model, where creation of a simulated network and analysis of simulation results are done, as shown in Figure 5-2 depicting the Opnet Modeler workflow.

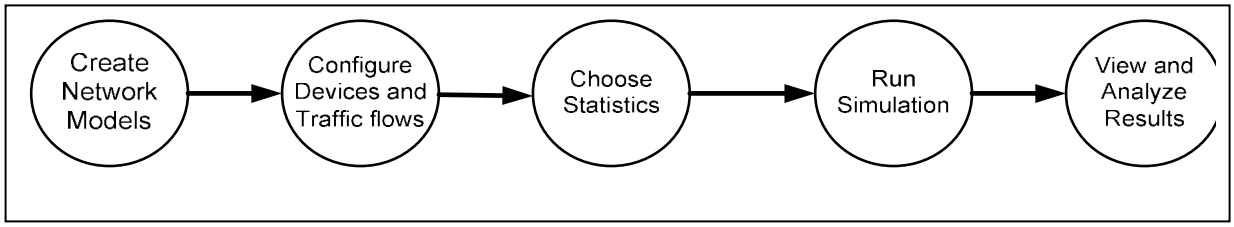


Figure 5-2 Opnet Modeler Workflow

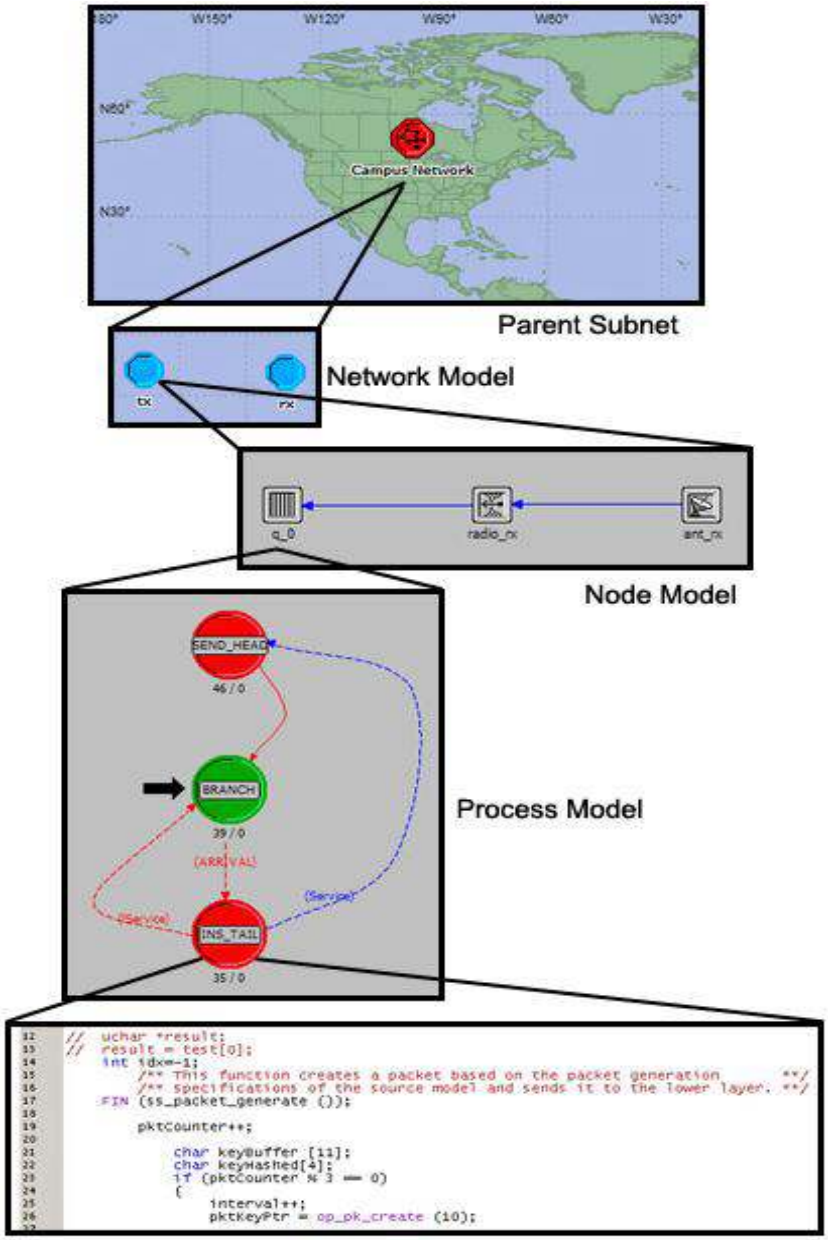


Figure 5-3 Opnet models hierarchy and internals

Node Model:

A node model specifies the internal structures and capabilities of an Opnet Modeler node. A node may contain multiple modules depending on the node capabilities; they are interconnected to each other to indicate traffic flow and statistic. The modules in the node are process models.

Process Model:

Process models define the underlying functionality of a node model, and are represented by finite state machines (FSMs) consisting of several forced or unforced states with state transitions among them. Operations performed in each state are described in embedded C or C++ code blocks [Opnet]. Figure 5-3 depicts the Opnet models hierarchy and internals.

5.2.1 Opnet Modeler as Application Simulator

Applications are the predominant sources of traffic in the network, they make demands on the bandwidth and the underlying network technology, and create load on the servers. Applications are modeled in terms of the size of the packets generated, the rate at which they are generated, and the transport protocol over which it runs (e.g., TCP, UDP, fiber channel, etc.). Opnet modeler supports standard application models and custom application models. The standard applications are already designed and useful for analyzing network configuration. But the custom application model is an application modelling framework which allows for defining custom application having specific traffic pattern for the study. The custom application model breaks down the application into smaller components known as tasks and phases, and allows configuring each detail of how and when the application sends requests and responses; how it sets up and reuses connections; and how much time is spent in processing. The custom application model is very useful for modeling multi-tier, complex application-layer signalling protocols whose architecture in terms of its transactions is well-defined.

5.2.1.1 Custom Application Architecture

Custom Applications generate network loads and server loads according to specified patterns. The Custom Application has the following characteristics:

- More than two hosts can be involved in the data transfer and processing.

- Client-Server interactions are task-based. A task consists of many interactions between a client and a server or among successive servers.
- The basic task consists of many phases. Each phase consists of a data transfer and/or a processing event, which can occur at any end device (at tier node). The entire task is complete only when the last phase of the task has been completed.

5.2.1.2 Custom Application Definition

A custom application is defined as a set of independent tasks, a task contains a set of interdependent phases, and a phase contains a group of request–response transactions among tier nodes. An application can be defined using following steps:

- Identify the tiers
- Identify the independent tasks
- Identify the task phases
- Breakdown each phase
- Determine the parameters

The Parameters of a transaction define the size, dependency, starting time, tier processing time. Figure 5-4 depicts an application modeling pattern.

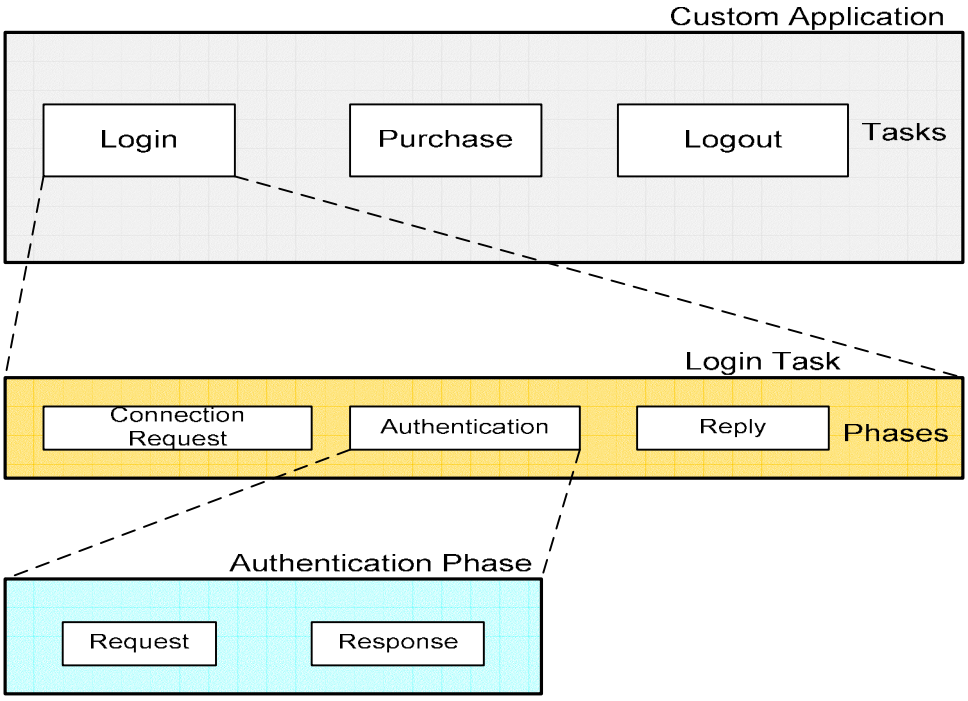


Figure 5-4 Application Modeling Pattern

In Opnet Modeler a task is configured in the task definition module, and then the application is defined as a custom application in the application definition module. An application running profile to generate traffic flows, are defined in the application profile definition module and applied to the application client nodes. The task can be configured manually or by using the ACE Whiteboard module. The ACE Whiteboard model editor provides a graphical interface to draw the traffic patterns on a network as a series of interdependent messages and allows for changing the message parameters. It also allows modeling a complex application behaviour using the Python logic scripts.

5.2.1.3 Task Definition using ACE Whiteboard

The ACE Whiteboard is an application design environment for modelling and studying different application designs or design modifications, including application logics and the module hierarchies before implementing them. It has a full featured message editor to design an application task entirely from the scratch. An application task can be created in the ACE Whiteboard editor using flowing steps:

- Creation of application tiers
- Creation on transaction messages
- Editing message attributes
- Adding logic scripts

(a) Creation of Application Tiers:

In the OPNET Modeler application tiers are defined using the ACE Whiteboard Wizard as shown in Figure 5-5 through following menu paths:

(1) File => New => ACE Whiteboard => Create application manually

(2) Enter tier names

(3) Click Next and Finish to create the tiers and switch to the message editor

(b) Creation of transaction Messages:

At the ACE Whiteboard message editor, stay on the Data Exchange Chart tab and create messages through following steps:

(1) From menus, select: Insert => Message. The Editor will be on the message creation mode.

(2) Click on source tier and then click on the destination tier. A message from a source to a destination will be created with default attributes.

(3) Right-click on blank portion of the message editor to end the mode.

(4) Save the ACE Whiteboard file.

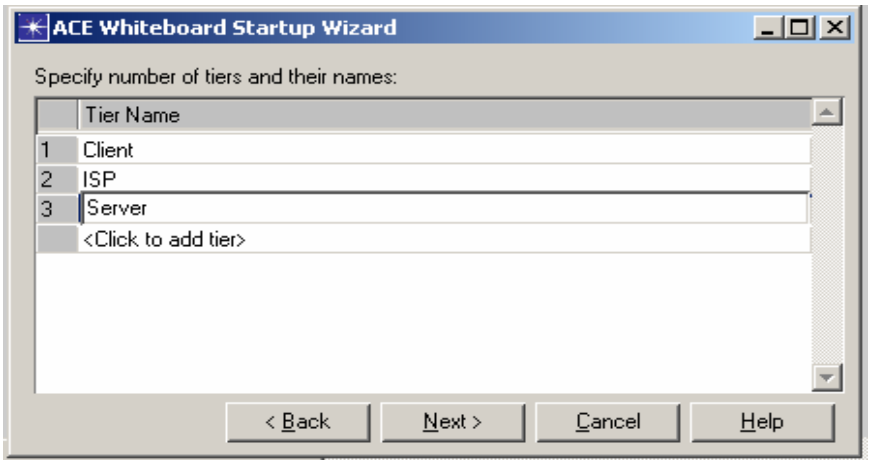


Figure 5-5 Creation of Application Tiers in ACE Whiteboard

(c) Editing Message Attributes:

The newly created messages have default attributes. The attributes mainly are massage size, tag description, dependency, processing time and the user time, may be required to modify according to an application design. Figure 5-6 depicts the OPNET Modeler ACE Whiteboard Editor where size of the message#1 is changed to 50 bytes and processing time of the message#3 is changed to 0.150 sec. The message modification work is done through following steps:

(1) Select messages using Ctrl+ Click

(2) Modify the message attributes as required

(3) Save the modified ACE file selecting File => Save.

(d) Adding Logic Scripts:

The ACE Whiteboard allows adding a Python logic script at the start of a message or at the end of a message. The Logic script is used to control the application flow; invoke child tasks; change message attributes according to the input parameters; and add new simulation statistics etc. Figure 5-7 depicts the Logic script Editor where program codes are added at the end of a message for a new simulation statistic. A Logic Script can be added or edited through following steps:

(1) Right-Click on the message link and then select **Add Logic Script at End**. A logic scrip icon will be added at the end off the message on the tier line. The script can be edited double-clicking on **Logic Script** icon. 

(2) Add the program codes as necessary.

(3) Save the script selecting File => Commit.

(4) Save the ACE file selecting File=> Save.

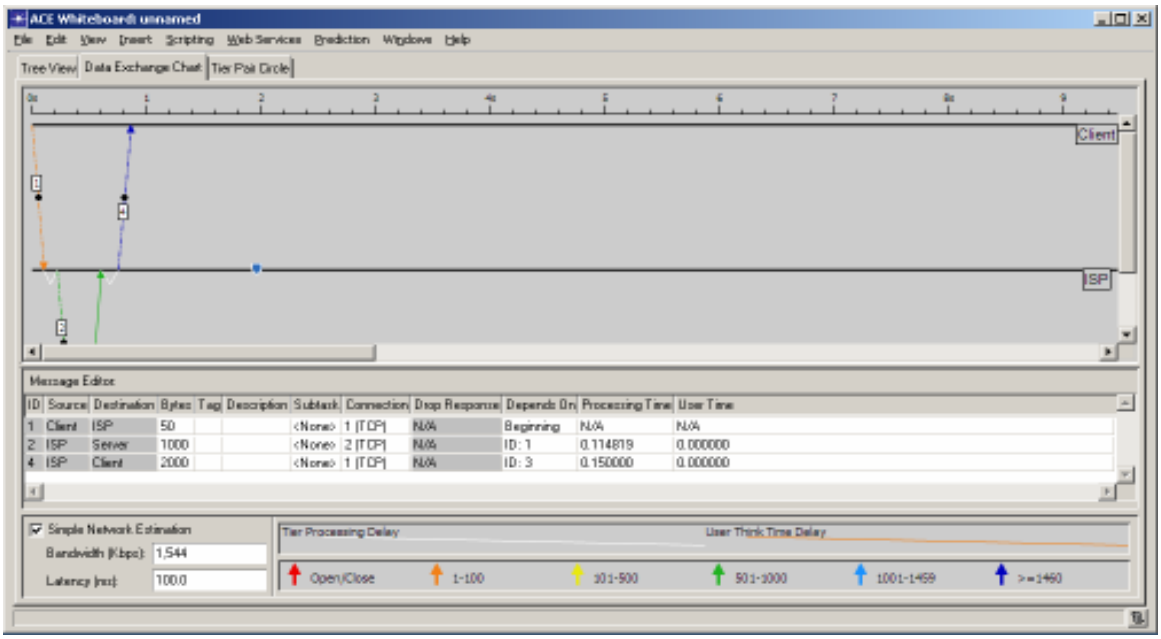


Figure 5-6 ACE Whiteboard Editor

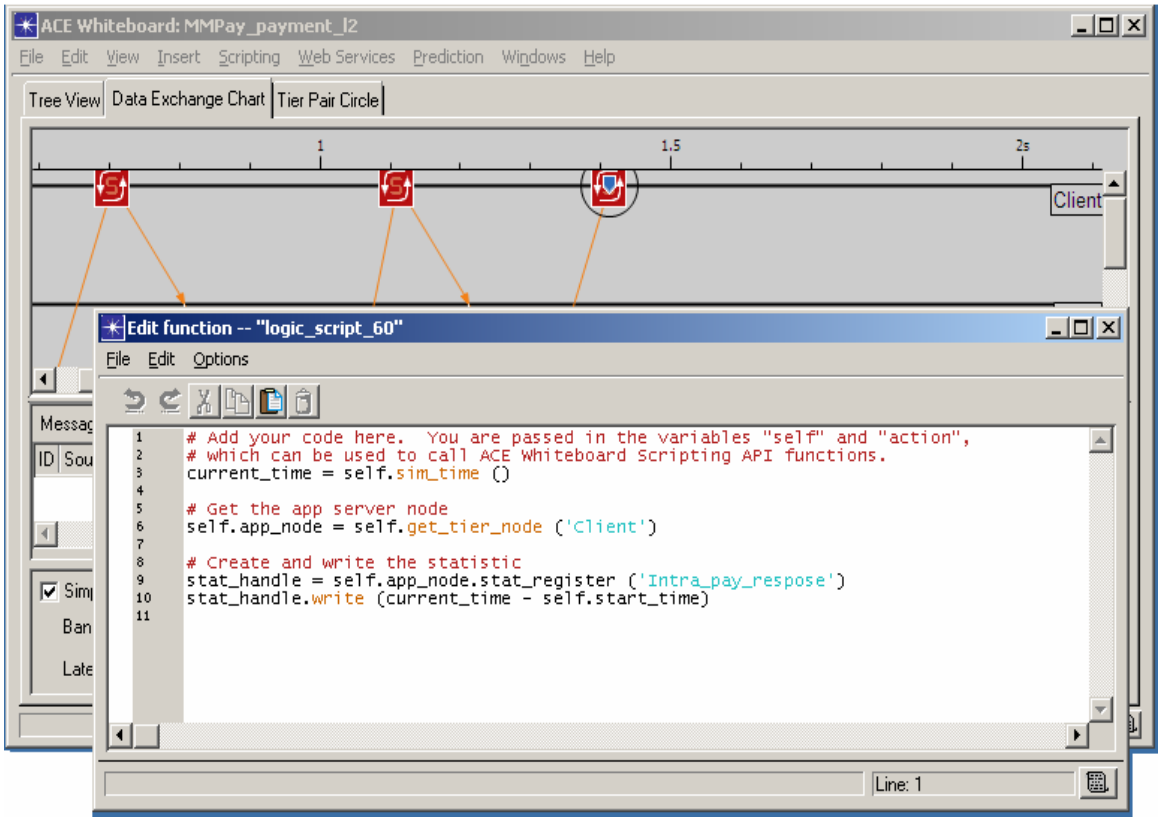


Figure 5-7 Logic Script Editor with Python Codes

5.3 Experimental Network Design and Configuration

For the deployment of the new protocol scheme, the project MMPay_xxx has been designed and a subnet, Toronto, has been configured as a wireless mesh network, where wireless servers are acting as a MPP and MAP(s), and wireless workstations are acting as Clients/Users. OLSR has been used as the mesh routing protocol as the Wireless LAN mesh networks use a hybrid wireless routing protocol combined with proactive and reactive protocols and the gateway routes are configured by the proactive protocol. The MMPay_xxx project contains a Task Definition module configuring custom application tasks; an Application Definition module configuring custom applications; a Profile Definition module configuring client application profiles; and a RX Group Config module setting the wireless receiver range. Figure 5-8 depicts top level network view of the MMPay_xxx project.

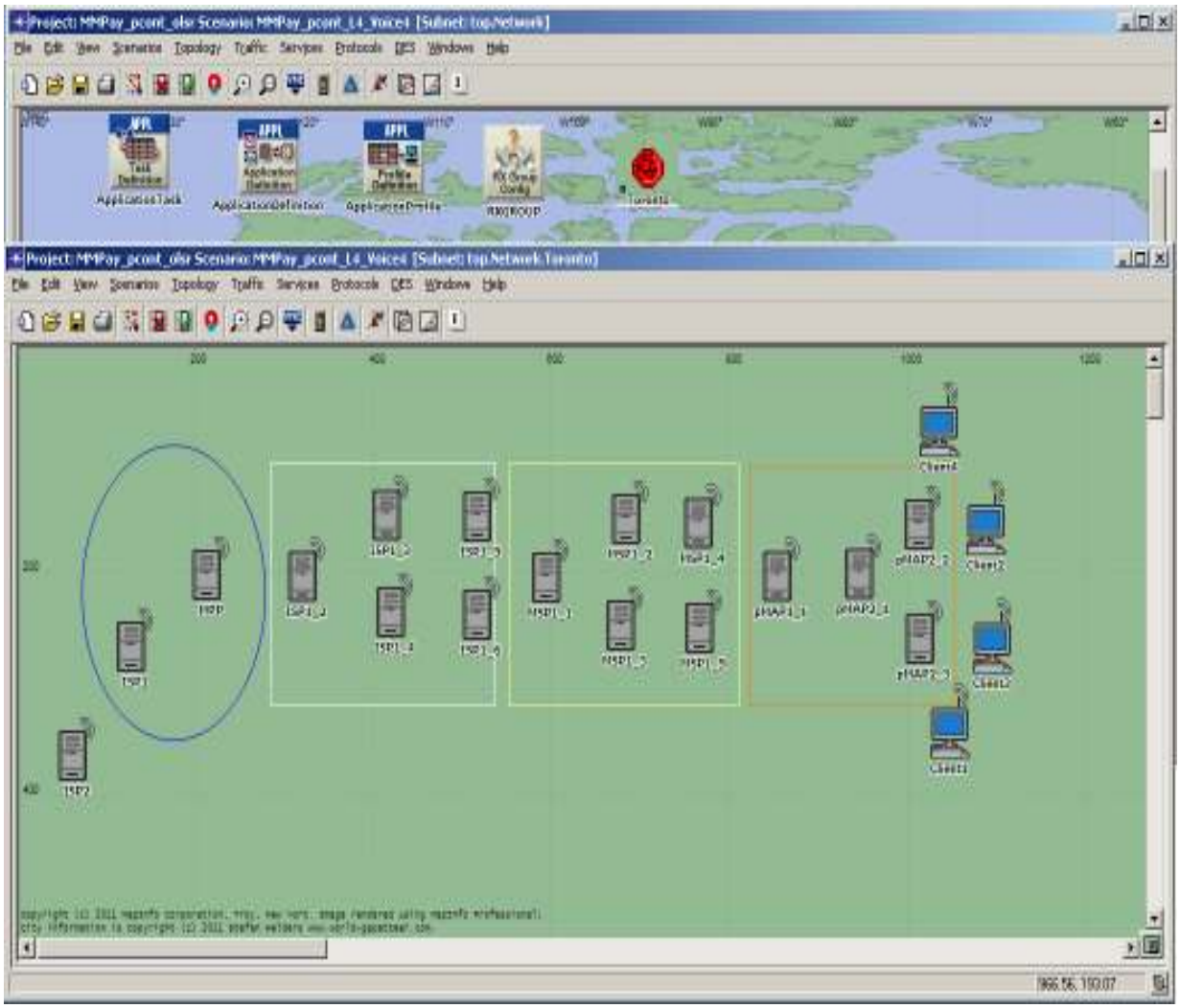


Figure 5-8 MMPay_xxx Project Network with Toronto Subnet

5.3.1 Utility Modules and Devices Configuration

Application utility modules, RX Group Config module, network links, network equipments, and the computing equipments have been configured to achieve the simulation network environment.

5.3.1.1 Custom Application Task Configuration

The custom application tasks are configured at the Task Definition module using different attributes. Five groups of tasks have been configured for the protocol scheme from ACE Whiteboard model files. Figure 5-9 depicts configured tasks for the pricing contract agreement sub-protocol.

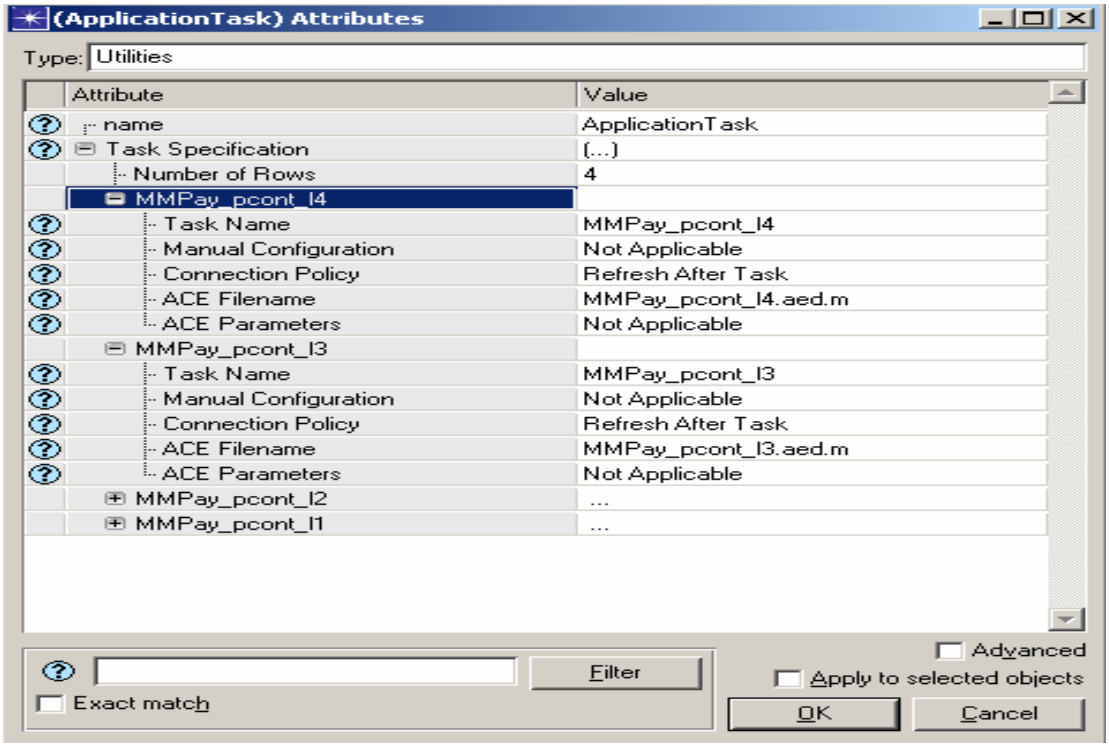


Figure 5-9 Task Configuration from ACE files

5.3.1.2 Application Configuration

Custom applications from the defined custom application tasks, a standard voice application, and a FTP application have been configured at the Application Definition module. For the custom applications, TCP/UDP has been identified as the transport protocol and Best Effort (BE) has been identified as the Standard voice application; it has been deployed providing base-load to the simulation network along with the sub-protocol applications. Different

attributes of custom applications and the standard voice application are shown below in Figure 5-10.

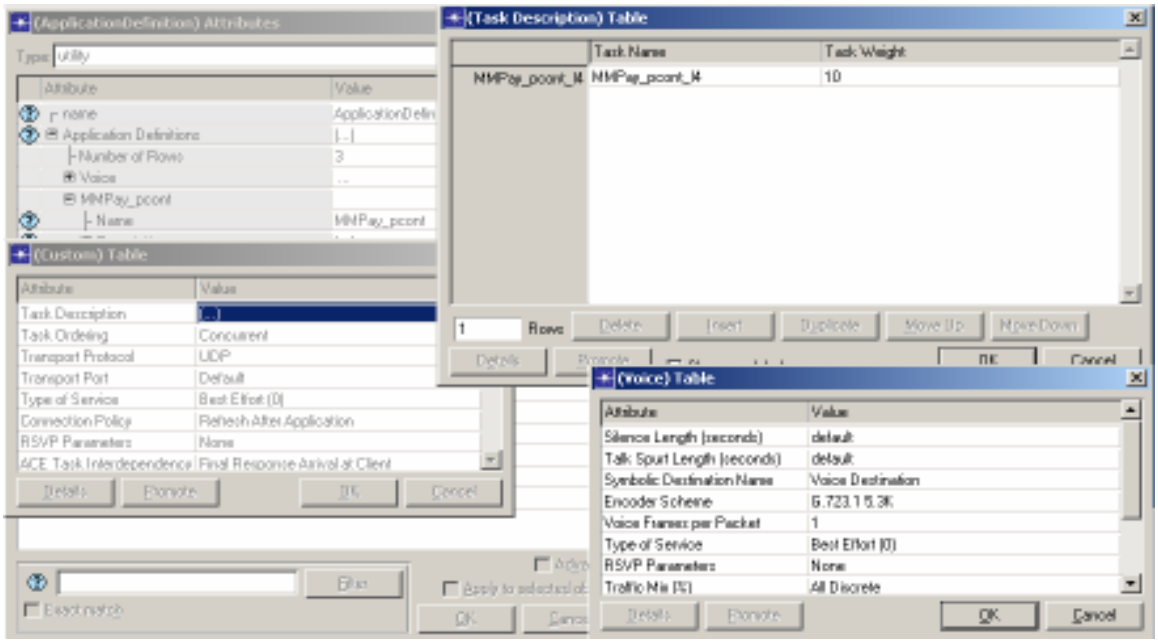


Figure 5-10 Configuration of Custom Application and Voice application

5.3.1.3 Application Profile Configuration

Application profiles have been defined for custom applications and the voice application. The profiles have been configured to the clients to generate application traffic to the network. A Custom application runs once at every minute but the voice application runs for the full simulation period. Figure 5-11 depicts a profile configuration for a custom application.

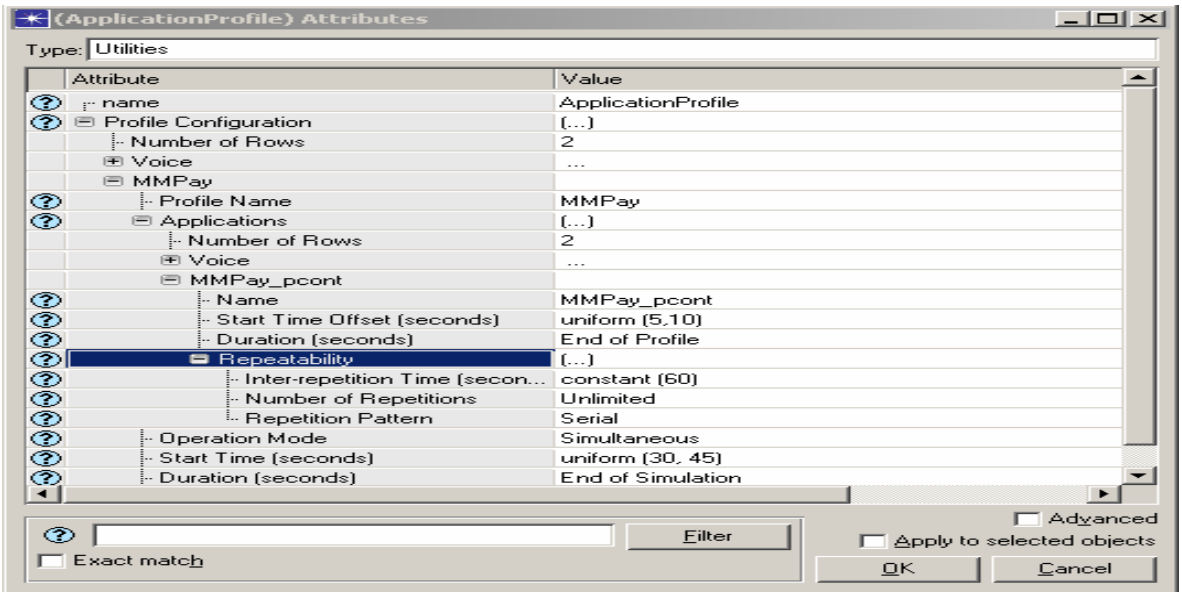


Figure 5-11 MMPay_xxx Profile Configuration for Custom Application

5.3.1.4 RX Group and Network Link Configuration

The RX Group Config module has configured for the receiver range to 110 meters for all the transmitters in Toronto subnet. WLAN parameters of the wireless devices have been set with physical characteristics as OFDM (802.11a), data rate as 54Mbps, BSS Identity as 10, ad-hoc routing protocol as OLSR, but all others parameters are set as default. OLSR routing parameters also have been configured as depicted below in Figure 5-12.

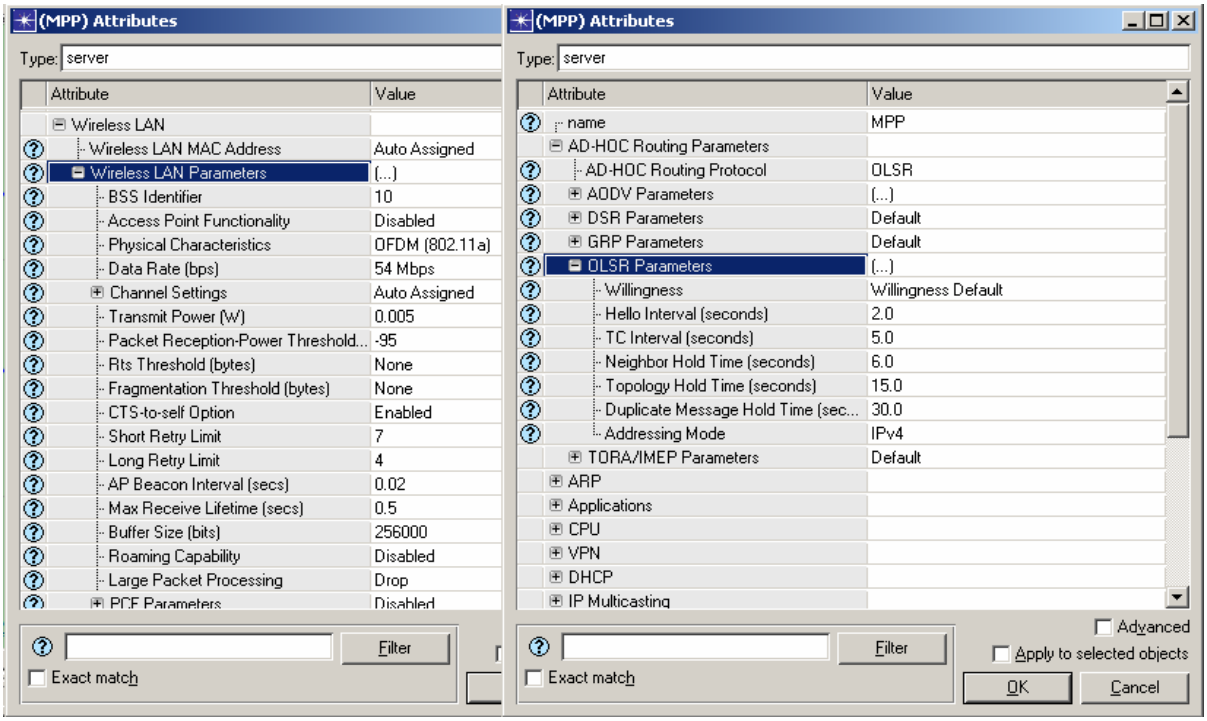


Figure 5-12 Wireless LAN Parameters and OLSR Parameters configuration

5.3.1.4 Configuration of Computing Devices for Application Deployment

Custom applications and the standard voice application have been deployed to the wireless server machines and workstations as the protocol application tier computing devices. Application parameters of the computing devices have been modified and different application tiers such as ISP, ISP2, MSP, pMAP1, pMAP2, Server, and Client have been deployed, to the specific devices at Application: ACE Tier configuration parameters, according to sub-protocol models. Voice application has been deployed to the specific devices as a voice-source and a voice-destination. Application profiles have been deployed to the specific devices generating application traffic at Application: Supported Profiles parameters. Figure 5-13 depicts a custom application and the voice application deployment at Client tier. The custom application

deployment to other tiers is the same as the Client tier but their tier-names are different and have no application profiles to be deployed.

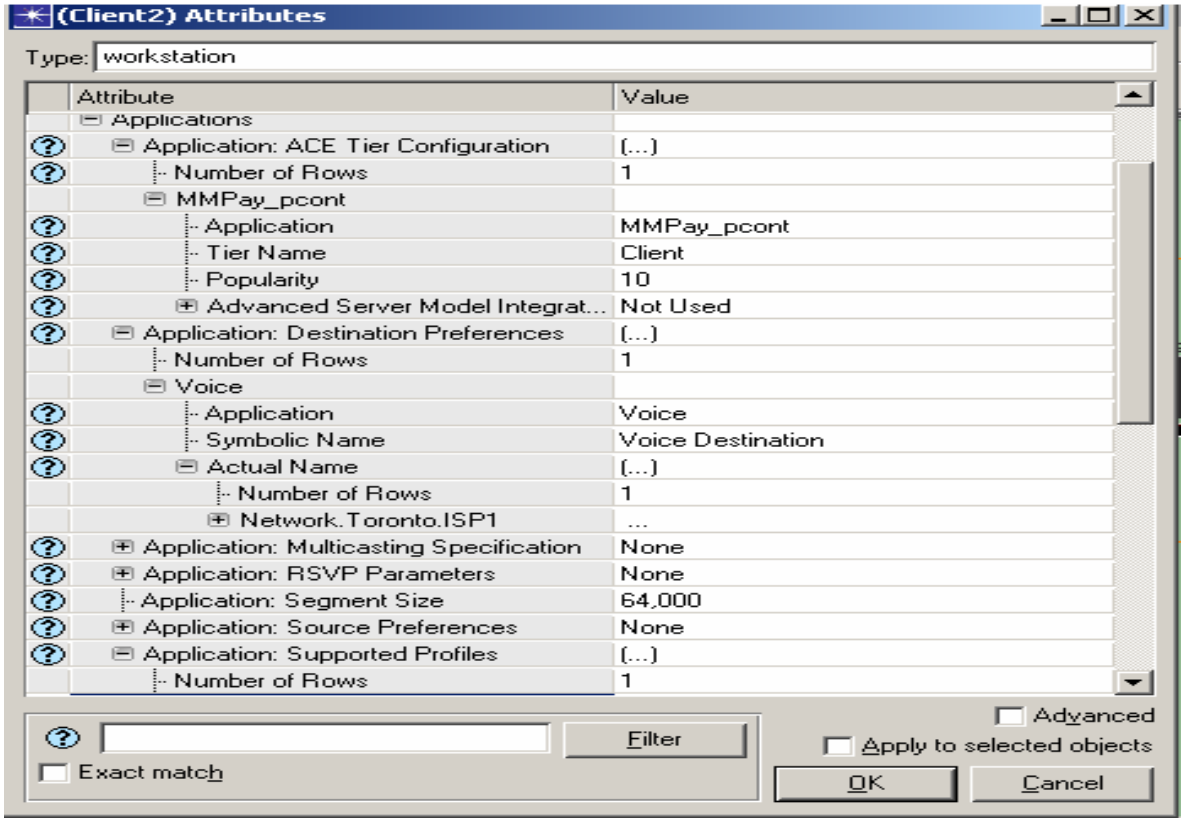


Figure 5-13 Custom Application Deployment at Client Tier

5.4 Simulation Strategies and Assumptions

The new multiparty micropayment protocol (MMPay) scheme has been simulated as custom applications over a multi-hop wireless ad-hoc mesh network. Wireless servers and the wireless workstations have been configured as mesh nodes along with OLSR as the wireless routing protocol. 10 wireless mesh hops are considered for simulation work as in the wireless mesh environment, data transfer performance is degraded after 10 hops [CCG09]. The protocol has been designed for the payment of internet access and thus, intra-domain and the inter-domain data transfer have not been considered for the simulation. However, payment for intra-domain and the inter-domain data transfer can be carried out by establishing a separate communication session through the ISP node. The protocol component, client registration sub-protocol, has not been considered for simulation as the client's physical presence with a government issued identity documents are required for registration. The payment certificate purchasing

sub-protocol has not been considered for the simulation as it uses an existing macro-payment scheme. Also the payment redeeming sub-protocol has not been simulated as it will work at off-time, off-line and in a batch process. The main objectives of the simulation work are to analyse the protocol performances at its other sub-protocol stages.

5.4.1 Simulation Strategies

The protocol scheme has been designed paying multiple entities involved in a communication session for internet access. An internet user can be connected to an ISP directly who provides ISP services and mesh communication services, or can be connected through multiple mesh service providers. The connection path has been considered through 4 (four) service providers in an average, and they are ISP/WISP, MSP, pMAP1 and pMAP2. In the simulation, mainly 4 (four) scenarios have been considered as follows:

- Scenario xxx_L1 (L1): User devices are connected directly to an ISP over a multi-hop mesh network
- Scenario xxx_L2 (L2): User devices are connected to an ISP through MSP over multi-hop mesh networks
- Scenario xxx_L3 (L3): User devices are connected to an ISP through MSP and pMAP1 over multi-hop mesh networks
- Scenario xxx_L4 (L4): User devices are connected to ISP through MSP, pMAP1 and pMAP2 over multi-hop mesh networks

For the competitive simulation result, all the user devices in all the scenarios are connected to an ISP over 10 hops of a mesh network. Voice application and the uncast IP-traffic to/ from an ISP to/ from others nodes having rate of 120000 bits/sec have been used providing the base-load to the simulation network. Simulations have been run for 10 minutes for the custom simulations statistics as defined in ACE Whiteboard files for the protocol scheme. Only one user has been selected for protocol application simulation for fair result in all the scenarios as in the wireless commutation users are dwelt to access the wireless network which cause different delays to deferent users. Figure 5-14 depicts the intra-domain pricing contract response-times for 4-users situation where users are directly connected to an ISP at the scenario L1, where it is evident that response-times are different for a sub-protocol at different users and at different sub-simulation points.

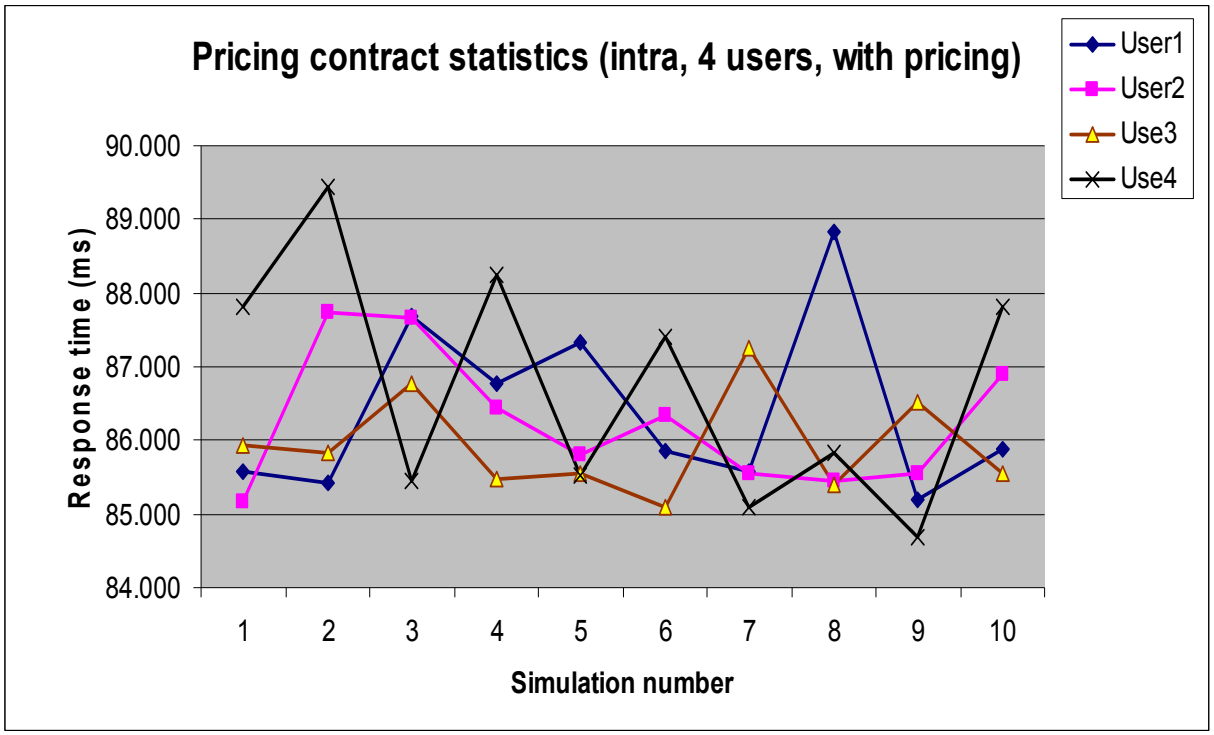


Figure 5-14 Response-times (intra-domain) with pricing for 4-users at scenario L1

All the protocol messages traverse through all MAP(s) along the communication path; MAP(s) should check the messages according to their capabilities and settings, but only the selected MAP(s) used as MMPay protocol tier nodes. The computation costs of all the other MAP(s) are considered to be suppressed by the IP layer communication costs as MANET has been used as the wireless network for the simulation. The low speed user mobility has been predicted for the Wireless LAN mesh networks as the communication rage of MAP is very short and it is about 100ft to 150ft, and the client mobility has not been considered for the simulation.

5.4.1 Assumption for Custom application Parameters

The protocol scheme has been simulated using a set of Opnet Modeler custom applications for different stages as sub-protocol components. The task of the custom application has been defined as an ACE Whiteboard model. The parametric assumptions have been made for defining the application tasks according to the protocol scheme.

A. Connection path:

(1) TCP has been used as the transport protocol as the WLAN mesh network transmit information hop-by-hop with an acknowledgement.

(2) A guide test message has been sent to the destination tier from the source tier to setting up the communication path before the transmission of original protocol messages.

B. Message size in the custom application task:

The protocol message sizes have been defined according to sub-protocol as mentioned above in Chapter 4. Some of them have been defined as follows:

(1) The price request messages have been defined 326 bytes, 338 bytes, 350 bytes, and 362 bytes among different tier nodes.
(2) Pricing contract and the hand-off pricing contract messages have been defined 304 bytes.
(3) The acknowledgement message has defined 36 bytes
(4) The payment message has defined 42 bytes.
(5) Data messages have been defined 1450 bytes.
(6) The signed pricing response message has defined 244 bytes.

C. Tier Processing Time:

At a custom application, different tier nodes generate, compile, and verify protocol messages. A user smartcard and an ISP node generate RSA signature and all the other tier nodes verify the signature and setup a communication session. The user smartcard also generates a payment hash chain, payment hashes and all the other nodes verify payment hashes. To perform these operations different tier nodes need different amount of time according to their computing capabilities. Peirce [Pei00] depicted the computation cost of 238 hashes is equivalent to a RSA signature verification cost, but the hash chain generation is required about 20% more time due to memory allocation and data placement in array elements. He also mentioned the time requirement for array lookup and for the array item comparison verifying payment is about 0.066 ms, but the time requirement for array look and message compilation is only 0.01 ms. According to the present cryptographic capability a midrange 30 MHz SLE66CLX360PE (M) [SLE66CLX] smartcard can generate a 1024 bits RSA signature at 41 ms, but can verify it only at 3 ms. An advance smartcard can generate a signature at 4 ms and can verify it only at 0.5 ms [SLE88CFX]. Haojin Zhu [ZLLHS08] in his paper mentioned the cryptographic performance of a Pentium-4 3.0 GHz machine with 1 GB RAM running on Fedora Core 4, can generate a 1024 bit

RSA signature at 4.49 ms and can verify it at 0.03 ms. He also mentioned the time requirement for user authentication and association with AP using 802.1X is about 20 ms per hop. According to the above mentioned crypto performance, we have assumed the tier processing time at the different tire nodes for the protocol simulation as follows:

Pricing contract agreement signing:

SL	Timing components with details		Time in ms	
1.0	Price request from a user node			20.1
	1.1	User authentication by AP	15.0	
	1.2	User association with AP	3.0	
	1.3	IP address association	2.0	
	1.4	Message compilation	0.1	
2.0	Adding the relay node identity to the price request message			0.1
3.0	Certificates and message verification, price response compilation at an ISP node			0.5
4.0	Pricing contract signing at an user device			55.5
	4.1	Generation of a hash chain of length 300 at the smartcard	5.0	
	4.2	Share key generation, hand-off hash generation, message compilation and session set-up at a user node	0.5	
	4.3	A 1024 bits RSA signature generation at the smartcard	50.0	
5.0	Contract verification and a session set-up at relay nodes and at an ISP			0.5

Ongoing Payment:

SL	Timing components with details		Time in ms	
1.0	A payment message generation			1.0
	1.1	A payment hash generation of step 15 at the smartcard and accounts update	0.9	
	1.2	A hand-off secrete generation and message compilation	0.1	
2.0	The payment hash verification at relay nodes			0.2
3.0	Payment hash and hand-off secrete verification at ISP			0.25

Intra-domain and inter-domain hand-off pricing contract:

SL	Timing components with details		Time in ms	
1.0	Intra-domain hand-off price request from a user node			3.1
	1.1	User association with AP	3.0	
	1.2	Message compilation	0.1	
2.0	Inter-domain hand-off price request from a user node			18.1
	2.1	User authentication by AP **	15.0	
	2.2	User association with AP	3.0	
	2.3	Message compilation	0.1	
3.0	Adding the relay node identity to the price request message			0.1
4.0	Message verification, price hand-off contract compilation and signing at an ISP node or at an ISP2 node			2.5
5.0	Hand-off pricing contract verification and session set-up at relay nodes and at an ISP node			0.5

** **Note:** When a user approaches to inter-domain hand-off, it can inform existing serving ISP to send encrypted temporal master key (TMK) to the neighbour ISP, then 802.1X authentication and costly key generation protocol are not required for inter-domain hand-off.

5.5 Simulation Results of Protocol Scheme

The simulation of the protocol scheme has been defined to estimate the performances of sub-protocols in response-time and latency. OPNET Modeler ACE Whiteboard models have been developed to identify the following simulation statistics as performance criterion:

- Protocol response-times for the pricing contract agreement
- Protocol response-times for the handoff pricing contract agreement
- Protocol latencies and response-times for the payment
- Effect of the protocol on end-to-end delay and throughput for data communications

5.5.1 Simulation of Pricing Contract

The simulation of the pricing contract sub-protocol has been done as a custom application. Four ACE Whiteboard models have been designed according to the sub-protocol message

transaction and timing for the four scenarios. The sub-protocol contains four messages and the ACE model files have been configured according to the message transactions detailed in the sub-protocol model in Section 4.3.3 of Chapter 4.

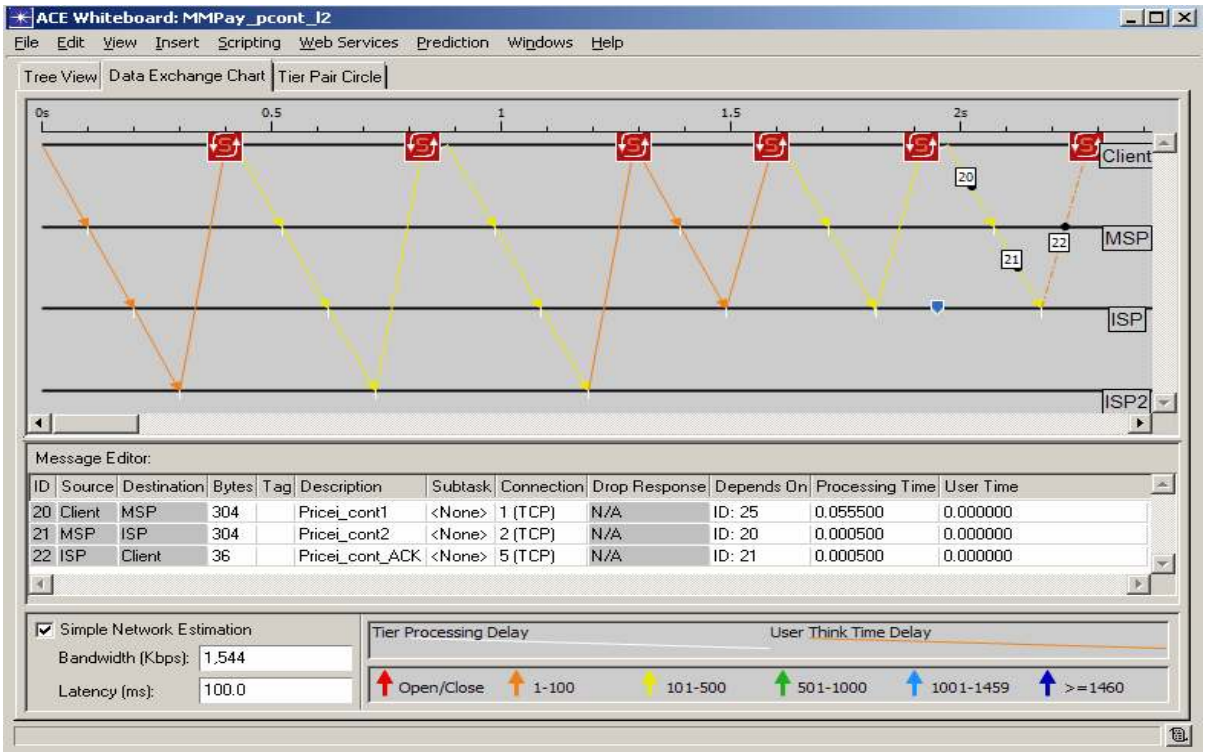


Figure 5-15 Pricing contract ACE Whiteboard model for scenario L2

Four scenarios L1, L2, L3, and L4 have been defined for the simulation depending on users association with an ISP. In the scenario L1 users are directly connected to the ISP, in L2 they are connect through a MSP, in L3 they are connected through a MSP and a pMAP1, and in L4 they are connected through a pMAP2, a pMAP1 and a MSP. All the scenarios also include intra-domain and the inter-domain situations. In the inter-domain situation users are still connected to the pervious serving ISP (ISP2) after the hand-off to a new destination ISP domain. 10 sub-simulations have been embedded in every scenario and run once at every minutes of the simulation. Figure 5-15 depicts the sub-protocol message transactions in an ACE Whiteboard task model for the scenario L2 where users are connected to an ISP through a MSP. For every scenario four simulation statistics as response-times have been collected, where two are the intra-domain statistics with and without pricing and another two are the inter-domain statistics with and without pricing.

Table 5-1, Table 5-2, Table 5-3, and Table 5-4 show the pricing contract simulation statistics in values. Figure 5-16 and Figure 5-17 depict pricing contract response-times with/without pricing for the intra-domain situation. And Figure 5-18 and Figure 5-19 depict pricing contract response-times with/without pricing for the inter-domain situation. Figure 5-20 depicts sample average of all the simulation statistics for all the four scenarios in a bar-chart graph.

Pricing contract response-times (inter, with pricing) in milliseconds				
Scenario/ Simulation	L1	L2	L3	L4
1	86.619	87.683	88.200	88.046
2	86.514	88.164	89.622	89.098
3	87.485	87.436	87.862	87.902
4	86.656	87.065	88.265	89.197
5	86.958	87.878	88.388	89.211
6	87.643	87.698	87.717	89.592
7	86.179	87.556	87.650	88.815
8	86.540	86.797	87.607	89.220
9	87.207	87.869	88.338	88.884
10	87.410	88.715	88.210	88.446
Average:	86.921	87.686	88.186	88.841

Table 5-1 Pricing contract response-times with pricing (inter-domain)

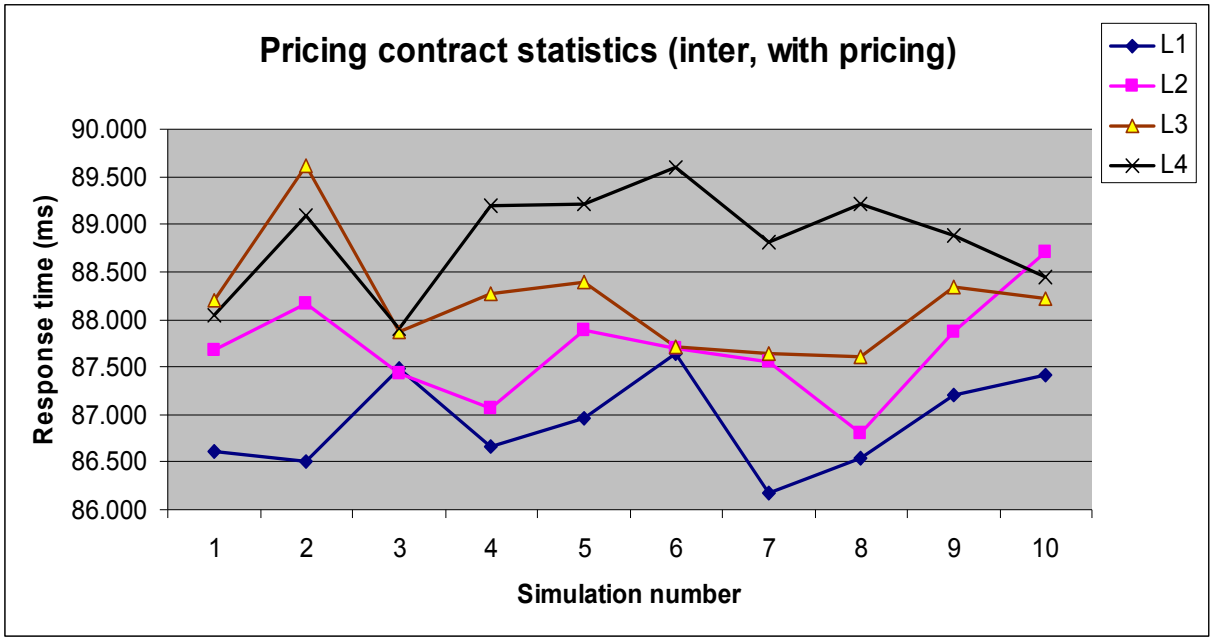


Figure 5-16 Pricing contract response-times with pricing (inter-domain)

Pricing contract response-times (inter, without pricing) in milliseconds				
Scenario/ Simulation	L1	L2	L3	L4
1	60.920	61.559	62.160	61.879
2	60.489	61.550	62.685	61.964
3	61.329	61.397	61.396	61.737
4	60.975	61.298	61.342	61.728
5	61.124	61.595	61.904	62.452
6	61.089	61.262	61.639	62.767
7	60.750	60.902	61.567	62.070
8	60.660	60.848	61.657	62.323
9	60.975	61.426	61.647	62.447
10	61.277	61.670	61.819	62.224
Average:	60.959	61.351	61.781	62.159

Table 5-2 Pricing contract response-times without pricing (inter-domain)

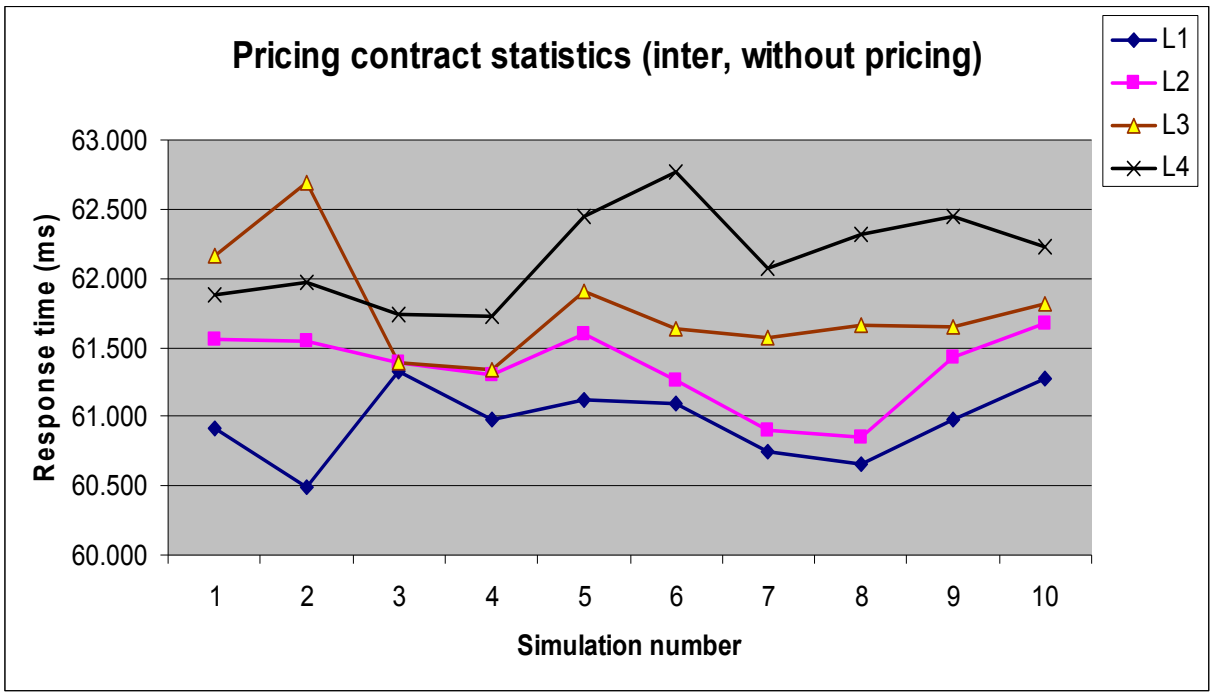


Figure 5-17 Pricing contract response-times without pricing (inter-domain)

Pricing contract response-times (intra, with pricing) in milliseconds				
Scenario/ Simulation	L1	L2	L3	L4
1	85.258	85.560	86.083	86.260
2	85.258	85.753	87.417	86.753
3	86.449	85.512	87.466	86.782
4	85.177	86.803	86.825	86.530
5	85.989	87.669	86.700	86.999
6	85.387	85.972	86.800	86.782
7	84.529	86.636	86.205	86.503
8	85.220	86.233	86.729	86.551
9	85.555	85.200	85.957	87.159
10	85.939	85.668	86.850	86.572
Average:	85.476	86.101	86.703	86.689

Table 5-3 Pricing contract response-times with pricing (intra-domain)

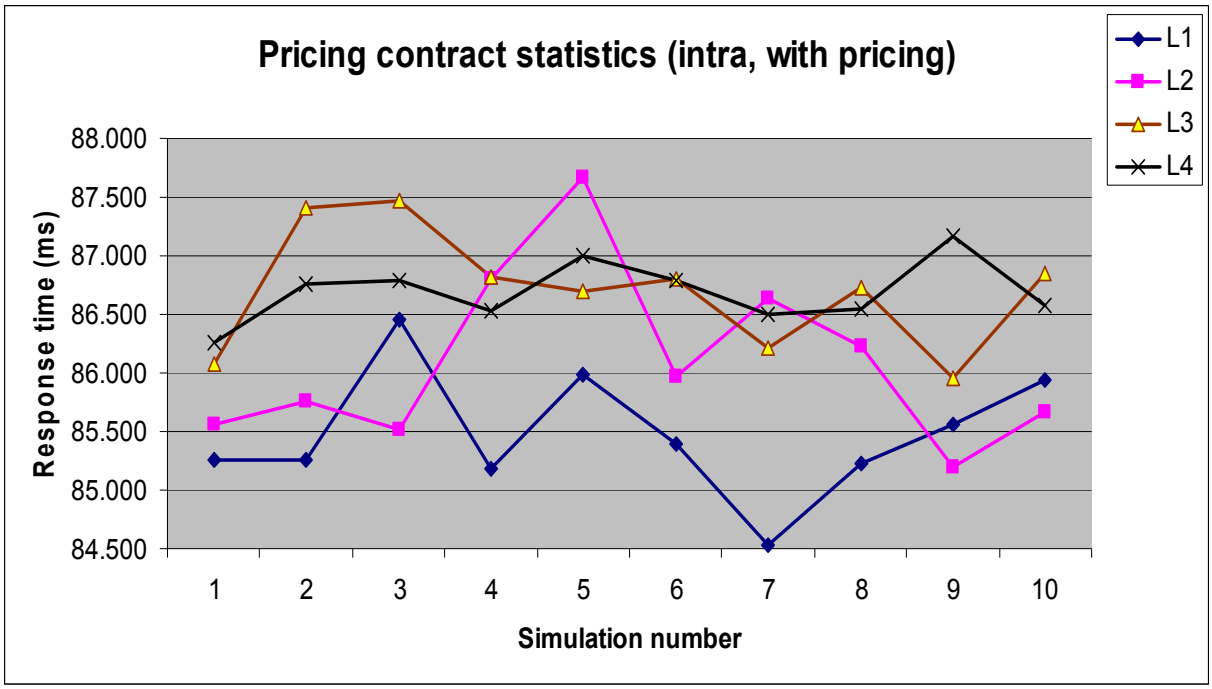


Figure 5-18 Pricing contract response-times with pricing (intra-domain)

Pricing contract response-times (intra, without pricing) in milliseconds				
Scenario/ Simulation	L1	L2	L3	L4
1	59.978	60.382	61.069	61.542
2	60.095	60.953	61.797	61.747
3	61.301	60.523	62.112	61.741
4	60.041	61.171	61.361	61.479
5	60.399	62.093	61.418	62.074
6	59.969	60.767	61.438	61.452
7	59.789	61.007	60.768	61.326
8	59.744	61.235	61.030	61.527
9	60.428	60.346	60.997	61.531
10	60.657	60.643	61.728	60.929
Average:	60.240	60.912	61.372	61.535

Table 5-4 Pricing contract response-times without pricing (intra-domain)

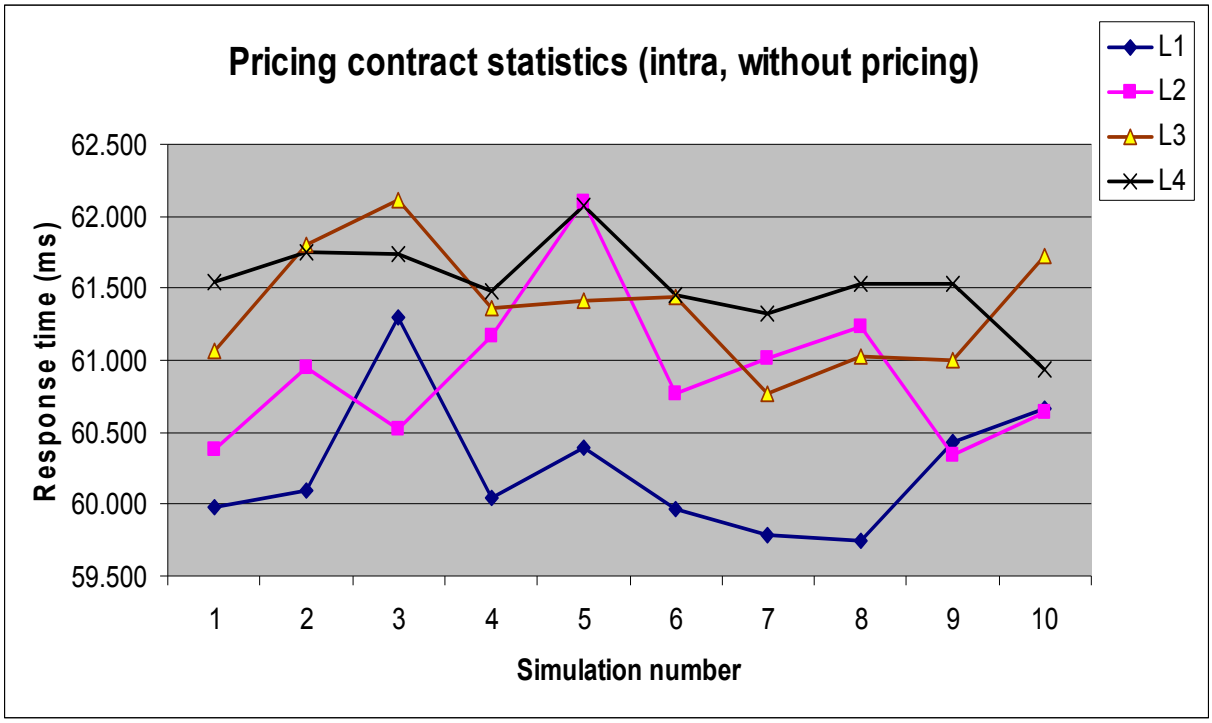


Figure 5-19 Pricing contract response-times without pricing (intra-domain)

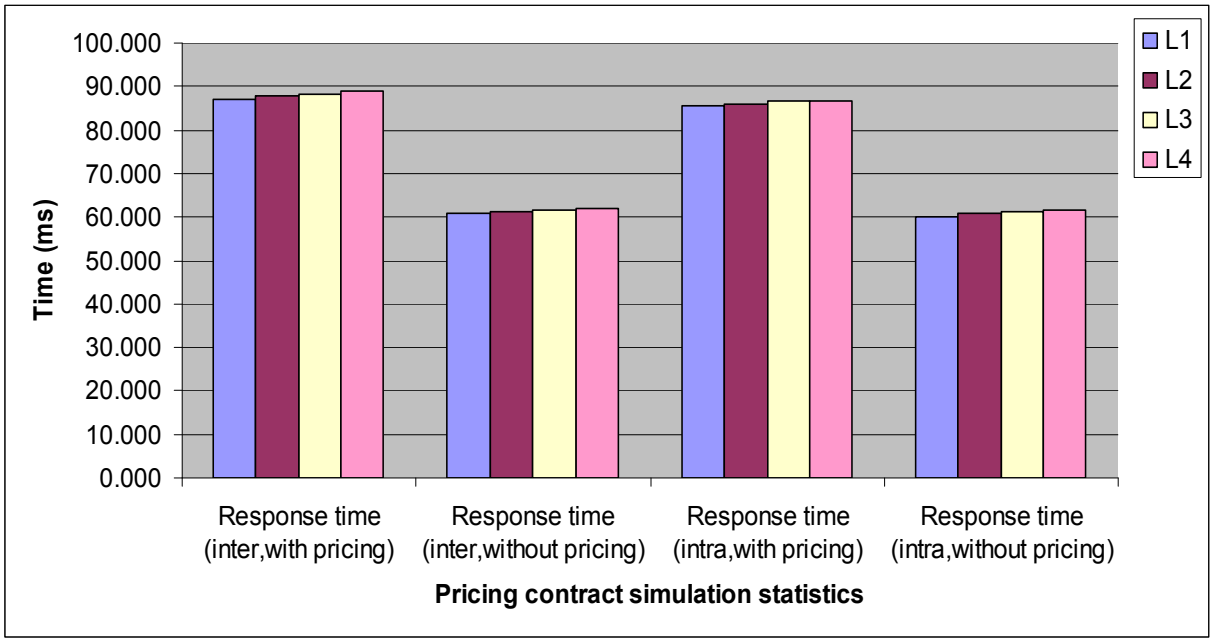


Figure 5-20 Average pricing contract response-times for all the scenarios

According to the design of the pricing contract sub-protocol every relay service provider tier node needs about 0.6 ms adding node identity in the price response message and verifying the signed pricing contract. The results shown in Figure 5-16 to Figure 5-19 indicate a clear trend that the pricing contract response-times are increased with the increase of the number relay service providers and thus, the scenario L1 has the lowest response-time as it has no relay service provider. But the differences among response-times of different scenarios are not fixed to 0.6 ms. The results at different sub-simulation numbers at the same scenario are also different and they are due to user dwelling for wireless access, routing protocol delay and the network load during the sub-simulation period. However, the bar-chart of the average statistics shown in Figure 5-20 clearly indicates that the number of intermediate relay tier-nodes has an effect on the pricing contract response-times but it is very little. Thus, the protocol effect may be overridden by the wireless network effect as the relay-tier processing delay is as little as tenths of a millisecond.

The simulation results presented in Figure 5-18 and in the corresponding data table show the intra-domain pricing contract response-times including price collection and user authentication. They indicate that they are from 85 ms to 87 ms and these are quite high due to usage of the slower client smartcard device signing the pricing contract and generating the payment hash chain. However, these times are only required the first time when users enter

into a new wireless network domain. First time users may also spend some more time for manual verification of network usage charges, internet access charges, and entering smart card PIN. Thus, the high value of the first-time pricing contract agreement response-time has no significance to the users and as well as for the communications as a user can only start data transfer or can access network for communication after a successful pricing agreement, communication session setup through relay service provider nodes, and distribution of the first payment hash value.

5.5.2 Simulation of Ongoing Payment

ACE Whiteboard task models have been designed for the ongoing payment sub-protocol according to the message transaction and timing. The payment messages traverse through all the involved relay service provider nodes as shown in Figure 5-21 for the scenario L3, where a single payment hash has been used to pay pMAP1, MSP, ISP and ISP2. The payment sub-protocol contains 2 (two) messages and the ACE model files have configured according to the message transactions detailed in the sub-protocol model in Section 4.3.4 of Chapter 4. Four scenarios L1, L2, L3, and L4 have been defined for the simulation depending on users association with the current serving ISP. In the scenario L1 users are directly connected to the ISP, in L2 they are connected through a MSP, in L3 they are connected through a MSP and a pMAP1, and in L4 they are connected through a pMAP2, a pMAP1 and a MSP. All the scenarios also include intra-domain and the inter-domain situations. In the inter-domain situation users are still connected to the pervious serving ISP (ISP2) after the hand-off to a new destination ISP domain. 10 sub-simulations have been embedded in every scenario and run once at every minutes of the simulation. In the inter-domain situation users make payment to current service ISP as a relay service provider who extends the service of ISP2 according to the inter-domain hand-off agreement. The ISP and its associated relay service providers are included in the hand-off pricing contract signed by the ISP2.

For every scenario four simulation statistics, response-times and latencies, have been collected, where two are the intra-domain statistics and another two are the inter-domain statistics. Table 5-5 & Table 5-6 and Table 5-7 & Table 5-8 show the payment latencies and response-times in values for the inter-domain situation and the intra-domain situation

respectively. Figure 5-22 and Figure 5-23 depict the inter-domain simulation latencies and response-times respectively. Whereas, Figure 5-24 and Figure 5-25 depict the intra-domain simulation latencies and response-times.

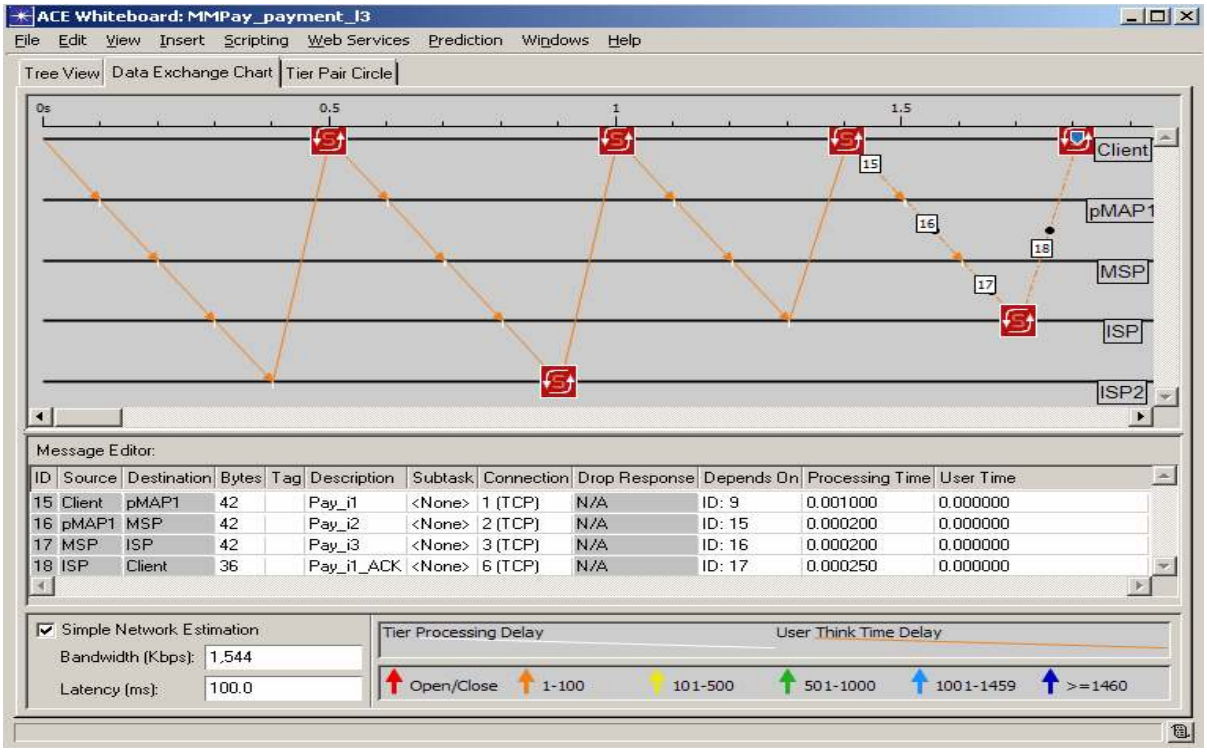


Figure 5-21 Ongoing Payment ACE Whiteboard model for Scenario (L3)

Payment latencies (inter) in milliseconds				
Scenario/ Simulation	L1	L2	L3	L4
1	3.155	3.499	3.666	4.120
2	3.454	3.744	3.686	4.255
3	3.139	3.809	3.544	4.172
4	3.229	3.444	3.786	3.604
5	3.481	3.346	3.904	4.434
6	3.580	3.582	4.019	3.929
7	3.472	3.465	3.713	4.112
8	3.535	3.816	4.169	3.913
9	3.283	3.465	3.801	3.199
10	3.445	3.726	4.156	4.255
Average:	3.377	3.590	3.844	4.000

Table 5-5 Inter-domain payment latencies for all the scenarios

The payment sub-protocol, the critical component of the protocol scheme, is mostly used; it is assumed the heart of the protocol scheme, and thus the simulation has also been done for all the scenarios for 4-users in the intra-domain situation to observe the user's dwelling effect for wireless access on the payment statistics at loaded situation.

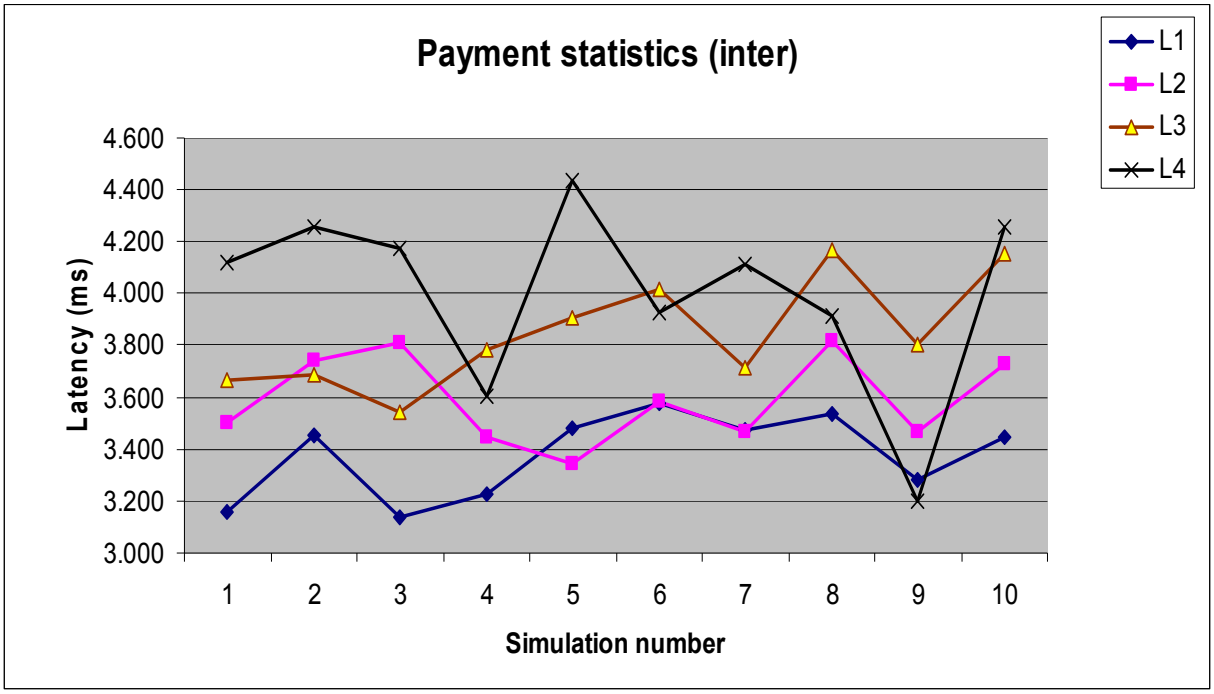


Figure 5-22 Payment latencies (inter-domain) for all the scenarios

Payment response-times (inter) in milliseconds				
Scenario/ Simulation	L1	L2	L3	L4
1	5.663	5.630	5.788	6.440
2	5.683	6.118	6.343	6.735
3	5.179	6.201	6.206	6.699
4	5.886	5.979	6.203	5.815
5	5.583	5.774	6.278	7.024
6	5.997	6.144	6.487	6.249
7	5.773	6.341	6.231	6.567
8	5.728	6.518	6.651	6.170
9	5.448	6.361	6.431	5.790
10	5.836	6.172	6.932	6.323
Average:	5.678	6.124	6.355	6.381

Table 5-6 Inter-domain payment response-times for all the scenarios

Figure 5-26 and Figure 5-27 depict the intra-domain payment statistics for 4-users situation. Figure 5-28 depicts sample average of all the simulation statistics for all the scenarios for the ongoing payment sub-protocol in a bar-chart graph.

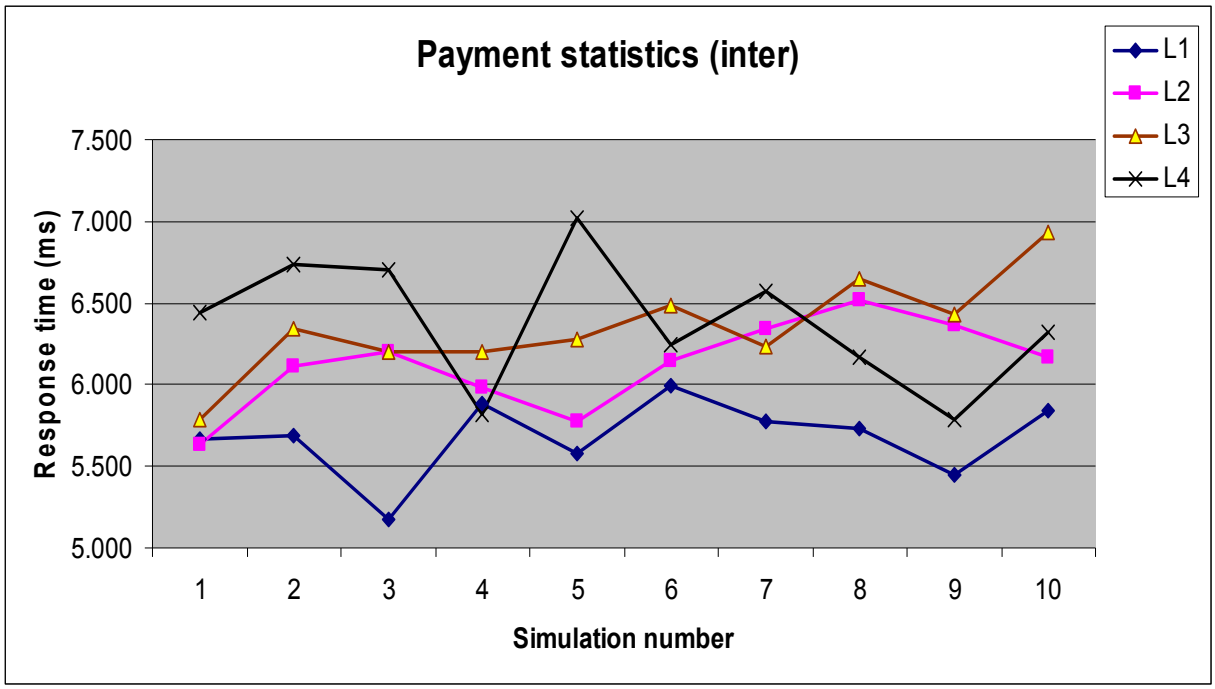


Figure 5-23 Payment response-times (inter-domain) for all the scenarios

Payment latencies (intra) in milliseconds				
Scenario/ Simulation	L1	L2	L3	L4
1	2.898	3.254	3.763	3.473
2	2.880	3.874	3.482	4.004
3	2.952	2.712	3.626	3.455
4	2.934	3.065	2.719	3.231
5	2.952	3.416	3.372	4.048
6	2.871	3.292	3.727	3.836
7	3.093	3.054	3.446	3.338
8	2.925	3.470	3.412	3.601
9	2.952	3.072	3.140	3.048
10	2.916	3.312	3.484	3.772
Average:	2.938	3.252	3.417	3.581

Table 5-7 Intra-domain payment latencies for all the scenarios

The single payment hash is used to make a payment to all the involved service providers for a communication session and every intermediate relay provider verifies the payment hash and it is estimated that every one of the relay providers introduces about 0.2 ms of delay.

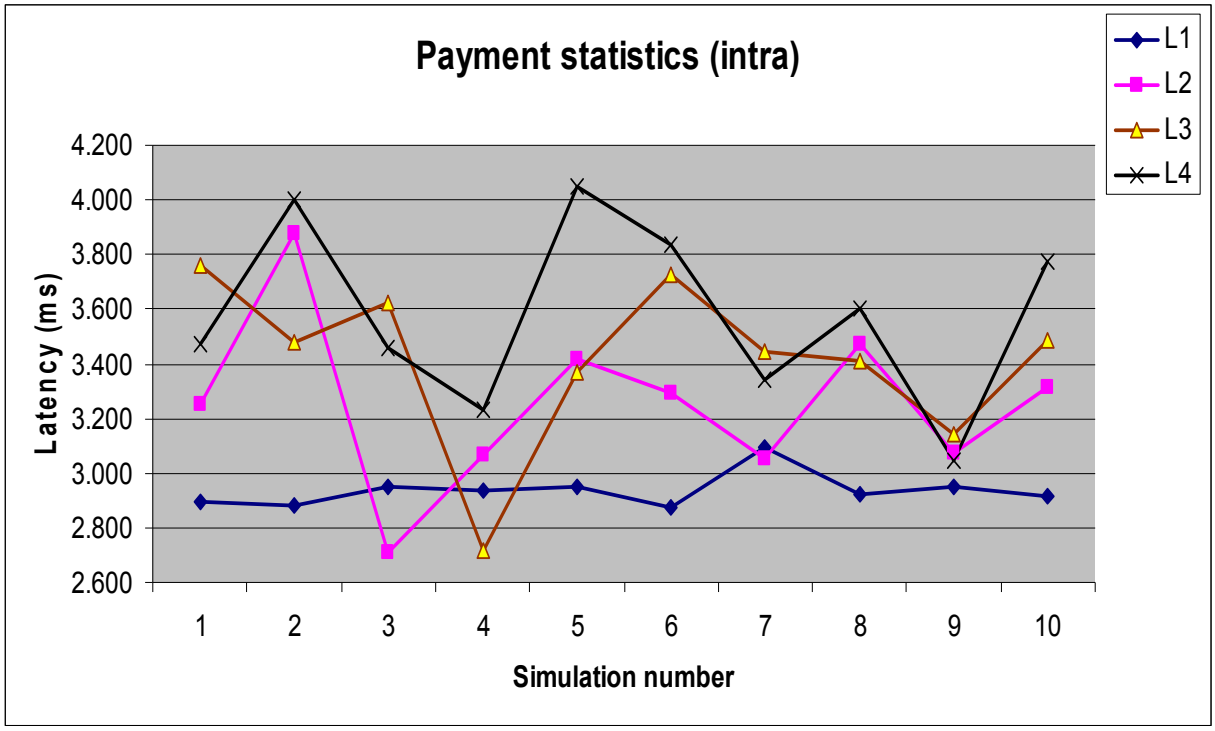


Figure 5-24 Payment latencies (intra-domain) for all the scenarios

Payment response-times (intra) in milliseconds				
Scenario/ Simulation	L1	L2	L3	L4
1	5.057	6.032	6.775	6.190
2	4.985	6.667	6.233	6.540
3	5.673	5.359	6.155	6.176
4	5.091	5.296	5.729	6.144
5	6.250	5.661	6.019	6.282
6	5.687	5.719	6.482	6.572
7	5.609	5.727	5.882	6.222
8	4.958	6.167	6.325	6.018
9	4.805	5.686	5.839	5.090
10	5.111	6.048	6.196	6.763
Average:	5.323	5.836	6.164	6.200

Table 5-8 Intra-domain payment response-times latencies for all the scenarios

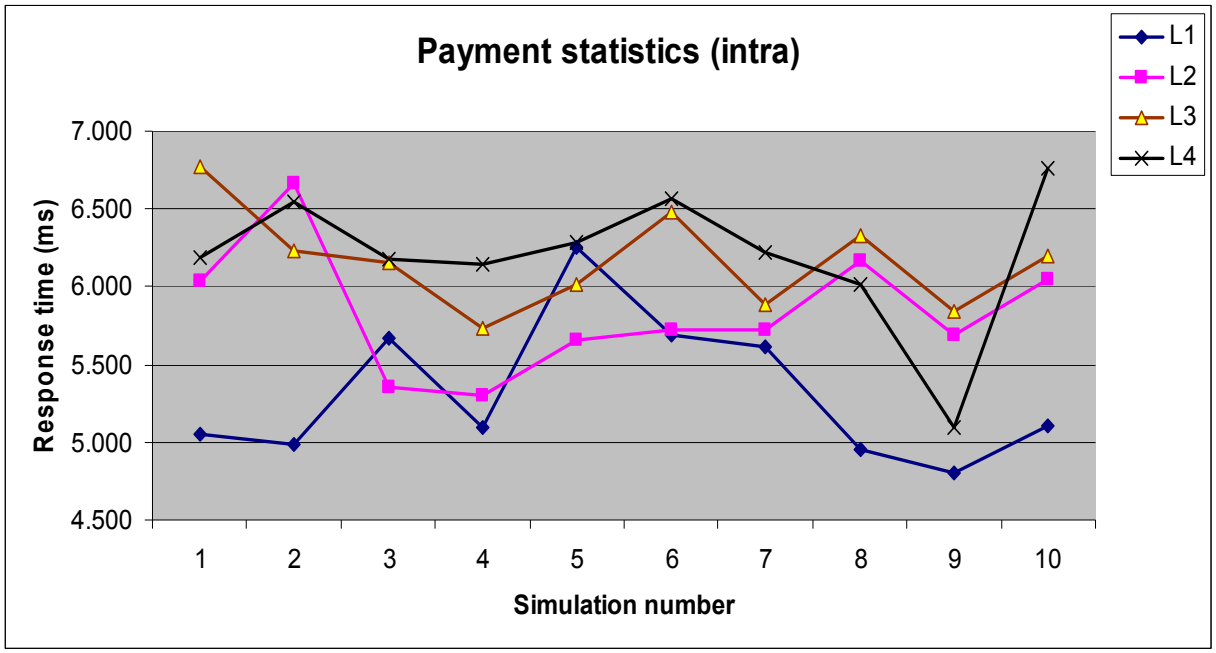


Figure 5-25 Payment response-times (intra-domain) for all the scenarios

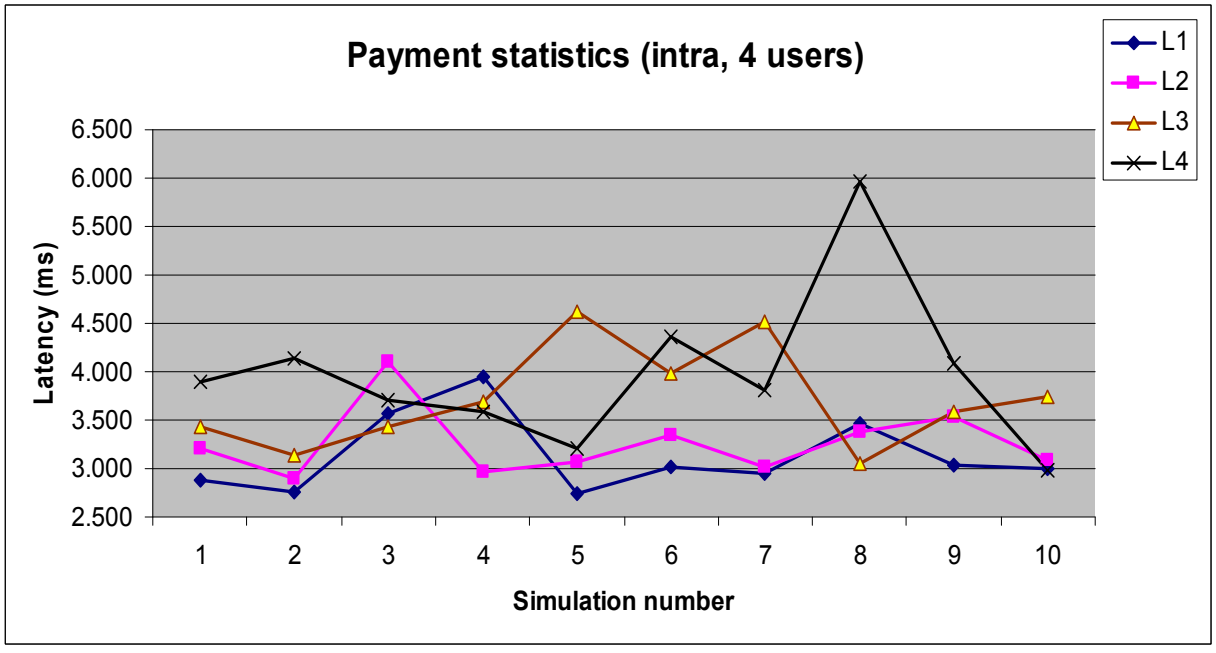


Figure 5-26 Payment latencies (intra-domain, 4-users) for all the scenarios

The simulation results for single user situation presented in Figure 5-22 to Figure 5-25 show that the payment latencies and response-times have a tendency to depend on the number of intermediate relay service provider nodes but it is very small.

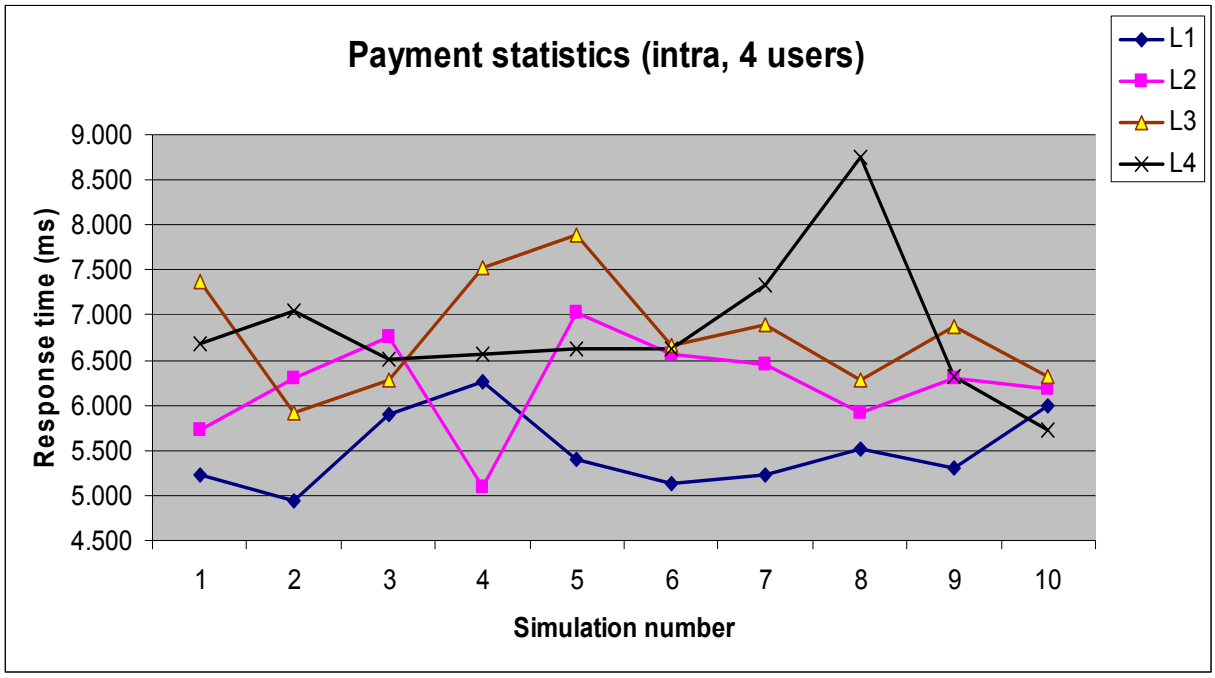


Figure 5-27 Payment response-times (intra-domain, 4-users) for all the scenarios

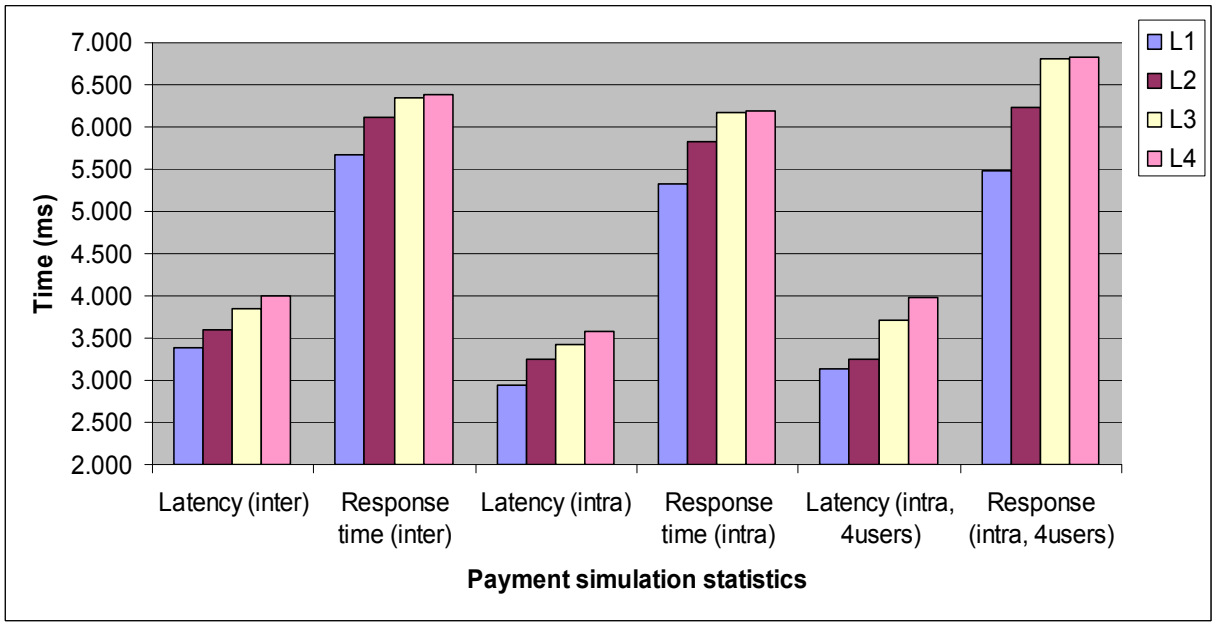


Figure 5-28 Average payment latencies and response-times

The bar-chart graph presented in Figure 5-28 also conforms that the average latency and response-time are changing depending on the number of relay providers but they are not consistent as the difference of intra-domain response-time between L1 and L2 is about 0.5 ms,

but others are less than 0.1 ms. At the different sub-simulation point, the simulation statistics are varying at all the scenarios and they are due to node dwelling time for wireless access, routing protocol delay, packet retransmission and the network load during the sub-simulation period. The simulation results for 4-users in the intra-domain situation as presented in Figure 5-26 and Figure 5-27 also indicate the tendency of having dependency on the number of relay service providers but it is inconsistent with the increase of sub-simulation number. However, the real WLAN mesh access point (MAP) has multiple radios for uplink, downlink and for user access. Thus, it has limited number of neighbours for dwelling to wireless network access as in single user situation and it has congestion control mechanism.

The simulation results presented in Figure 5-24 and Figure 5-25 show the intra-domain payment latencies are from about 3 ms to 4 ms and the payment response-times are from about 5 ms to 7 ms. Some times these payment latencies and response-times may be increased to the big numbers due to network congestion and wireless access delay as in the 4-users situation, where the maximum latency is about 6 ms and response-time is 9 ms for the scenario L4 at the sub-simulation number 8. The high value of any payment latency may cause the data communication delay and degradation of data communication throughput, and it may even cause the termination of an ongoing session. However, the presence of data-transmission-credit-balance field in the protocol scheme will help to overcome these unwanted situations by designing the proper credit threshold for the payment points. Also the protocol implementation should consider the payment retransmission if a payment acknowledgement is not reached within a predefined time window.

5.5.3 Simulation of Hand-off Pricing Contract

Figure 5-29 depicts the ACE Whiteboard task model that has been designed for the hand-off pricing contract for the scenario L2 according to the sub-protocol message transaction and timing. The hand-off pricing contract sub-protocol contains 2 (two) messages and message transactions are according to the sub-protocol model as described above in Section 4.6 of Chapter 4. For the simulation of the hand-off pricing contract sub-protocol, four scenarios L1, L2, L3, and L4 have been defined depending on users association with the current serving ISP. In the scenario L1 users are directly connected to the ISP, in L2 they are connect through a

MSP, in L3 they are connected through a MSP and a pMAP1, and in L4 they are connected through a pMAP2, a pMAP1 and a MSP. All the scenarios also include intra-domain and the inter-domain situations.

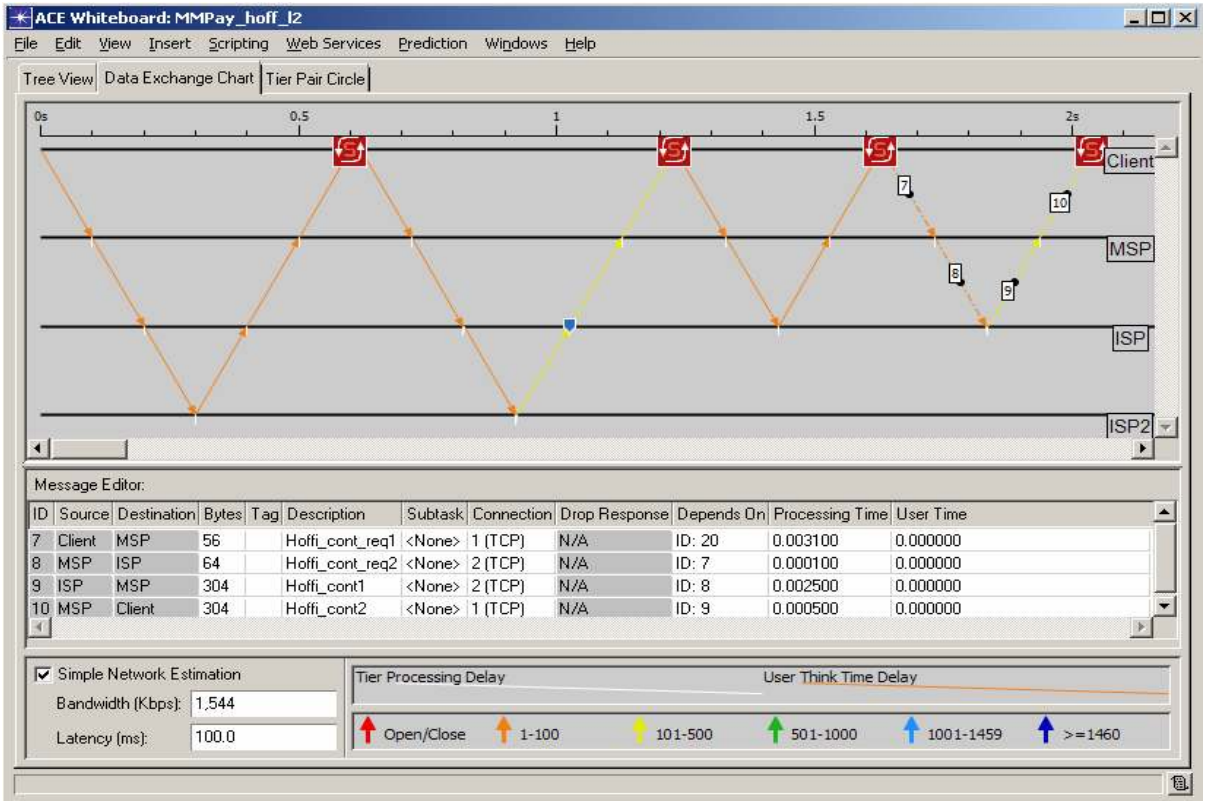


Figure 5-29 Hand-off pricing contact ACE Whiteboard model for scenario L2

Hand-off response-times (inter) in milliseconds				
Scenario/ Simulation	L1	L2	L3	L4
1	25.249	26.003	26.368	26.644
2	26.633	25.985	25.675	26.515
3	25.438	26.493	25.873	26.194
4	25.249	26.080	27.086	26.473
5	25.312	26.035	26.239	26.455
6	25.492	25.886	26.170	26.473
7	25.708	26.021	26.201	27.347
8	25.735	25.922	26.296	27.173
9	25.882	25.823	26.717	26.416
10	25.378	25.971	26.098	26.599
Average:	25.607	26.022	26.272	26.629

Table 5-9 Hand-off pricing contract response-times (inter-domain)

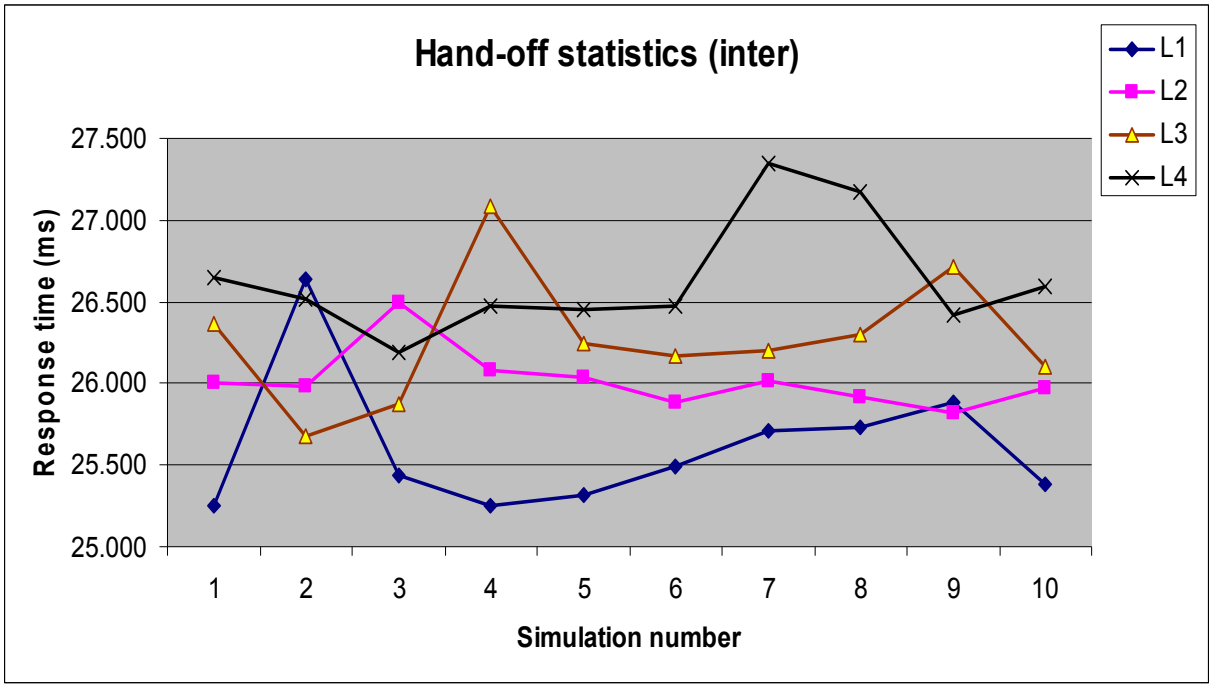


Figure 5-30 Hand-off pricing contract response-times (inter-domain)

Hand-off response-times (intra) in milliseconds				
Scenario/ Simulation	L1	L2	L3	L4
1	9.811	9.787	10.251	10.842
2	10.327	10.056	10.530	10.943
3	10.191	11.104	10.534	10.680
4	9.568	10.003	10.494	10.914
5	9.874	10.772	11.468	10.770
6	10.303	10.605	10.233	11.381
7	10.108	10.201	10.386	11.794
8	9.469	10.345	10.557	10.662
9	10.029	10.334	10.494	10.671
10	9.910	10.198	10.539	11.506
Average:	9.959	10.340	10.549	11.016

Table 5-10 Hand-off pricing contract response-times (intra-domain)

In the inter-domain situation users need authentication and need to develop primary master key (PMP) with the new serving ISP. But the user is still connected to the pervious serving ISP (ISP2) after hand-off to the new ISP. 10 sub-simulations have been embedded in every scenario and run once at every minutes of the simulation. In the intra-domain situation users make fast hand-off only by association with the new MAP using previous PMK which is

distributed to the neighbour MAP(s) by the previous associated MAP or by the ISP. But in the intra-domain hand-off within domain mobility group, user needs re-authentication with the ISP regional controller/gateway using previous PMK.

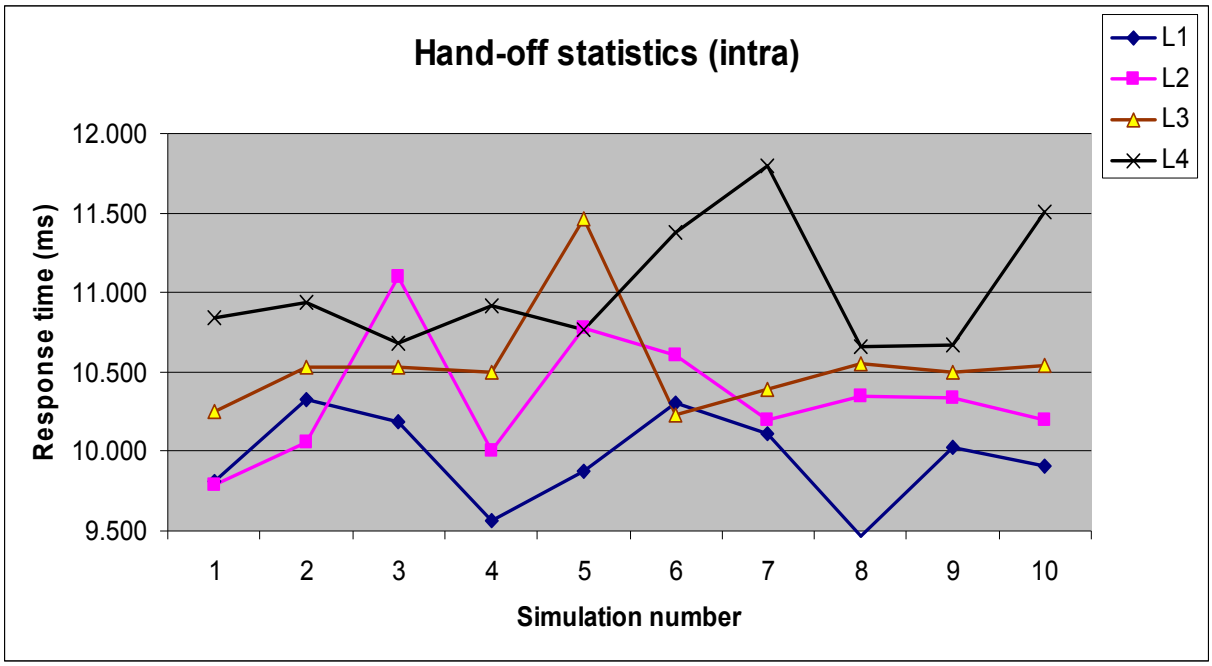


Figure 5-31 Hand-off pricing contract response-times (intra-domain)

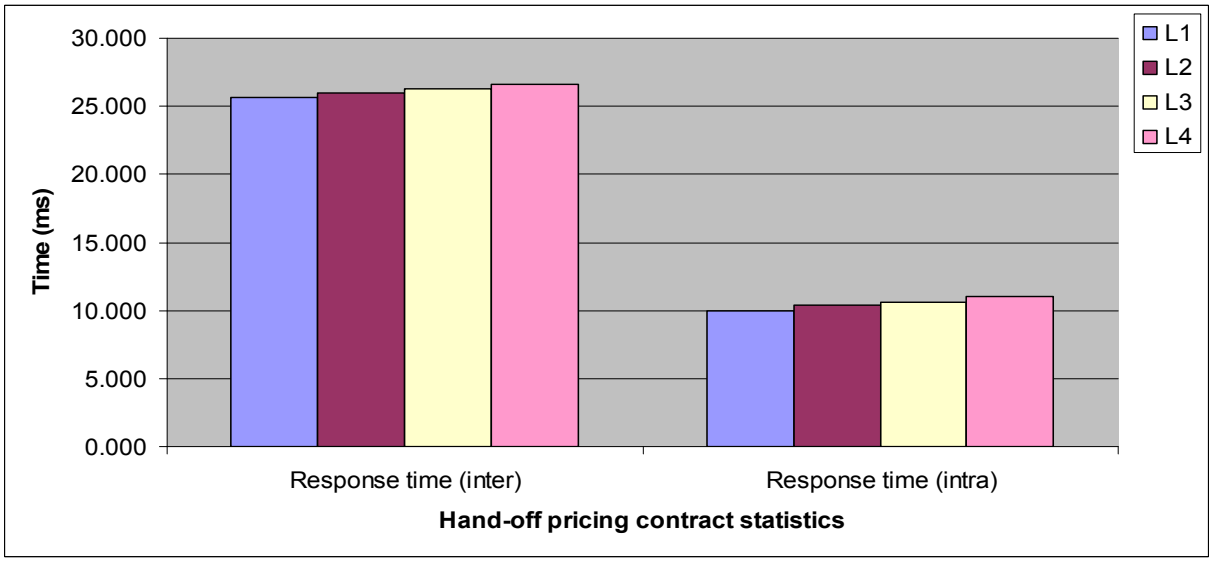


Figure 5-32 Average hand-off pricing contract response-times for all the scenarios

Two simulation statistics have been collected as inter-domain hand-off pricing contract response-times and the intra-domain hand-off response-times for all the four scenarios. Table 5-9 and Table 5-10 show the inter-domain and intra-domain hand-off pricing contract response-times in values. Figure 5-30 and Figure 5-31 depict the inter-domain hand-off statistics and intra-domain hand-off statistics for all the four scenarios in a single user environment. Figure 5-32 depicts sample average of both the statistics in a bar-chart graph.

The simulation results show that both the inter-domain and intra-domain hand-off pricing contact response-times have dependency with the number of relaying service provider nodes like the simulation results of the pricing contract sub-protocol. The average statistics presented in the bar-chart in Figure 5-32 confirms the number of relaying service providers have a clear but little impact on the sub-protocol response-times. The simulation results presented in Table 5-9, Table 5-10, Figure 5-30, and Figure 5-31 show the intra-domain hand-off response-times are from about 9 ms to 12 ms, but they are from about 25 ms to 28 ms for the inter-domain. For the uninterrupted communication after the hand-off, users have to pay to all the service providers along the new communication path. Thus the total times including payment response-times for the inter-domain hand-off are from about 32 ms to 35 ms. This range of inter-domain handoff response-times may not be suitable for the fast hand-off situation with the low-range MAP devices. However, in a wireless LAN mesh network environment the ISP mesh controller maintains the registration profiles for all the associated users and MAP devices in the domain along with their Primary Master Keys (PMK). For the fast intra-domain hand-off, ISP controller devices also maintain mobility group, in the group all the controllers exchange registration profiles and maintain EOIP tunnel to transfer Ethernet frames over the IP-network. For the fast inter-domain hand-off, ISP can maintain inter-domain mobility group and can build EOIP tunnel with its neighbour ISP(s) having share secretes. A user approaches to an inter-domain hand-off can make a request to the current serving ISP to distribute encrypted temporal master key (TMK) to the target ISP. Using this TMK, a user can authenticate himself with target ISP without the costly authentication and key management procedure. Then the total response-times including a payment will be reduced to the range of 20 ms to 23 ms. The presence of data-transfer-credit-balance in the protocol scheme also provides the opportunity of uninterrupted communication without a payment at the beginning

of the hand-off session. Then the inter-domain hand-off response-times are from about 13 ms to 16 ms, these will make the scheme suitable even for the speedy users and at the fast hand-off situation using the low range MAP devices.

5.5.4 Protocol Effect on ETE Data Communication delay and Throughput

To determine the effect of the protocol scheme on the end-to-end (ETE) data communication latency and throughput, ACE Whiteboard task models have been designed where 10 data packets of size 1450 bytes have been transmitted over the communication channel from the user node to the application server node through intermediate relay service provider nodes. In the protocol scheme all the relay service provider nodes also maintain account balance for their real-time remunerations. In the simulation, the accounting time-delay at the tier nodes has been considered as 0.2ms. The average of the ETE delay has been calculated. The wireless link-speed has been configured as 54 Mbps, and a then user node in the 10-users situation can transfer only one packet at every 5 ms. Thus, to calculate the data communication throughput, the transmission of 199 data packets has been considered.

In general, data packets are transmitted from a user node to the application server node only through ISP node for accounting purpose or directly from a user node to the application server node. Five scenarios L0, L1, L2, L3, and L4 have been defined for the simulation depending on users association with the current serving ISP. In the scenario L0 users are directly connected to the application server, in L1 they are connected through an ISP, in L2 they are connect through a MSP and an ISP, in L3 they are connected through a pMAP1, a MSP and an ISP, and in L4 they are connected through a pMAP2, a pMAP1, a MSP and an ISP. 10 sub-simulations have been embedded in every scenario and run once at every minute of the simulation.

Two statistics have been collected for the uplink communication and downlink communications for both the ETE delay and throughput at all the scenarios. Table 5-11, Table 5-12, Figure 5-33 and Figure 5-34 depict the ETE communication delay simulation statistics for all the scenarios. Figure 5-35 depicts sample average of all the ETE delay statistics in a bar-chart graph.

Downlink ETE communication delay in milliseconds					
Scenario/ Simulation	L0	L1	L2	L3	L4
1	4.713	4.836	4.953	4.902	5.076
2	5.141	5.259	5.163	5.325	5.328
3	5.083	4.985	5.251	5.233	5.130
4	4.872	5.081	5.135	5.494	5.258
5	5.492	5.090	5.335	5.418	5.382
6	4.942	5.006	5.199	5.264	5.233
7	5.046	5.166	5.184	5.164	5.180
8	4.848	5.218	5.059	5.303	5.465
9	4.955	5.264	5.168	5.278	5.328
10	4.774	5.186	5.419	5.172	5.257
Average:	4.986	5.109	5.187	5.255	5.264

Table 5-11 Downlink ETE data communication delay for all the scenarios

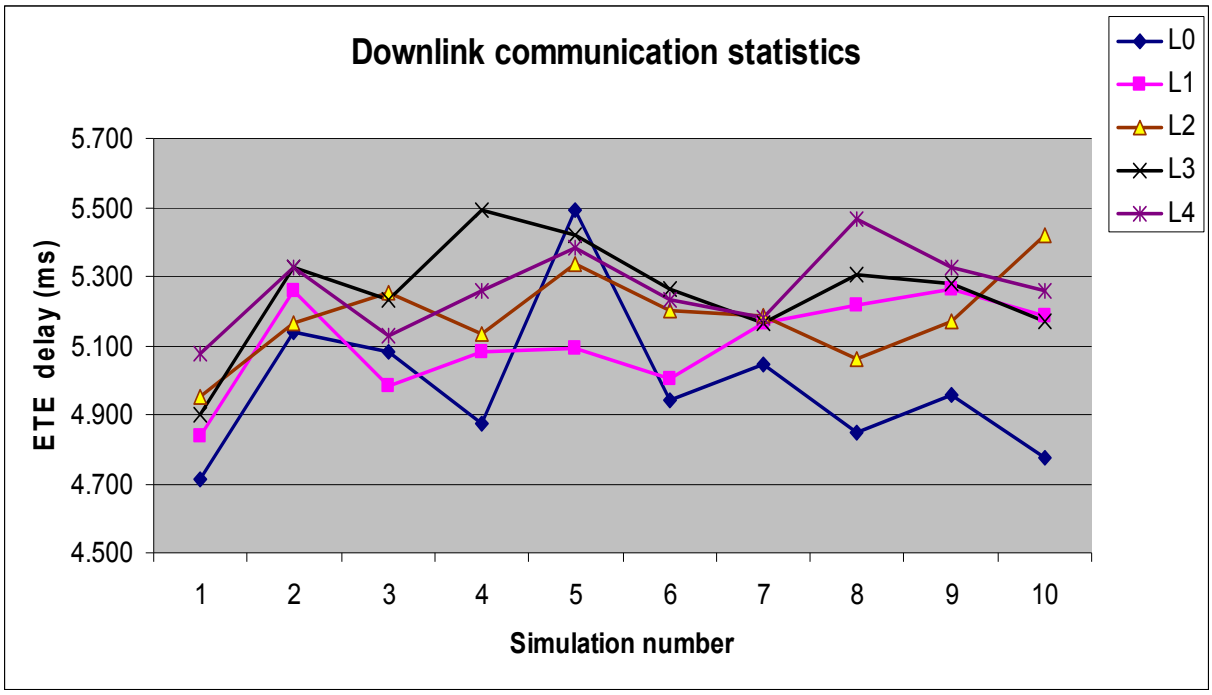


Figure 5-33 Downlink ETE data communication delay for all the scenarios

The simulation statistics for ETE delay presented in data Tables and Figures show the protocol has very little impact and the ETE delay is varying depending on the number of intermediate relay service providers. The ETE delay is lowest when a user directly communicates with the application server. But the ETE delay differences among the scenarios are not consistent due

to the wireless network effect as shown in Figure 5-33, the ETE delay for the scenario L0 is the highest at the sub-simulation number 5. The average uplink ETE delay shown in Figure 5-35 indicates the delay difference between scenarios L0-L1 and scenarios L1-L2 are too little so that it is likely there is no impact of the protocol scheme.

Uplink ETE communication delay in milliseconds					
Scenario/ Simulation	L0	L1	L2	L3	L4
1	4.823	4.944	4.829	5.091	5.009
2	5.127	5.254	4.911	5.120	5.261
3	4.913	5.294	5.446	5.251	5.230
4	5.013	5.015	5.310	5.253	5.408
5	4.978	5.284	5.214	5.310	5.303
6	5.236	5.236	5.330	5.302	5.658
7	5.000	4.996	5.185	5.237	5.622
8	5.722	5.074	5.322	5.257	6.132
9	5.326	5.468	4.982	5.312	5.283
10	5.197	4.926	5.056	5.491	5.378
Average:	5.133	5.149	5.158	5.262	5.429

Table 5-12 Uplink ETE data communication delay for all the scenarios

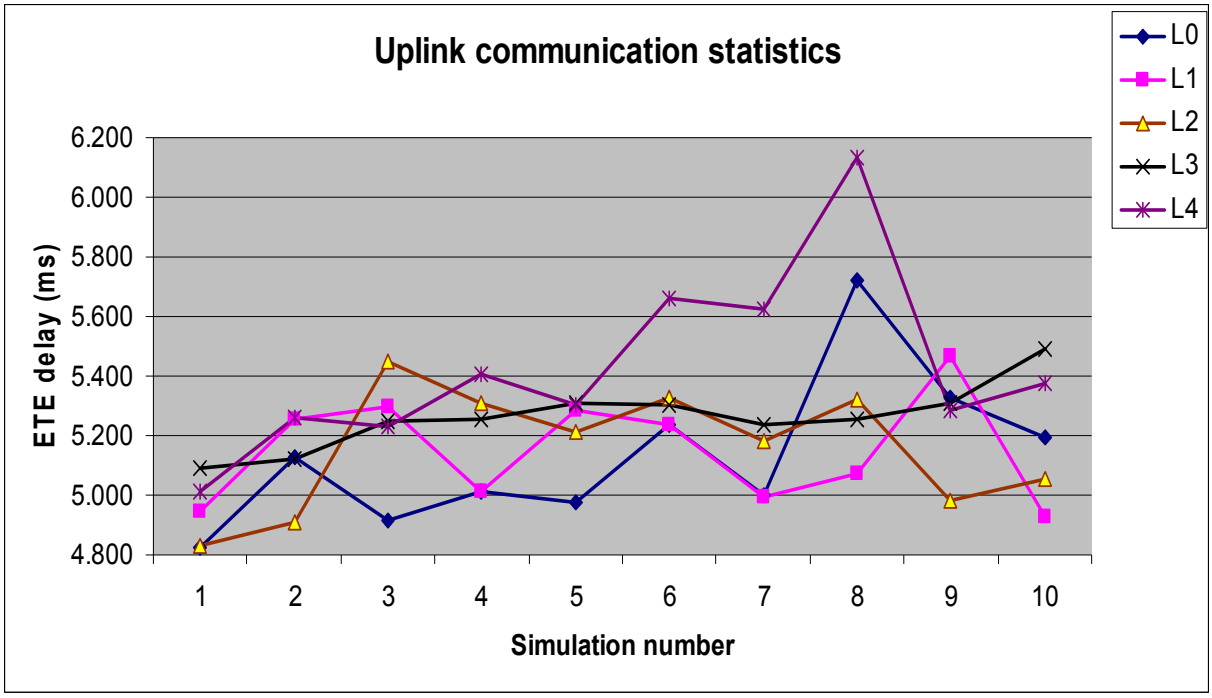


Figure 5-34 Uplink ETE data communication delay for all the scenarios

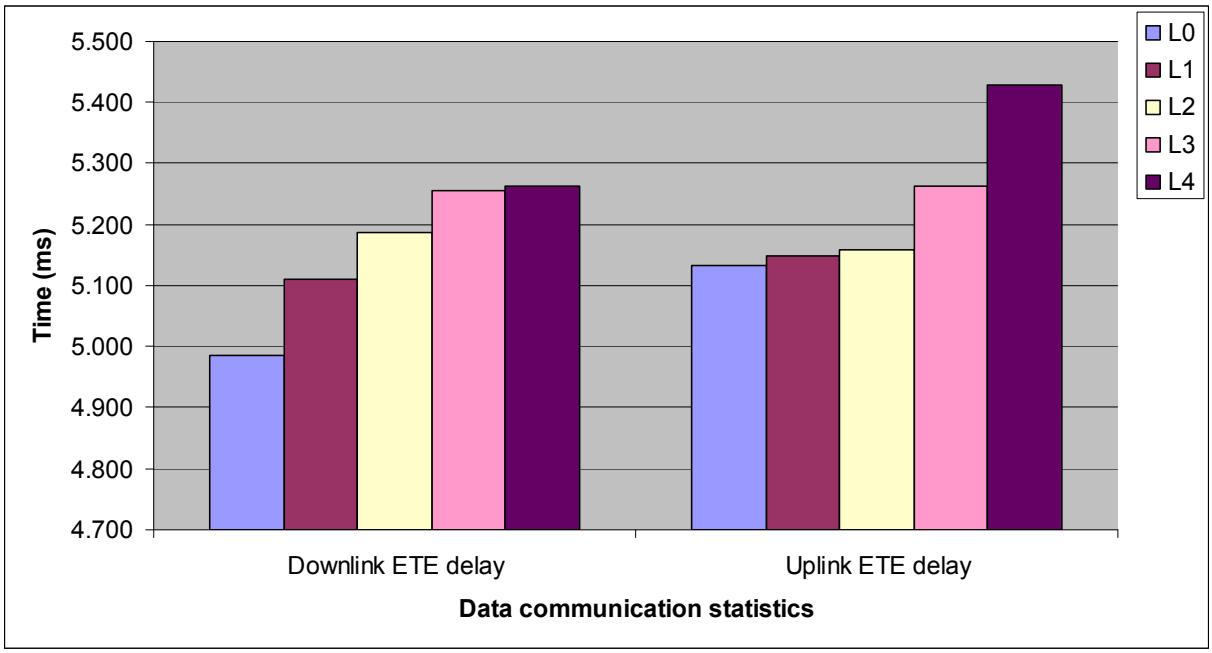


Figure 5-35 Average ETE data communication delay for all the scenarios

The simulation statistics for the data communication throughput are depicted in Figure 5-36 and Figure 5-37 for downlink and the uplink respectively. The Figure 5-38 depicts sample average of both the throughput statistics in a bar-chart graph.

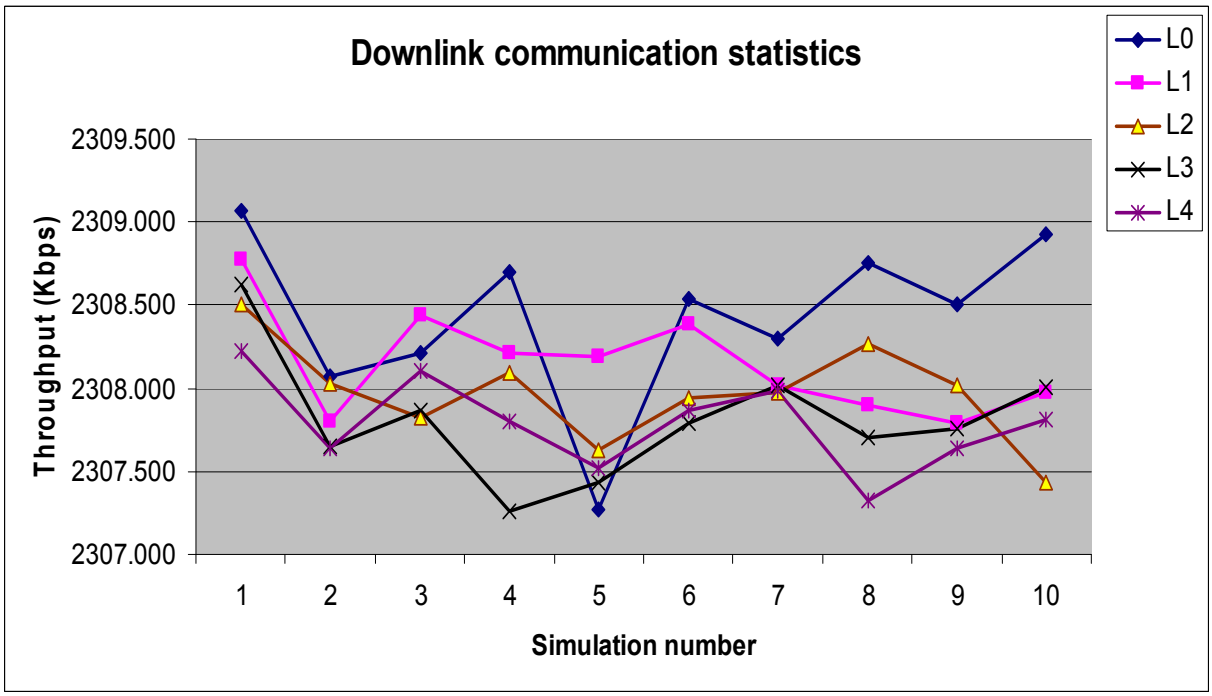


Figure 5-36 Downlink data communication throughput (Kbps)

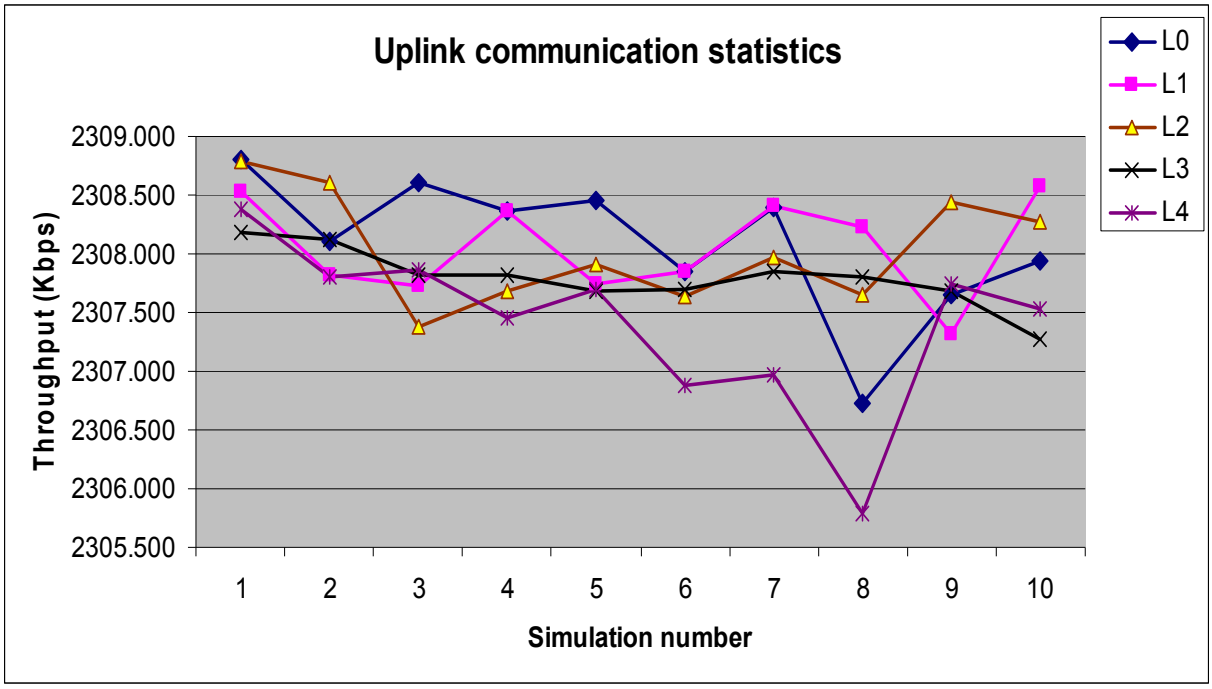


Figure 5-37 Downlink data communication throughput (Kbps)

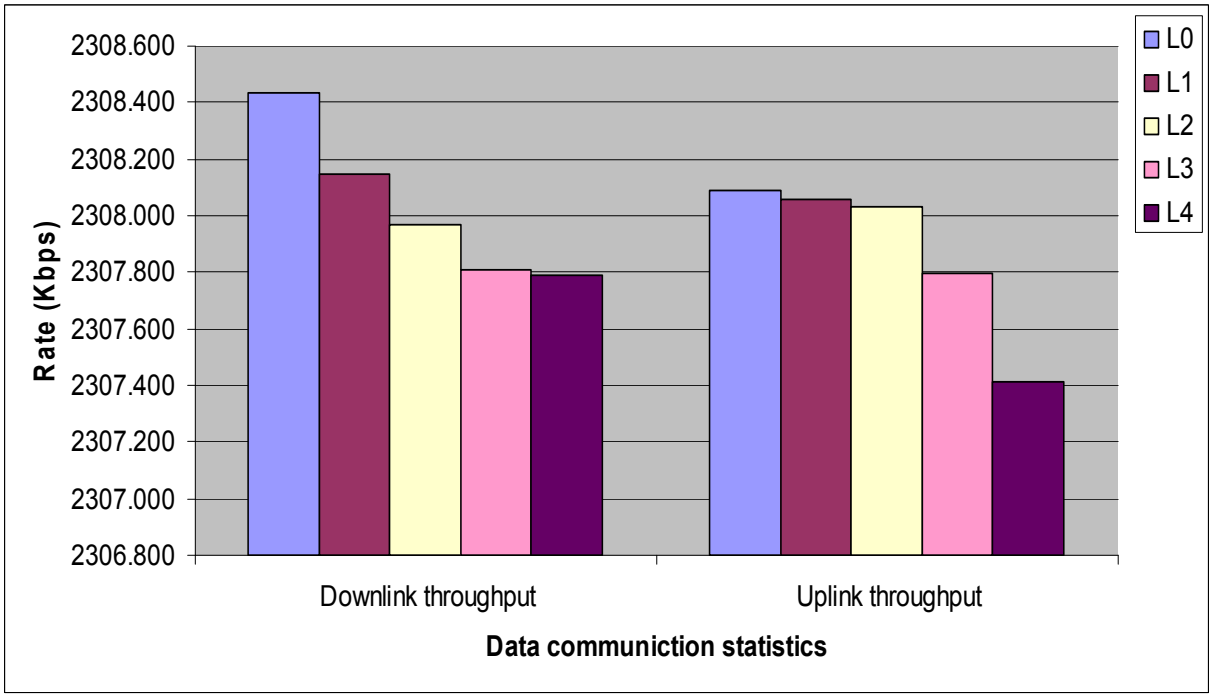


Figure 5-38 Average data communication throughput for all the scenarios

Results show like the ETE data communication delay, the maximum data communication throughput has a very little dependency on the MMPay protocol scheme. The bar-chart graph presented in Figure 5-38 for average throughput shows the uplink through differences among

the scenarios are in the range of few bytes, those are negligible compare to the overall Mbps range throughput.

5.5.5 Summary

(1) The simulation results of the MMPay protocol scheme, presented as MS Excel graph reports above in Section 5.5, shows that protocol have a clear but a small impact on the protocol message response-time, message latency, ETE data communication delay and data communication throughput.

(2) The response-times of the user signed pricing contract vary from about 85ms to 87 ms as the slower smartcard device is used, but these high values have no impact on data communication as the communication starts after successful distribution of the pricing contact agreement along with the first payment throughout the communication path.

(3) The intra-domain payment response-times are from about 5 ms to 7 ms and the payment latencies are from about 3 ms to 4 ms. However, the maximum response-time is 9 ms at loaded situation but about 6 ms for the payment latency. To cope with these varying payment response-times and payment latencies, careful selection of payment threshold and payment retransmission is necessary for uninterrupted communication service.

(4) The intra-domain hand-off pricing contact response-times are from about 9 ms to 12 ms, but they are about 25 ms to 28 ms for the inter-domain hand-off. For uninterrupted communication services, after the hand-off users have to pay to all the service providers along the new communication path, and then the total times including payment response-times for inter-domain hand-off are about 32 ms to 35 ms. These inter-domain hand-off response-times can be reduced by about 60% to the range of 13 ms to 16 ms by distributing TMK to the inter-domain mobility group and careful usage of data transfer credit specified in the hand-off pricing contract. The communication range of a MAP is about 50 meters, thus the range of 13 ms to 16 ms for inter-domain hand-off response-time is expected to be suitable for a speedy hand-off. In the case of practical implementation only ISP(s) and MSP(s) are expected to serve speedy users, where the frequent hand-off pricing contract is not necessary.

Chapter 6: Conclusions

The main goals of this thesis were devise a secure multiparty micropayment protocol scheme for internet access over WLAN mesh networks and simulation of the protocol scheme in OPNET to analyse its suitability. We have proposed a new protocol scheme for internet access over multi-hop wireless WLAN mesh networks as a variant of the multiparty micropayment protocol scheme for ad-hoc networks [Pei00]. The new protocol scheme resolves the difficulties and security vulnerabilities of existing multiparty micropayment schemes, but at the same time accommodates all the good attributes of existing micropayment schemes. Also the protocol scheme is assumed to be suitable for general purchasing from a single vendor over the internet and for localized usages. We have studied the wireless mesh networks for their capabilities and applications. We also studied existing communication billing systems and their emerging problems. Micropayment payment schemes and multiparty micropayment schemes as discussed in Chapter 2 and Chapter 3.

According to the capability and suitability, a huge number of independent and cooperative WLAN mesh network service providers are expected to emerge as access networks to the backhaul internet access. Users who have credential for network access can access the network anytime and anyplace and with a variety of interne-based services. The existing micropayment schemes and their underlying cryptography indicate the hash chain is the most suitable for session-based small-valued communication services; this is also confirmed by the comparative study of Peirce [Pei00]. Accordingly we proposed a new protocol scheme (MMPay) presented in Chapter 4 to overcome existing difficulties and to accommodate good capacities of multiparty micropayment as follows:

(1) The hash chain has been proposed as the payment instrument for fault-tolerant and lightweight cryptography.

(2) The signed pricing contract has been proposed to pay multiple parties using a single payment hash, and it allows variable and dynamic charging for a communication session using a single contract for all the QoS(s) and uplink/downlink traffic.

(3) CBC along with IBC or short signature scheme has been proposed as public-key cryptography for a user prepaid payment certificate, which enables user access to any party, anywhere and anytime with the local authentication option.

(4) The user smartcard has been proposed to protect the private-key and to provide secure protocol accounting services using inexpensive user mobile devices or universal devices.

(5) The share pricing contract signing approach has been proposed to overcome the public-key signing bottleneck by the user smartcard devices.

(6) The pricing contract and hand-off pricing contract protocol messages are authenticated by keyed-hash to limit DoS attacks.

(7) A distributed approach for protocol deployment has been proposed to reduce protocol load of a large MSP.

(8) The payment structure along with an authentication hash chain have been proposed to use multiple small length payment hash chains in a communication session where the ISP-signed hand-off pricing contract will prevent the security vulnerability. The release of a next authentication hash along with the first payment of a new session provides user non-repudiation. The use of a hand-off secrete makes the part of the payment chain unique for a session.

(9) The proposal of synchronization of data transfer will provide accounting accuracy and will confirm data transfer between a user and an ISP.

(10) Signing of the intra-domain hand-off contract using keyed-hash by the ISP provides fast hand-off with low computation.

(11) A data transfer credit balance has been proposed in the pricing contract to confirm accurate payments to all the participating parties in a hand-off situation and to make a payment at the predefined interval.

(12) Redemption has been proposed to be performed only by the ISP, which will reduce the huge communication and processing cost of redemption processes. Combining the hand-off pricing contract with a single signature for the redemption will further reduce the communication and processing cost of the redemption processes.

(13) The proposal of an inter-domain mobility group will provide fast user authentication at the hand-off.

The simulation of the MMPay protocol scheme has been performed as custom application in the OPNET Modeler for sub-protocol response-times and latencies, and the protocol effect on

the data communication ETE delay and throughput. In simulations, four or five scenarios are considered and in the entire scenarios users are attached to the ISP/ISP2 over at least 10 hops of mesh networks. The simulation results presented in Chapter 5 show the protocol scheme has very little effect as the number of relay service providers increases. The user signed pricing contract response-times are little lengthy but have no effect on data communication as communication starts after successful distribution of the pricing contract and the first payment hash. The payment latencies are low as they are approximately 3 ms to 4 ms but they may be increased to approximately 6 ms at a loaded situation; thus, they demands a careful implementation of payment threshold with a retransmission option. The intra-domain hand-off response-times are roughly 9 ms to 12 ms; those are suitable even at the fast mobile environment. But the inter-domain hand-off response-times are approximately 25 ms to 28 ms and including payment they are in the range of 32 ms to 35 ms. The proposal of an inter-domain mobility group and data transfer credit balance will reduce the inter-domain hand-off response-time by approximately 60%, making the MMPay protocol scheme suitable for seamless roaming across different service provider networks.

The MMPay protocol scheme is secure and lightweight, efficient and implementable according to the protocol design, analysis and simulation results.

Bibliography

[AMS96] R. Anderson, H. Manifavas, and C. Sutherland. NetCard - a practical electronic cash system, In Proceedings of the 4th Security Protocols International Workshop (Security Protocols), Lecture Notes in Computer Science vol. 1189, Springer-Verlag, Berlin, pp. 49-57, 1996.

[And98] M. M. Anderson, "Financial Service Markup Language (FSML) version 1.17.1", technical report, Financial Services Technology Consortium, Oct 1998.

[ATYY06] Hidenori Aoki, Shinji Takeda, Kengo Yagyu, and Akira Yamada, IEEE 802.11s Wireless LAN Mesh Network Technology, NTT DoCoMo Technical Journal, vol. 8, pp. 13-21, 2006.

[AWW05] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," Computer Networks, vol. 47, no. 4, pp. 445–487, Mar 2005.

[Bal98] Baltimore Technologies, J/Crypto guide for developers, version 3.0, IFSC House, Dublin, Ireland, 1998.

[BBCM+94] J. P. Boly, A. Bosselaers, R. Cramer, R. Michelsen, S. F. Mjolsnes, F. Muller, T. P. Padarsen, B. Pfitzmann, P. Rooij, B. de Schoenmakers, M. Schunter, L. Vallee, and M Waidner, "The ESPRIT Project CAFÉ-high security digital payment system", in Proc. ESORICS, pp. 217-230, 1994.

[Bel95] Bellare, M. et al. iKP – a family of secure electronic payment protocols, In Proceedings of the 1st USENIX Workshop on Electronic Commerce, New York, USA, pp.89-106, Jul 1995.

[BF01] D. Boneh and M. Franklin, "Identity-based encryption for Weil pairing", in Proc. Crypto 2001, UK, pp. 213-229, 2001.

[BGHH+00] M. Bellare, j. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G.Tsudik, E. Herreweghen, and M. Waidner, "Design, implementation and development of a

secure account-based electronic payment system", IEEE J, Select. Areas Commun., vol. 18, pp. 611-627, Apr 2000.

[BH01] L. Buttyán and J.-P. Hubaux, "Nuglets: A Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks", Tech Report DSC/2001/001, Swiss Federal Institute of Technology, Lausanne, 2001.

[Blu99] Bluetooth Consortium, Specification of the Bluetooth system, Volumes 1 and 2, Version 1.0, Dec 1999.

[Bog00] K. Bogestam, Paying your way in the mobile world, Telecommunications International, 34(1):57-8, Horizon House Publications, Jan 2000.

[CAN98] ACTS Project AC014 CANCAN, Final report, Sep 1998.

[CCG09] Erlon R. Cruz, Daniel Camara and Hélio, "Providing Billing Support in WiMAX Mesh Networks", 2009 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, Morocco, pp. 161-166, Oct 12-14, 2009.

[CM99] S. Corson and J. Macker, Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations, Request for Comments: RFC 2501, Jan 1999.

[CMC99] S. Corson, J. Macker and G. Cirincione. Internet-based mobile ad hoc networking, IEEE Internet Computing, 3(4):63-70, Jul 1999.

[CMS96] J. Camenisch, U. Maurer, and M. Stadler, "Digital payment systems with passive anonymous-revoking trustees", in Proc., ESORICS, pp. 33-43, 1996.

[Col99a] M. Collins. Telecommunications crime, part 1, Computers & Security, 18(7):577-86, 1999.

[Col99b] M. Collins. Telecommunications crime, part 2, Computers & Security, 18(8):683-92, 1999.

[Col00] M. Collins. Telecommunications crime, part 3, Computers & Security, 19(2):141-8, 2000.

[CP10] The Canadian Press, Date: Friday Oct. 29, 2010 6:55 AM ET.

[DA99] T. Dierks and C. Allen, The TLS Protocol version 1.0. Internet Network Working Group, Standards Track, Request for Comments: RFC 2246, Jan 1999.

[DAG06] X. Dai, O. Ayoade and J. Grundy, Off-line Micro-payment Protocol for Multiple Vendors in Mobile Commerce, Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, 2006, PDCAT '06, Taiwan, pp. 197-202, 2006.

[DL99] Dai, X. and Lo, B.: NetPay – An Efficient Protocol for Micropayments on the WWW, Fifth Australian World Wide Web Conference, Australia, 1999.

[ETSI00d] ETSI TS 101 321: Telecommunications and Internet protocol harmonization over networks (TIPHON); open settlement protocol (OSP) for inter-domain pricing, authorization, and usage exchange, version 2.1.0, May 2000.

[ETSI99c] ETSI TS 100 616: Digital cellular telecommunications system (phase 2+); event and call data, version 7.0.1, Jul 1999.

[Eng98] R. England, Payoff deferred, Banking Strategies, 76(2), Mar 1998.

[ES97] Elsevier Science, Telecoms fraud in the cellular market: how much is hype and how much is real? Computer Fraud & Security, x(x):11-14, Jun 1997.

[FKK96] A. Frier, P. Karlton, and P. Kocher, The SSL 3.0 protocol, Netscape Communications Corporation, Nov, 1996.

[FTC98] U.S. Federal Trade Commission, Truth-in-billing and billing format, Federal Communications Commission Comment, CC Docket No. 98-170, Nov 1998.

[FW96] A. Furche and G. Wrightson. SubScrip - an efficient payment mechanism for pay-per-view services on the Internet, In Proceedings of the 5th IEEE International Conference for Computer Communication and Networks, Maryland, pp. 16-19, Oct 1996.

[Ger06] A. Gerkis "A Survey of Wireless Mesh Networking Security; Technology and Threats", Mesh Networking Security – GIAC Gold Paper, Sep 2006.

[GMA+95] S. Glassman, M. Manasse, M. Abadi, P. Gauthier and P. Sobalvarro. The Millicent protocol for inexpensive electronic commerce, In Proceedings of the 4th International World Wide Web Conference, World Wide Web Journal, 1(1):603-18. O'Reilly & Associates, Dec 1995.

[Haa00] J. Haartsen, The Bluetooth radio system, IEEE Personal Communications, 7(1):28-36, Feb 2000.

[HP98] G. Horn and B. Preneel, Authentication and payment in future mobile systems, In Proceedings of Computer Security – ESORICS '98, Lecture Notes in Computer Science vol. 1485. Springer-Verlag, Berlin, pp. 277-93, 1998.

[HHMM+98] G. Horn, P. Howard, K. Martin, C. Mitchell, B. Preneel and K. Rantos. Trialling secure billing with trusted third party support for UMTS applications. In Proceedings of the 3rd ACTS Mobile Communication Summit, Vol 2, Rhodes, Greece, pp 574-79, Jun 1998.

[HALSV02] K. Heikki, A. Ari, L. Lauri, N. Siamak, and Valtteri, UMTS Networks-Architecture, Mobility & Services, John Wiley & Sons Inc., 2002

[HSW96] R. Hauser, M. Steiner, and M. Waidner. Micro-payments based on iKP, In Proceedings of the 14th Worldwide Congress on Computer and Communications Security Protection, Paris, pp.67-82, 1996.

[HY97] A. Herzberg and H. Yochai. Mini-Pay: charging per click on the Web, In Proceedings of the 6th International World Wide Web Conference, Santa Clara, California, Apr 1997.

[IPDR00] IPDR Organization, Network data management – usage (NDM-U) for IP-based services, version 1.1, Jun 2000.

[ITU97b] ITU-T Recommendation E.164: The international public telecommunication numbering plan, May 1997.

[ITU99a] ITU-T Recommendation H.323: Packet based multimedia communications systems, Sep 1999.

[KKA02] M. Koutsopoulou, A. Kaloxylos, A. Alonistioti, "Charging, Accounting and Billing as a Sophisticated and Reconfigurable Discrete Service for next Generation Mobile Networks", Proc. VTC 2002 Fall, Vancouver, BC, Canada, Sep 2002.

[KL03] Kim S and Lee W, A PayWord-based micro-payment protocol supporting multiple payments, In Proc. of the International Conference on Computer Communications and Networks, pp. 609-612, 2003.

[Lam81] L. Lamport, Password authentication with insecure communication, Communications of the ACM, 24(11):770-72, Nov 1981.

[LC01] Y. B. Lin, and I. Chlamtac, Wireless and Mobile network Architecture, John Wiley & Sons Inc., 2001 ISBN: 0-471-39492-0.

[LLCC09] Hui-Tang Lin, Ying-You Lin, Wang-Rong Chang, Rung-Shiang Cheng, "An Integrated WiMAX/WiFi Architecture with QoS Consistency over Broadband Wireless Networks", CCNC-2009, 6th IEEE, pp. 1-7, 2009.

[LM94] S. Low, and N. Maxemchuk, "Anonymous credit cards", in Proc., 2nd ACM Conference on Computer and Communications Security, pp. 108-117, 1994.

[LCFJL08] Phone Lin, Hung-yueh Chen, Yuguang Fang, Jeu-yih Jeng, and Fang-sun Lu, "A Secure Mobile Electronic Payment Architecture Platform for Wireless Mobile Networks", Wireless Communications, IEEE Transactions on Volume: 7 ,Issue: 7, pp. 2705-2713, 2008.

[Man95] Manasse, M. The Millicent protocols for electronic commerce. In Proceedings of the 1st USENIX Workshop on Electronic Commerce, New York, USA, pp. 117-123, Jul 1995.

[MN93] F. Medvinsky and B. Neuman, "NetCash: a design for practical electronic currency on the Internet", In Proc., First ACM Conference on Computer and Communications Security, Fairfax, VA, USA, pp. 102-106, 1993.

[MPMH+98] K. Martin, B. Preneel, C. Mitchell, H. Hitz, G. Horn, A. Poliakova, and P. Howard. Secure billing for mobile information services in UMTS. In Proceedings of Intelligence in Services and Networks (IS&N '98), Lecture Notes in Computer Science vol. 1430. Springer-Verlag, Berlin, pp. 535-48, 1998.

[NH07] Dusit Niyato and Ekram Hossain, "Integration of WiMAX and WiFi: Optimal Pricing for Bandwidth Sharing", IEEE Commun. Mag., vol. 45, no 5, pp. 140-146, May 2007.

[NIST93] National Institute of Standards and Technology (NIST), *FIPS Publication 180: Secure Hash Standard (SHS)*, May 1993.

[Opnet] OPNET Modeler Help, last visited Aug 29, 2011.

[Pat00] P. Patsuris, New payment systems hope to cash in, Forbes E-business, Jun 9, 2000.

[Pei00] M. Peirce, "Multi-party Micropayments for Mobile Communications", PhD Thesis, Trinity College Dublin, Ireland, Oct 2000.

[Ped96] T. Pederson, Electronic payments of small amounts, In Proceedings of the 4th Security Protocols International Workshop (Security Protocols), Lecture Notes in Computer Science vol. 1189. Springer-Verlag, Berlin, pp. 59-68, 1996.

[PHS98] T. Poutanen, H. Hinton, and M. Stumm. NetCents: a lightweight protocol for secure micropayments, In Proceedings of the 3rd USENIX Workshop on Electronic Commerce, Boston, Massachusetts, pp.25-36, Sep 1998.

[RS96] Rivest, R., Shamir, A, PayWord and MicroMint: two simple micropayment schemes, In Proceedings of the 4th Security Protocols International Workshop (Security Protocols), Lecture Notes in Computer Science vol. 1189, Springer-Verlag, Berlin, pp. 69-87. 1996.

[RK08] Hassen Redwan and Ki-Hyung Kim, "Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks", IEEE-2008, pp. 1-5, 2008.

[SET97] Mastercard and Visa, SET Secure Electronic Transactions Protocol, version 1.0 edition, Book One: Business Specification, Book Two: Technical Specification, Book Three: Formal Protocol Definition, May 1997.

[Sey98] B. Seymour., The brain behind fraud control. Telecommunications International, 32(11):71-2, Horizon House Publications, Nov 1998.

[SFPW98] B. Stiller, G. Fankhauser, B. Plattner, and N. Weiler, "Charging and accounting for Internet services – state of the art, problems, and trends", In Proceedings of the 8th Internet Society Conference on Internet Networking (INET'98), Geneva, Switzerland, Jul 1998.

[Sha1985] A. Shamir, "Identity-based cryptosystems and signature schemes", in Proc. CRYTO 84 on Advances in Cryptology, pp. 47-53, 1985.

[SLE66CLX] http://www.infineon.com/dgdl/SPI_SLE66CLX360PE_1106.pdf, last visited Aug 25, 2011.

[SLE88CFX] http://www.soiseek.com/INFINEON/SLE88CFX4000P/5.htm, last visited Aug 25, 2011.

[SP03] Tommy Svensson, Alex Popescu, "OPNET Modeler", Blekinge Institute of Technology, Jun 2003.

[ST95] Sirbu, M., Tygar, J.D. NetBill: an Internet commerce system optimized for network delivered services. IEEE Personal Communications, 2(4):34-39, Aug 1995.

[SUSI99] ACTS Project AC320 SUSIE. Premium IP services, SUSIE Deliverable 4, Apr 1999.

[SUSI00] ACTS Project AC320 SUSIE, Project recommendations, SUSIE Deliverable 7, Feb 2000.

[SV97] Stern, J., Vaudenay, S. SVP: a flexible micropayment scheme. In Financial Cryptography ’97 Proceedings, Lecture Notes in Computer Science vol. 1318. Springer-Verlag, Berlin, 161-71. 1997.

[TCS] Pitta Satya Sai Kumar, “Revenue Assurance-A Competitive Edge”, Tata Consultancy Services, www.tcs.com, last visited Aug 28, 2011.

[TM01] Hitesh Tewari and Donal O'Mahony, Multiparty Micropayments for Ad Hoc Networks, NTRG, Dept of Computer Science, Trinity College, Dublin - 2, Ireland, 2001.

[WAP99a] WAP Forum, Wireless application protocol (WAP) wireless transport layer security (WTLS) specification. Nov 1999.

[WiFi97] IEEE Std.802.11-1997 Information Technology- Telecommunications and Information Exchange between Systems- Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, technical report IEEE Std.802.11-1997, 1997.

[WiM04] IEEE Standard for Local and Metropolitan Area Networks-Part 16: Air Interface for Fixed Broadband Wireless Access Systems, technical report IEEE Std.802.16-2004, 2004.

[Whe96a] D. Wheeler. Transactions using bets, In Proceedings of the 4th Security Protocols International Workshop (Security Protocols), Lecture Notes in Computer Science vol. 1189. Springer-Verlag, Berlin, pp. 89-92, 1996.

[Whe96b] D. Wheeler, MicroMint extensions, Computer Laboratory, University of Cambridge, UK, Nov 1996.

[WMS2009] H. Wang, J. Ma, and J. Sun, “Micro-payment Protocol based on Multiple Hash Chains”, Electronic Commerce and Security, 2009. ISECS '09, Second International Symposium on Volume: 1, pp. 71-74, 2009.

[YHH99] S. Yen, L. Ho and C. Huang, “Internet Micropayment Based on Unbalanced One-way Binary Tree”, Proc. CrypTEC’99, Hong Kong, pp.155-62, Jul 1999.

[YLH99] S. Yen, C. Lee, and L. Ho. PayFair: a prepaid Internet micropayment scheme promising customer fairness, In Proceedings of the International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC’99), Hong Kong, pp.213-21, Jul 1999.

[YLT04] Z. Yang, W. Lang, and Y. Tan, “A new fair micropayment system based on hash chain”, in Proc. IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE’04), Taipei, Taiwan, pp. 139-145, 2004.

[ZF07] Y. Zhang and Y. Fang, “A secure authentication and billing architecture for wireless mesh networks”, Wireless Networks, vo. 13, no.5, pp. 663-678, 2007.

[ZGWWMR07] A. Zimmermann, M. Gunes, M. Wenig, U. Meis, J. Ritzerfeld, “How to Study Wireless Mesh Networks: A hybrid Testbed Approach” 21st International Conference on Advanced Networking and Applications (AINA'07), Niagara Falls, Canada, pp. 853-860, 2007.

[ZLLHS2008] Haojin Zhu, Xiaodong Lin, Rongxing Lu, Pin-Han Ho, and Xuemin (Sherman) Shen, “SLAB: A Secure Localized Authentication and Billing Scheme for Wireless Mesh Networks”, Wireless Communications, IEEE Transactions on Volume: 7, Issue: 7, pp. 3858-3868, 2008.

[ZWM04] Zhu, J., Wang, N. and Ma, J.: A Micro-payment Scheme for Multiple-Vendor in M-Commerce. Proceedings of the IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East’04), Beijing, China, 2004