THE UNIVERSITY OF THE SOUTH PACIFIC
LIBRARY

DIGITAL THESES PROJECT

Author Statement of Accessibility- Part 2- Permission for Internet Access

Name of Candidate : OLUWATOMI AYOADE

Degree : MASTER OF SCIENCE IN COMPUTER SCIENCE

Department/School : The University of the South Pacific

Institution/University : ----------

Thesis Title : MICRO-PAYMENT ADOPTION FOR MULTIPLE VENDORS IN MOBILE COMMERCE ENVIRONMENT

Date of completion of requirements for award : APRIL 27, 2007

1. I authorise the University to make this thesis available on the Internet for access by USP authorised users. Yes/No

2. I authorise the University to make this thesis available on the Internet under the International digital theses project Yes/No

Signed: tomi ajoade

Date: 11 | 04 | 07

Contact Address

P. O. BOX 461
U. S. P,
SUVA.

e-mail : tomiayoade@yahoo.com

Permanent Address

e-mail: tomiayoade@yahoo.com

Micro-payment Adoption for Multiple Vendors in Mobile Commerce Environment

Oluwatomi Ayoade

School of Computing, Information and Mathematical Sciences.
Faculty of Technology,
The University of the South Pacific.

A thesis submitted for the partial fulfillment of the
requirements for the degree of
Master of Science (Msc.) in Computer Science.

April, 2007.

Acknowledgement

My deepest and unconditional appreciation goes to my husband-Dr John Ayoade for his love, spiritual, financial and moral support for bringing my heart desire to fulfillment and in making this work a reality. I am also indebted to my dearest children-Opeyemi and Ayodeji for their understanding and cooperation throughout the period of my study. My heartfelt gratitude goes to my entire families-the Ayoades and the Obembes who have been a source of inspiration for the completion of this work.

My appreciation goes to my supervisor-Dr Sharlene Dai for introducing me to the research topic, sharing her valuable time and giving me constructive suggestions. My profound gratitude goes to the Head of School-Dr Jito Vanualailai, School of Computing, Information and Mathematical Sciences (SCIMS) for his approval and support to further my studies.

In addition, I will like to express my profound gratitude to Dr Robert Whelan and Dr James Terry who helped to proof read the thesis. I will equally like to thank the examiners Dr John Grundy and Mr Prakash Narayan for sharing their knowledge and comments on this thesis.

I will like to thank all supporting staff of SCIMS and friends for their moral support and encouragement and all those who contributed to the great success of this work.
With the whole of my heart, I will like to say thank you all!!!

Dedication

This thesis is solely dedicated to my beloved late father-Presiding Elder Titus Adenipekun Obembe who loved me unconditionally and would have wished to be alive and witness the great success of my studies and career in life. May his gentle soul continue to rest in perfect peace in the bosom of our Lord and Saviour.

Declarations

I hereby declare that this thesis is my own work and that, to the best of my knowledge and belief, it contains no material which has been previously accepted or published for the award of any other degree or diploma at any University or equivalent institution, except where due reference or acknowledgement is made in the text of the thesis.

Oluwatomi Ayoade

April 2007

Abstract

Across the spectrum of wireless services (mobile games, location-based services, entertainment), development is hampered by unsuitable payment methods. There are several existing and competing mobile micro-payment systems, protocols and models for payment of low-value and high-volume transactions in mobile commerce. Most of these protocols are not suitable for payment to multiple vendors. They also have high transaction costs (communication, computation, operational, managerial, and processing) of payment for individual transactions. More so, they do not provide high security, ease of use and convenience of payment transactions to customers most especially "the Mobile Users".

Mobile electronic payment systems must provide secure, efficient, usable and reliable environments which are the key issues in mobile commerce system development. Solutions to existing problems of mobile micro-payment will require considerations for the high volume (frequency) of transactions and low value items. In addition, it must consider the ease of access to make payments, and convenience of using funds or an alternative for purchasing services, commodities and information on the Internet via mobile and wireless devices. Wireless payment must also incorporate the two essential features added to electronic commerce: accessibility and mobility. These considerations have motivated the research conducted in this thesis.

This thesis focuses on evaluating existing and competing frameworks and protocols for mobile payment. A framework is introduced to overcome the limitations of wireless network and solve the problems arising from the current existing micro-payment schemes of mobile payments. The major focus of this thesis is to propose a more practical method for making micro-payment over wireless devices such as mobile phones particularly for low value, high frequency purchases that will be more easily accessible and mobile.

Table of Contents

List of Tables

List of Figures

List of Publication(s) from the Thesis

Parts of the research in this thesis have been published in the following conference and journal paper.

1. Xiaoling Dai, Oluwatomi Ayoade, and John Grundy: Offline Micro-Payment Protocol for Multiple Vendors in Mobile Commerce at the 7th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06) 4-7 December 2006 - Taipei, Taiwan.

2. Oluwatomi Ayoade, Xiaoling Dai and John Grundy: Evaluation of Micro-payment Models for Mobile Commerce System (to be submitted to the Journal of Electronic Commerce Research)

Chapter 1 Introduction

1.1 General Overview

In electronic commerce (e-commerce) of today, existing macro-payment systems are the most widely used method of electronic payment. These systems use online payment methods that frequently involve the interaction of a Trusted Third Party (TTP), or an authorised person in every transaction. This places high transaction and over head costs.

Most electronic payment protocols (e.g. Secure Electronic Transfer - SET, iKP) are computationally expensive computationally because they make use of digital signatures and are difficult to administer. They provide support for heavy weight credit card and digital cash payments that are suitable for high-value, low-volume transactions and they are difficult to implement for micro-purchases.

Consequently, macro-payment systems are not suitable for high-volume, low cost products or services [27]. Credit card purchasing is a method of payment that is nowadays widely trusted and used by the general public. Although their handling is familiar to most consumers and they are considered to be relatively safe [31] but they seem to simply be unprofitable for the seller at purchases for small amount of money [32] even their system work well enough.

The use of credit cards for every transaction, as is usually done with electronic commerce is impractical for providers of inexpensive items because the credit card fees and associated costs eat up sellers' profit [14]. For example, a minimum fee between 15 to 40 cents is usually charged per transaction and this represent all or much of expected profit on many sales.

In addition, macro-payment systems cannot be directly applied to wireless networks due to certain constrains in this environment such as slower link, battery powered, power constraints, limited bandwidth and higher cost. These constrains will be discussed more in detail in section 2.4.1. Macro-payments also introduce some bottlenecks and

limitations as means of payment for low value and high volume transaction to be purchased via wireless and mobile devices due to some certain resources that limit wireless and mobile devices. These limitations are speed, size, capacity, interface and they will be discussed further in section 3.4.2.

New solutions and technology are required for the introduction of some lightweight cryptographic techniques that may be appropriate for low-value, high-frequency transactions. This is where micro-payment systems deserve attention. In contrast to macro-payments, micro-payments are lightweight payment schemes designed to support low-valued transactions of the order of few cents [26]. In a micro-payment system, the use of a public key cryptosystem is usually replaced with cryptographic hash functions.

From the viewpoint of micro commerce, micro-payments can be seen as one possible solution to allow pay for downloadable, intangible, low value items such as news articles, music clips, information and other services [24]. Micro-payment technology is presumed to have a promising future for wireless e-commerce [12].

In contrast to wired e-commerce, wireless e-commerce has many differentiating characteristics that make micro-payment suitable. These features include commonality of high-frequency, low-value transactions, large numbers of content vendors and the ever-increasing need for flexible and accessible solutions. Therefore micro-payment systems will be a better and suitable tool for payment in mobile commerce system.

1.2 The Problem Description of Mobile Commerce Payment

The aim of business and service providers is to minimise cost and maximise profit. The goal of consumers is to maximise utilities and service being paid for. The sale of inexpensive goods and services such as online digital contents (ringtones, games, music, and video) which are presently being downloaded and offered for free on the Internet are expected to grow in the next few years. This will boost the generation of revenue from individual sales and will encourage content and service providers to introduce more new products.

In recent times, mobile phones have become platforms of choice for delivering rich digital data, used for recording and downloading photos, video and music, Internet access, Podcasts, and transmitting payments [22]. However, it is expected that future mobile system will involve a large number of users who will access a variety of information, services, goods or commodities provided by content providers and pay for such transactions. Thus, future pervasive wireless connectivity is expected to create new opportunities for mobile commerce.

Mobile commerce (m-commerce) brings opportunities to small businesses both to sell new services and to operate more efficiently [16]. Mobile computing enables Internet-enabled cell phones, Personal Digital Assistants (PDAs), and other wireless computing devices to access digital information on the Internet from any location and at anytime. This is otherwise known as *wireless electronic commerce (m-commerce)*.

There is no commerce without payment and mobile commerce requires appropriate payment methods [6]. Mobile payment systems are an essential part of the emerging m-commerce and mobile business (m-business) markets and will not only make purchasing activities more ***flexible*** and ***convenient*** but also create unimagined new markets [18]. The question of charging for intangible goods and services (such as information, immaterial commodities or resources) on the Internet has been a long standing issue for both e-commerce and m-commerce.

At present, there are no effective means of charging for downloading various low value digital contents such as music, images and games that are provided free today on the Internet because the existing payment system are seemingly unsuitable for charging or payment [24]. This creates the need for an efficient payment system which can handle such trade. Consumers expect online low value products and services to be free and likewise expecting to benefit more from new services provided by content providers that do not currently exist.

On the other hand, service providers are optimistic for new opportunities for them to provide and sell more new products and services in order to maximise profits rather than offering them for free. Most content providers want to be compensated for their hard effort and substantial utilisation of resources [24]. According to Kurt Huang[1], providers of inexpensive content see micro-payment technology as a way to generate revenue [14].

There are many existing mobile micro-payment schemes for the payment of low value and high volume transactions in mobile commerce such as those proposed by Zhu *et al.* [11], Zheng *et al.* [25] and Boddupalli *et al.* [26]. Most of these protocols are unsuitable for payment to multiple vendors as they do not allow the use of a single wallet to be used for several purchases (funds transferability). This is as a result that most of the exchange mediums (payment tokens) for these systems are vendor specific (specific to only one Vendor) and are not transferable. This problem makes micro-payment system for such models to be less efficient, as buyers need to access and make payment (for multiple purchases) to variety of service and content providers

In addition, a range of potential mobile micro-payment protocols have high transaction *cost* (communication, computation, operational, managerial, processing) of processing payment. Some do not provide *high* security, ease of use and convenience of payment transaction to customers/users. Customers/users of these models require contacting the Trusted Third Party (such as the Bank or Broker) for payment authorisation in every transaction. This problem makes current mobile micro-payment models not to be cost-effective and flexible as they place high communication burden on the Broker. The Customer can neither make payment nor continue making purchases without the use of the Broker. Mobile micro-payment is expected to provide easy mobility and accessibility.

[1] The president, founder and chief product officer of electronic payment technology.

1.3 The Objectives and Meaning of the Research

This research focuses on motivating the use of micro-payment system in the mobile commerce applications domains. To be precise, it focuses on transaction payment for mobile information content such as ringtones, music, video, games and wallpapers. The electronic wallet (e-wallet) stored by the mobile device will involve the use of payment tokens in the form of electronic coins "e-coins" for payment of low valued items. The two major key issues involve in micro-payment systems will be taken into consideration for the new protocol to be proposed in this thesis. These are **low value** (use of hash function to reduce cost overhead) and **high volume.**

The thesis describes the main functional characteristics of existing and competing micro-payment protocols in the mobile device application domain. It also focuses on new enhancement (development) of an existing wired micro-payment approach. A qualitative analysis of a range of potential mobile micro-payment system will be presented and evaluated. A range of criteria will be used to assess their strengths and weaknesses. Overall, a new mobile micro-payment protocol will be presented, assessed and compared to other existing and competing approaches.

The main objective of this thesis is to provide solution to major problem areas of the existing mobile micro-payment models; to meet up with the new industrial trend of wireless e-commerce[2] and design an efficient mobile micro-payment model suitable for mobile commerce system. A new mobile micro-payment protocol[3] with high performance and security in a wireless environment as opposed to payment in the conventional wired network will be proposed.

This thesis will also investigate approaches on how a wired micro-payment protocol "NetPay" could be applied or re-designed for use in wireless Network environment. The issue of integrating the wired micro-payment into a wireless e-commerce mode suitable

[2] The distribution and payment of digital information that will be mobile and easily accessible.

[3] An enhancement of an existing protocol

for various services (digital content) on wireless devices will be investigated. This will involve an enhancement of NetPay (a micro-payment protocol) by incorporating a network provider and modifying the client-vendor-broker protocols.

A new mobile micro-payment protocol called "Mobile NetPay (MOBAPY)" which is the wireless successor of the wired NetPay will be proposed. MOBPAY is more efficient than its predecessor (NetPay) because of its increasing mobility and accessibility for micro-payment in mobile commerce.

The main focus of MOBPAY is to provide solution to the major problem of its predecessor (wired NetPay) and to build up more efficient micro-payment system in a virtual world of wireless connection. MOBPAY protocol provides high performance and security in a wireless environment as opposed to payment in the conventional wired network.

The MOBPAY protocol will focus on the micro-payment protocol required for payment of low valued, high volume transactions by the use mobile or wireless device. The MOBPAY protocol will be evaluated (compare and contrast) with other existing mobile micro-payment models for m-commerce system and in conclusion gives direction for future research work.

1.4 Limitation and Scope of Study

Mobile electronic commerce has a broad concept and fields such as technology, payment processing and security issues. However, the key to innovation in wireless services is payment [6]. Payment mechanisms such as micro-payments are an essential feature of m-commerce. This research study will be narrowed down to payment processing involved in m-commerce.

To be precise, the main focus will be on investigating approaches and designing a protocol suitable for mobile information content micro-payment applications with client

side electronic-wallet storage by the mobile device. The scope of study will be limited to the payment protocol in terms of processing transaction payment on mobile devices.

The major focus and consideration will be on how mobile information (digital) content application or downloadable media and items such as ringtones, music, video, games, wallpapers, web pages and information could be purchased over a wireless network. In short, this thesis aim to offer solutions to the problems of micro-payment schemes use for goods delivered over virtual channels.

1.5 Organisation of the Thesis

The thesis is structured into seven chapters. This Chapter presented the motivation to carry out this research on mobile micro-payment system. The goals, objectives, limitation and scope for this thesis were also presented in this chapter.

Chapter 2 presents the detailed literature review of payment systems. This chapter presents their general characteristics, merits, demerits and their appropriateness for different kinds of electronic business (E-business) transactions. This chapter discusses the parties, features, benefits and challenges of micro-payment systems in respect of m-commerce. The comparison between electronic commerce and mobile commerce systems as well as the need to focus on micro-payment schemes (not macro-payment) for mobile content payment will be discussed.

Chapter 3 presents the overall view of the conceptual recent work on mobile commerce system highlighting its technologies, service, and scenarios. This chapter enumerates the importance and application of mobile devices. The main focus will be on mobile commerce micro-payment systems and discussion will be on what brought about mobile micro-payment in terms of their revolution, high demand in recent years, payment categories, channels, payment protocol and the roles of Mobile Network Operator.

Chapter 4 presents a general overview of current and competing micro-payment models for mobile commerce systems. This chapter presents an in-depth discussion on how

lightweight cryptographic operations have been applied to these models. Also, it discusses the phase of transaction payment processes for each of the model, compares and contrasts these models bringing out their strength, weaknesses and identifying their major problem area.

Chapter 5 overviews and analyses a new mobile micro-payment protocol called Mobile NetPay (MOBPAY) for mobile commerce system. This chapter discusses intensively the three main transaction processes that exist between various actors and the requirements of MOBPAY protocol.

Chapter 6 discusses a qualitative assessment of MOBPAY protocol extensively bringing out its merits, benefits, evaluation and limitation. The current (existing) token-based micro-payment models of mobile commerce presented in chapter 4 will be evaluated and compared with the new proposed mobile micro-payment protocol.

Chapter 7 presents the general conclusion for this thesis. This chapter provides a summary of the thesis and proposed future work on mobile micro-payment systems. In particular, this chapter provides an outline of future work and development for the new proposed mobile micro-payment protocol (MOBPAY).

Chapter 2 Electronic Payment Systems

Electronic commerce (e-commerce) involves the online purchase (buying and selling) of goods, products, information and services over the Internet. Hertzberg (1996) said provision of content is one of the main attractions and benefits of the Internet [30].

In the virtual world, electronic payment oils the economies and it is the lifeblood of e-commerce [6]. One long promised aspect of electronic commerce (electronic micro-payments) has remained unfulfilled after the long years of online purchasing [14]. This is the charging or payment for low value intangible items.

This chapter reviews the fields and characteristics of electronic payments in respect to mobile commerce which will incorporate the payment for very low value and high frequency transactions via mobile and wireless devices.

2.1 Types of Payment Systems

There are two fundamental e-commerce payment systems in an electronic environment. These are macro-payment and micro-payment systems. The choice of which payment scheme to use depends on the volume and value of information, services and commodities being exchanged.

2.1.1 Macro-payment Systems

The macro-payment system is a type of electronic payment systems that is specifically designed for large fee payment, usually of high-value and low-volume transactions. They are the most common method for charging for goods and services today, since they provide support for credit card and digital cash payments.

The model for this payment system can either utilise the use of a broker so that both the buyer and the seller are authenticated only by PINs (Personal Identification Numbers) that are sent through a secure web connection, or by the use of credit card information that is being sent directly from the buyer to the seller in an encrypted and signed form [36].

The most distinctive advantages of using macro-payment systems are as follows:

- **High Security:** most macro-payment systems use strong cryptographic technique that provides very high security for the payment of bulk purchases. Macro-payment is considered by many users to be relatively safe and secured.
- **Large Consumer Base:** credit card purchasing is a publicly accepted paying method and the handling of them is familiar to most consumers. Many users prefer to make macro-payment by the use of credit card due to the fact that their system work well and it provides much conveniences for bulk purchases of high value.
- **Online validation:** most macro-payment systems allow online payment authorisation by the use of a Trusted Third Party usually called the Bank. This enhances much confidence in users of this system.

Factors that make macro-payment systems undesirable for use in purchasing via mobile devices are discussed below:

- **Higher transaction time**: the transaction time for accepting a credit card or processing on a standard land-line terminal could be slower than a wireless terminal depending on the mobile device coverage and type [47]. These payment schemes are based on online, time-of-payment authorisation and require the use of heavy weight encryption technology.
- **Wireless constraints**: macro-payments are difficult to implement on mobile devices due to certain constraints of wireless environments or poor mobile device capabilities such as computational resources, weaker graphical interface, weaker input capabilities and weaker internal and external security [12] than the fixed or wired terminals and devices.
- **Complexity**: most electronic payment protocols (e.g. Secure Electronic Transfer - SET) are computationally expensive because they make use of digital signatures. For instance, the existing heavy weight credit card payment (macro-payment) is not suitable for low value and high frequency transactions due to the overhead cost (computation and communication) of payment processing. This is especially the case for payments on wireless or mobile devices.

- **High cost of transaction**: customers or users of macro-payment systems are usually charged certain bills called base costs which have a direct influence on the pricing policy of products and services and on the interest of potential customers [24]. The banks and clearing house always charge certain percentages and have fixed prices for every transaction they perform.

2.1.2 Micro-payment Systems

Micro-payment systems can be defined as a subset of electronic payment systems which is suitable for the payment of low-value items, information or services. They are payments under $10 to buy and sell digital goods over the Internet. Micro-payment system has the ability to handle very low transactions as small as 1¢ [18]. Micro-payment methods must be suitable for the sale of non-tangible goods for low-valued items such as ringtones or small multimedia clips, web pages or information over the Internet.

Micro-payments are very appropriate for mobile commerce applications. They have the potential to provide high volume and low value pay-as-you-go transactions for a wide variety of mobile applications. They are based on lightweight cryptographic techniques which in turn are cost effective for users of high frequency purchasing. Micro-payment technology is presumed to have a promising future for wireless e-commerce as it has the potential to provide non-intrusive, high-volume and low-cost pay-as-you-use services for a wide variety of web-based applications.

For mobile commerce, micro-payment -based techniques will be more appropriate for supporting low- value and medium-high-volume transaction payments of the order of few cents than the macro-payment based technique and systems [9], [10], [11], [14]. According to Kearney's m-commerce survey [39], more customers tend to use micro-payment systems than macro-payment systems, especially for small cash transactions such as transit fares on public transport or for buying items from vending machines. This thesis will focus on micro-payment system for mobile commerce payment because macro-payment system is not appropriate.

There are various roles to be performed in any form of commerce. In an electronic commerce payment scheme, these roles include functions such as payment authorisation and settlement, customer authentication and service/product provision. These roles are assigned and performed by these main actors: The Buyer/Customer /Mobile User, Seller/ Vendor/Merchant, and usually the Broker/Bank.

1. **The Buyer:** usually initiates a purchase, registers with the payment service provider such as the Broker (who authorises payment for the buyer and refund to sellers).
2. **The Seller**: sells a product to the Buyer, forward purchase request to the Broker, relay authorisation request back to Buyer and delivers content. The growth of mobile payment market is not possible without high participation of the merchants [18]. The Merchant's product in the course of this research is assumed to be a downloadable digital content.
3. **The Broker**: is responsible for payment process, controls the transaction flow between the Buyer and the Seller. The Broker provides support for payment related interactions and is responsible for the registration and debiting of the Buyer's account. The Broker authorises payment for the buyer and refund to sellers. The Broker is also in charge for crediting the Seller's account during the time of redemption

All micro-payment schemes have some common features and characteristics. These micro-payment scheme characteristics will be viewed in respect of the scope of mobile payment. These are technical and non-technical characteristics in terms of structure, function, social, economic and usability aspects of micro-payment systems. Róbert Párhonyi et al. [20] and Müller and Schmidt [36] have both distinguished technical features as follows:

- **Technical Characteristics**

These describe the internal structure and functionality of micro-payment systems [20]. The technological factor consist of the requirements for micro-payment systems whose fulfillment is mainly an issue of proper (technical) implementation [36]. These include:

- **Account based/Token based**: it specifies the medium of value exchange. In account-based systems, customers and merchants have accounts at a broker or bank. The Customer authorise the broker to transfer money from his account to merchant's account. However, the buying power in token–based systems is the tokens or the electronic coins (e-coins).
- **Ease of use or convenience**: relates to the user interfaces and underlying hardware and software systems. It also relates to the easy usage of the system for both new and experienced Users.
- **Anonymity:** concerns the amount of knowledge other parties have of others using the same system of transaction [35]. This is defined the same way according to [38] as the protection of the identity of the parties participating in the protocol. Generally, when defined with respect to all the parties of micro-payment system, Merchants or Broker does not have anonymity. Therefore, it is only relevant to Customers.
- **Scalability**: refers to the ability to cope with increasing payment volume and user base without significant performance degradation. According to [35] micro-payment system design should be able to respond to the growing markets in the Internet both in terms of technology and business-wise. A scalable distributed design is required (in micro-payment system) to prevent the possible bottlenecks that may emerge if the system fails to respond to the requirements set by the potentially rapid increase of the transaction traffic through it [36].
- **Validation** (online or offline): determines whether a payment system is able to process payments with (online) or without online (offline) contact with a Trusted Third Party (TTP) such as the broker or the micro-payment system operators. Micro-payment system should not force User to always contact a TTP during every transaction. This is a very important criterion considering the very hard latency requirements for the micro-payment transactions [35].

- **Security**: is partly an issue of the security of the technology used in the micro-payment system. However, we will refer to this in the context of this thesis as the prevention and detection of attacks on payment system and fraud attempts, and protection of sensible payment information. The main security concerns are non repudiation, authentication, authorisation, confidentiality and data integrity [20].
- **Reliability:** the micro-payment system must serve Customers 24 hours in a day and seven days in a week, having no point of failure in the system at any time [36]. Matonis introduced the concept of availability from the view point of the requirements on electronic money in general that the system must be available at anytime for any (valid) Customer and it must be off-line capable so that no online TTP involvement in respect of authentication is required [37]. This is a very important criterion in this thesis as we are considering a mobile payment that will be easily available and accessible at anytime (mobility) and anywhere.

- Non-technical Characteristics

Róbert Párhonyi et al. [20] and Müller and Schmidt [36] further classified micro-payment requirement framework as relating to social, economics and usability of micro-payment system as follows:

- **Trust:** refers to User's confidence with respect to the trustworthiness of the micro-payment system and its operator. Security techniques increase the trust Users feel and trust is considered as a precondition for a blooming commerce.
- **Customer base:** refers to the coverage or size or number or percentage of the customers and merchants that can use the micro-payment system and its operator. The term coverage is synonymous to acceptability and penetration.
- **Privacy:** relates to the protection of personal and payment information. This is closely related to the security issues as stated above. A payment system provides privacy protection depending on information type.
- **Convertibility:** currency applied to micro-payment systems must have monetary value and must be exchangeable to and from the currency the bank uses. In short, currencies must be convertible with each other in order to be used amongst several payment systems.

- **Pre-paid or post-paid:** determines how customers use a payment system. Pre-paid systems require customers to transfer money to the system before they can initiate micro-payments. Post-paid systems authorises customers to initiate micro-payments up front and pay later.

- Extended Characteristics

According to Chi [34], the following features are common in each micro-payment scheme:

- **Money generation:** money or currency used for micro-payment scheme could either be certified (created) by a Broker or generated by the Customer of the micro-payment scheme. Certification by Broker is a debit approach as the Customer has to purchase a specific form of money in advance prior to transaction period (pre-pay). In the second option, the Customer does not need a direct certification by a broker and the Customer account will be debited after purchase or transaction. This is a credit approach or postpaid method.
- **Redemption:** this is the process whereby the merchants deposit received token or e-coins (value of the buying power) from the Customer with the broker in exchange for real money or asks the broker to transfer money from the Customer's account into his own account at a specified period after the transactions process. This is assumed to be off-line when used in a micro-payment scheme [34]
- **Double Spending detection:** different protocols make use of different sets of data and these data are usually kept in a database and verified in order to prevent double spending.

According to Gabber *et al.* [33], all micro-payment system shares the goal of minimizing the cost overhead of a single transaction. They tend to save costs including financial risk-management costs, operational cost (including communication, processing and storage) and set up cost. Apart from the cost factor, there are other goals and benefits emanating from the use of micro-payment systems [47]. These are highlighted as follows:

1. Flexibility and convenience in purchasing activities: Micro-payment system aim to provide a simple user interface to make selling and buying a product or service as easy as possible.
2. They generate or provide alternative revenue for content provider beyond advertisement or content being offered for free today on the Internet or through subscription method.
3. Create unimaginable new markets thus improving productivity. Users of micro-payment system will benefit from and enjoy new services that do not presently exist.
4. They provide revenue streams for service Providers offering different types of services for free on the Internet due to non effective method to charge for them at present.

There are many challenges facing the slow growth of micro-payment system over the Internet. The key challenges for micro-payment technology are: security, ability to handle high transaction, ease of use. These challenges can be described in terms of how they affect the payment processing scheme (techniques) and also general acceptance by both buyers and sellers.

- All micro-payment systems are capable of handling arbitrarily small amounts of money but the problem is keeping the cost for the individual transaction as low as possible.
- It imposes requirements on the speed and cost of payment processing. These problems are classified as the pprocessing time (non efficient) of public key computation and cost of the overhead of transaction process or running the system which must be suitable for the sale of non-tangible goods over the Internet.
- According to Odiyzko [43], the increase in flexibility of the existing framework (credit card) can be a barrier as well
- Shirky [44] put this challenge as complicated pricing method. Thus, it may not be accepted by both the buyer and seller of the system.

- The major concern for the User is the ease of use and security as most mobile devices use the blue tooth wireless technology that can be interfered in an open air wave.
- Out of all the highlighted challenges of micro-payment system, the biggest reason for its struggle and failure can be traced back to ***User disapproval*** due to lack of knowledge of what Buyer (user) and Seller actually need.

Therefore, for real growth to occur there must be open framework that will allow users to transact with any merchant over the Internet. Denis [6] pointed out that when the business and technology challenges are overcome; the benefits of micro-payment systems will be enormous, regardless of the micro-payment method. The critical success factor or key to success remains the volume of transactions. This volume creates a new scale of trading required and can only grow when some tough issues are addressed.

2.2 General Features of Electronic Payment Systems

In general and in practice, the requirements for any payment systems are as highlighted below:

1. **Validation**: this refers to the approach used to verify the medium of exchange between the buyer and the seller. This approach may involve the use (online) or without the use (offline) of a Trusted Third Party (TTP) during payment processing for payment authorisation.
2. **Efficiency** (storage size): the storage size requirement for the payment system has to be minimised as much as possible for greater efficiency.
3. **Security** in terms of
    a. Prevention of double spending: this is the ability to prevent buyers from using the same money (associated with their payword chain) to make multiple purchases. The payword chain must remain active at only one seller at a time and the same payword chain cannot be used to purchase from several sellers. Every spent coin needs to be authorised by the broker in order to prevent double spending.

b. Prevention of double depositing: this is with respect to the seller and it is the ability to prevent the seller from claiming the same money twice or several times from the broker during the redemption time (after the transaction)
c. Prevention of fraud: this is the ability to prevent the buyer from making a large number of purchases against an account with insufficient funds.
d. Forgery prevention: this involves the verification that the medium of exchange being sent from the buyer to the seller is authentic. This gives assurance to the seller that this medium can be redeemed at a later time with the broker.
e. Customer anonymity: this involves the ability to protect the identity of the participating parties in a payment protocol especially with respect to the customers or the mobile users.That is, the relationship between the buyer and their purchases is untraceable. Macro-payment schemes always compromise customer anonymity but this is usually preserved in most mobile payments in the same way as traditional cash payment.

2.3 Comparison between Macro-payment and Micro-payment Systems

According to Asano *et al.* [12], the major characteristics that distinguish both payment systems (Macro and Micro) are *less computational* (processing time) and *Storage cost or requirement.* Table1 illustrates the main characteristics of Macro-payment and Micro-payment systems.

Characteristics	Macro-payment	Micro-payment
Volume / Frequency	Low	High
Value (goods or services)	High	Low
Computational (Processing) cost	High	Low
Storage Cost	High	Low
Money Transfer	Large	Small
Validation	Online	Online or Offline
Cryptographic	Public Key	Hash Function

Table 1 Characteristics of Macro and Micro-payment Systems

2.4 E-Commerce versus M-commerce Micro-payment Systems

Electronic and mobile commerce micro-payment systems have certain common feature and commonality. However, the major difference between micro-payment schemes for e-commerce and m-commerce is that wireless communication technology added two more features to the existing e-commerce micro-payment scheme. These are ***mobility and accessibility*** for payments of low value and high frequency transactions.

Micro-payment protocols for wired e-commerce applications are not ideally suited for m-commerce applications on mobile devices. This is from the fact that current handheld devices have small displays, limited user input facilities, limited memory, and only low performance computational resources [19]. However, it currently seems that the gap between mobile and fixed devices regarding processing power is getting narrower [19].

2.4.1 Wired Internet versus Wireless Networks

The existing wired Internet is not applicable to Wireless Networks due to some factors. According to Agrawal *et al.* [23], the most significant difference is that data in a wireless network is transmitted over the broadcast medium, which can be received by all nodes in the vicinity.

Therefore, data transmission in an open network can easily be intercepted, altered and are prone to certain degree of risk from attackers such as lack of confidentiality, integrity, modification and repudiation. Also the communication pattern in a wireless network has limitations such as:

a. **Slower link (Frequency)**: there is usually a frequency limit for data transmitted in a wireless environment. Also the speed of connection and transmission from one node to another might be very slow.
b. **Battery power**: mobile and wireless devices are usually battery powered and have short life span. They need to be constantly recharged.
c. **Power constraints**: disconnected operations are very common in wireless networks [23].
d. **Limited bandwidth**: wireless networks have frequency restriction of receiving and transmitting data. Thus, they have very low performance rate compared to the wired network. The greater mobility of wireless local area networks (LANs) helps offset this performance disadvantage.
e. **Higher cost**: cost adopters and access point in a wireless network might be higher than that of cables, hubs and switches in a wired network. However, most products have dropped in price considerably with the release of 802.11, and obviously, bargain sales can be found if shoppers are persistent [50].

This section has been able to show clear distinctions between a wired and wireless network using several limitations of wireless network. However, due to increased efforts in the development of wireless standard, most of these limitations have been overcome [50]. For example, mobile computing provides high mobility and accessibility compared to fixed terminals of wired Internet. Mobile computers do not need to be tied to a fixed position and users can freely roam within the wireless local area network (WLAN) range

In addition, some WLANs protect their data through the use some encryption standard such as Wired Equivalent Privacy (WEP) that makes wireless communications reasonably as safe as wired ones in homes [50]. Table 2 below summarises the comparison of the wired and wireless network payment models.

Characteristics	Wired Network	Wireless
Cost	Inexpensive cables, hubs and switches; free software packages.	High cost of wireless adopters and access points. Cost may be three times higher than the wired.
Reliability	Have reliable cables, hubs, routers and switches.	Unreliable wireless signals which are prone to interference from other home appliances including microwave ovens, cordless telephones, and garage door openers.
Performance	Have ability to offer superior performance of higher bandwidth (although they might cost more).	Have limited bandwidth. The performance of most wireless connection usually makes use of access point.
Security	Hubs and switches connected in a wired network do not provide support for firewalls that is a major security consideration in this environment. .	The weaknesses of wireless security are more theoretical than practical. In theory, wireless signals are less secured. Signals in wireless network can easily be intercepted Over The Air (OTA).

Table 2 Summary of the Comparison of Wired and Wireless Networks

2.5 Focus on Micro-payment

Recently, m-commerce received attention considerably and it has potential for high growth rate. In a similar way with the electronic commerce, wireless e-commerce demands appropriate payment method and in order to allow "pay-per-use" of digital and physical content. Micro-payment systems (payment for high volume, low value transactions) are expected to play an important role.

Wireless communications development is expected to drive the demand for mobile payment as wireless e-commerce has many differentiating characteristics than the wired e-commerce based. There is a need to study and understand these attributes as they give more insight on why wireless micro-payments are very important and appropriate for mobile commerce [12].

Wireless e-commerce is believed to have many differentiating characteristics (suitable for micro-payment) than the wired e-commerce as this gives reasons why we need to focus on micro-payment schemes for mobile commerce payment. The four main advantages resulting through the use of wireless e-commerce and which provides support for micro-payment scheme are:

a) **Portability**: most wireless devices are easy to access and they can be used to make easy purchases by accepting few inputs from the users. For example, PDA has a special tool to perform hand-writing recognition. However, the type of purchase has to be for a very simple and cheap (low value) item. This attribute of a wireless device makes it easier to purchase low value goods such as a copy of wall street journal.
b) **Computational cost (cost effective):** macro-payment systems have higher processing cost as they are based on heavy-duty cryptographic and public key operations. Micro-payments are designed to use fewer computational resources in which the payment cost must be higher than the processing cost for purchases made.

c) **Security:** although low value items are prone to certain degree of risk from attackers but micro-payment makes it difficult for hacker to profit on a security breach for example a crime can easily be committed if its benefits outweighs the effort expended [8]. Also low value transactions deploy the use of hash functions and symmetric key operations as main cryptographic operations that satisfy most of transaction security properties.

d) **Interface:** Inexpensive products are usually easier to describe and have fewer components than the expensive product. Generally, hand held devices have small size and weaker resolutions which provides support to purchase and bill small amount of transaction Therefore, a wireless micro-payment will be appropriate for billing such low-valued transactions.

2.6 Summary

This chapter presented detailed review of two fundamental electronic payment systems (macro-payment and micro-payment). This chapter revealed that electronic payment systems are beneficial for the development of e-commerce. The fields and scope of electronic payments in respect to mobile commerce was presented. This incorporated the payment for very low value and high frequency transactions via mobile and wireless devices.

The two electronic payments were presented in detail bringing out their features/properties, requirements, advantages, disadvantages and comparisons. This chapter also revealed the main distinguishing features between micro-payment systems of electronic commerce and mobile commerce as mobility and accessibility. It was argued that mobile micro-payment schemes support the payment of downloading digital contents at anytime and at anywhere by being characterised with these essential features provided in wireless communication.

In addition, this chapter gave support why it is difficult to implement wired micro-payment schemes on mobile devices by comparing the wired Internet with wireless network. This chapter finally presented the reasons for focusing on micro-payment

scheme (not macro-payments) for mobile content payment in m-commerce. Therefore, the new mobile payment protocol to be proposed will incorporate the use of micro-payment system based on the information and findings of this chapter.

Chapter 3 Mobile Commerce System

Mobile commerce (m-commerce) is a type of e-commerce conducted through mobile devices such as mobile phones, personal digital assistants (PDAs) and other devices with a wireless connection [16]. In other words, it involves the use of the Internet for purchasing goods and services and also for transmitting messages using wireless mobile devices. M-commerce is rapidly expanding and is expected to be the second largest industry in the world by 2010 [46].

Many consumers have become used to making mobile phone calls anywhere **(mobility)** and at any time **(accessibility)** and m-commerce builds on that capability. In the short term, mobile commerce will be characterised by large volumes of transactions that are of low values and highly time sensitive [6] and that depend on the availability of mobile connectivity.

This chapter presents the conceptual framework for the development of a mobile commerce system. The various services and applications that could be deployed on wireless and mobile devices will be investigated. Mobile commerce payment systems will be discussed in terms of their various categories, channels and payment protocols. In addition, the general roles of mobile network operators (NO) will be enumerated in this chapter.

3.1 Wireless E-Commerce

Wireless e-commerce entails the integration of mobile communication with e-commerce. This could be defined as the integration of wireless networks with data communications combined with e-commerce. Today, with the proliferation of wireless networks, mobile devices and customers' increasing desire for more purchasing power and convenience, micro-payments come to have increasing relevance [13], [15].

Wireless e-commerce was initiated by the Wireless Data Forum (WDF) which is a leading trade association for the wireless data industry. The WDF was initiated and established for two main goals:

1. To help wireless industries to use the Internet to sell products and services
2. To help wireless industries to develop and extend electronic commerce products and services.

3.1.1 Essential Features of Mobile Commerce

Wireless communications technology provides the essential elements missing in previous micro-payment schemes: ***mobility and accessibility*** [18]. These are the two main distinguishing features added to existing e-commerce which make mobile commerce more flexible and convenient to general users of wireless micro-payment systems. Mobility and accessibility offer improved opportunities for promoting mobile business, especially to mobile device users, and to access information in remote areas as they roam about in different location. Users can easily access online information, services and products just as they were using fixed terminals.

Rather than being attached to the fixed terminals of personal or desktop computers, mobile commerce involves the use of wireless and mobile devices. This provides greater mobility of wireless Local Area Networks (WLAN) as mobile device users have more opportunity to access the Internet for Any low value item at Anytime and Anywhere (AAA). The Mobile device users do not need to be tied to fixed terminals (cable) and can roam freely within the WLAN range. The AAA syndrome couple with the volume of transactions will greatly increase user approval and adoption of mobile commerce micro-payment systems.

3.1.2 Benefits of Wireless Communication

According to Adelstein *et al.* [17], the main advantages resulting from the adoption of wireless communication include:

- The reduced cost of not providing cabling for wired connections: e-commerce involves various connections of wired cables and installation of additional software for Internet access.

- The flexibility of mobile connections: wireless communication provides much greater flexibility in connecting mobile and wireless devices in a wireless network.
- The freedom to deploy individual sensors anywhere: provides easy access to usage of wireless and mobile devices as their users roam on the network.

3.2 M-Commerce Technologies

M-commerce is built on several key technologies. Some of these technologies are very well established while others are much newer and less common. In general terms, technological advances will allow a payment scheme designed to address one problem - payment for digital content to be applied to physical world payments [6].

3.2.1 History of Mobile Phone Technology

In the short history of the number of changes in the standards mobile phones, three generations are distinguished [16]. The first generation (1G) was based on analog phones which are primarily used for making voice calls. As digital systems were not yet available, more analog standard followed with analog voice transmission. Most analogue networks were later switched off by 2000 [19].

Second generation phones (2G) use of digital technologies that are commonly used today. Apart from voice transmission, the services offered include fax, data transmission via modem and electronic mail [19]. After this, came the development of 2.5 generation (2.5G) digital phones that support the transmission of data using General Packet Radio Service (GPRS).

More recently, the 3rd generation (3G) digital phones support both voice and data transmission at greatly increased speeds. 3G combines both the features of 1G and 2G mobile phones standard. The concept of GPRS and 3G wireless technologies represent a shift from voice-centric (like Global System for Mobile Communications-GSM) to data-oriented services [25].

The development of m-commerce focused on the use of 3G phone technology since 3G supports services that are not possible with earlier technologies. 3G services include:

- Video calls that can be made and received from other 3G mobile phone users.
- Video and other types of media such as music can easily be downloaded to play on a mobile phone.
- 3G phones often have cameras which can take and transmit digital pictures.
- Some 3G mobile phones have colour screen display and graphical user interfaces.

3.2.2 Types of Mobile Phone Technology

The various types of mobile phone technologies in existence will be presented in this section:

- **Wireless Application Protocol (WAP)**

WAP builds on digital phone technology that allows users to access information instantly. WAP enables mobile devices to browse the Internet because the web browsers built into these devices support hypertext markup language (HTML) and extensible markup language (XML). These two languages are commonly used for Internet content. WAP-enabled devices run what are called **micro-browsers.** These are applications that suit the small memory size of handheld devices and the low-bandwidth constraints of a wireless-handheld network.

- **Short Message Service (SMS)**

SMS is another important m-commerce technology that allows short text messages to be sent to and from mobile devices at low cost [16]. Mobile phone users can alternatively send or receive simple text messages rather than making phone calls (voice call or message). This service also has a wide application in m-commerce technology.

- **Bluetooth Wireless Technology (BWT)**

BWT has a specification for short range, low cost and small form-factor that enables user-friendly connectivity among portable and handheld personal devices, and provides connectivity of these devices to the Internet [42].

Thus, Bluetooth-powered mobile devices are a promising tool for micro-payments over the network because Bluetooth technology can easily offer ***accessibility and mobility*** to mobile users [18] and is considered more secure than most other wireless technologies.

3.3 Wireless and Mobile Devices

With the growth of mobile computing technologies, the popularity of mobile devices such as mobile phones and PDAs has increased over the past few years. A wide range of software applications can be deployed on these mobile terminals and can communicate with other applications or information systems through a wireless network.

The potential role of using wireless and mobile devices to access the web is enormous. Mobile devices are appropriate instruments to support payment for low value and high frequency transactions. In addition to this, they act as the channels through which m-commerce payment can be made feasible.

These transactions may involve multiple vendors as mobile users move from site or vendor on the Internet to another. Although mobile users cannot use their credit card as a mobile phone but soon they will be able to use your phone as a credit card [18].

3.3.1 Types of Wireless and Mobile Devices

There are no specific categories or classification for existing wireless and mobile devices in terms of their weight, size, shape and computing power. Jochen [19] gave some list of examples of wireless and mobile devices graded by increasing performance (CPU, memory, display, input devices) as follows:

a. **Pocket computer:** this device offers tiny keyboards, color displays and simple versions of programs (spreadsheet, text processing) found on desktop computers. They are the next step towards the invention of full computers
b. **Pager:** has a tiny display for short text messages but cannot send any messages.
c. **Mobile phones:** are devices with text display which can send or receive voice or short messages. Recent model mobile phones can display color graphics, have a touch screen and Internet browsers. More advanced models have the ability to be

used as payment instruments for mobile commerce. The tremendous success of mobile phones replaced is making the pager redundant in many countries. Short messages sent on mobile phones have replaced paging.

d. **Personal Digital Assistant (PDA):** this is a device which uses a pen (as input device) with built-in character recognition for translating handwriting into characters. These devices offer a simple version of office software such as notepads, mail. Software packages and web browsers are also available for them.

Amongst all the above named devices, the use of mobile phones and PDA will be adopted for payment system in mobile commerce environment. The most distinctive advantages of wireless or mobile devices for use in electronic commerce are ***ease of access*** and ***convenience of use*** [12]. These are used:

1. To bridge the e-commerce world and the physical world by giving consumers a pay-as-you-go service option via mobile phones.
2. To offer mobile payment for vast market in dying world where mobile phones rather than computers are the main mode of connection to the Internet.

3.3.2 Features and Limitations of Mobile Devices

Wireless connections provide lower bandwidth, require more power from the nodes and are less reliable than traditional wired connections [17]. Therefore, in considering the potential benefits of m-commerce, we should also consider certain resources (memory, security, communication facilities and battery power) that limit mobile devices. These are:

1) **Speed**: mobile solutions will probably never be as fast as fixed-connection unless advanced technologies such as 3G services are implemented on them.
2) **Size**: mobile devices such as mobile phones are small in size and have weaker resolutions. Therefore, it might be difficult to view large complex diagrams with lots of details on them as they usually have smaller displays compared to fixed devices such as personal computers.
3) **Capability**: wireless devices have weaker internal processors, less memory and are unable to perform power intensive tasks (low performance computational

resources). They have much less storage capacity compared to devices in a fixed environment.

4) **Interface:** Mobile devices have limited user input facilities to enter text messages unlike the keyboards used in fixed terminals.
5) **Security / Privacy**: a wireless device is easier to eavesdrop on during conversations in public areas (over the air-OTA). As a result, security can be compromised if conversation is unencrypted. Micro-payments can replace cash to some extent and because of this there are possibilities for fraudulent and criminal use such as money- laundering [16].

3.4 M-commerce Services and Application

The main focus of wireless applications today is on the download of digital content such as music, information and games. Mobile commerce applications provide transaction-based services. These applications enable users to securely purchase goods and services via their mobile devices.

However, future pervasive wireless connectivity will create new opportunities for commerce to provide new services [6]. These services are categorised as follow:

- **Transaction-based services**: This involves purchasing of goods and products such as stocks, concert tickets, music, or games; searching for the best price for an item using a cell phone and buying it in a physical store or on the Web.
- **Information-based services**: various information based services such as sending and receiving email; instant or text messaging, searching for a movie or restaurant can be made available trough the use of a cell phone or handheld PDA.
- **Location-based services:** Tourists and other users can use their mobile phone to find out about their present location and consult a map of their intended destinations. This service is otherwise known as Geographic Positioning System (GPS) and it may incorporate location based services such as database lookup or proxy services.

- **Personalised services:** Services that anticipate what a customer wants based on that person's location or data profile, such as updated airline flight information or beaming coupons for nearby restaurants.

3.4.1 Mobile Content Providers

There are many goods and services that can be provided by content and service providers in mobile commerce or micro-commerce. We have discussed some of them above. Jones [28] classified providers and their respective intangible goods as follows:

1. Traditional content providers of newspapers, magazines, clip art, book and music publishers.
2. Individual content providers of personal essays, cookbooks or access to similar shared resources.
3. New content providers of shopping agents, buyer and seller brokering, interactive games, search engines, micro-gambling and currency conversions

3.4.2 Wireless E-Commerce Scenarios

There are many wireless e-commerce scenarios in existence and more are expected to emerge, as the volume of transactions in mobile commerce is a key success factor for micro-payment. Consider a Mobile device User using the mobile device to perform the following Tasks:

- Reading both free and pay-per-click web sites on the device browser such as headlines of news article.
- Purchasing images, videos, music clips and ring-tones.
- Purchasing tickets wirelessly (without the physical presence at the site of concerts) for concerts and booking reservation seats for concerts or plays.
- Making available pictures and videos for others to use or possibly purchase.
- Accessing various information sources for tourism such as finding the map of a present or future location; weather forecast broadcast, shopping such as finding outlets or a list of sales in the vicinity.
- Downloading of games or ringtones onto mobile devices like phones and played on the move.

- Downloading music so that the phone becomes a portable music player to be used anytime.
- Pictures can be used as backgrounds to accompany ringtones or just as entertainment; short video sequences onto 3G devices, opening up the sports and pop video marketplace for phones [48].

3.5 M-Commerce Payment Systems

Electronic commerce and payment systems have been in existence for many years. Many of these involve the purchase of online content such as services, information and commodities on the Internet via wired or fixed devices and terminals such as desktop and personal computer.

In recent years, the use of mobile phones has spread quickly. This is especially common in places where connection to a fixed device is not available, cannot be afforded or reached. For example, there is growing popularity of acquiring and using mobile phones in developing countries where users find mobile phones more affordable.

In addition, the use of mobile handsets as a payment device for purchases of information content is spreading. This includes the use of mobile phones for payments for low value items of high volume such as games, images (graphics), reservations, clipart, ring tones or multimedia, video clips, music, weather forecasts, tourist locations and news.

Wireless micro-payments are payments schemes designed for small transactions of digital money spent wirelessly using an integrated wireless modem for its transfer in exchange for services or contents from hand-held wireless devices. Mobile wallets are very useful and they can make shopping more efficient.

3.5.1 Revolution of Mobile Commerce Payment Systems

The key to commercial innovation in wireless services is payment [6]. Researchers have paid greater attention to payment issues in recent years. The demand for digital or wireless content might not only bring a revolution in payment, as a larger scale of trading

community ***(high volume of transaction)*** is presumed to provide the scale of trading community required for successful micro-payment. Therefore, in order to bring about change in how payments are made, there is need to consider other wireless enabled services and applications.

With the development of m-commerce, more and more content providers are switching from free content or services to a subscription-based paid model or pay-per-click model, largely reducing the revenue gained from the advertisement market. These revenues will mostly add up from the payment of the individual products only being utilised rather than subscription method of underutilised products.

Current payment systems include using a credit card approach, a subscription-based (pre-paid) mobile account, billing or a micro-payment strategy. Subscription-based approaches, whether administered by the mobile account provider or by the vendor have the major disadvantages of being limited to a subset of vendors (or a single vendor) and paying for bulk content and services that may not be fully utilised.

Therefore, the ability of consumers to buy inexpensive items conveniently (anywhere and at anytime) would eliminate the need for buyers to pay large subscription fees for the entire sets of material when they only want selected pieces of content [14]. Users of subscription based approaches might prefer other options to pay only for the content or services they utilise.

Alternatively, several micro-payment protocols and schemes have been proposed for m-commerce [11], [25], [26], [29] based on different cryptographic operations. Several of these schemes are not appropriate for **payment to multiple vendors.** This is a key factor in the payment of low value, high frequency transactions. In a micro-payment system, a large number of users are expected to access a variety of content, information and services as frequently as possible provided by a range of providers.

In the next few years, users of mobile or wireless devices will find it more convenient to purchase a range of goods and services such as digital content of low cost from various service providers using a mobile device just the same way as they would in the real world when making purchases with real money. This expectation will be considered as part of the backbone for the new protocol to be proposed in this thesis.

3.5.2 Micro-payment Demand for Mobile Commerce Systems

Mobile micro-payments are already in use and have reached the market place in regions such as South Korea, Japan and Hong Kong as well as Western Europe [18]. For example, in the year 2003, there was a significant expansion in the number of micro-payment schemes using mobile devices to facilitate payment for electronic newspapers, car parking fees and subway tickets in some part of Asia and Western Europe.

The existence and use of mobile micro-payment provides more markets for mobile commerce systems. Well-established markets for mobile transactions, in addition to various service and content providers, are believed to be essential prerequisites to reach high usage rates for mobile payments [18].

In the next few years, the market for low value items such as web pages, ring tones or multimedia clips and online content (music and videos) is expected to grow substantially [11], [14]. Also, intangible goods such as information (articles, clip arts and music tracks), software (computer games), metered access (databases, applications) or other common services are paid for, but the price is generally so low that conventional payment methods would be clumsy and overly complicated. Instead they rely on micro-payments [16]. Therefore, to allow "pay-per-use" of such content, micro-payment systems are expected to play an important role.

3.5.3 Categories of Mobile Payment

Mobile payments may be characterised into various categories as transaction type, transaction settlement type, content type and content value [22].

A. Transaction Type

- ***Pay per Unit***: the Mobile User pays for each unit of content (in terms of duration or volume) provided by the Content Providers. The payment (in terms of amount of units) may be per byte or per minute of viewing or accessing content such as music tracks, games or streams of video on the Internet.
- ***Pay per view***: the Mobile User pays for each view or increment of the desired content such as video clips.
- ***Flat rate***: the Mobile User pays a recurring periodic amount to access content such as online magazines or newspaper articles on an unlimited basis during the period.

B. Transaction Settlement Type

- ***Prepaid (pay-before) payment system***: the mobile user pays in advance of obtaining the goods or services with a prepaid account or token which is deducted after each payment session or during redemption time. This involves the use of electronic purses and wallets, electronic cash or certified checks for transaction payments. There has been substantial increase in the number of prepaid systems in use today. Examples include Webcent, Softpay and Bitpass.
- ***Pay-now payment systems***: the mobile user pays for service through debit cards. According to Denis [6], debit cards are more efficient for low value payments, but most are designed for physical world use (requiring PIN authentication in hardware) and not virtual transactions.
- ***Post-paid (pay-after) payment system***: the mobile user receives and uses the services or goods before they pay for it. The mobile user is billed after the access to the content is obtained such as in a billing system. This system requires a long-term contract with consumers in which an evidence of money source should be provided [20]. This policy makes it difficult for those who do not have such evidence to use this payment system. An example of post-paid system is "Click & Buy".

C. Content Type

The Mobile User pays for varieties of content such as:

- *Digital goods* (downloadable music, video, information).
- *Physical goods and services* (books, clothes).
- *Ticketing* (plane, cinema, and train).

D. Content Value

The customer pays for content provided by the content providers in terms of the value (monetary value) of transactions:

- **Macro-payment**: is characterised by high monetary value transactions.
- **Micro-payment:** is characterised by low monetary value purchases.

3.5.4 Channels for Mobile Payment

A payment system should be as convenient and secure as using a credit card (as for macro-payment systems) and as anonymous as using cash [22]. To make payment transactions over mobile channels, **a mobile payment platform** is required. Typically this incorporates a wallet server, and a means of routing transactions to a payment instrument such as a bill, a stored value account or a payment card [6].

According to Wael [8] and Denis [6], wireless micro-payment systems can be classified by the use of operator billing, digital wallets (Electronic-cash or e-cash) techniques, credit card and direct payments. To be precise, buyers of low value digital content make purchase by either a prepayment approach or billing method.

The following subsection presents present each of these classes and approaches to payment in more detail.

A. Operator Billing

Today, a mobile user can use mobile phone bills to pay for services ranging from ring tones and logos to Java games and car parking [6]. Mobile network Operators (NO) are experienced at billing small value transaction and their charges are usually based on individual users. They can track the usage of the service at any location.

Prior to the transaction process between the consumer and the service providers (SP), the SP must have an agreement with the NO. The consumer initiates a transaction with the NO and receives the service or product. The NO pays the SP and at a later time or specified period, the consumer receives a bill from the NO after making (numerous) small purchases. Examples that are in use today are VodaPhone's *mpay bill* in Europe, Cingular wireless *DirectBill* in the US, AT&T wireless, One Connect's *mONE* payment in Austria, Paypal and NTT-DoCoMo in Japan.

However, there are risks and limitations to this approach. The NOs need to carefully consider that they are not liable to transaction payments for which they cannot directly collect the funds. The business users are at greater risk of increased costs of non-related services[4] which they may be held accountable for [6]. One solution to these problems might be for the SP to track customers' purchases and they consider the benefit of doing this not to justify their expended efforts or investment.

B. Digital Wallets (Prepayment)

The digital wallet is similar to the prepaid method. At the initial stage of making purchases, the consumer exchanges money for digital cash and stores the digital cash in the device (mobile). The consumer then purchases a service and pays with the digital cash previously stored. The vendor later exchanges the digital cash for real money from the bank.

On the other hand, the mobile user might as well give single vendor large prepayments that would cover multiple purchases [14]. This could be termed as a subscription method of payments.

[4] These are non-beneficial costs incurred due to mismanagement of business resources such as the misuse of voice and data calls by employers for non-business purposes.

C. Credit Card

This approach is very similar to web payments whereby the vendor delivers a product and then bills the credit card company. According to Dennis [6], the use of credit cards as a channel for mobile micro-payments are classified into two types

a) Top-up of prepaid accounts using a payment card or bank account: this involves the use of a cash based system at point of sale.
b) Authentication for non face-to-face payment transactions: The mobile phone offers a personal and secure authentication for Internet and other non face-to-face modes of payments.

3.5.5 M-Commerce versus E-Commerce Payment Scenarios

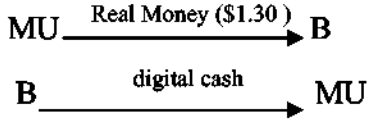
Consider a trading community consisting of the broker (B), Mobile User/Customer (MU/C) and Vendor (V). The major roles of these participants have been discussed in Chapter 2 (section 2.1.2). In this payment scenario, B is assumed to be a honest party and trusted by other participants. This trading community engages in the sales of downloadable music tracks (electronic music) and it is assumed that the first music track costs 30cents, second music track costs 52cents and the third one costs 48cents.

In the current mobile commerce payment system, MU can access these downloadable music tracks by billing or a micro-payment strategy.

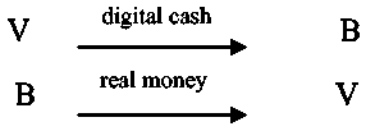
The billing approach incorporates the usage of a Network Operator (NO). Prior to the transaction between MU and V, V must have a contract (agreement) with the NO. MU initiates the purchase of the first music track (30c) with the NO. The NO responds to MU's message by allowing MU to download this track from the specified V. The NO pays V for this service being made available or provided to MU. MU can make further purchases of the second (52c) and third (48c) music tracks in a similar way from V(s). At a later time, the NO later sends an aggregate bill of $1.30 to MU at a specified period for the three music tracks downloaded.

For the micro-payment approach, the method could either be through the use of a digital wallet or a pre-paid account.

For the digital wallet, the MU exchanges real money for the digital cash with B and stores this digital cash as electronic wallet (e-wallet) on the mobile device.



MU purchases the first music track and pays 30cents (digital cash equivalent) to V
MU may wish to continue to purchase the second (52c) and third (48c) music tracks using the same method. At a specified time, the V(s) exchanges the digital cash for real money from B



On the other hand, MU may decide to use the pre-paid account method to offer a single V large prepayment for several purchases this method is known as the subscription method.

However, in a conventional e-commerce, the downloading of music tracks is usually done by a micro-payment method. This macro-payment approach involves the use of prepaid account. Prior to service utilisation, C opens account and deposit funds with B. C authorises B to transfer money from his/her account to V's account whose service(s) is being utilised. The prepaid system is a debit-based approach.

C logs to the website he/she wishes to access for the first music track, the amount (in terms of volume or duration of each music track) is being deducted from this large prepaid account. This approach has a major setback as V is limited to a subset of Vs and the service paid for may be under utilised. The Table 3 below summarises the comparison of the payment approach of m-commerce and e-commerce.

Properties	M-Commerce	E-Commerce
Payment System	Micro-payment (prepay) and billing	Macro-payment and Micro-payment
Liability	High (NO may be liable to pay if MU refuses to bay after service utilisation)	Low (users pay upfront before they can access services or information)
Mobility	High (users can roam about a range of location to download service or information)	Low (users has to be connected to their PC in a fixed terminal to access information)
Accessibility	High (provides great support to access any service at anytime)	Low (provides less support to access service at anytime)
Utilisation	High (all services paid for are being fully utilised)	Low (subscription method restrict users to access a set of service which might not be fully utilised)
Transaction cost (operational)	High cost associated to access points and wireless adopters	Low cost of cables and some sites have free packages

Table 3 Summary M-Commerce and E-Commerce Payment Scenarios

3.6 Payment Protocols

Payment protocol involve the mechanisms for payment approval by the mobile user (MU) where the MU agrees to pay and payment authorisation by the payment service provider (PSP) who indicates that there are enough funds to cover the payment [22].

In most micro-payment systems, the MU contacts the PSP to approve the payment and to request the PSP to authorise the payment order (PO). The PSP sends the authorised PO as a response to the MU who later forwards it to the vendor or merchant.

In this thesis, the main focus will be on the micro-payment protocols and their applicability to wireless environments because the payment protocol plays the most important role in any payment system. Payment information systems can be categorised into two types based on the medium of value exchange or the organisation of the money transfer: *account-based* and *token-based* electronic payment systems.

3.6.1 Account-Based Mobile Payment Protocol

In the account-based system, the mobile user and the merchant set up accounts with the broker as a kind of contract before the execution of actual transaction payment. The mobile user authorizes the bank or broker to transfer money from their account to the vendors account during the payment-clearing period of transaction. This is similar to the banking system in the physical world.

This protocol uses symmetric-key operations with lower computation demands and also satisfies transaction security features provided by public key based payment protocol such as SET and iKP. This could be either a credit-based (SET credit-card payment scheme) or debit-based. The debit-based approach is usually based on a prepaid account as opposed to an electronic-money (e-money) account. The users of a prepaid account purchase a service from the phone company and utilise it over time.

However, this approach is not very convenient for mobile users as they have to prepay separately for different services they wanted to access and purchase. Thus, there is a need to shift from the prepay approach to e-money based or stored value in order for mobile users to use the stored funds (value) to access in an open network.

3.6.2 Token-Based Mobile Payment Protocol

The 'token' or 'digital coin' can be referred to as the micro-payment instrument and this can be an encoded, signed and encrypted field in a payment protocol message [24]. In the token-based payment system, the customer exchanges real money for payment tokens (e-coins) from a broker (who deducts the equivalent amount from the customer's account) to pay the vendor for services or information. At a specified time or at the end of the

transactions, the vendor sends (redeems) the received tokens to the broker who exchanges them real money.

The main advantages resulting from the use of this protocol with respect to users of the system are highlighted below:

a. They have lower communication and operational cost than the account-based approach as it does not require a customer's payment authorisation from the bank in every transaction. The Broker does not have to be involved in the payment process for every transaction.
b. From the mobile users' perspective, this approach is more convenient as they can use stored tokens to pay for a range or different (varieties) of goods and services (such as digital content) of low value.
c. Also, this approach ensures that users can only spend money they have, and transactions can thus be processed quickly over any channel [6]

The token-based payment system is suitable for low-value and high-frequency transaction payments (micro-payment). This could be either a debit-based (pre-paid) or credit-based (postpaid) payment system.

A. Debit-Based Approach

This approach requires the customer or user to purchase payment tokens by requesting the bank to debit (deduct the real money from) her account in order to receive the payment tokens in return. The client can spend the payment tokens with vendors for different mobile services or information as they visit make purchases. This method assures the product providers of getting paid by the broker for their services or goods. The merchants collect the payment tokens and redeem the money from the bank at a later time.

B. Credit-Based Approach

There is no direct certification by the bank in this approach. The user is permitted (by the bank) to generate payment tokens by herself and spend them up to the credit limit specified to each vendor. The user's account will not be debited until the redemption of

funds takes place. At the end of a cycle or number of transactions, the vendor redeems all the received payment tokens for real money from the bank.

3.7 Mobile/Network Operators

Network operators (NOs) are well suited to deliver payment services for mobile content due to their expertise in the area of billing [22]. Further, Denis [6] indicated that as the owners of the licensed spectrum, NOs are well placed to take advantage of mobile commerce opportunities. They have the need and ability to tackle the micro-payment challenge using their billing and roaming experience to provide efficient processing of low value transactions.

The NOs find processing micro-payments to be simpler and cheaper as transaction values are lower. They are not expected to generate revenue from payment processing as the benefit will come from airtime and revenue sharing for the services enabled by the payment scheme [24]. They do not have to work within the confines of the model developed by banks and do not require strong user authentication from mobile users as the possession of a mobile device may just be enough and transaction exceptions (such as reversals and credits) can be minimised. Also, the incidence of fraud and disputes will be lower [6]

However, the immediate problem facing NOs is the monetisation of digital content [6]. The NOs are uninterested in acting as payment brokers as they will be faced with investing heavily on such payment models. Operators can use their existing billing systems and customers' accounts to act as micro-payment providers. Thus, most issue and activity in mobile payment revolves around the need for micro-payment. In the next few years, NOs are expected to offer one or more micro-payment option(s) - billing and stored value. Their choice will depend on their market profile and regulatory environment. Charging and payment are at the center of wireless data systems and form part of their infrastructure [6].

Wireless carriers employing their customer base, technical know-how, and billing experience will play an active role in the mobile payment market as mobile users' access their networks to perform all transactions [40]. Further, as the role of wireless carriers increases, the tensions between the wireless carriers and banks [41] as well as the new strategic alliances will become more prevalent.

3.7.1 Major Roles and Duties of Mobile Network Operators

The roles of mobile network operators (NOs) cannot be over emphasised in the context of mobile micro-payment design. They perform the following tasks:

- Manage point-of-sale accounting for their clients such as purchases by monthly phone bills or direct payment "pay as you go" accounts.
- Handle the direct sale formalities such as customer authentication, payment processing, response processing.

3.8 Summary

This chapter presented the overall view of the conceptual framework. The history of mobile technology and various services and applications that could be deployed on mobile and wireless devices were presented. Of all these devices, more emphasis was laid on the use of mobile phones and PDAs as the most common devices used for accessing information, services and commodities on the Internet. These two devices can be used extensively for the purchase of downloadable items such as music, video clips, articles, tourist information and news on the Internet.

Wireless and mobile devices are appropriate instruments for mobile commerce payment systems. This chapter also presented some wireless e-commerce scenarios that a mobile device user can perform via their devices. Although they have certain features that may limit their usage for macro purchases, they are well-suited to deliver payment for low value and high frequency transactions.

This chapter also discussed the revolution in mobile commerce and success for micro-payment as the volume of transaction and user approval. In addition, micro-payment

schemes are viewed to be in high demand to provide more markets for mobile commerce systems. Different categories of mobile payment were presented and argued that a prepaid approach will best suit the purchasing of digital content in a mobile micro-payment system.

The reason for adopting a prepaid debit based approach is to limit the fraud possibilities by guaranteeing the payments for service or content providers prior to goods and service utilisation [20]. The appropriate channel for a mobile micro-payment system was presented and critically observed that the usage of digital wallet will best suit a prepaid system for the new protocol to be proposed.

In conclusion, it is obvious that the adoption of a token-based approach (debit-based type) will be most appropriate for the intended propose mobile micro-payment protocol to be discussed in Chapter 5.

Chapter 4

Micro-payments Models in Mobile Commerce

This chapter presents an overview of three micro-payment systems designed for mobile commerce applications [11], [25], [26]. This involves critical examination of how existing and competing mobile payment systems work and how various cryptographic techniques have been applied to them.

We will present the main functional characteristics of existing wireless micro-payment systems and evaluate their strengths and weaknesses by comparing and contrasting them. This involves critical examination based on certain requirements and criteria peculiar to micro-payment systems

4.1 Mobile Commerce Token-based Micro-payment Systems

The choice of payment system suitable and appropriate for mobile commerce (micro-payment) had been discussed in chapter 2 of this thesis. Apart from taking the volume and value of information, services and commodities into consideration, this choice depends on the micro-payment features and characteristics (technical, non-technical and extended) enumerated in chapter 2

Micro-payment systems can be used to support payment to vendors from customers in client-server networks. There are a number of micro-payment systems for fixed or wired client-server networks in various stages of development from proposals in the academic literature to systems in commercial use [2], [7], [9], [10], [30].

As a matter of fact, electronic micro-payment systems were originally designed for fixed (wired) environments. They cannot therefore be directly applied to wireless environments due to a number of limitations discussed in chapter 2 (section 2.4.1). To overcome such limitations, several payment models and protocols have been proposed for mobile or wireless commerce.

In recent years, there has been little ongoing research or projects on micro-payment models suitable for mobile commerce payment [1], [11], [25], [26]. Table 4 shows the year of inception for various protocols or models of mobile micro-payment. Most existing mobile micro-payment models were either design:

a. To migrate the existing fixed network payment systems to wireless networks or
b. Specifically for wireless networks.

This chapter will discuss and focus on existing micro-payment models that were designed originally for wireless networks. Most micro-payment models for mobile commerce have common goals and are based on the following considerations:

1. They take the constraints of wireless environments (emanating from mobile device or wireless networks) into account.
2. In order to reduce their communication and computational load, various kinds of *lightweight cryptographic techniques have been applied to them.*
3. They focus on the payment protocol (mechanisms for ***payment approval*** by the customer who agrees to pay; and ***payment authorisation*** by the payment service provider), which have to be lightweight and provide sufficient security.

Mobile Micro-payment Protocols	**Year of Inception**
Zheng's Model	2002
Boddupalli's Model	2004
Zhu's Protocol	2004
Mobile NetPay Protocol	2006

Table 4 Summary of Mobile Token–based Micro-payment Systems

4.1.1 Basic Notations and Terminologies

The following basic notations will be adopted to describe the transaction and payment flow for the existing models (protocols) for mobile payments:

MU →	Mobile User
B →	Broker
V →	Vendor
NO →	Network Operator
MU → B	Mobile User sends a message to the Broker.

One-way Hash Function - hashing is one of the mechanisms used for data integrity assurance. Hashing is based on a one-way mathematical function, which is relatively easy to compute but significantly harder to reverse [51]. A hash function takes a long string (or message) of any length as input and produces a fixed length string as output, sometimes termed a ***Message Digest*** (MD).

There is no practical way to calculate a particular data input that will result in a desired hash value, so it is also very difficult to forge in a well designed one-way Hash Function operation [52]. Authenticity and integrity of data are guaranteed by applying a one-way hash function. Functions intended for strong cryptographic hashing, such as MD5 [49] have to be one-way and collision-resistant. They are commonly used as stock hash functions.

4.2 Evaluation Criteria

The evaluation criteria for existing mobile payment protocol comparisons are based on several factors. Comparison criteria are also based on selected references [6], [27]. However, for a more comprehensive evaluation and comparison of the systems the readers can refer to Párhonyi *et al.*. [9] for a thorough description of criterions 1-4 in this section.

The following criteria will be used to evaluate each of the mobile micro-payment models outlined in this chapter.

1. ***Security***: refers to the approach used for preventing and detecting attacks on a payment system and the protection of sensitive payment information. This could be double-spending detection, fraud attack detection and prevention, and avoidance of forgery.
2. ***Privacy/Anonymity***: refers to the protection of personal and payment information and it also entails the protection of the identities of the participating parties in a payment protocol especially with respect to the customers or the mobile users. Preservation of customer anonymity makes mobile payments more like traditional cash payment – whereas subscription-based payment or heavy weight credit card payment almost always compromises customer anonymity.
3. ***Support for multi-currency and range of payment:*** the ability to support multiple currencies by converting them within or outside the system. This also entails the specification of the minimum and maximum payment values allowed by a system.
4. ***Validation (online/offline) and communication load***: this is the ability of a payment system to process payments with or without the need for online contact with a third party (broker) for verifying the payment tokens during transactions. Online validation means that the vendor needs to contact the broker for each payment while Offline validation does not involve the broker for payments. This validation factor affects the frequency of communication between the broker and the mobile user involved in the transaction payment. Offline payment always reduces transaction costs and the communication load with the broker.
5. ***Ease of use:*** this is the ability to use the system easily without being familiar with the system's user interface and/or without requesting any information on identification or authentication (such as PIN number or login) at each transaction.
6. ***Transferability:*** ideally the e-coins used for payment should be transferable between vendors to enable users to benefit from the same electronic coins to make payments to multiple vendors or merchants. The e-coin should be flexible enough to make multiple purchases and should not be specific for payment to just a single vendor.

7. ***Divisibility:*** this specifies the minimum and maximum payment values supported by the system. Ideally, the system should be able to support a range of payment values and multiple denominations.
8. ***Disconnected Operations /Robustness***: this refers to the ability of users to continue accessing services or information during temporary failures or disconnection of the system /network/broker/vendor or any authoriser's down-time.

4.3 Zheng's Mobile Micro-payment Model

Zheng's model provides support for online mobile micro-payment with the use of payment tokens [11]. This is an electronic cash payment based on Brands' restrictive blinding signature to ensure untraceability. The signature of this model is an electronic payment token[5].

The various roles for payment transactions are performed by three entities: MU, B and V, as shown in Fig. 1 below.

[5] A payment token must contain a number to indicate its value and its recipient name similar to a cheque in the real world.

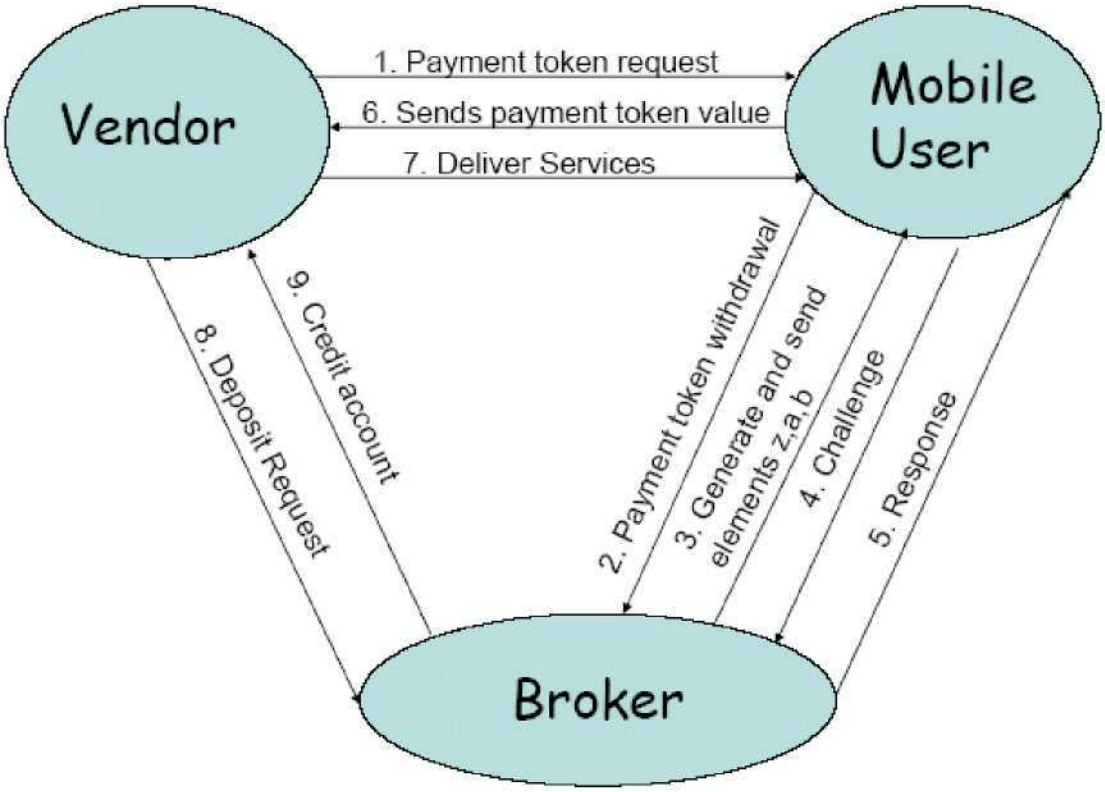


Fig. 1 Transaction Flow in Zheng's Mobile Micro-payment System

4.3.1 Zheng Model Transactions

The following is an outline of how this model works.

(i) Payment initialisation Protocol

- MU first opens an account with B and must prove ownership of the account before he can withdraw a payment token from B.
- B chooses a generator g, selects a secret key x which is kept secret, and also selects a collision hash function ***H (…).***

(ii) Payment Token Withdrawal Protocol

- V asks MU to provide /issue a payment token and makes sure that B issues this payment for MU to pay him as shown below:

  V → MU **M1= payment token request**

- MU sends a digitally signed payment token withdrawal request to B. MU, B and V all participate in this withdrawal process.

MU → B **M2=payment withdrawal request**

- B signs this value with MU's secret key x. B generates a random number w and sends the elements in M3 below to MU:

  B → MU **M3= $z=value^x$, $a=g^w$, $b=value^w$**

- MU generates a challenge c, by using four random numbers (s, t, u, and v). These numbers are used to blind (conceal) messages sent between MU and B. MU computes the hash value c′ = H (value s, t, z′, a, b′, rm) and sends c to B:

  MU → B **M4=c** where c=c′/u mod q.

- B replies with a response r=w+cx mod q:

  B →M U **M5=r**

(iii) Payment Protocol

This involves the interactions of MU and V in the following way:

- MU uses both *c* and *r* from M4 and M5 above to validate the payment token sent from B and can then accept the signature.
- MU can hide this signature by computing r′=ur+v mod q. Thus the payment token is the pair {value, s, t (z′, a′, b′, r′, rm)}
- MU sends the payment token to V:

  MU →V **M6= {value, s, t (z′, a′, b′, r′, rm)}.**

- V calculate and validate the payment token with B. V makes the service available to MU if it is valid:

  V→MU **M7=Service download.**

(iv) Deposit Protocol

V interacts with B in this protocol.

- V sends to or deposits with B:

  V→ B **M8=Deposit request.**

- B validates the payment token and checks the database to see if it has been previously deposited. If not, B credits V's account and adds the pair to his database

  B → V **M9=credit account.**

4.3.2 M-Commerce Payment Scenario using Zheng's Model

Using the same example of downloading music tracks of section 3.5.5, Zheng's model works in the following way:

MU send a purchase request of music track 1 to V. V requires 30cents to be sent by MU and ensures 30cents is issued from B. MU sends a withdrawal request (of 30cents) to B in which all participants are involved. B generates g=30c and signs g with MU's secret key.

MU generates the challenge (c) and computes h(c) = c' and sends to B. B replies with response (r). MU uses (c) and (r) payment token (30cents) validation sent from B. MU computes r' to hide payment token and sends the payment token to V. V accepts this payment token and delivers the first music track to MU.

This system does not support multiple payments to a range of potential vendors. Thus, if MU wishes to make further purchase of the second and third music tracks, the above defined process has to be repeated.

4.3.3 Evaluation of Zheng's Mobile Micro-payment Model

The eight criteria in section 4.2 will be used to evaluate the effectiveness and efficiency of Zheng's mobile micro-payment model as follows:

- ***Security:*** Without knowing the secret key of B, it is impossible to forge a valid payment token. MU cannot overspend or double-spend a valid payment token as M keeps records of the received tokens to avoid MU sending them twice. V cannot double deposit because B stores the payment token received from V to his database.
- ***Privacy/Anonymity:*** The privacy of MU is guaranteed even if B collides with V. B knows the value of a valid payment token. MU does not leak any information about the pair that he chooses randomly to make a purchase. However, MU can loose a weak linkage of the value of the payment token to B as a result of the weak linkage that exists between the withdrawal and deposit protocol.

- ***Support for multi-currency:*** the model provides support for multiple currencies to be used within the system.
- ***Validation/Communication load:*** The system is totally online and the user needs to contact the broker or third party for each payment. The communication load is light-weight only in withdrawal protocol as the exchange of the four messages (value, content, challenge, and response) between MU and B takes less than one second if next- generation 3G mobile communication services were to be used.
- ***Ease of Use***: this system requires the User (MU) to sign digitally in order to withdraw a payment token from B and generate a challenge to blind messages exchanged with B.
- **Transferability**: a payment token ("e-coin") is vendor-specific and has no value to other vendors. Therefore, users cannot use the same e-coin for multiple payments to different vendors.
- ***Divisibility***: the e-coin can be divided into a range of payment values as pairs {value, s, t (z′, a′, b′, r′, rm)}
- **Disconnected Operations/Robustness:** It is impossible for the user to continue to access information or make payments during a broker's down-time or during communication loss with the broker as this protocol is a fully-online approach.
- ***Other Comment***: There exists a weak link in the value of the payment between withdrawal and deposit protocols. B knows this value and can easily tell a set of Vs where MU has spent his payment token but not exactly at which V.

4.4 Boddupallis Mobile Micro-payment Model

This protocol was initiated by Boddupalli et al.. [26]. It uses the Millicent payment scheme which is based on two scrips[6] namely the broker scrip (B-scrip) and vendor scrip (V-scrip). A V-scrip consists of:

a) The scrip body (SB): this is subdivided into the identification material (Vendor ID, Scrip ID, and the Customer ID) and the certificate material (scrip value, expiring date, other parameters).

[6] Scrips are ***specific*** to Vendor and may be ***validated*** by a Broker.

b) The certificate is the result of hashing the scrip body and the master scrip secret (MSS).

Thus, V-Scrip= SB, H (SB, MSS) and

where SB= ID material and Certificate material.

H =one-way collision resistant hash function.

The various processes in the transactions are assigned and managed by three major entities: MU, B and V as shown in Fig. 2

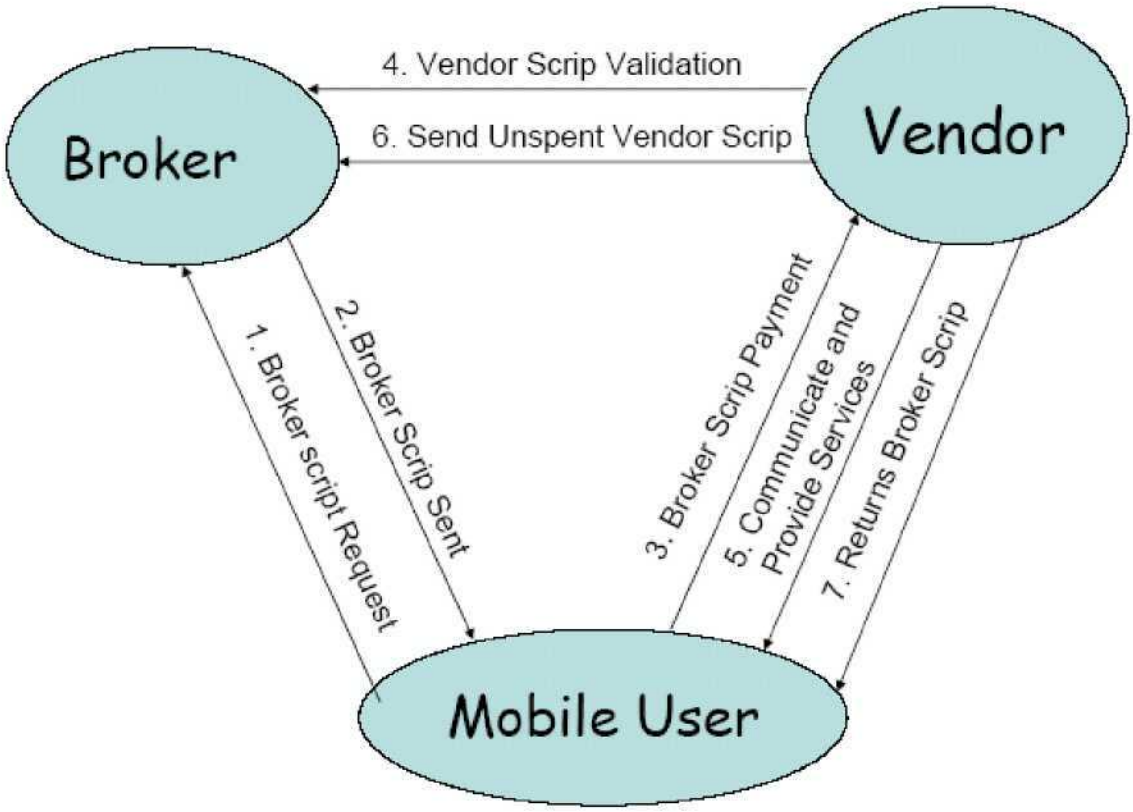


Fig. 2 Transaction Flow in Millicent Mobile Micro-payment System

4.4.1 Millicent Transactions

The flow of transactions among the three entities for this model is discussed as follows:

(i) Broker and Vendor Scrip Request

The Mobile User (MU) buys the broker scrip at the initial payment phase with real money and the broker returns the initial broker scrip and associated secret. MU requests the vendor scrip by paying with the broker scrip obtained from the broker.

There are three models in which the broker gets the vendor scrip.

a) ***Scrip warehouse model***: the broker requires the scrip directly from the vendor.
b) ***Licensed scrip production model***: if a broker buys a lot of scrips for a specific vendor, the vendor sells the right to the broker to generate vendor scrips that the vendor can validate and accept.
c) ***Multiple brokers' model***: a customer's broker needs to contact vendor's broker to buy the scrip.

After the broker gets a vendor's scrip, the broker sends the scrip, associated secret and "change" broker scrip to the customer [9]. MU may buy the corresponding V scrip from B if they have prior knowledge of V to interact with. However, the use of brokers eliminates the need for MUs to set up accounts with multiple Vs. In this case, V does not need to contact B for validation as they validate the V scrip locally. This feature of validating the Vendor scrip locally allows the mobile Millicent protocol to survive a network disconnection in a wireless computing environment [26].

(ii) Withdrawal Process

- MU sends a request to B to obtain a broker scrip (B-scrip) using some form of macro-payment from B (M1,M2) to be spent in order to utilise V service:

  MU → B **M1=Scrip request**

- B responds by sending the broker scrip requested to MU:

  B → MU **M2=B-scrip sent**

(iii) Principle of Payment (Payment Protocol)

- MU connects to V over a secure channel and tenders the B-scrip to the V:

  MU → V **M3=B-scrip payment**

- V validates this B-scrip with B. V contacts B only once for validating the B-scrip and afterwards validates the V scrip locally:

  V → B **M4=B-scrip validation**

- If the B-scrip is valid, V returns the Vendor scrip (V-scrip), a certificate (ct) and a session key (k) to MU that is used to encrypt any sensitive communication between MU and V:

  V → MU **M5=V-scrip, ct, k and service download**
- After the transaction is completed, V sends and translates any unspent V-scrip into B-scrip with B:

  V → B **M6=Unspent V-scrip**
- V returns the new B-scrip (the translated unspent V-scrip) to MU. When MU makes a purchase with a scrip, the cost is deducted from the scrip and a new scrip (value) is returned to MU.

  V →MU **M7=new B-scrip.**
- The new scrip can be used for further transaction payments to the same V. After the transaction, MU can "cash in" the remaining value scrip. Millicent is optimised for repeated micro-payments to the same Vendor.

(iv) Redemption Protocol

MU always makes a purchase with a V-scrip. Therefore, this protocol does not require V to redeem for payment as V gets the profit when she/he sells the scrip [34].

4.4.2 M-Commerce Payment Scenario using the Millicent model

Using the same example of downloading music tracks of section 3.5.5, the payment protocol of Boddupalli Millicent transaction model will be discussed below.

Prior to making purchases, MU purchases broker scrip (BS) (such as $5) with real money from B using a macro-payment system approach. B returns an associated (equivalent) BS to MU.

To commence a transaction with V, MU connects and pays the BS to V. V validates this BS with B and sends an equivalent vendor scrip (VS - $5), certificate and a session key to MU in return. MU pays the VS (equivalent of 30c, 52c and 48c) to V (one at a time in order to download the three music tracks respectively). For example, MU purchases the

first music track with VS (equivalent of 30c), MU has only $4.70 left in the VS to use for further purchasing of the second and the third music tracks. At the end of downloading the three music tracts, the total transaction cost is $1.30. V translates any unspent VS into BS with B and returns a new BS to MU (a value of $3.70). MU can use the BS for further purchase with the same V or a different V.

4.4.3 Evaluation of Boddupalli Mobile Micro-payment Model

- ***Security:*** the system prevents double spending by the use of Vendor-specific scrip. Millicent uses no public-key cryptography and is based on light encryption of the issuer's specification.
- ***Privacy/Anonymity***: B knows who and where but not what. Therefore the anonymity of MU is not being protected. The vendor knows what (service or information) but not who.
- ***Support for multi-currency***: the currency must match with the scrip. Hence, the system does not provide support for multi-currency.
- ***Validation***: The system is semi-online; MU has to be connected to the B (online) in order to be able to make further purchases and payments to a new or different or next V. However, vendor scrip bought from B can be validated locally and this prevents double-spending without the overhead of contacting the B.
- ***Ease of Use***: the system is easy to use but the overall transaction process may become complicated to set up when both MU and V have different Bs.
- ***Transferability:*** vendor scrip is Vendor-specific and has no value to other Vs though the new scrip returned to MU from the first V after the initial purchase can be used for further transaction payments to the same V.
- ***Divisibility:*** this model provides support for a range of payment values using particular Vendor scrip.
- ***Disconnected Operation***: the MU cannot continue to access information and make payment to another V during the B's down-time. MU has to purchase a new B or V's scrip from B in order to continue making purchases with different Vs.

- ***Other comments***: The overall transaction processing becomes very complex and the system is complicated to set up when both MU and the V have different brokers.

4.5 Zhu's Mobile Micro-payment Protocol

This model uses payment tokens[7] that are based on hash chain constructions. A mobile user (MU) attaches to the network through an access network operator (NO) and releases a stream of micro-payment token to pay all the Vendors (Vs) as he/she continues to make purchases.

The connection may pass through one or more other network operators (home or foreign) before reaching the destination (final) vendor. This protocol is an off-line token-based micro-payment system designed for wireless networks. The flow of transaction payments for this protocol involves the MU, V, B and NO as shown in Fig. 3

[7] The Mobile users purchase payment tokens from online brokers.

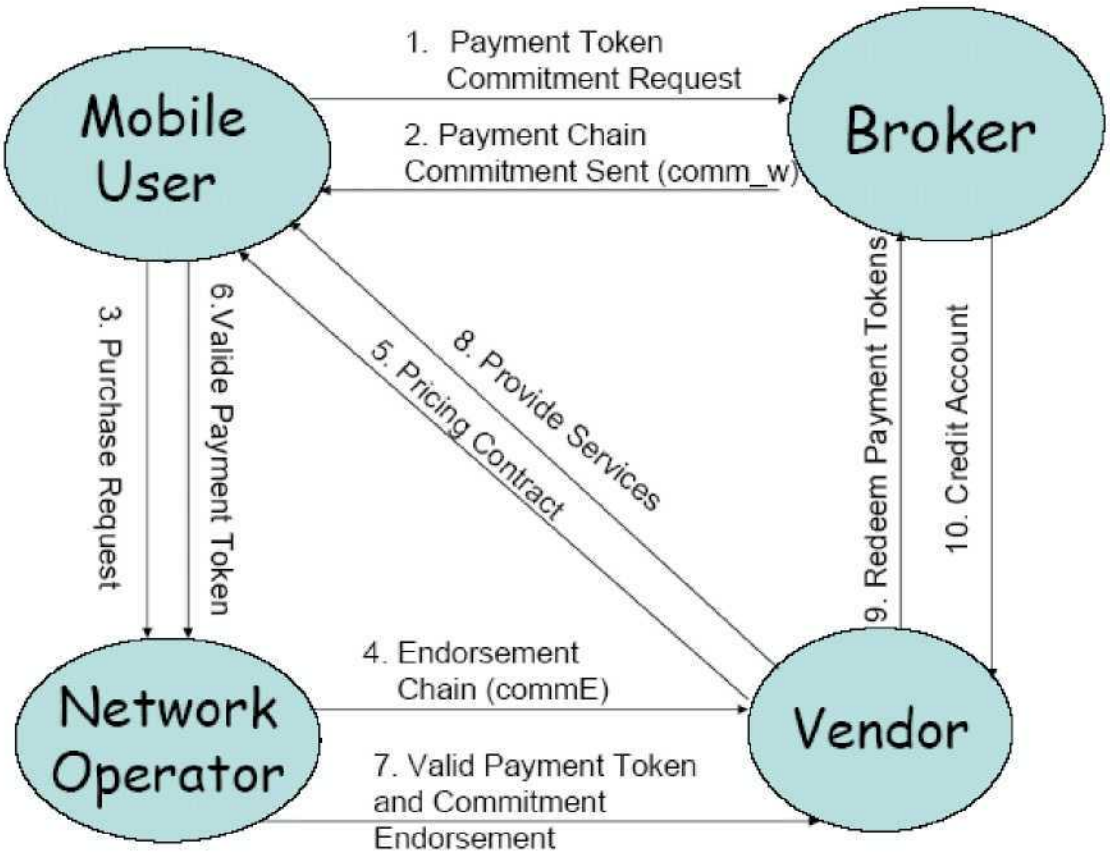


Fig. 3 Transaction Flow in Zhu's Mobile Micro-payment System

4.5.1 Zhu's Model Transaction

The flow of transactions among the four entities for this model is discussed below.

(i) Payment Chain Purchase

- The MUs generate their own electronic coins "e-coins," or paywords. These are sent to NOs and Vs and then verified by B. MU initially creates the tokens by using a one-way hash function to root Wn to generate their own coins (payment hash chain).
- MU randomly picks a payword seed Wn and then computes a payword chain by repeatedly hashing Wn, Wi-1 = h (Wi) where i=1, 2, n. MU later makes a macro-payment to B by sending a message[8] which contains the final hash value (Wo),

[8] The message sent is a request to obtain a payment chain commitment, as the chain has no monetary value until committed by a Broker.

chain length (cl), total chain value (cv) and the NO's identity (NOid) by encrypting with the Broker's public key:

MU → B **M1 = {Wo, cl, cv, NOid}** $_{PK-B}$

- The Broker commits the hash chain by digitally signing the payment hash chain and sending it to MU.

B → MU **M2= Comm-w = {Wo, cl, cv, NO, expire date}.**

The message M2 (commitment) reveals that MU's paywords or the payment hash values from the chain are pre-paid value and are redeemable from the broker.

(ii) Pricing Contract (PC)

- MU sends a purchase request containing the vendor's identity (Vid), service type (ST) and quality of service (QTY) to NO:

MU →NO **M3 = {Vid, ST, QTY, Comm-w}.**

- The NO signs an endorsement chain commitment in M4 below for each visit and sends to V:

NO →V **M4=(CommE)**[9]

- A signed PC containing a transaction identifier (TID) is generated by Vs (Vids) involved in the services in order to allow verifiable dynamic tariffs; fix the starting hash (Ws); decide the value per payment hash (Wv); create a record for MU (MUr); and link a single payment commitment to multiple Vs for MU's visit.

V →MU M5=TID, Vids, Charge, Comm-w, Ws, Start, Wv, CommE, MUr.

(iii) Payment Processes

- MU releases a stream of valid micro-payment tokens at regular intervals into the network to pay all the Vs as the transaction progresses:

MU →NO **M6=W1, W2.....Wn**

where **n** represents the number of tokens MU wishes to spend.

- MU also sends the requirement of the information goods to the NO.

[9] A hash chain commitment has the final hash as CommE={E0} sigNO

- The NO verifies that the payment hash is valid by performing a one–way hash function on it to obtain the previous one.
- The NO then forwards the payment hash (W1, W2……Wn) and its own corresponding endorsement hash (E1, E2……..En) to other Vs:

  NO →V **M7= W1E1, W2E2, W3E3……..WnEn.**
- Each V verifies both the payment hash and the endorsement hash of M7. V continues to provide the service to MU agreed in the pricing contract and MU can then download the downloadable media from the vendor. MU can terminate and stop releasing the e-coins if he does not receive any more service:

  V →MU **M8= Service Download**

(iv) Redeeming Payment Hashes

- At the end of each day, V sends the highest payment token received (Paywords-Wx), a corresponding endorsement hash (Ex) and pricing contract (PC) to B as follows:

  V →B **M9=WxEx, PC**

  where x represents the highest value of the paywords or endorsement hash
- The broker verifies the payment tokens, using the root P_0 and knows how much to pay the vendor from the contents of the PC:

  B →V **M10= credit the Vendor's account.**

4.5.2 M-Commerce Payment Scenario using the Zhu's Protocol

Using the same example of downloading music tracks of section 3.5.5, the payment protocol of Zhu's transaction model will be discussed below:

Prior to making purchases, MU generates the e-coins (such as $5) using a one-way hash function to root W501 (W0, W1 …. W500) and later sends the final hash value Wo, length (500) and value of hash chain to B using a macro-payment system approach. B sends the correspondent committed hash chain (W1, W2 …. W500) to the MU.

MU initiates a purchase request (consisting of V's identity, the committed hash chain, type of service (music tracks) and the quantity (first music track – 30c)) and sends it to NO. The NO signs the endorsement chain (E1 … E30) after receiving the purchase request from MU and sends them to V. V generates the PC and sends this to MU.

To commence transaction with and make payment to V, the MU sends the valid e-coins (W1,…,W30) at regular intervals through the NO to V. The NO first validates the e-coins by performing hash function on the e-coins and generates its corresponding endorsement hash chain as payment e-coins (W1E1, …, W30E30). NO later forwards the generated payment e-coin (W1E1, …, W30E30) for music track 1) to V. V validates these payment e-coins and allows MU to download the first music track as agreed in the PC.

4.5.3 Evaluation of Zhu's Mobile Micro-payment Model

- ***Security***: every payment needs to be authorised by the NO in order to prevent double spending from MU. The NO also needs to generate a corresponding endorsement hash and sends them to the vendor in every payment. The security aspect of this model was critically analysed in Zhu's model [11] in terms of preventing fraud from outside attacker, vendor, the MU, NO and the B.
- ***Privacy/Anonymity***: the protection of personal and payment information is moderate as the MU releases payment tokens to vendors through connection to the NO and releases a stream of micro-payment tokens to pay all the vendors as the MU continues to make purchases. Also, this connection may pass through one or more other network operators (home or foreign) before reaching the destination V.
- ***Support for multi-currency:*** the model provides support for multiple currencies to be used within the system.
- ***Validation/Computational load***: the protocol is an off-line system, as MU only needs to contact the broker at the beginning of each commitment lifetime in order to obtain a newly-signed commitment. The system aims to minimise the computational time of public key operations required per payment by using hash

operations instead of heavy encryption techniques whenever possible. However, the protocol is almost an online one with respect to the NO. The NO needs to generate a corresponding endorsement hash for every payword chain, which is sent by the MU. The NO will have to send the valid paywords (W1,... Wi) and its corresponding commitment (E1,... Ei) to V in every transaction. The e-coins (paywords) in the system are user and vendor-specific. This greatly limits the portability of the paywords and may often require the MU to over-purchase credit.

- ***Ease of use:*** there is no request for MU to be familiar with this system. However, the Network Operator (NO) will be required to sign a hash chain commitment for every transaction.
- ***Transferability***: an endorsement chain commitment has to be signed by the NO for each transaction. Also, a signed PC message has to be generated by the vendors to decide the value per payment hash and link a single payment commitment to multiple vendors for MU's purchasing.
- ***Divisibility:*** the vendors decide the range of payment values during the period of signing the PC.
- ***Disconnected Operation:*** the MU cannot continue to access information and services during the NO or vendors down-time because an endorsement chain commitment has to be signed by the NO for each transaction and the vendors have to link a single payment commitment to multiple vendors for the MU's purchasing.

4.6 Comparing and Contrasting Existing Mobile Micro-payment Models

The three existing micro-payment systems presented in this chapter are suitable for micro-payment in mobile commerce environments. They reduce computational cost through the use of one-way hash functions instead of public key cryptography to improve performance. Table 5 summarises the comparison for the mobile micro-payment models using the eight criteria discussed in section 4.2

Characteristics/ Features	Zheng et al.'s Protocol	Boddupalli et al.'s protocol (Millicent)	Zhu et al.'s Protocol
Security	**High** (U and M cannot double spend and double deposit a valid payment token as M and B keep record of received tokens in their databases).	**Medium** (double spending can be prevented by the use of Vendor-specific scrip).	**High** (NO authorises payment and generates a corresponding endorsement hash for V in every payment).
Privacy/ Anonymity	**Medium** (there is a weak link in payment information "value" which is known to B)	**Low** (B knows who and where but not what; V knows what not who)	**Medium** (User releases payment token to vendors through connection to NO)
Multi currency	Supported	**Not Supported** (must match with scrip)	Supported
Validation/ communication load	**Online** (system is totally online and requires U to contact B for each payment. / **Very High** (heavy burden on B as U contacts it for each transaction)	**Online and semi off-line** (MU has to be connected to the B (online) in order to be able to make payment to a new V) / **Medium** (V's scrip bought from B can be validated locally without the overhead cost of contacting the B)	**Offline** for B and **Online** for NO (MU contacts to the NO (online) in order to verify paywords and generate the corresponding endorsement paywords for V in every transaction) / **Low** for B and **High** for NO
Ease of use	**Low** (U signs digitally to withdraw from B and generate a challenge to blind messages exchanged with the B).	**Medium** (complicated to set up if MU and V have different Bs).	**Medium** (requires NO to sign a commitment hash chain for each visit)
Transferability (Funds)	**Very low** (token withdrawn from the B is vendor-specific).	**Low** (Vendor scrip is Vendor-specific and has no value to other vendor)	**Medium** (generation of endorsement chain commitment for each visit)
Divisibility	**High** (e-coin can be divided into a range of payment values as pairs {value, s, t (z′, a′, b′, r′, rm)}	**High** (provides support for a range of payment values using a particular Vendor scrip)	**Medium** (SPs decide the payment values by signing the Pricing Contract)
Disconnected Operation	**Very High** (discontinued transaction during the broker's downtime)	**Low** (MU cannot continue to access services and possibly makes payment with a new B or V's scrip to another V during the B's down time).	**High** (operation will be disconnected during NO & SPs down-times).

Table 5 Summary of the Comparison of the Existing Mobile Micro-payment Models

According to Table 5 above, it was observed that most of these mobile payment models have their own strengths and weaknesses. More importantly, they are not suitable for micro-payments to multiple vendors due to non-transferability of funds in the form of payment tokens, and that some models rely extensively on the use of a broker or network operator for payment authorisation. For example, Zhu et al.'s protocol is an offline, token-based micro-payment protocol with respect to the broker but online with respect to the network operators.

4.7 Summary

In meeting the challenges of mobile micro-payment design, providers have taken a number of different protocols and models on the subject of enabling payment through mobile devices by the use of micro-payment protocols. This chapter discussed and evaluated several existing mobile micro-payment models in terms of their payment protocols and transaction performances.

Moreover, the details of how various cryptographic techniques have been applied to several existing models of payment techniques in mobile commerce were discussed. This chapter presented in details those models or protocols that are token-based in respect to their medium of value exchange as discussed in Chapter 3 (section 3.6.2)

In addition, this chapter focused on the transactions flow (payment protocol) between mobile ser and vendors involved in three different existing protocols designed specifically for mobile token–based micro-payment systems in a wireless environment. Their general approaches are based on the security, cost and ease of use of the mobile micro-payment system to users and service/content providers. Some of the models were able to fulfill some of the general requirements while others failed.

The various existing mobile micro-payment models were compared and it was observed that their major problem areas are; high communication burden on the broker for payment authorisation and difficulty in transferring funds for multiple purchases. Solutions to

these two problem areas of the existing mobile micro-payment models will be presented in the next chapter.

Chapter 5

Mobile NetPay Protocol for Mobile Micro-payment

In chapter 1, a micro-payment protocol "NetPay" was mentioned as a wired predecessor for the new mobile micro-payment protocol called Mobile NetPay (MOBPAY). The features of the proposed formal model of wired NetPay was reviewed and evaluated. Based on the client-side e-wallet of NetPay protocol, an adaptation to a new mobile micro-payment protocol that is suitable for wireless network environments will be developed and propose in this chapter.

The strategies and approaches of using NetPay protocol to build the new protocol suitable for mobile information content micro-payment applications with client side electronic-wallet storage by the mobile device were investigated. The electronic wallet (e-wallet) stored by the mobile device will involve the use of payment tokens in the form of "e-coins" for payment of low valued items.

In addition, the formal model of MOBPAY will be based on assessing a range of existing and competing micro-payment systems for mobile commerce. This chapter proposes a new solution to solve their major problem areas. MOBPAY is a wireless protocol for cashless payment using an e-wallet which works in a similar way to traditional transaction payment in the real world when making multiple purchases.

This chapter will briefly present the wired NetPay protocol in the following section bringing out its major limitations. In addition, the main functional characteristics of MOBPAY for making payment to multiple Vendors which provides more flexible, mobile and accessible mobile micro-payment solutions will be discussed.

MOBPAY will be discussed in detail in terms of the transaction steps and processes among the various actors involved. Some scenarios of how MOBPAY could be applied in the virtual world of transaction payment for mobile information content such as ringtones, music, video, games and wallpapers will also be presented.

Furthermore, the MOBPAY protocol will be evaluated in terms of its strengths and weaknesses with other various existing and competing models of mobile payment for m-commerce of low valued items. This involves critical examination based on certain requirements and criteria peculiar to micro-payment systems (section 4.2) and how various cryptographic techniques have been applied to them.

5.1 Wired NetPay Protocol

A wired micro-payment protocol called NetPay was developed by Dai [2] which provides a secure, cheap, widely available, and debit-based protocol for an off-line micro-payment system. This protocol was purposely designed for use for payment of low value but high frequency transactions on the Internet in a standard land-line terminal.

Dai [3], [4] developed NetPay-based systems for client-server broker, vendor and customer networks and also designed three kinds of electronic wallets (e-wallets) to manage electronic coins (e-coins) in the client-server NetPay systems [3], [4], [5].
In one model, the e-wallet is hosted by vendor servers and is passed from vendor to vendor as the customer moves from one site to another. The second is a client-side application resident on the client's Personal Computer (PC). The third is a hybrid that caches e-coins in a web browser cookie for debiting as the customer spends at a web site.

The client-side e-wallet is an application running on the client PC that holds e-coin information. Customers can buy articles or content using the client-side e-wallet at different sites without the need to log in after the e-wallet application is downloaded to their PC. Their e-coins are resident on their own PC and so access to them is never lost due to network outages to one vendor.

The e-coin debiting time is slower for a client-side e-wallet than the server-side e-wallet due to the extra communication between vendor application server and customer PC's e-wallet application. In a client-side e-wallet NetPay system, a Touchstone and an Index (T&I) of a customer's e-wallet are passed from the broker to each vendor.

Dai et al. [3], [4], [5] designed the NetPay protocol so that the vendor application server communicates with broker application servers to obtain the T&I to verify e-coins received from the client. The vendor application servers also communicate with another vendor application server to pass the T&I without the use of the broker.

The main problem with this approach is that a vendor system cannot get the T&I during the previous vendor's down time. Therefore, the customer cannot continue to make further purchase as the previous vendor needs to send the T & I to the next vendor for the customer to proceed. A possible solution to solve this problem is for the current vendor to contact the broker to get the T &I information [29].

However, there is another problem of placing the communication burden only on the broker (who has to be online) for every transaction. This would amount to a higher cost of payment processing as well as delay transaction time for multiple purchases of low value items. Tin the following section, the new mobile micro-payment protocol "MOBPAY" will be presented to address this limitation of the wired NetPay micro-payment protocol.

5.2 Mobile NetPay (MOBPAY) Protocol

MOBPAY is a debit-based mobile micro-payment system that uses a one-way hash function to generate a payword chain by repeated hashing of the paywords. MOBPAY offers and provides high performance and security in wireless as opposed to a fixed or wired network by using one-way hash functions for e-coin encryption; reducing the communication burden on the Broker and detecting double spending during the transaction process.

The new and improved proposed protocol (MOBPAY)[10] will offer a better solution with the following features:

[10] Offline, token and debit- based micro-payment protocol for payment in mobile computing environment.

1. The two major key issues involve in a micro-payment scheme will be considered for designing the new mobile micro-payment protocol. These are low value (usage of hash function to achieve a lightweight payment transaction which reduces cost overhead) and high volume/frequency (payments to multiple vendors with a single e-wallet residing the e-coins).
2. This wireless, cashless micro-payment protocol will satisfies two requirements of new features added to the existing e-commerce micro-payment scheme as follows:
    - Easy to access **(accessibility).** This is the ability to use the system easily without being familiar with the system's user interface or without constantly requesting for any information on identification or authentication (such as PIN number or login).
    - Convenient to use **(mobility).** This is the ability to use the same e-coin to make purchases with many Vendors as the User moves from one site or Vendor to another.
3. The new wireless micro-payment protocol will be more flexible and will deploy the use of a mobile operator (on behalf of the Broker or content Providers) to ensure payments are not based on the assumption of continuous connectivity and real time payment transactions.

5.2.1 Entities/Actors of MOBPAY

The mobile payment value chain has various roles which need to be managed [46]. Basically, there are various roles performed by four main actors involved in the transaction (payment) process. These actors in MOBPAY are Broker (B), Vendors (Vs), Mobile User (MU), and Network Operator (NO).

The roles of the first three actors of MOBPAY were discussed in section 2.1.2. The general roles and duties of the NO have also been discussed in section 3.7.1. In addition to these obligations, the NO in MOBPAY protocol is expected to perform the specific tasks highlighted below:

a. NOs will serve as an intermediary to route transactions between the Mobile Users (MU) and the Vendors. NOs provide connectivity for the MU and act as middleman to monitor transaction flows between the MU and the vendors.

b. NOs are expected to provide the clearing and settlement tasks, carrier and portal services to mobile users.

c. NOs are assumed to provide large databases of MUs who will put trust in them and are likely to adopt mobile services, like mobile gambling or shopping.

d. NOs are expected to keep records of certain transaction processes as the mobile user moves from one V to another.

5.2.2 MOBPAY Terminologies

There are a number of cryptography and micro-payment terminologies used in the MOBPAY micro-payment protocol. Mobile devices are not capable of performing the same operations which are used for fixed or wired devices. For example, they cannot perform high computational cryptographic functions due to their low communication and computational resources.

An alternative lightweight cryptography operation that best suit their design and capacity is the **hash function** (hf). The hf has been discussed in chapter 4 (section 4.1.1). The use of the **payword chain** of hash values to represent a set of **electronic coins** (e-coins) which will reside as electronic wallets (e-wallets) in the mobile device will be deployed. The details of these three terminologies are as follows:

1. ***One-way Hash Function*** - the one-way hash function (MD5) to will be used in the MOBPAY implementation having the following properties:
    - Mathematically, given a value x as data input, it is easy to apply (compute) the one-way function to x to give the desired hash value y=h(x), but, given y, it is not feasible to compute the corresponding $x=h^{-1}(y)$ where h (...) represent the hash function operation. This value of a mathematical function is a real or complex number.
    - It must be computationally infeasible to construct two messages which hash to the same digest [51].

2. ***Payword Chain*** – A "payword chain" is generated by using a one way hash function. To generate a payword chain of *k*th paywords, a payword seed W_{k+1} will be randomly selected and then a payword chain will be computed by repeatedly hashing as follows:

   $W_k = h(W_{k+1})$, $W_{k-1} = h(W_k)$, ……,

   Let assume that the payword chain k has two paywords (where k=2). A seed W_3 will be randomly picked and a payword chain will be computed by hashing it repeatedly

   $W_2 = h(W_3)$, $W_1 = h(W_2)$, $W_0 = h(W_1)$

   The h( ) represents the hash function such as MD5 and W_0 is the last value computed known as the root for the payword chain. This payword root is not part of the payword chain and is embedded in a Mobile User-Vendor specific commitment [34]. This payword root will be used to verify the validity of the paywords generated in the new propose mobile micro-payment.

3. ***Electronic coins*** – e-coins are tokens used for online transaction of sub-dollar values, also known as micro-payments. E-coin is the unique, low cost, convenient, secure and reliable way for Vendors to set up their powerful world wide distribution channels for MU to buy services and digital content anytime and anywhere [53]. E-coins technology provides the opportunities, benefits and conveniences with little efforts required for the Vendor and the Mobile User to set up.

5.2.3 Basic Notations of MOBPAY

The following are the basic **notations** used to describe the process of transaction payment for MOBPAY (the new protocol of mobile micro-payment system) as shown in Fig. 4. The following notations will be adopted for clarification of MOBPAY protocol:

IDe → e-coin's identity (electronic coin)

H & P→ Host and Port.

T & I → Touchstone and Index.

SK-a → A's digital signature

PK-a → A's public key

{x}SK-a → x signed by A.

{x}PK-a → x is encrypted by A's public key

{x}SAK- a→ x signed by A using A's asymmetric key.

MU → B Mobile User sends a message to the Broker.

IDa → pseudonymous identity of party A in the trade community issued by the broker.

5.2.4 MOBPAY Transaction Flow

The overall model of transaction flow in the MOBPAY protocol is represented in Fig. 4 below. This figure gives the general pictorial view of the transaction processes that exist among all the four main actors (MU, Vs, B and the NO) of MOBPAY protocol. The overall model will be further broken down into transaction subsections to demonstrate the three main key transactions that exist among the various actors of the MOBPAY protocol under section 5.3

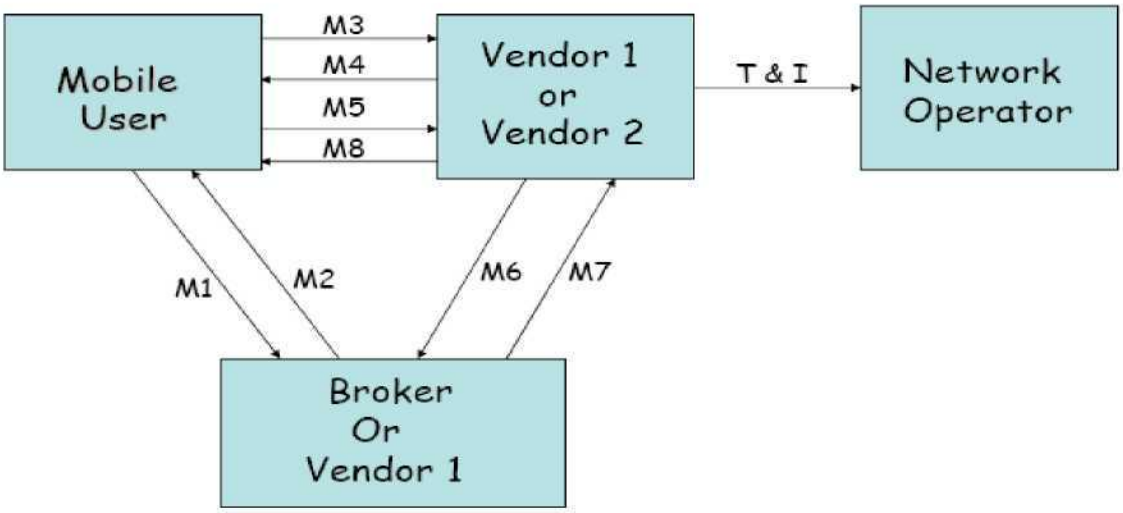


Fig. 4 Transaction and Payment Flow in the Mobile NetPay (MOBPAY) System

Prior to purchase, MU sends M1 to deposit funds with B and B sends paywords to MU in M2. MU sends a purchase request (M3) to V_1 and V_1 sends the price, H & P to MU in

M4. MU sends paywords to V_1 in M5. V_1 sends M6 to B to obtain the T & I and B responds to V_1 by sending M7. T is used to verify the paywords and I is used to prevent MU from double-spending and to resolve disputes between Vs. If the paywords are valid, V_1 makes the service available to MU in M8 and MU downloads the media. V_1 signs the current T & I and sends them to NO.

If MU intends to make a purchase from a new Vendor 2 (V_2), V_2 sends a price, H & P to MU in M4. MU sends paywords to V_2 in M5. V_2 requests for and receives the current T & I from V_1 in M6 and M7 respectively. If the paywords are valid, V_2 makes the service available to MU in M8. However, during any of the previous Vs' down time, V_2 sends M6 to NO to obtain the T & I. This Payment cycle continues in a similar way as long as MU makes multiple purchases with several Vs.

5.3 MOBPAY System Transaction

Let us consider a large trading community consisting of a mobile user (MU), a network operator (NO), Vendors (Vs), and a Broker (B). MOBPAY protocol will be based on the following assumptions:

a) B is honest and is trusted by the NOs, Vs and MUs.
b) The MUs and Vs may or may not be honest.
c) The MUs open accounts and deposit funds with the B.
d) Vendors open accounts with the same B as MU.
e) Payment transaction will involve V or Vs, NO, MU and B.
f) MU knows the price of a downloadable media from vendors' site prior to purchase.

The following sub-sections will describe the three key transactions in the MOBPAY protocol in detail to demonstrate this new model for mobile payment systems:

1) Mobile User to Broker transaction **(MU → B)**
2) Mobile User to Vendor(s) (Single and Multiple) transaction **(MU → Vs)**
3) Vendors - Broker transaction **(V → B)**

5.3.1 Mobile User to Broker Transaction

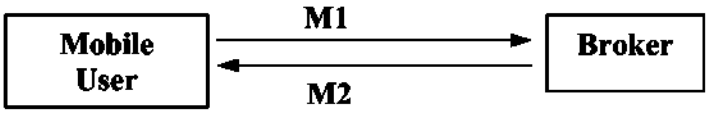


Fig. 5 Mobile User to Broker Transaction

- MU first registers (opens an account) and deposits funds with B. MU sends an integer (n) representing the number of paywords in a payword chain to B in order to make a purchase with the first vendor (V1)

  MU→B **M1=n**

- B performs the following tasks after receiving M1.
  a) B debits the account of MU and creates a payword chain W_0, W_1, $W_2,\ldots,W_n$, W_{n+1} which satisfies $W_i = h(W_{i+1})$.
  where i = n, …, 0. (H (...) is a one way hash function).
  b) B uses root W_0 to verify the validity of the paywords W_1, W_2, …, W_n by Vs.
  c) B keeps the seed W_{n+1} to be used to prevent the MU from overspending and forging paywords in that chain.
  d) B computes the touchstone (T) for the payword chain where T = {IDe, W_0} $_{SK\text{-}broker}$
  e) B stores the root Wo, W_{n+1}, value (amount) and IDe in his database.
  f) B sends the payword chain (W_1, $W_2,\ldots,W_n$) and ID_e (e-coin ID) that are encrypted by MU's public key to MU as shown in M2

  B→MU **M2={ID_e, W_1, W_2, … ,W_n}$_{PK\text{-}MU}$**

An illustration

For example, if MU sends n=50 to B, the following process then takes place:

- B randomly selects W_{51} and generates the IDe=1 and payword chain {W_0, W_1, W_2, … , W_{50}, W_{51}}.

- The MU's e-wallet which resides on the MU's mobile device only receives the IDe=1 and Paywords $\{W_1, W_2, \ldots, W_{50}\}$
- B saves IDe, W_0, W_{51} and 50 to his database.

5.3.2 Mobile User to Vendors Transaction

MU to Vs transaction process is the heart of the MOBPAY protocol. This entails the investigation of the transaction processes that exist between these two actors. This subsection presents the payment authorisation involved in the transaction process, how funds (e-coins) are transferred from MU to Vs and how services are made available to MU.

Micro-payment systems usually involve high frequency (volume) of purchasing from multiple Vendors. Therefore, the three main transaction processes of MU purchasing with the first Vendor (V_1), multiple purchases with the same Vendor (V_1) and multiple purchases with a new Vendor (V_2) will be presented as follows respectively:

A. Mobile User to Vendor 1 (V_1) Transaction

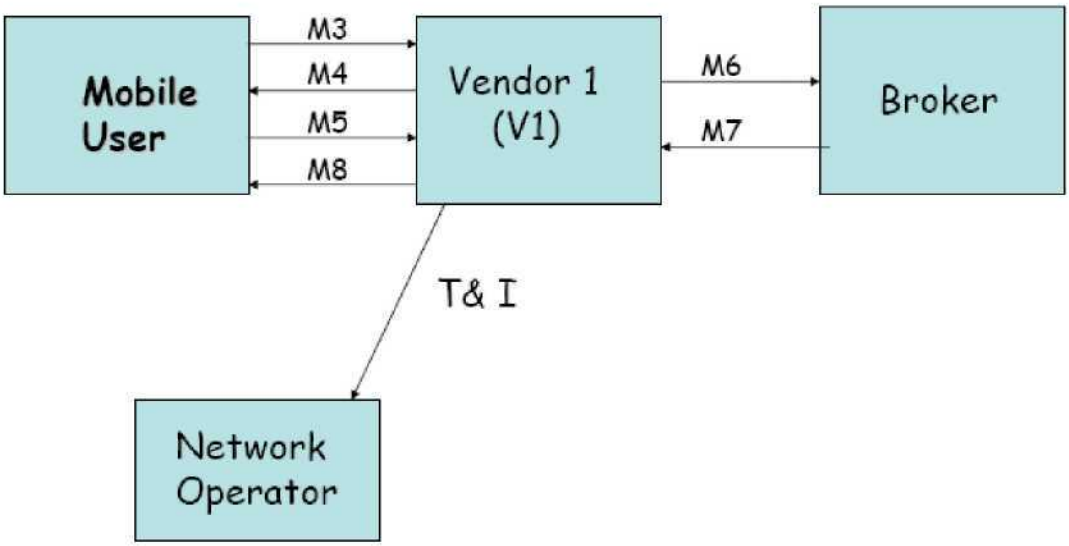


Fig. 6 Mobile User buys Downloadable Media

The following is the sequence of messages that takes place between a MU and V_1 in the event of making payment for downloadable content or services.

MU interacts with the first Vendor (V_1) in the following way when MU attempts to purchase downloadable digital content or services from V1.

- MU initiates the purchase of a downloadable media from the first Vendor (V_1) by sending a purchase request to V_1 through connection to a Mobile Network Operators (NO)

  MU→ V_1 **M3=Service Type, Quantity, IDV_1**

- V_1 responds to this request by sending a message (4) to MU's e-wallet to activate it.

  V_1→ MU **M4=Price (m cs), V_1's H & P**

- The e-wallet of the mobile device compares the H and P in M4 with the previous H and P. If different, the e-wallet sends M5 to V_1

  MU→ V_1 **M5=IDe, W_1, W_2, … ,W_m, B's H & P, IDNO)**

  For example, to make a mcs (m=2) payment, MU sends W_1, W_2 to V_1.

- V_1 sends a message (IDe) to B requesting for T

  V_1→B **M6= IDe**

- B responds by sending M7 to V_1

  B→ V_1 **M7={IDMU, T, Index=(1)}** $_{SK\text{-}B}$

- V_1 performs the following tasks after receiving M7:

  a) Uses the received T & I to verify the paywords by using root W_0. The paywords are verified by taking the hash of the paywords in the order W_1 first, then W_2, and so on. It is hard for V_1 and attackers to create W_1 even though they know W_0 since the generation of a value that would hash to W_0 is computationally infeasible due to the nature of the one-way hash function.

  b) Signs the current Index $\{IDv_1, m\}_{SK\text{-}v1}$ with his secret key (index=m).

  c) Stores the valid paywords (W_1, W_2, … ,W_m) which are later sent to B in exchange for real money during the redemption process.

  d) Stores the T & I in his database which will be sent to the next Vendor. T is used by V_1 to verify the electronic currency (paywords), and I is used to prevent MU from double-spending and to resolve disputes between Vs.

e) Sends a copy of the current T & I to NO to be stored in NO's database. This makes the current T & I available for the next V (V_2) if the previous vendor system (V_1) is down.

- V_1 later makes the service available to MU in M8.

  $V_1 \rightarrow$MU **M8= Downloaded Content**

B. Multiple Purchases with Vendor (V_1)

MU can further make purchases of another downloadable product with the same Vendor (V_1). The phase of multiple purchases with the same or previous vendor will be presented by using Fig. 7

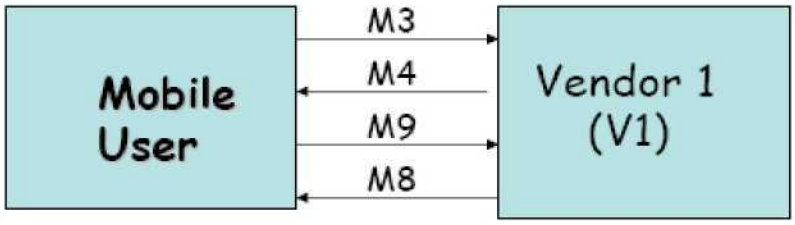


Fig.7 Multiple Purchases with Vendor 1

The following transaction flow takes place in the event of MU making multiple purchases with Vendor 1 (V_1).

- The MU sends a similar purchase request or message (M3 of section 5.3.2) to V_1 specifying a new service type and quantity in terms of volume of usage or duration time.
- V_1 responds to this request by sending a similar message M4=Price (i cs), V_1's H & P to MU.
- The e-wallet of MU will be activated and compares the H & P in M4 with the previous received H and P. If this is the same, the e-wallet responds by sending a new set of paywords in message (M9) to V_1

  MU$\rightarrow$ V_1 **M9=IDc, W_{m+1}, W_{m+2}, … W_{m+i}, IDNO, IDV_1**

  NOTE: Since **V_1** has records of the previous T & I stored in the database, **V_1** verifies the received paywords (W_{m+1}, W_{m+2}, … W_{m+i}) offline without

contacting the broker.

- V_1 also performs the following tasks after receiving M9:
  - **a)** Signs the current Index $\{IDv_1, m+i\}_{SK\text{-}v1}$ with his secret key.
  - **b)** Stores the valid paywords (W_{m+1}, W_{m+2}, … W_{m+i}) which are later sent to B in exchange for real money during the redemption process.
  - **c)** Stores the T & I in his database which will be sent to the next Vendor.
  - **d)** Sends a copy of the current T & I to NO to be stored in NO's database.
- V_1 later makes the service available to MU in M8.

$V_1 \rightarrow$MU **M8=Service Download**

C. Multiple Purchases with New Vendors

MU can further make purchases of new downloadable products with a new Vendor (V2). This phase of purchasing from a new Vendor is represented in Fig. 8 and discussed below:

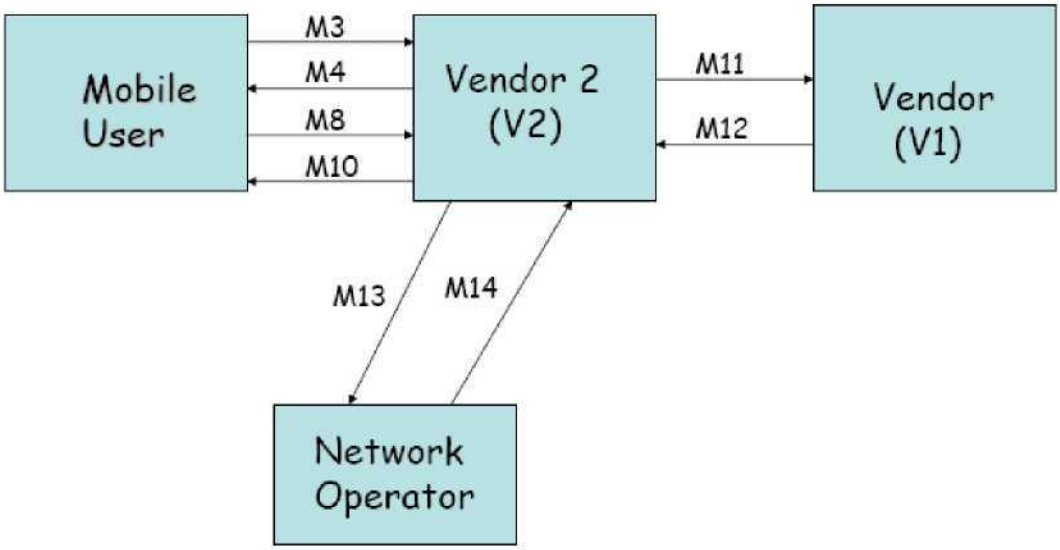


Fig. 8 Multiple Purchase with New Vendors

The following transaction flow takes place in the event of MU purchasing from a new Vendor (V_2).

- The MU sends a similar purchase request or message (M3 of section 5.3.2) to V_2 specifying a new service type and quantity.
- V_2 responds to this request by sending a new message (M4) to M's e-wallet

  $V_2 \rightarrow$ MU **M4=Price (j cs), V_2's H & P**
- The e-wallet of MU compares the H & P in M4 with the previously received H and P. If this is different, the e-wallet respond by sending a new set of paywords in message (M10) to V_2:

  MU$\rightarrow V_2$ **M10= W_{m+i+1}, W_{m+i+2}, … W_{m+i+j}, IDe, IDNO, IDV_2, V_1's H & P**
- V_2 sends the IDe of M10 to V_1 requesting the current e-coin index (I) and the Touchstone (T) in Message M11 in order to verify the new e-coins received from MU.

  $V_2 \rightarrow V_1$ **M11=IDe**
- V1 sends the requested T & I to V_2.

  $V_1 \rightarrow V_2$ **M12=T & I where I=m+i**
- V_2 verifies the paywords using the T & I offline without contacting the broker and also performs the following tasks:
  a) Signs the current Index $\{ID\ V_2, m+i+j\}_{SK\text{-}v2}$ with his secret key.
  b) Stores the valid paywords (W_{m+i+1}, W_{m+i+2}, … W_{m+i+j}) which are later sent to B in exchange for real money during the redemption process.
  c) Stores the T & I in his database which might be sent to the next Vendor.
  d) Sends a copy of the current T & I to NO to be stored in NO's database.
- V_2 later makes the service available to MU in M8.

  $V_2 \rightarrow$MU **M8=Service Download**

  However, if any of the previous Vendor's system (V_1) is down, the following actions take place between V_2 and NO.
- V_2 could send an enquiry message to NO to get the Touchstone and Index in order to proceed with the transaction during previous Vendor's (V_1) down time.

  $V_2 \rightarrow$ NO **M13=Ide**
- NO sends the requested current Touchstone and index stored in the database to V_2 in M14.

  NO$\rightarrow V_2$ **M14=T & I where I =m+i**

- V_2 verifies the paywords using the T & I offline and then makes the service or content available to MU in M8.

5.3.3 Vendor to Broker Offline Redemption Process

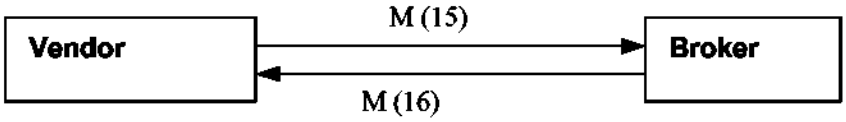


Fig. 9 Vendor to Broker Redeem Transaction

At the end of each day (or other suitable period), for each payword chain, all Vendors need to send all the paywords that they received from MUs to B in order to redeem them for real money. They do this by using the received T & I previously sent to them from B in the following way:

- The Vs must aggregate the paywords by each e-coinID and send them to B.

  V→B **M15=IDv, IDe, Payments**

- B verifies each payword received from Vs by performing hashes on it and counting the amount of paywords. If all the paywords are valid, B deposits the amount to and credits the Vendor's account.

  B→V **M16=Deposit real money**

5.4.M-Commerce Payment Scenarios using MOBPAY Protocol

This section provides the detail of how MOBPAY protocol can be applied in virtual world of mobile commerce. Consider two trading communities consisting of a single broker (B), Mobile User (MU) and Vendors (Vs). The trading communities engage in the sales of downloadable music tracks/electronic music (e-music) and electronic newspaper (e-newspaper). Assumption will be based that the MU wishes to download two music tracks from the same V and one e-newspaper from a different V. The first music track costs 7cents and the second one costs 5cents. The article in the e-newspaper site costs 8cents.

Prior to purchasing the above three-named downloadable items, MU opens an account and deposit funds (real money) with B using a single macro-payment approach. Also MU sends an integer (n=500c) to B specifying the number of paywords required. B creates the payword chain ($W_0, W_1 \ldots\ldots\ldots\ldots W_{501}$) and uses the root chain (W_0) to verify their validity. B also computes the Touchstone (T=IDe, W_0) where IDe= identity of the electronic coins. B stores the IDe , W_0, W_{501}, and 500 in the database. The electronic wallet (e-wallet) of MU receives the (IDe=1) together with the associated payword chains ($W_1, W_2, \ldots, W_{500}$) generated by B.

- Downloading the first Music Track

  MU sends a purchase request to the music V to initiate the purchase of the first music track (7c). The V responds by sending a message to activate the MU's e-wallet. The MU's e-wallet sends the IDe, $W_1, W_2, \ldots, W_7$ to V. V sends the IDe to B requesting for T.

  B responds by sending the T and the index (I=1) to V. On receiving the T&I from B, V signs the current index (m=7); stores the valid paywords ($W_1, W_2, \ldots, W_7$) and the T&I; and sends the current T&I to NO. At the end, MU can download the first music track.

- Downloading the Second Music Track from same Vendor

  MU sends a purchase request to the same music V to download the second music track (5c). The V responds by sending a message to activate the MU's e-wallet. The MU's e-wallet compares the Host and Port (H&P) of V. The MU's e-wallet sends the IDe and new payword chain ($W_8, W_9, \ldots W_{12}$) to V. V verifies the payword chain offline since he/she has the current T&I.

  V later signs the current index (=12); stores the valid paywords ($W_8, W_9, \ldots, W_{12}$) and the T&I; and sends the current T&I to NO. MU can now download the second music track.

- Downloading the E-newspaper from a New Vendor

  MU sends a purchase request to an e-newspaper site to download the one news article (8c). The V responds by sending a message to activate the MU's e-wallet. The MU's e-wallet compares the H&P of V. H&P are different from the previous music V, the MU's e-wallet sends the IDe and new payword chain (W_{13}, W_{14}, ... W_{20}) to e-newspaper V. The e-newspaper V sends IDe to the previous music V requesting for the current T&I. The previous music V sends the T&I to the e-newspaper V where I=12.

  The new V verifies the paywords offline using the T&I. V later signs the current index (=20); stores the valid paywords and the T&I; and sends the current T&I to NO. MU can download the news article. In case of any down time from a previous V, the new V needs to contact the NO for the T&I. The new V needs to send the IDe to NO to get this T&I. The new V verifies this T&I offline and makes the news article available to MU.

5.5 Requirements of MOBPAY

MOBPAY requirements will be categorized in terms of general and design requirements of micro-payment system for use in mobile commerce.

5.5.1 General Requirements

In a mobile communication system, the low computing power of mobile devices and a lower bandwidth and higher channel error rate than wired networks should be considered in designing a mobile micro-payment system [1].

The new mobile micro-payment protocol is expected to use a mobile phone device or other wireless device that can receive information and make payments for small amount of transactions or purchases via a wireless network, using an integrated wireless modem.

Prior to defining the requirements for the new mobile micro-payment protocol design, a qualitative analysis was performed on the wired Internet micro-payment system (NetPay)

to provide sufficient information for its enhancement. This study is necessary before proposing set of new requirement for MOBPAY. This can be achieved by providing mobile devices or PDA-hosted micro-payment applications with a client side "e-wallet" storage on the mobile device.

5.5.2 Design Requirement

MOBPAY-enabled applications need to provide HTML (web browser) and WXML (Wireless Extensible Markup Language) for mobile user interfaces and support a wide range of input devices. The new protocol application needs to provide more advanced language 'WXML (Wireless Extensible Markup Language)' than the contemporary Hypertext Markup Language (HTML) of a web browser. This is a consequence of the limited bandwidth supported in a wireless environment.

The main focus will be on the digital wallets (e-cash) technique for the new mobile payment approach and protocol design. The e-wallet stored by the mobile device will involve the use of payment tokens in the form of "e-coins" for the payment of low valued items. The two major issues involved in micro-payment schemes will be considered for designing the new propose mobile micro-payment protocol. These are the ***low*** value (use of hash function to reduce cost overhead*)* and ***high*** volume (less involvement of Brokers to reduce burden and cost).

MOBPAY requires a trusted broker to manage the generation of e-coins for the Mobile User (debiting) and redemption of e-coins for the Vendors (crediting). Replicated vendor and broker servers can be used to provide load balancing and failure tolerance for the architecture. MOBPAY incorporates the use of a client side electronic-wallet as a channel for making payments. The user of this protocol can make prepayments from the broker using a form of mobile macro-payment. Consumers then use the stored prepayment to make purchases from multiple content/service providers.

5.6 Summary

This chapter presented a protocol called "MOBPAY" for mobile micro-payment with high performance and security in a wireless environment as opposed to micro-payment in the conventional wired network. This new mobile micro-payment protocol (MOBPAY) is an enhancement of the NetPay protocol which incorporates a network provider and modified client-vendor-broker protocols. This implies that MOBPAY is based on the proposition of new modification strategies to an existing approach.

The main functional characteristics and the design on which this new mobile micro-payment protocol (MOBPAY) for a wireless micro-payment protocol is built were also presented. The MOBPAY protocol takes into consideration the two key issues (low value and high frequency transactions) of micro-payment schemes and the two requirements added to the existing e-commerce micro-payment schemes (mobility and accessibility).

A general schematic view and discussion of the transaction process involved in the MOBPAY protocol was presented for better understanding of the proposed protocol. The three basic transaction steps involved in the protocol was presented and described in this chapter. The details of the flow of transactions that exist between various actors involved in the transaction process of the MOBPAY protocol were also presented.

The introduction of a new actor 'the mobile network operator" in mobile micro-payments to act as a mobile micro-payment provider is to ensure payments are not based on the assumption of continuous connectivity to the broker (online) and for real time payment transactions.

MOBPAY minimises the use of a Trusted Third Party (Broker) for payment authorisation per purchase and connectivity during any of the previous Vendor's down time. In addition, this chapter gave the requirements and specifications for the implementation of the new mobile micro-payment protocol.

Chapter 6

The MOBPAY Protocol Discussion

In the previous chapter, a token debit-based and offline protocol (with respect to both the broker (B) and network operators (NOs)) suitable for micro-payments in mobile networks was presented. The protocol satisfies the requirements for security that a micro-payment system should have by preventing the mobile users (MUs) from double spending using an e-coin Index and any internal and external adversaries from forging.

The use of a single e-wallet[11] as a channel for mobile users to make purchases from multiple Vendors (Vs) was introduced. This e-wallet stores the paywords (e-coins) which are to be used for micro-payment purposes. In this case, the real money goes first from the buyer to the payment-service vendor (broker) in exchange for payment tokens, which then pays V at a later time. This will greatly increase the efficiency and ease of use of making multiple purchases as the mobile user roams. In addition, it increases Vs' confidence and builds their trust in getting paid after the utilisation of their resources.

In terms of communication and computational cost, the protocol is economical since it does not involve public-key operations and payment authorisation from B for each/per purchase. The MU needs to contact B (Trusted Third Party-TTP) prior to making single or multiple purchases. They do not have to repeatedly do this for every transaction and during any of the previous V's down time to get the Touchstone (T) and the current Index (I).

The MU to B transaction phase guarantees no overspending and forging. The B selects the seed W_{n+1} to create the payword chain which satisfies $W_n = h(W_{n+1})$, $W_{n-1} = h(W_n)$, …, $W_1 = h(W_2)$, $W_0 = h(W_1)$, and keeps the seed W_{n+1} secret. B knows or has the seed W_{n+1}, i.e. a well designed cryptographic hash function is a "one-way" operation and there is no practical way to calculate a particular data input that will result in a desired hash

[11] This holds or stores the electronic coins in the mobile device prior to making purchases

value, so it is also very difficult to forge. Therefore, it is impossible for MU or other attackers to generate or forge other paywords in that chain by knowing some of them in the chain since h( ) is a truly one-way hash function. [49].

The first Vendor (V_1) signs the current Index = $\{IDv_1, i\}_{SK\text{-}v1,}$ sends T and I to NO to be stored in NO's database. T & I can be made available for further transactions or purchases during any of the previous V down time. If the paywords are valid, V_1 will store them for later redemption with the Broker and make the service available to MU. MU could then download the purchased media from V_1. Also, the MU could continue to buy other downloadable media with either the V_1 or a new/different Vendor (V_2) .

However, if V_1 system is down, V_2 can send a message to NO to obtain T and I. The MU could continue to buy other downloadable media with the V_2. This process of transaction has many advantages as highlighted below:

1) The transfer of the message between Vendors does not involve the broker. It reduces the communication burden of the broker. The major thrust of MOBPAY protocol is that it shifts the communication traffic bottleneck from the broker and distributes it among the vendors, thus placing some processing burden on all the Vendors when a mobile user wishes to purchase from different Vendors.
2) The message being sent between the Vendors or between the Vendor and the NO provides high security for MOBPAY protocol. This message includes the Touchstone (T) that is signed by the Broker (B) and an e-coin index (I) of the paywords signed by Vendors (Vs). Thus, it prevents the MU from double spending when the MU purchases from another vendor.
3) MOBPAY can easily handle multiple transactions between vendors. MU can continue to make purchases to multiple Vendors (V1, V2, V3,.....Vn where n represents the number of Vendors) with a single e-wallet of electronic coins (paywords). These paywords are not Vendor-specific, allowing a single e-wallet to provide payment across a wide range of vendors of mobile content.
4) MU can continue accessing services or information (and possibly make payment) during temporary failures or down time of either the Broker or Vendor. This

increases the response time for the transaction of payment processes; service availability; and makes the system more efficient. Thus, MU finds it easy to access **(accessibility),** utilise services at anytime and anywhere **(mobility).** MOBPAY supports a "previous vendor off-line" scenario by allowing the mobile user's network operator to cache limited information of the current T&I from the previous Vendor (which has been previously stored in the NO's database).

5) The advantage for the V is that the MOBPAY guarantees redemption of valid e-coins from B. It also allows the V to focus on content provision.
6) The B provides cash-handling functionality with a bank. This makes the MOBPAY protocol suitable for new and emerging Vs with a low adoption cost for the micro-payment protocol.
7) MOBPAY provides much greater network latency and reduces bandwidth on mobile networks unlike the wired NetPay micro-payment protocol. MOBPAY attempts to minimise network traffic and data exchange between the MU's device, V and B.

6.1 Evaluation of Mobile-NetPay (MOBPAY) Protocol

The MOBPAY protocol will be evaluated based on the criteria in section 4.2 as follows:

- ***Security:*** it is impossible for MU and other attackers to forge and generate other paywords in the payword chain (created by B using a one-way hash function) if they do not know the secret key of B. B keeps the **Seed W_{n+1}** in order to prevent the MUs and Vs from overspending and forging paywords in that payword chain. The current e-coin index of the paywords is sent among the Vs and NO, this prevents the MU from double spending. It should be noted that this security will be viewed as non-technical such as the detection and prevention of overspending by the MU, over depositing by the Vendors, fraud and forgery by both the MU and Vs. In addition to this, a micro-payment makes it difficult for hackers to profit on a security breach as the effort expended usually outweighs the benefits [8].

- ***Privacy/Anonymity***: the MU's personal (identity) and payment information is shielded or protected from the Vendor. Thus, the privacy of MU is protected and this anonymity is preserved.
- ***Support for Multi-currency***: this model provides support for multiple currencies but only needs conversion support.
- ***Validation/communication load:*** the transfer of the messages (touchstone and the current e-coin index) between the Vendors does not involve the B. Therefore, this reduces the communication burden of B; and also encourages an offline e-coin verification process.
- ***Ease of Use:*** this model provides support for MU to use the system without having to become familiar with the system's user interface and without requesting any information on identification or authentication. MU first registers with B and only needs to send an integer (number of payword) to B to start purchasing.
- ***Transferability:*** e-coins can be transferred to purchase from multiple Vs. This enables the MU to use the same or a single payword chain of electronic coins to make payment to multiple Vs. The e-coin is not Vendor-specific.
- ***Divisibility:*** e-coins can be divided into smaller values known as "paywords". This model supports a range of payment values.
- ***Disconnected operation:*** MU can continue to access services or information during the previous Vendor's down time. The next V can easily get the last T & I from the Network Operator.
- ***Other comments:*** Short message and light computational load is easily implemented in a mobile environment. This model uses a lightweight hash function technique to generate paywords in a payword chain that is relatively small in size.

6.2 Benefits of MOBPAY

There are several benefits of MOBPAY to both the Mobile User and the vendor. These benefits will be discussed in the following subsection respectively:

6.2.1 Benefit to the Mobile Users

The following are the main benefits of MOBPAY for the Mobile Device Users:

1) **Convenience of use**: customers do not need to enter any identification pin number or be familiar with the software or hardware to purchase online content using the e-wallet.
2) **Carry less card**: at the initial payment stage, MU exchanges real money for payment token (e-coins) and the e-coins reside in the mobile phone as an e-wallet. MU does not need to carry credit card.
3) **Flexibility**: MU can order and pay at the same time from the same phone as they move from one location to another.
4) **Accessibility**: easy to access anytime, anywhere and for purchase of low value items.
5) **Security**: unlike most current payment systems using a credit card, MOBPAY avoids dealing with stolen credit cards and unauthorised transactions.

6.2.2 Benefits to the Vendors

The following are the main benefits of MOBPAY for the Content and Service Providers (Vendors):

1) Reduced card and check transaction as done in the traditional payment system.
2) Deliver convenience to Mobile device User.
3) Faster transaction time.
4) Reduced fraud and charge-backs by the Broker.
5) Ability to deliver Value Added Stock (coupons and targeted real time ads right to the customer's device).

6.3 Limitations of MOBPAY

Most of the limitations peculiar to all wireless networks, protocols and models have been discussed in this thesis. Most of these limitations affect communication patterns (not payments) in a wireless environment. However, it has been discussed and revealed that, due to tremendous development in wireless standards and protocols, most limitations (not all) have been overcome.

The MOBPAY protocol is a token-based protocol that deploys the use of paywords with some limitations properties as follows:

- **Security**: the security of MOBPAY in exchange of paywords between the MU and V can be compromised if conversation is unencrypted. The exchange of paywords between MU and Vs can raise alarm through the security properties of the protocol. Payment information on a mobile device can be readable by anyone who has the public key and can trace the consumer's spending behaviour. However, micro-payment system makes it difficult for hackers to profit on a security breach as the efforts expended usually outweigh the benefits.
- **Communication load:** MOBPAY shifts the communication burden from the broker and distributes it among the Vendors thereby placing the burdens of processing transactions on the Vendors when the customer wishes to purchase from a new Vendor.

6.4 Evaluation of Micro-payment Models for Mobile Commerce System

The three existing mobile micro-payment models for m-commerce in purchasing and making payments for low valued items have been presented in Chapter 4. More so, these three models were compared and contrasted to evaluate their strengths and weaknesses. It was observed that some of the systems were able to reduce communication burden or online storage and computation by the use of offline validation. A mobile user's anonymity was also protected in some of the models.

Table 6 below summarises the comparison of both the existing mobile micro-payment models in Chapter 4 and the new proposed mobile micro-payment protocol (MOBPAY), using the eight criteria discussed in section 4.2.

Characteristics / features	**Zheng et al.'s Protocol**	**Boddupalli et al.'s protocol(Millicent)**	**Zhu et al.'s Protocol**	**Mobile-NetPay**
Security	**High** (U and M cannot double spend and double deposit a valid payment token as M and B keep record of received tokens respectively in their databases).	**Medium** (double spending can be prevented by the use of Vendor-specific scrip).	**High** (NO authorises payment and generates a corresponding endorsement hash for V in every payment).	**Very High** (B keeps the **Seed** $\mathbf{W_{n+1}}$ to prevent MU and V from overspending and forging paywords in a payword chain. NO and Vs also keep the T & I to prevent double spending).
Privacy/ Anonymity	**Medium** (there is a weak linkage in payment information "value" which is known to B)	**Low** (B knows who and where but not what; V knows what not who)	**Medium** (User releases payment token to vendors through connection to NO)	**High** (user's identity is fully protected from the Vendor)
Multi currency	Supported	**Not Supported** (must match with scrip)	Supported	**Supported** (but needs conversion)
Validation / communication load	**Online** (system is totally online and requires U to contact B for each payment. / **Very High** (heavy burden on B as U contacts it for each transaction)	**Online and semi off-line** (MU has to be connected to the B (online) in order to be able to make payment to a new V) / **Medium** (V's scrip bought from B can be validated locally without the overhead cost of contacting the B)	**Offline** for B and **Online** for NO (MU contacts to the NO (online) in order to verify paywords and generate the corresponding endorsement paywords for V in every transaction) / **Low** for B and **High** for NO	**Offline** (encourages offline e-coin verification process) / **Low** (transfer of T & I between the Vs or via NO does not involve B)
Ease of use	**Low** (U signs digitally to withdraw from B and generate a challenge to blind messages exchanged with the B).	**Medium** (complicated to set up if MU and V have different Bs).	**Medium** (requires NO to sign a commitment hash chain for each visit)	**High** (easy to use as User only sends an integer (number of paywords in a payword chain) to B).

Transferability (Funds)	**Very low** (token withdrawn from the B is Vendor-specific).	**Low** (Vendor scrip is Vendor-specific and has no value to other vendor)	**Medium** (generation of endorsement chain commitment for each visit)	**High** (coins can be transferred freely between Vs for multiple purchases).
Divisibility	**High** (e-coin can be divided into a range of payment values as pairs {value, s, t (z′, a′, b′, r′, rm)}	**High** (provides support for a range of payment values using a particular Vendor scrip)	**Medium** (SPs decide the payment values by signing the Pricing Contract)	**High** (coins can be divided into smaller denomination or payment values "paywords")
Disconnected Operation	**Very High** (discontinued transaction during the broker's downtime)	**Low** (MU cannot continue to access services and possibly makes payment with a new B or V's scrip to another V during the B's down time).	**High** (operation will be disconnected during NO & SPs down-times).	**Low** (user enquires and gets T & I from previous V or the NO in order to continue accessing information or services).

Table 6 Summary of the Comparison of MOBPAY and Existing Mobile Micro-payment Models

The major problem areas for many of the mobile micro-payment approaches are validation/communication load and transferability of funds. Most of the existing protocols for mobile micro-payment involve the use of a Broker for payment authorisation for each purchase. They have high transaction *cost* (communication, computation, operational, managerial, processing) for processing payment.

In addition, most of these protocols are not capable of handling payment for multiple purchases, as they do not allow the use of a single wallet to be used for several purchases (funds transferability) in a similar way to conventional (traditional) payment with real money. The MOBPAY protocol provides access and mobility to MU for multiple purchases with a single e-wallet. It also reduces communication load on the Broker.

The MOBPAY protocol offers the "best" solution to overcome major limitations of the existing mobile micro-payment schemes as shown on the comparison table. These

solutions provided by the MOBPAY protocol are shown as having an overall strength over two weaknesses of other existing protocols as shown under the characteristics of the validation and transferability of funds properties in Table 6 above.

6.5 Summary

This Chapter presented an extensive discussion of the MOBPAY protocol. The specific roles of the Network Operator (NO), merits and benefits of MOBPAY protocol with respect to both mobile device users and the vendors were also discussed. It was argued that the new proposed offline mobile micro-payment protocol is useful for mobile device users performing multiple purchases with a variety of service and content providers and who need to move from one vendor to another.

In addition, the MOBPAY protocol was evaluated in terms of its payment protocol and transaction performance using certain characteristics of section 4.2. The major advantages (solutions) provided by the MOBPAY protocol over its predecessor wired NetPay micro-payment are that it provides the means for mobility, accessibility and continuous connectivity for multiple purchases during any of the actors' down time.

In conclusion, the MOBPAY protocol was compared with three existing mobile micro-payment models of Chapter 4. After this comparison, it was concluded that MOBPAY protocol provided the best solutions to two problem areas of the existing mobile micro-payment protocols. The application of the MOBPAY protocol can be extended to purchasing information, services and commodities of low value from any web site at anytime and anywhere via mobile devices.

Chapter 7

Conclusion and Future Work

7.1 Contributions

The use of a micro-payment system in the mobile application environment/domain was emphasised in this thesis. There are several existing and competing micro-payment systems designed and proposed for mobile-commerce. A qualitative analysis of a range of potential mobile micro-payment system in terms of their main functional characteristics were presented, discussed and evaluated. The existing mobile micro-payment models were assessed in this thesis to weigh their weaknesses and strengths.

Most of the existing mobile micro-payment models do not allow the storage of electronic coins (e-coins) as electronic wallet (e-wallet) on mobile device. The e-wallet serves as payment instruments across a wide range of content or service providers (multiple Vendors) by using a single hash chain on e-coins. This requirement provides high efficiency for payments of low-volume and high-frequency transactions in mobile commerce.

These existing models for mobile commerce lack this principle requirement, as the e-coins in most models are vendor specific. In addition, it was observed that some of these existing protocols require frequent communication with the Trusted Third Party (TTP) (usually the broker) for payment authorisation for every transaction. This communication pattern is associated with higher operational cost as it places heavy burden on the broker.

In order to overcome these major limitations of the existing mobile micro-payment protocols, a proposed modification strategies and a new mobile micro-payment protocol called 'MOBPAY' was introduced. The MOBPAY protocol is an enhancement of an existing wired micro-payment system. The MOBPAY protocol provides support payment-enabled wireless micro-payment systems that will be more cost effective, secure, efficient, flexible, mobile and accessible.

In addition, the MOBPAY protocol offers better transaction performance solutions in handling low- value, high-volume transactions involving multiple Vendors. MOBPAY protocol incorporates a network provider and modified client-broker-vendor protocols. The protocol is assessed and compared to other competing mobile micro-payment system.

MOBPAY uses prepaid token- based micro-payment system for its payment protocol. The protocol minimises the number of expensive public key operations required by payment [10] and deploys the use of lightweight cryptographic technique such as cryptographic hash functions. These functions ensure lower processing cost and enhance transaction security in detecting and preventing fraud, forgery, double spending and double depositing.

Mobile wallets are very useful in wireless environment and they make shopping more efficient [22]. To enable token-based mobile micro-payment system, the use of e-wallet which resides on the mobile device was introduced. This e-wallet stores the e-coins or payment token and act as the payment instrument. The e-coins can be used in a similar way as real money to make payment to multiple purchases from a variety of Vendors across the spectrum of mobile services and applications.

MOBPAY protocol uses an offline verification process to minimise the use of broker in every transaction. This reduces processing cost (connection and transaction) and heavy burden/load (computation and communication) on the broker. The use of mobile network operator to act as micro-payment provider reduces the disconnected time of accessing and purchasing digital contents during any of the previous Vendor's down .This will enhance real time processing and operations for purchasing high volume of contents or services from a wide range of Vendors.

Furthermore, it is obvious that the application of MOBPAY protocol will not be limited to purchasing only an individual item but can also be used to conduct wireless commerce of multiple low-value transaction. The unlimited demand and appropriate payment

protocol (change in how payments are made) for low value items are presumed to bring about great revolution in mobile commerce. This volume of transaction or large user base is presumed to provide the scale of trading community required for successful micro-payment.

7.2 Conclusion

Payment is the key innovation for mobile commerce. Mobile commerce demands an appropriate, efficient and effective payment system for the need of growing industrial trend in wireless technologies. That is, the distribution of digital information that will be mobile and easily accessible. Mobile payment systems allow users of mobile devices such as PDA and mobile phone to perform wireless transactions on the Internet. In recent years, the popularity of mobile devices has increased substantially due to the growth of mobile computing technologies.

Mobile devices are appropriate payment instrument to support low value and high volume transaction (micro-payment) which employs lightweight cryptographic technique with low operational, management and processing cost. Although these devices are characterised by certain resources which limits their usage for macro-payment in wired environment but they still have the capacity to provide support for micro-payment to be implemented on them.

Macro-payment system, payment processing of high value and low volume such as the use of credit card requires high cost, expensive computation operations and heavy communication load. This payment system is not easily implemented on mobile devices due to certain constrains and features peculiar to mobile devices. Mobile micro-payment systems are especially used for transaction of low value and high frequency.

The proposed mobile micro-payment protocol (MOBPAY) brings easy mobility and accessibility to information-hungry-consumers (the mobile users). More so, it brings more opportunities for knowledge-rich service and content providers to provide and sell more new products. MOBPAY protocol can be used as a major guideline for

transferability of funds, mobility, accessibility, practicability of token-based mobile micro-payment systems with high performance rate and security.

In conclusion, the data and results obtained from this thesis may be extensively useful for protocol designers and system implementers to design and implement token-based mobile payment systems. These results may also be used to analyse most existing mobile micro-payment system if it meet up with the standard industrial trend of mobile commerce.

7.3 Future work

Future mobile system will involve a large number of users who will access and purchase a variety of information, services and commodities provided by content providers. Also, one might likely see more network operators offering more micro-payment options such as stored e-coins rather than billing in the next coming years.

At present, there are key challenges facing the development and adoption of mobile micro-payment such as wireless network security, ease of use, ability to handle high transaction volumes, economic factors (low profit margins for providers due to low value), and insufficient demand from buyers or low user base [14]. Therefore, much work has to be done in other aspects of m-commerce such as the standards, protocols and user interface design before mobile micro-payment can be adopted on a viable scale [22].

This thesis presented the theoretical aspect of the new proposed mobile micro-payment protocol without the real implementation. The future research will focus on the implementation and application of the new proposed protocol in real world of mobile commerce. This will involve modeling/prototyping the proposed protocol, comparing its performance, size of data transferred and response time with other competing approaches. This prototype of MOBPAY protocol will enable mobile user to purchase content (music clips, articles, tourist information and news) using a single micro-payment approach across multiple vendors.

In particular, the usability evaluation and performance evaluation will be taken into consideration. The usability evaluation is good for assessing and understanding MU perceptions of using MOBPAY systems bringing out its advantages and disadvantages. The performance evaluation assesses the performance of MOBPAY enabled websites to determine the overhead cost of the micro-payment extensions made to the mobile phone user particularly in regard to mobile device user response time.

Bibliography

[1] Dai X., Ayoade O. and Grundy J. : Off-line Micro-payment Protocol for Multiple Vendors in Mobile Commerce. The 7th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06), 4-7 December 2006, Published by IEEE Computer Society

[2] Dai, X. and Lo, B.: NetPay – An Efficient Protocol for Micro-payments on the WWW. Fifth Australian World Wide Web Conference, Australia (1999)

[3] Dai, X., Grundy, J.: Architecture of a Micro-payment System for Thin-Client Web Applications. In Proceedings of the 2002 International Conference on Internet Computing, Las Vegas, CSREA Press, June 24-27, 444—450

[4] Dai, X. and Grundy J.: Customer Perception of a Thin-client Micro-payment System Issues and Experiences, Journal of End User Computing, 15(4), pp 62-77, (2003).

[5] Dai X. and Grundy J.: Three Kinds of E-wallets for a NetPay Micro-payment System, The Fifth International Conference on Web Information Systems Engineering, November 22-24, 2004, Brisbane, Australia. Lecture notes in Computer Science 3306, pp. 66 – 77

[6] Denis C.: "Mobility and Micro-payments", online: http://www.epaynews.com/downloads/zafion_WP.pdf , June 2003

[7] Gabber, E. and Silberschatz, A.: "Micro-payment Transfer Protocol (MPTP) Version 0.1". *W3C Working Draft*, 1995. http://www.w3.org/pub/WWW/TR/WD-mptp

[8.] Hassan W.: Lecture III M-commerce Architecture http://66.102.7.104/search?q=cache:FV7f3Q-gwzsJ:www.kti.ae.poznan.pl/conferences/i3e/papers/R_Parhonyi_L_J_M_Nieuwenhuis.p

df+Second+generation+micro-
payment+systems:+lessons+learned&hl=en&ct=clnk&cd=3

[9] Manasse, M.: The Millicent Protocols for Electronic Commerce. First USENIX Workshop on Electronic Commerce. New York (1995)

[10] Rivest, R. and Shamir, A.: PayWord and MicroMint: Two Simple Micro-payment Schemes. Proceedings of 1996 International Workshop on Security Protocols, Lecture Notes in Computer Science, Vol. 1189. Springer (1997) 69—87

[11] 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), 2004

[12] Hitoshi A., Oka A., Ramzan S., Zhu J.: Wireless Electronic Commerce Security http://theory.lcs.mit.edu/~zulfikar/papers/NokiaFinalNoConclusion1205.pdf

[13] Lesk, M.: Micro-payments: An idea whose time has possed twice? *IEEE Security & Privacy* (2:1), 2004, pp. 61-63.

[14] Geer, D.: E-Micro-payments Sweat the Small Stuff. Journal of Industry Trends. August 2004 http://csdl2.computer.org/comp/mags/co/2004/08/r8019.pdf

[15] Wilson, T.: Micro-payments Rise Out of the Trash Can. 2000
http://www.Internetweek.com/columns00/bits030600.htm

[16] The Essentials of Mobile Commerce.
http://www.businesslink.gov.uk/bdotg/action/layer?topicId=1075386889

[17] Adelstein F., Gupta S., Richard G., and Schwiebert L. : Fundamentals of Mobile and Pervasive Computing

[18] Luo, X. and Lee, C.: Micro-payment in Wireless M-commerce: Issues, Security and Trend. Journal of Internet Banking and Commerce, July 2004, vol. 9, no.2 http://www.arraydev.com/commerce/jibc/0402-10.htm

[19] Schiller J.: Mobile Communications Second Edition

[20] Robert P. Nieuwenhuis L. and Pras A. Second Generation Micro-payment System: Lessons Learned.

[21] "Wireless E-Commerce: A New Business Model" http://www.wirelessInternet.com/wireless2.htm (The website is dynamic)

[22] McKitterick D. : A Web Services Framework for Mobile Payment Services https://www.cs.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-59.pdf September 2003

[23] Prakash D., Agrawal., Zeng Q.: Introduction to Wireless and Mobile Systems second Edition 1

[24] Kytöjoki J., Kärpijoki V.: Micro-payments - Requirements and Solutions. http://www.tml.tkk.fi/Opinnot/Tik-110.501/1999/papers/micro-payments/micro-payments.html

[25] Zheng H. and Kefei C.: Electronic Payment in Mobile Environment. Proceedings of the 13th IEE International Workshop on Database and Expert Systems Applications (DEXA '02),2002.

[26] Boddupalli P., Al-Bin-Ali F., Davies N., Friday A., Storz O. and Wu M.: Payment Support in Ubiquitous Computing Environments. Available online at http://www.cs.cmu.edu/~jasonh/courses/ubicomp-f2004/papers/151_Boddupalli_P.pdf

[27] Dai, X., Grundy J. and Lo B.: Comparing and Contrasting Micro-payment Models for E-commerce Systems. Available Online at http://www.cs.auckland.ac.nz/~john-g/papers/icii2001.pdf

[28] Jones R., *MilliCent Update - Presentation*, MilliCent Marketing, Digital Equipment Corporation, 1997. Presented at the Electronic Payments Forum held on March 2-31998, San Francisco. Available Online at <ftp://ftp.xiwt.org/xiwt/EPFMarch98/Jones.ZIP>

[29] Dai, X., Grundy, J.: Three Kinds of E-wallets for a NetPay Micro-payment System. Lecture Notes in Computer Science, 3306:66-77, 2004.

[30] Hertzberg, A. and Yochai, H.: Mini-pay: Charging per Click on the Web, 1996. Available online at http://www.ibm.net.il/ibm_il/int-lab/mpay

[31] Tennant H. & Associates, 5 Payment Models on the Internet, 1997. Available online at http://www.htennant.com/hta/askus/5models.htm

[32] Croker, S., The Siren Song of Internet Micro-payments, The Magazine on Information Impacts, ISSN 1523-4541, April 1999. Available online at http://www.cisp.org/imp/april_99/04_99croker.htm>

[33] Gabber, E. and Silberschatz, A.: " W3C Common Markup for Micro-payment per-fee-links". *W3C Working Draft*, 1999. Available online at http://www.w3.org/TR/Micro-payment-Markup/

[34] Chi E.: Evaluation of Micro-payment Scheme, 1997.

[35] Aukia. P. and Lehmann, J., Mechanism in Electronic Commerce using Micro-payments., 1998. Available online at <http://studwww.eurecom.fr/~lehmann/study/allin1.html>

[36] Scmidt, C. & Müller, R.: A Framework for Micro-payment Evaluation., 14.6.1997.Available online at
<http://www.wiwi.hu-berlin.de/IMI/micro-payments.html>

[37] Matonis, J.: Digital Cash and Monetary Freedom. April, 1995. Available online at
<http://www.eff.org/pub/Privacy/Digital_money/matonis_on_dig_cash.paper>

[38] Neumann B. & Medvinsky G.: Requirement for Network Payment: The NetCheque Perspective. Proceedings of IEE Copcon '95, San Francisco, March 1995.
<ftp://prospero.isi.edu/pub/papers/security/netcheque-requirement-compcon95.ps.Z>

[39] Kearney A.T.: Mobinet 5.Accessed December 2006 (available online at http://www.atkearney.com/main.taf?p=5,4,1,60)

[40] Varshney U.: Wireless I: Mobile and Wireless Information Systems: Applications, Networks and Research Problems, Communications of the Association for Information Systems (12:11) 2003, pp1-23.

[41] Hoffman K.E: New Options in Wireless Payments, Internet World (7.7) 2001, p. 37.

[42] Bisdikan, C.: An Overview of the Bluetooth Wireless Technology. IEE Communications Magazine (39:12), December 2001, pp 86-94.

[43] Odlyzko A.: The Case against Micro-payments, 7th International Conference Financial Cryptography, Springer, 2003.

[44] Shirky, C. The Case against Micro-payments. Referred December 2006, (available online at http://www.open2p.com/lpt/a/515) (2003: Nov. 15) 2000.

[45] GSM World Technology (available online at www.gsmworld.com) June 2003.

[46] Rao, M. South Korea Aims for Global Leadership in Wireless, Broadband Internet Markets in Information Age (available online at http.//unpan1.un.org/intradoc/groups/public/documents/apcity/unpan006689.pdf (2003: September 1) 2000.

[47] Kuchinskas S.: Speed the Wireless Payment, February 28, 2005.

[48] Practical Advice for Business
http://www.businesslink.gov.uk/bdotg/action/layer?topicId=1075386889

[49] Rivest, R.: The MD5 Message-Digest Algorithm. RFC1321. Internet Activities Board, 1992.

[50] Mitchell B.: Wired VS Wireless
http://compnetworking.about.com/cs/homenetworking/a/homewiredless.htm (referred December 2006)

[51] Panko R.: Corporate Computer and Network Security, ISBN 0-13-038471-2

[52] Hash Function http://en.wikipedia.org/wiki/Hash_function

[53] http://www.ecoin.net/help/what.htm