secure and seamless payment for wireless mesh networks

by  
SERHAT CAN LELOĞLU

Submitted to the Graduate School of Engineering and Natural Sciences   
 in partial fulfillment of  
the requirements for the degree of  
Master of Science

Sabanci University  
January 2013

SECURE AND SEAMLESS PAYMENT FOR WIRELESS MESH NETWORKS

APPROVED BY

Assoc. Prof. Dr. Albert Levi ........................................

(Thesis Supervisor)

Asst. Prof. Dr. Cemal Yılmaz ........................................

Assoc. Prof. Dr. Erkay Savaş ........................................

Assoc. Prof. Dr. Özgür Erçetin ........................................

Assoc. Prof. Dr. Yücel Saygın ........................................

DATE OF APPROVAL ........................................

© Serhat Can Leloğlu 2013

All Rights Reserved

SECURE AND SEAMLESS PRE-PAYMENT FOR WIRELESS MESH NETWORKS

Serhat Can Leloğlu  
Computer Science and Engineering, MS Thesis, 2013  
Thesis Supervisor: Assoc. Prof. Albert Levi  
Keywords: Prepaid Payment Systems, Security, Micropayments, Wireless Mesh Networks

Abstract

Wireless Mesh Network (WMN) is a multi-hop high-speed networking technology for broadband network access. Compared to conventional network service providing systems such as base stations, WMNs are easy to deploy and cost-effective systems. We propose a secure and seamless pre-payment system for Internet access through WMNs. The proposed system is called SSPayWMN. This system is fair to both clients and to service providers. Since network service providers intentionally or unintentionally overcharge the clients, SSPayWMN offers cryptographic proofs for the given Internet service.

Micro payment systems generally put partial trust in operators; however in real life, operators may unintentionally overcharge their clients. This misbehavior in the system may cause disputes between the clients and the operators. Even when the operator is right, it is very difficult to convince the customer since the operators generally do not have justifiable proofs that can easily be denied by the clients.

The proposed system’s main goal is to provide a secure payment scheme, which is fair to both operators and clients. Using cryptographic tools and techniques, all system entities will be able to authenticate each other and provide/get service in an undeniable way. Implementing the system on a network simulator proves the proposed system’s effectiveness. Network simulation results ensure real life performance results for critical use cases.

Untraceability is a system property, where it is unable for an adversary to trace the actions of a client. SSPayWMN protects clients’ anonymity and provides untraceability for clients. The implementation of the system is conducted on a network simulator and simulation results are presented. SSPayWMN has achieved remarkable results in the simulations; system protocols reached steady state in every simulation, which ensures the stability of the system.

KABLOSUZ ÖRGÜ AĞLARI İÇİN GÜVENLİ VE KESİNTİSİZ ÖN ÖDEMELİ SİSTEM

Serhat Can Leloğlu  
Bilgisayar Bilimi ve Mühendisliği, Yüksek Lisans Tezi, 2013  
Tez Danışmanı: Doç. Dr. Albert Levi  
Anahtar Kelimeler: Ön Ödemeli Sistemler, Güvenlik, Mikro Ödeme, Kablosuz Örgü Ağlar

Özet

Kablosuz Örgü Ağları (KÖA) geniş alanda erişilebilir, ağ paketlerini çok zıplamalı şekilde hedefe ulaştırabilen, yüksek bağlantı hızı sağlayabilen bir ağ teknolojisidir. Alışılagelmiş yollara nazaran kurulumu daha kolaydır ve daha ekonomiktir. KÖA geniş alanlarda hareketli ve hareketsiz kullanıcılara bağlantı sağlayabildiği için ağ hizmeti sağlayıcı sistemler için uygun teknolojilerdir. KÖA ağlarındaki elemanlar ağ içinde bir elemana paket gönderdiklerinde kullandıkları rotayı hafızalarında tutarlar. Bu da onlara bir sonraki paket teslimatında daha hızlı olmalarını sağlar. Rota tabloları isteğe göre önden de yüklenebilir.

Önerilen sistemde güvenilir bir üçüncü parti (GÜP) görev alıyor. GÜP’ün yanı sıra kullanıcılar ve servis sağlayıcı operatörler de mevcut. GÜP aktif olarak sistemin içerisinde yer alıyor ve operatörler servis sağlanacak olan bölgeye belli aralıklarla erişim noktaları koyacaklar. Kullanıcılar sinyal gücü en yüksek olan erişim noktasını tercih edecekler bu da operatörler arasında daha iyi servis sağlamak için bir rekabete sebep olacak. Kullanıcılar belli bir operatörün sabit müşterileri olmayacaklar. Sinyal gücünde değişiklik olursa veya daha güçlü bir ulaşım noktasının yakınından geçiliyorsa kullanıcı hizmet aldığı ulaşım noktasını değiştirebilir. Bu değişiklik kullanıcıya servis bekleme süresinde artış veya bağlantı kesintisi şeklinde yansımayacak.

Sistemin ana amacı operatörlere mutlak güven ilkesinin benimsenmediği durumları kapsayacak bir ödeme yolu sağlamak. Önerilen sistem operatörlerin de bilinçli veya bilinçsiz şekilde fazladan para almasını engelleyecek. Sağlanan hizmet kriptografik yollarla kanıtlanabilecek bunun yanı sıra sağlanmayan hizmet için kanıt sunulamazsa bu hizmetin hiç sağlanmadığı anlaşılacak. Sistemin doğru ve efektif bir şekilde çalıştığını gösterebilmek için ağ simülasyonları da yapıldı. Gerçek hayata daha yakın sonuçlar elde edebilmek için kullanıcı tipleri düşünüldü. Simülasyonlar bu kullanıcı tiplerini de katarak yapıldı.

To my dear family

# acknowledgements

I would like to thank my thesis supervisor, Albert Levi, who has offered me this project at the beginning of my master studies. He has always been very helpful and understanding.

I would like to thank Yücel Saygın for introducing a new area of computer science to me with Information Retrieval and Data Mining courses. He was very kind by accepting to join the jury.

I would like to thank Erkay Savaş for giving me my cryptographic basis in my undergraduate studies. I would like to thank him for being a part of my jury.

I also thank Özgür Erçetin and Cemal Yılmaz for devoting their time for jury during their tight schedule.

I would like to thank my wife Suna Yeltekin Leloğlu, my mother Zerrin Leloğlu and my sister Seden Leloğlu Seçilir, for their support on every step of my life.

I would like to thank Can Yücel for explaining the project to me and also helping me to choose the network simulator.

Finally, I thank Türk Telekom for funding my project and scholarship.

Table of Contents

[acknowledgements vii](#_Toc345882469)

[list of figures x](#_Toc345882470)

[list of tables xii](#_Toc345882471)

[1. INTRODUCTION 1](#_Toc345882472)

[Contribution of the Thesis 2](#_Toc345882473)

[Organization of the Thesis 3](#_Toc345882474)

[2 Background information and literature survey 4](#_Toc345882475)

[2.1 BACKGROUND ON WIRELESS MESH NETWORKS 4](#_Toc345882476)

[Network Architecture 4](#_Toc345882477)

[Characteristics of Wireless Mesh Networks 6](#_Toc345882478)

[2.2 BACKGROUND ON CRYPTOGRAPHIC ALGORITHMS 7](#_Toc345882479)

[Hash Functions 7](#_Toc345882480)

[Hash Chains 8](#_Toc345882481)

[HMAC Functions 9](#_Toc345882482)

[Symmetric Cryptography 10](#_Toc345882483)

[Public Key Cryptography 11](#_Toc345882484)

[2.3. LITERATURE OF PAYMENT SYSTEMS AND SIMILAR WORKS OF SSPAYWMN 12](#_Toc345882485)

[2.4. DIFFERENCES AND SIMILARITIES WITH AN EARLIER WORK 15](#_Toc345882486)

[2. requırements and protocols of the system 20](#_Toc345882487)

[2.1. REQUIREMENTS OF SSPAYWMN 20](#_Toc345882488)

[Requirements of the Network 21](#_Toc345882489)

[General Overview of the Proposed Scheme 21](#_Toc345882490)

[Network Topology and General System Design 24](#_Toc345882491)

[Connection Card Structure 25](#_Toc345882492)

[Alias Computation 26](#_Toc345882493)

[2.2. PROTOCOLS OF THE SYSTEM 27](#_Toc345882494)

[Initial Authorization and Reuse of a Connection Card 27](#_Toc345882495)

[Access Point Authentication 30](#_Toc345882496)

[Packet Transfer 31](#_Toc345882497)

[Changing Alias 32](#_Toc345882498)

[Update Packets 36](#_Toc345882499)

[Disconnection 37](#_Toc345882500)

[Distributing Access Point Public Keys 39](#_Toc345882501)

[Seamless Mobility and Roaming (Payment Related) 41](#_Toc345882502)

[Payment to the Operators (Settlement) 43](#_Toc345882503)

[3. sımulatıons of sspaywmn 47](#_Toc345882504)

[3.1. SIMULATION ENVIRONMENT 47](#_Toc345882505)

[Cryptographic Operations and Their Timings 48](#_Toc345882506)

[3.1. UNIT TEST RESULTS 49](#_Toc345882507)

[Unit Test Result for End-to-End Two-Way Protocols 49](#_Toc345882508)

[Unit Test Result for Access Point Authentication 50](#_Toc345882509)

[Unit Test Result for Seamless Mobility and Roaming 51](#_Toc345882510)

[Unit Test Result for Packet Transfer 52](#_Toc345882511)

[Unit Test Result for Update Packets 53](#_Toc345882512)

[3.2. USER MODELING AND MOBILITY 53](#_Toc345882513)

[User Actions 54](#_Toc345882514)

[Client Types 55](#_Toc345882515)

[User Mobility and Timing 56](#_Toc345882516)

[3.3. SIMULATION RESULTS FOR REAL-LIFE SCENARIO 58](#_Toc345882517)

[Overview 58](#_Toc345882518)

[Real-Life Scenario Simulation Result for Initial Authorization 60](#_Toc345882519)

[Real-Life Scenario Simulation Result for Reuse of a Connection Card Protocol 61](#_Toc345882520)

[Real-Life Scenario Simulation Result for Changing Alias 62](#_Toc345882521)

[Real-Life Scenario Simulation Result for Disconnection 63](#_Toc345882522)

[Real-Life Scenario Simulation Result for Update Packets 63](#_Toc345882523)

[Real-Life Scenario Simulation Result for Seamless Mobility in Home Operator Protocol 64](#_Toc345882524)

[Real-Life Scenario Simulation Result for Roaming Protocol 65](#_Toc345882525)

[Real-Life Scenario Simulation Result for Packet Transfer 66](#_Toc345882526)

[4. discussion 67](#_Toc345882527)

[5. Conclusion 69](#_Toc345882528)

[6. References 70](#_Toc345882529)

# list of figures

Figure 2.1. Infrastructure/Backbone WMNs. (taken from [1]) 5

Figure 2.2. Client WMNs (taken from [1]) 6

Figure 2.3. Hybrid WMNs (taken from [1]) 6

Figure 3.1. Hash Function Example [7] 8

Figure 3.2. Hash Chain Depiction and Usage [8] 9

Figure 3.4. Symmetric Key Cryptography [16] 10

Figure 3.5. Public Key Encryption [17] 11

Figure 3.6. Validating a Signature [18] 11

Figure 5.1. Network Topology 24

Figure 7.1. Initial Authorization and Reuse-CC 28

Figure 7.2. Access Point Authentication 30

Figure 7.3. Packet Transfer 31

Figure 7.4. Changing Alias 34

Figure 7.5. Update Packets 36

Figure 7.6. Disconnection 38

Figure 7.7. Distributing Access Point Public Keys 40

Figure 7.8. Seamless Mobility (if X == Y) or Roaming (if X != Y) 42

Figure 10.1. End-to-End Two-Way Protocols Unit Test Result 50

Figure 10.2. Access Point Authentication Protocol Unit Test Result 50

Figure 10.3. Seamless Mobility and Roaming Protocols Unit Test Result 51

Figure 10.4. Packet Transfer Protocol Unit Test Result 52

Figure 10.5. Update Packets Protocol Unit Test Result 53

Figure 11.1. State Diagram of Clients 54

Figure 11.2. User Movement from A to B 57

Figure 12.1. Total Amount of Service Usage Times for Client Types vs. Total Delays 59

Figure 12.2. Average Service Usage Times for Client Types vs. Average Delays 59

Figure 12.3. Real-life Simulation Result for Initial Authorization Protocol 60

Figure 12.4. Real-Life Simulation Result for Reuse of a Connection Card Protocol 61

Figure 12.5. Real-Life Simulation Result for Changing Alias Protocol 62

Figure 12.6. Real-Life Simulation Result for Disconnection Protocol 63

Figure 12.7. Real-Life Simulation Result for Update Packets 63

Figure 12.8. Real-Life Simulation Result for Seamless Mobility Protocol 64

Figure 12.9. Real-Life Simulation Result for Roaming Protocol 65

Figure 12.10. Real-Life Simulation Result for Packet Transfer Protocol 66

# list of tables

Table 5.1. System Entities 21

Table 5.2: The List of the Symbols 22

Table 9.1: AP Specifications 47

Table 9.2: Platform Specifications 48

Table 9.3: RSA-2048 Timings 48

Table 12.1: Simulation Results for Client Types 58

# INTRODUCTION

WMNs [1] offer broadband network access with high speed network connection. WMNs are easy to deploy and cost effective compared to conventional Internet service providing infrastructures such as high-powered servers. Mesh networks dynamically organize themselves and do not need a centralized element; they are a subset of ad-hoc networks. Mesh nodes deliver packets from source to destination in a multi-hop manner, thus extends network coverage. WMNs could interconnect with conventional Wi-Fi connections and also other network types other than the ones that use the IEEE 802.11 family of standards such as WiMax [4], ZigBee [5] and 3G-radio access [29] could also interconnect with WMN structure.

WMNs are cost effective and they extent the network coverage, thus they could be used for network service providing. A necessity for a billing system automatically emerges for a network service providing scheme. Such systems require secure billing protocols that ensure anonymity and confidentiality of the client. A secure billing scheme should guarantee that a client could not get service without payment and service provider can not overcharge the client.

There has been extensive research about micropayment systems for network service providing systems. Rives and Shamir [43] proposed Pay-Word for micropayment purposes. Their work opened a new research area and many modifications and improvements [44] were performed on their scheme. New algorithms increased performance and flexibility. The research on micropayment schemes are still ongoing, there are some modern approaches on micropayment such as [52]. In [52] authors suggested to use hash chains [32] and public key cryptography to provide confidentiality, anonymity and untraceability for clients.

Micro-payment systems put partial or full trust in network service providers in general. This application gives service providers power to force clients to stick with them, which decreases the flexibility of the system. Furthermore, network service providers could overcharge the clients; there is a necessity for some protocol to protect client’s rights. Clients should be able to object an overcharge situation with undeniable proofs. A system with these properties should also ensure good performance with confidentiality, anonymity and untraceability for the clients.

SSPayWMN implements a prepaid billing scheme with simple structure and trust models. Authentication, confidentiality, non-repudiation and client privacy are taken into the consideration in the system design. SSPayWMN employs some cryptographic primitives to ensure system security. The billing system counts on hash chains [32] and uses every element of the hash chain as a token, which buys time intervals of Internet service. SSPayWMN employs a Trusted Third Party (TTP), which ensures an honest usage of the system by every party.

## Contribution of the Thesis

In this thesis we propose a secure and seamless prepayment system for WMNs. SSPayWMN covers anonymity and untraceability deficiencies of similar pre-payment systems.

Authentication, confidentiality, non-repudiation, fraud protection is provided in the system. The users are not be able to deny using credits for the services that are received; the operator is not be able to charge more than the usage amount. Additionally, inter-operator settlement is performed in a secure way such that each operator have cryptographic proofs of use for the services that they provide to other operators' customers. In order to provide privacy of individuals, our scheme provides untraceability such that no unauthorized entity will be able to track down a particular user with certain limits.

Since the clients are mobile, they may handover among different mesh routers (i.e. access points) of the same operators. They may also roam among different operators, not only due to coverage reasons, but also for having a better quality service. Our system aims to have seamless mobility and seamless roaming for payment purposes. These purposes are such that when the client gets service through a new AP or switch to another operator, authentication and authorization are not performed from scratch.

From a security point of view, we aim to have a mutual authentication between client and the network in our protocols. Anonymity of the clients and untraceability across different usage periods (a.k.a. unlinkability) are privacy related goals of the protocols.

From the payment point of view, our main aim is to have a fair system in which all the claimed transactions bear cryptographic proofs. In this way, the clients cannot repudiate using a service and the operators cannot claim for services that they do not provide. The latter is especially important during inter-operator settlement; it is also important to resolve client disputes.

We evaluated the performance of SSPayWMN using network simulations. These simulations are conducted in two groups. The first group is unit tests, aims to simulate protocols of protocols of SSPayWMN, independent from each other to analyze the delay caused by protocols. The analysis of the unit test results show that all of SSPayWMN protocols reach steady state. SSPayWMN is designed to reckon with real-life challenges such as stable Internet service during client mobility and overweight network service demand in rush hours. In the second simulation group, called real-life scenario simulations, the clients are selected considering human behavior and they are categorized. In real-life scenario simulations the system also reached steady state, which ensures system stability.

## Organization of the Thesis

The organization of the thesis is as follows. Brief background information is given in Section 2. Cryptographic primitives and algorithms are explained in Section 3. In Section 4 the literature and similar works with SSPayWMN are described. Requirements for a secure and seamless pre-payment system are described in Section 5. Section 6 discusses the evolution of SSPayWMN. In Section 7 the designed protocols for the proposed system are presented. In Section 8 the settlement of the operators and money exchange system are explained. In Section 9 there is a discussion about the success of the proposed system on meeting the previously explained system requirements. Unit test results are located in Section 10. Client types and mobility are described in Section 11. Real life scenario simulation results are placed under Section 12. Finally, Section 13 gives the conclusion.

# Background information and literature survey

In this section we give background information about WMNs in Section 2.1. Section 2.2 gives brief background information on cryptographic primitives. A literature survey will be given and related works of SSPayWMN will be explained in Section 2.3. The proposed system is the improved version of a previous project [38], the evolution of SSPayWMN will be explained in Section 2.4.

## 2.1 BACKGROUND ON WIRELESS MESH NETWORKS

Wireless Mesh Network (WMN) [1] is a multi-hop type of wireless networking, designed as an alternative to traditional centralized wireless networking achieved by mesh routers. Mesh routers and mesh network clients form up WMNs. Each mesh node functions as a host and also as a router, relaying packets on behalf of other nodes, connecting nodes that are not located within the transmission range of each other. WMNs create ad-hoc networks, which are dynamically self-organized and self-configured. WMNs are easy to deploy and cost-effective systems, they are easy to maintain and provide robustness and reliable service coverage.

WMNs comprise of two types of nodes: mesh routers and mesh clients. A wireless mesh router provides mesh networking by using routing functions that do not exist in common wireless routers with gateway/repeater capabilities. Mesh routers have multiple wireless interfaces to expand flexibility of WMNs. Mesh routers in WMNs achieve wider coverage compared with conventional routers by using multi-hop technology with lower transmission power. Moreover it is possible to hypothesize improved scalability by optimizing the medium access control (MAC) protocol in a mesh router.

## Network Architecture

WMNs are categorized into three considering the operation of the nodes in the network. These categories are infrastructure, client and hybrid WMNs.

*Infrastructure/Backbone WMNs:* The architecture of this WMN is shown in Figure 2.1. Both wireless and wired networks comprise infrastructure WMNs, in Figure 2.1, dash lines depict wireless connections; whereas, solid lines depict wired communications. Mesh routers establish an infrastructure to mesh clients to connect. The infrastructure is a cloud from the clients’ point of view. It is a black box that delivers packets originated from the clients to the gateways.



Figure 2.1. Infrastructure/Backbone WMNs. (taken from [1])

The mesh routers are self-configured and self-healing. In a case of node addition or removal, mesh backbone configures itself by forming up neighborhood. Additionally, mesh routers could connect to the Internet with gateway functionality. Infrastructure meshing provides easy to access to Internet by forming up clouds for clients. Bridging and inter-networking functionalities of WMNs enable clients to connect to mesh backbone with conventional Wi-Fi or cellular devices and also via Ethernet links. As depicted in Figure 2.1, base stations could also connect to mesh backbones, which provide Internet connectivity for all the clients of base stations.



Figure 2.2. Client WMNs (taken from [1])

*Client WMNs:* Client meshing is a subset of Infrastructure meshing. As previously explained mesh routers establish a backbone for mesh clients, however in client meshing case the whole network is a backbone and whoever wants to join the network has to be a part of the backbone and provide routing functionality. As shown in Figure 2.2, client meshing is a commune type of networking.

*Hybrid WMNs:* This architecture is combination of two previously explained mesh architectures. Mesh clients can access Internet through mesh backbone moreover they can communicate with each other by using a simple ad-hoc network.



Figure 2.3. Hybrid WMNs (taken from [1])

As shown in Figure 2.3, mesh backbone provides Internet connectivity; whereas, Client WMNs provide connectivity to mesh backbone for distant mesh clients.

## Characteristics of Wireless Mesh Networks

Characteristics of WMNs are explained as follows:

* *Multi-hop Wireless Network:* Main accomplishment of WMNs is providing extended wireless network coverage without increasing transmission power or additional antennas.
* *Support for Ad-hoc Networking:* WMNs provide flexible networking, which has abilities like self-configuring and self-healing. Deployment, node addition and removal are easy to accomplish since mesh routers form up routing paths by themselves.
* *Mobile Dependence on the Type of Mesh Nodes:* Mesh routers usually do not change their locations, whereas mesh clients are assumed to be mobile.
* *Multiple Types of Network Access:* Mesh routers are accessible via IEEE 802.11 protocols and also from peer-to-peer protocols.
* *Dependence of Power-Consumption Constraints on the Type of Mesh Nodes:* Mesh routers usually do not have power-consumption constraints but it is advisable for mesh clients to have some forms of power consumption techniques.
* *Compatibility and Interoperability with Existing Wireless Networks:* WMNs are compatible with IEEE 802.11 protocols [2, 3], therefore WMNs could communicate with conventional Wi-Fi and also other standards such as WiMax [4], ZigBee [5] and 3G-radio access [29].

## 2.2 BACKGROUND ON CRYPTOGRAPHIC ALGORITHMS

To establish a secure system, cryptographic primitive algorithms are employed. A brief explanation and introduction to cryptographic primitives are provided in this thesis.

In following sections, hash functions, hash chains and HMAC functions are explained. Moreover symmetric cryptography is described. Finally public key cryptography is explained at the end of this section.

## Hash Functions

Hash functions [7] are irreversible mathematical functions that map input strings of variable length to fixed sized output strings. Hash functions operate fast and it is infeasible to find the input string of a given ahs value.

A cryptographic hash function should have at least the following three properties:

* Pre-image resistance: Given a hash value v, it should be infeasible to find the an input string x such as (hash of x).
* Second pre-image resistance: Given an input , it should be infeasible to find another input string such that .
* Collision resistance: It should be infeasible to find to input string and such that .



Figure 2.4. Hash Function Example [7]

Figure 3.1 depicts the hash function flow. The function maps a message to a fixed size string. The output length depends on the hash algorithm; various hash algorithms have different output sizes.

Once well regarded and now outdated hash algorithms are MD5 [24] and SHA1 [23]. Improvement of cryptanalytic attacks and computational power these hash functions are not considered as secure anymore. Up to date, popular and well regarded hash functions are SHA2 [23], which is a set of SHA-256, SHA-384 and SHA-512 and SHA-3 [53] also known as Keccak.

## Hash Chains

Applying a hash algorithm to a value and using the output as an input for the next hash function forms a hash chain. Every output of a hash algorithm represents a link in the chain. Length of the hash chain [32] is determined by the number of times the hash algorithm is executed.



Figure 2.5. Hash Chain Depiction and Usage [8]

Since hash functions are irreversible, as shown in Figure 3.2 it is easy to go forward in the chain but it is not computationally feasible to go backwards.

A hash chain with *n* elements is denoted as:

Knowing the first link in the chain, which is , gives the opportunity to verify the following links in the chain as well. If one could establish a system, successful at distributing the first link in the chain, it is feasible to use hash chains as future keys for other cryptographic functions or tokens for micropayment.

Hash chains are easy-to-deploy and cost-effective therefore they are widely used in prepayment systems. Especially for systems that have delicacy for computational delay.

## HMAC Functions

A Message Authentication Code (MAC) [7, 16] is a short message which is calculated to provide authentication and message integrity. A MAC algorithm is a function which generates a MAC using a secret key. The integrity of the message is checked by calculating the MAC of the message and comparing the values. If the values are equal then the integrity of the message is verified. Authentication is also provided because a party, who is able to calculate a specific MAC value, proves that she knows the secret key.

HMAC [10] is one of the most popular MAC functions that use a keyed hash function. Hash functions are fairly fast algorithms, which makes HMAC fast.

## Symmetric Cryptography

Symmetric cryptography is the oldest kind of cryptographic primitive, which provides confidentiality. This primitive employs shared secret keys between two parties. These secret keys are used in encryption of plainttexts and decryption of ciphertexts. The security level of a symmetric cryptographic algorithm mostly depends on the key size. Modern algorithms use at least 128-bit long keys.



Figure 2.6. Symmetric Key Cryptography [16]

As shown in Figure 3.4, a plaintext is used as a parameter with the shared secret key in an encryption algorithm. Encrypted data is transmitted through an insecure medium. The receiver of the encrypted message decrypts the cipher text by using the shared secret key in the decryption algorithm.

Modern symmetric cryptographic functions could be categorized under two classes, which are stream ciphers and block ciphers. Stream ciphers encrypt data byte by byte. RC4 [15] is a popular example for stream ciphers. Secure Socket Layer (SSL) and Wired Equivalent Privacy (WEP) employs RC4. On the other hand, block ciphers encrypt an input data as fixed size blocks, and produces same-sized outputs. Data Encryption Standard (DES) [11] is once considered as the most popular symmetric key cryptography standard but it is not considered as secure any longer. RC5 [13] and Blowfish [14] are some other examples of symmetric key cryptography. Modern cryptographic systems use Advanced Encryption Standard (AES) [12].

## Public Key Cryptography

Public Key Cryptosystem (PKC) differs from Symmetric Key Cryptosystem according to number of keys used. PKC uses two separate keys; one of them is the public key the second one is the private key. The owner secretly keeps private key; whereas, the owner or a trusted third party broadcast the public key. It is computationally infeasible to calculate private key by exploiting the public key.



Figure 2.7. Public Key Encryption [17]

PKC is used for confidentiality purposes, i.e. for encryption and decryption. It is also used for authentication and non-repudiation purposes i.e. digital signing and verification. The type of encryption key defines the purpose of the algorithm. If the sender uses the public key for encryption then the algorithm operates for confidentiality purposes as shown in Figure 3.5.



Figure 2.8. Validating a Signature [18]

Authentication and non-repudiation are provided by using private key as the encryption key as depicted in Figure 3.6. Since no one could know the private key of the owner, only private key owner could produce the encryption of a plaintext encrypted with a private key, thus this operation digitally signs the plaintext. This kind of encryptions could be decrypted using the public key. Since the public keys are broadcasted, anyone could verify the digitally signed plaintext.

Some of the widely known, well-regarded asymmetric key cryptographic algorithms are Elliptic Curve Cryptography (ECC) [19, 54], Digital Signature Algorithm (DSA) [20], ElGamal [21] and the most known one is RSA [22] algorithm.

## 2.3. LITERATURE OF PAYMENT SYSTEMS AND SIMILAR WORKS OF SSPAYWMN

There has been extensive research on billing systems for network access. In this section a brief explanation will be given about similar works of SSPayWMN.

E-Payment schemes [42] could be grouped under two classes:

* Online Payment: The seller checks the payment by consulting a trusted party before verifying it.
* Offline Payment: The seller does not check the payment before serving the client.

Online payment schemes could be subdivided into two subgroups:

1. Payment by Transaction: Buyer and seller do not need a previous arrangement before the payment.
2. Payment by Account: There exists an account or a previous engagement between seller and buyer.

Micro-payment systems are built on e-payment systems. Micro-payment schemes [46] generally employ a type of electronic currency (e-cash/e-coin). General requirements [47] for micro-payment schemes are:

* Anonymity: A payment should not reveal buyer’s identity.
* Divisibility: The amount of money should be divided into e-currency. The e-currency should have a unit value.
* Transference: The e-currency should have approximately equal value when it is transferred between parties.
* Prevention of Double Spending: Clients should not be able to use e-currency for a second time.

Rivest and Shamir [43] introduced two simple micro-payment schemes called Pay-Word. Their protocol uses RSA algorithm for public key cryptography and hash-chains as payment tokens. In Pay-Word protocol the buyer generates a hash chain for a specific seller before making a purchase. The seller checks if the user is an authenticated Pay-Word user and the hash chain is indeed generated by this particular user. The amount of purchase is determined by the hash operation count performed on a value. The buyer selects the value and after the purchase deletes the hash chain. The seller collects the deserved money from the Bank, which appears to be a trusted third party in the system.

Pay-word is a credit-based payment scheme. The drawback of the system is that the hash chains are seller specific. Clients should store information about the sellers to be able to generate seller specific hash chains. Every time a new seller is added to a system the clients should be notified. In the existence of large amount of sellers the system becomes infeasible. Furthermore, the user should store different hash chains for every seller and store the last used hash token for all of the hash chains.

With this study Rivest and Shamir opened up an exciting field of research since then there has been modifications to their work. In [44], authors propose a new algorithm, which increases the performance of the previous work. They suggest an efficient payment system that uses RSA-typed blind signature [45]. The system supports anonymity and untraceable payments. However the system does not deal with mutual authentication, the user is not completely sure whom she is communicating with. The blind signature step of the algorithm takes a considerable amount of time to finish, which makes the system inappropriate for time sensitive tasks. Furthermore the past values between entities are huge numbers, which makes this system a poor choice for a network service providing scheme. Nevertheless it is useful for payment systems dealing with low amount of payment count.

Hwang and Sung [48] proposed a new micropayment scheme in 2006. Their micro-payment scheme uses one-way property of hash chains and elliptic curve cryptography [49] for blind signatures and for the purpose of providing anonymity. The system has three phases:

1. Registration Phase: Buyer and seller registers to the system by authenticating themselves to the trusted party.
2. Blinding Phase: The buyer executes a withdrawal protocol with the trusted party before purchasing for any service.
3. Transaction Phase: The buyer requests service from the seller and send the e-currency in this stage.
4. Redemption Phase: The seller communicates with the trusted party to redeem the deserved money.

The proposed scheme of Hwang and Sung remains secure and it provides anonymity as well. However the system fails in cost-effectiveness. The blinding phase employs elliptic curve cryptography and remains as the bottleneck in the system.

In 2009, an improvement [49] on Hwang and Sung’s algorithm is proposed. The proposed improvement is the replacement of elliptic curve cryptography at the blinding phase with RSA-based blinding signature. The new setting improved the scheme and made it gain considerable speed, however the necessity of signature before every transaction makes the system infeasible for micro-payments with high frequency.

Up to now, general e-payment schemes have been described. In this thesis, we focused on micropayment schemes for broadband Internet access using WMNs. In the rest of this section, we explain payment schemes for broadband network access in WMNs and other network types.

Chen, Jan, and Chen [50] proposed a micro-payment system for GSM calls, which uses hash-chains as e-currency. They introduced a TTP, which is actively present in the flow of the system. Their proposition was that there was no need for public key operations on client side to provide an undeniable and secure payment scheme. However their assumption was falsified by Li, Wang, Zhou and Chen [51]. In [51] it is shown that a dishonest mobile user could make calls without payment and also a misbehaving service provider could overcharge for it’s service. The authors propose a new billing scheme in [51] and in their scheme TTP generates two signatures for a service, which are *Starting Time* Signature and *Finishing Time* Signature. The duration between these signatures determines the duration of the GSM call. There exist 5 communication steps and 4 public key operations. A limitation of the system is the billing scheme adds extra time to the call and makes the client pay more without getting service.

In [30], the authors use a high-level approach for billing and propose an architecture. Their focus is mostly its performance on a threshold based bandwidth management algorithm. Untraceability is not supported in the system. In [31], the authors propose UPASS; a double hash chain based prepaid billing architecture for WMNs. Their trust model is based on both classical certificate-based public-key cryptography and identity-based cryptography. The drawbacks of [30] are the complex trust and payment structures, missing simulative and/or analytical performance model, and disregarding users' anonymity/privacy. Similarly, UPASS does not consider client anonymity and untraceability.

Qi, Zhao, Wang and Choi [52] have introduced a security authentication and an undeniable billing protocol for WMNs. The proposed scheme uses RSA public key encryption for authentication purposes and elements of hash chains as e-currency. The proposed authentication protocol has key generation steps, which slows down the system. Furthermore the system has no interest to provide anonymity and untraceability.

Many research on billing systems for WMNs have been done and many challenges have been tackled using cryptographic techniques. The general situation of the proposed systems is a lack of anonymity and untraceability support or bad performance for a high frequency payment scheme. SSPayWMN offers stable and affordable performance for payments with high frequency (needs to be verified by TTP too often) and also secure authentication with anonymity and untraceability properties.

## 2.4. DIFFERENCES AND SIMILARITIES WITH AN EARLIER WORK

The idea of SSPayWMN was first found and rooted by Can Yücel, in his thesis [38]. The motivation behind our thesis is same with [38], to build a secure and seamless micropayment system for wireless mesh networks. A basic is taken over and improved.

The topology of the network used is analogous to previous network topology. System flow is very similar except some changes that have been inserted. The packet flow used was from access points to operators, with mesh backbone and gateways in-between. The connection mediums between clients to the gateways were not encrypted and insecure lines. Gateways and operators however were connected with secure links. The assumption of secure lines between gateways and operators was not changed but also brought symmetric cryptography based security between gateways and access points. New system has become securer.

Simulation environment of current version of SSPayWMN uses the same network devices such as mesh routers, gateways and servers. Previous version used RSA-1024 however we have used RSA-2048 to improve the security of the system. We have used symmetric key encryption using AES-128 which was lacking in [38].

Most of the protocols have been changed; moreover we have added a new protocol, i.e. *Distribution of Public Keys*. However *Access Point Authentication* protocol is used intact as it appears in [38].

The main addition to the system is a Trusted Third Party (TTP), which brings an ultimate authority to the system. The usage of TTP and it’s servers provide credibility. Operators settle by communicating with TTP. Firstly clients pre-pay to TTP for the Internet service they are going to receive. Operators receive their payment from the TTP as they show the logs of their service.

[38] used operator as the end point of end-to-end protocols. We use TTP as the end point in order to provide undeniable verification and validation for critical applications.

In [38] some system entities were assumed to have public keys but an algorithm to distribute these keys were lacking. Existence of a TTP brings a possibility to use certificates in the system. SSPayWMN employs certificates for distribution of public keys. The distributed public keys could be broadcasted since they are signed by the TTP. This mechanism is added to SSPayWMN in this thesis.

Previous version of SSPayWMN did not clarify how the access points of the operators will be placed in the metropolitan area and the distribution of access points between operators. In SSPayWMN simulations two operators were assumed to exist. Operators share the area in-between and compete to serve the users with stronger access points. There is a rivalry between operators since clients connect to stronger access points. An operator with low amount of investment for the system could not survive since high amount of access points are needed to serve in a wide range. The clients would not connect to an access point with a low signal rate if there is another access point with high signal rate in their range. As it will be explained later, there is no difference between operators in the sense of payment for the clients.

Anonymity and untraceability of the clients were not provided in [38]. These properties of the system should be provided by the system as long as there is no request for user actions and identity by a formal authority such as the police department. Current version of SSPayWMN provides anonymity and untraceability to some extent. Using aliases as client identity provides anonymity in the system. The aliases are changed periodically therefore only the actions between the periods can be tracked. The time period and detailed design will be explained in upcoming chapters of this thesis.

In [38], roaming between operators was costly therefore it was not 100% seamless to the client. Clients were customers of a particular operator, which implies an overcharge in the case of roaming to another operator. Current version of SSPayWMN makes every user of the system a client to the TTP. The TTP pays operators for their services. The new setting enables SSPayWMN to provide pure seamless roaming. In return *Seamless Mobility in Home Operator* and *Roaming* protocols have been changed to Seamless Mobility and *Seamless Roaming* respectively.

Internet service providing is simplified in the current version. The pre-payment was for a total packet size. In our version, clients buy hash tokens that ensure Internet service for a predefined period of time. Seamless micropayment is preserved. Furthermore, we have increased the Update Packets interval in the system. In SSPayWMN, we set the update packets interval to a value slightly larger than . In a situation where a client that does not send the next hash token within this period, that means the client is dropped. Therefore the burden on the system caused by update packets is reduced significantly and with the new settings it is easier to handle the dropped clients.

In [38], simulations of the proposed scheme were done considering the same type of client. In this thesis, we have divided the clients into groups considering their socio-economical status. Speed, traveling distances, client’s frequency of system usage are all affected by the client types and deterministic random distributions. Earlier version of SSPayWMN was lacking simulations of real-life situations, which are covered in the current version. Possible situations in real-life such as the diversity in mobility or system usage in time were not properly covered in [38]. In [38], burst scenario only covered users trying to authenticate themselves into the system on the same time. A rush hour scenario was lacking in which clients try to authenticate themselves in close time periods, but not necessarily on the same exact moment. Current version covered most of the possible scenarios within an ordinary day.

[38] employed the Random Way Walk Model [39] of the network simulator. In this model, clients’ mobility patterns were totally random, with no logical base. These mobility patterns were not systematic, which causes unrealistic results in simulations. In this thesis, clients move from one point to another for a purpose. The new setting brings more realistic simulation results. The new network simulations are designed considering a real metropolitan area. We have used a model similar to Manhattan Mobility Model [41]. The setting of the roads is a grid, and the clients move from one location to another by using these roads. We have replaced the movement probabilities of the original Manhattan Mobility Model with random speeds and destinations. Speed and distances to destination are random but they are also affected by client types. Additionally our simulations cover a larger area with more access points than the simulations in [38]. Simulations in [38] had 32 access points with 16 gateways. Our simulations have 100 access points with 32 gateways.

A very significant improvement on [38] is the change of the network simulator used to simulate the system. In [38], the system was simulated using the Discrete Event Simulator: OMNET++ [40]. OMNET++ has offered GUI support and strong network simulation tools but it was lacking IEEE 802.11s [25] support. Therefore, an ad hoc network simulation was executed to mimic the simulation of a real wireless mesh network. Converting the previous simulation results to a new network simulator was not feasible because there was no connection between OMNET++ and another network simulator. It was inevitable to implement the system from scratch on another network simulator, which has IEEE 802.11s wireless mesh network support. We have chosen network simulator 3 (ns-3) [6]. ns-3 supports IEEE 802.11s. However ns-3 did not support internetworking for mesh networks. It was infeasible for us to implement full internetworking and bridging functionalities for mesh networks on ns-3. As a solution, we have implemented virtual bridges between network nodes, and write every packet sent or received on text files. Every node in the system checks for packets to send in the text files. Every node in the mesh backbone had two interfaces in our design. The delay of passing the packets from one interface to another was neglected. This is, actually how internetworking and bridging functionalities of wireless mesh networks was mimicked.

Detailed and more realistic simulation settings and scenarios brought higher quality results. In this thesis, we focused on latency metrics for both independent protocol performances and for overall system performance. In [38], some latency tests have been done, but this did not reflect the typical behavior.

To conclude, in this thesis we have considerably improved [38] from both design and implementation (simulation) aspects.

# requırements and protocols of the system

In this section we will explain the requirements of the system and general system design. Then we will give brief explanation for system protocols. Finally we will explain the settlement of the protocols and money flow in the system.

## 2.1. REQUIREMENTS OF SSPAYWMN

A secure prepayment scheme for WMNs requires following attributes:

* **Wide Coverage:** Users should be getting service within a large area.
* **Seamless Roaming:** Users should connect and maintain their connection and continue to get service even while they are moving. Designed connection method should apply to different operators. From payment point of view, Users should be able to switch between operators as they move without a service interruption.
* **Seamless Mobility (Handoff):** Users should be able to switch between access points of the same operator as they move without a noticeable delay.
* **Anonymity:** It should not be feasible to track down a user’s network actions from their payments (unless law enforcement requires doing so).
* **Mutual Authentication:** For preventing malicious use of network, both user and network should be mutually authenticated.
* **Two-way honesty:** Clients cannot deny that they did not take service. Operators cannot claim that they provide service more than they actually provide. These are to be guaranteed by using strong cryptographic protocols.
* **Preventing Double Spending:** A payment token should not be used to get more services than its value. In particular, the payment token should not be used twice or more.
* **Untraceability:** It must not be possible to relate connection sessions of the users with other connection sessions. In this way, higher level of privacy could be provided.
* **Performance:** System should work effectively with stable performance. Additional caused by the system should be minimal.

## Requirements of the Network

Our SSPayWMN system does not only consist of a mesh backbone, but also Wi-Fi clients and wired servers. Mesh backbone basically relays the packets from clients to server so that the clients are able to get service.

Servers of the operators are wired and will be communicated via regular 802.3 Ethernet protocol in its local area. Mesh backbone will communicate within itself using IEEE 802.11s protocol. Clients will use IEEE 802.11a/b/g Wi-Fi protocols to connect to the access points/mesh routers.

## General Overview of the Proposed Scheme

The proposed system supports user identification, authentication as well as authorization and accounting. The main objective is to design and develop a secure payment infrastructure for WMNs that also considers users' privacy and fairness. Our system model assumes the existence of mobile clients and operators, who will be charging the service they give. The operator's mesh backbone is made of several mesh routers, which are actually Access Points (APs) with IEEE 802.11s support. This backbone is connected to operator's server via a gateway. There exists a TTP (Trusted Third Party), which is reachable through an operator. These system components are listed together with their icons, used in the protocol figures, in Table 5.1.

Table 2.1. System Entities

|  |  |
| --- | --- |
| C:\Users\Public\Pictures\client.png | Mobile user (client) |
| C:\Users\Public\Pictures\ap.png | Access Point (AP) with mesh routing capability. From now on in this document, it is called as AP, but please note that it also has routing capability. |
| C:\Users\SUUSER\Documents\GitHub\worddoc\thesisImages\meshBackbone.png | Mesh backbone of the operator |
| C:\Users\Public\Pictures\gateway.png | Gateway (GW) that connects the mesh backbone to outer world and also to the operator's server |
| C:\Users\Public\Pictures\operator.png | Operator's server (OP). Keeps necessary logs and user info. |
| C:\Users\SUUSER\Documents\GitHub\worddoc\thesisImages\ttp.png | Trusted Third Party (TTP). Payment related logs are mostly to be generated by the TTP. |

Since the clients are mobile, they may handover among different mesh routers (i.e. access points) of the same operators. They may also roam among different operators, not only due to coverage reasons, but also for having a better quality service. Our system aims to have seamless mobility (handoff) and seamless roaming for payment purposes such that when the client gets service through a new AP or switch to another operator, authentication and authorization are not performed from scratch.

From security point of view, we aim to have mutual authentication between client and the network in our protocols. Anonymity of the clients and untraceability across different usage periods (a.k.a. unlinkability) are privacy related goals of the protocols.

From payment point of view, our main aim is to have a fair system in which all the claimed transactions bear cryptographic proofs. In this way, the clients cannot repudiate using a service and the operators cannot claim for services that they do not provide. The latter is especially important during inter-operator settlement; it is also important to resolve client disputes.

The protocols detailed in this deliverable are designed by considering the abovementioned requirements. The symbols used in this document are given in Table 5.2.

Table 2.2: The List of the Symbols

|  |  |
| --- | --- |
|  | XOR operation |
|  | Concatenation |
|  | Encryption of using the key |
|  | Decryption of using the key |
|  | Taking hash of times |
|  | Taking HMAC of using the key |
|  | th element of the hash chain (usage order) |
|  | Public key of TTP |
|  | Private key of TTP |
|  | th Access Point or its identity |
|  | th Operator or its identity |
|  | Public key of |
|  | Private key of |
|  | Serial Number |
|  | Nonce created by entity |
|  | Previous Alias |
|  | New Alias |
|  | Public key certificate of |
|  | Initialization Vector |
|  | Timestamp |
|  | Connection Request |
|  | Disconnection Request |
|  | Roaming Request |
|  | Change Alias Request |
|  | Mobility Request |
|  | Response (used in various protocol as positive acknowledgment) |
|  | Disconnection Acknowledgement |
|  | Roaming Acknowledgement |
|  | Mobility Response |

## Network Topology and General System Design

Secure and Seamless Pre-Payment System employs previously explained system entities. The system entities are assumed to be located in a metropolitan area. While access points establish a mesh backbone and wait for clients to connect to them, gateways transmit the packets received from the access points to servers of the operators.



Figure 2.1. Network Topology

Figure 4.1 shows the topology of the network and connections between entities. Connection between serving access points is wireless and they use IEEE 802.11b/g Wi-Fi protocol, and they use IEEE 802.11s protocol [25]. The mesh backbone emulates a cloud from the mobile user’s perspective. It is a black box; which receives packets from mobile user and delivers them to the gateway in a multi-hop manner. Mesh backbone uses Hybrid Wireless Mesh Protocol (HWMP) [26], which is a hybrid routing protocol, which has routing tables.

Connection medium between mesh backbone and gateway (GW) is either wireless or wired. GWs and operators communicate through wired connection. The connection between an operator and TTP is also wired. These connections use 802.3(Ethernet protocol) [27].

## Connection Card Structure

*Connection Card* is the main deed that clients buy from the TTP and use to get Internet service. We use a prepaid system, in which connection cards include credits as tokens. Hash tokens are generated using hash chains as discussed below. Connection cards also have unique *Serial Numbers* (), which are to be used for alias computation.

Tokens for getting Internet service are basically links in a hash chain. For each set of tokens, the TTP picks on a random *Initialization Vector* () and takes hashes of it many times. The number of hash operations is actually the number of token in a set. For example, if the client wants a hundred hash tokens, then the hash of is taken hundred times. More formally a hash chain with 100 tokens is constructed in the following way.

…

is the first token to use. Then we use the token in the increasing order of token index. In this way, we exploit one-way property of hash algorithms such that an attacker cannot learn the next token even if she knows the previous ones.

Connection Cards are refillable with hash tokens, which are to be sold by the TTP. Operators compete with each other to provide high-quality service for broadband access in the WMN since the users are assumed to have free roaming.

Serial Number is a 128-bit value. With this setting, the system is able to support up to users. Hash tokens are to be generated using SHA-256 hash algorithm; hence they are 32 bytes long.

Considering current technology, smart cards are suitable tools to be connection cards. A simple Connection Card with 4 KB memory could store an and more than 1000 hash tokens.

## Alias Computation

Aliases are temporary identifiers for clients. They change frequently using a secure protocol. Anonymity is achieved by changing aliases by the previously stated way however it is only durable to some extent.

The serial number (SN) of the Connection Card, which is bought from an operator, will be used as a base for client’s aliases. An alias will be computed by performing the following operations:

1. Client will pick a random 128-bit unsigned number and call it his nonce .
2. Perform XOR operation with and his nonce; take the hash of the output.
3. Client will use this alias whenever his identity is required.

Aliases are 128-bit values; even if it is a very small possibility to have the same alias with another client at a given point of time, there is still a nonzero probability. To address this problem, TTP checks the proposed alias to be a unique one. This check is done in Change Alias protocol, which will be mentioned in Section 6.

The nonce values used in computation of the aliases are to be sent in encrypted messages to the TTP in the related protocol. Therefore only the client and the TTP can relate the aliases originated from a particular .

## PROTOCOLS OF THE SYSTEM

In this section, we will explain the protocols of the system. There are 10 protocols in the system. End-to-end Two-way protocols consist of Initial Authorization and Reuse-CC, Disconnection and Change Alias protocols. These protocols send packets from clients to the TTP and return the packets back to clients. Update Packets protocol is a End-to-end One-way protocol, which sends packets from clients to the TTP. Other protocols i.e. Seamless Mobility, Seamless Roaming, Packet Transfer and Access Point Authentication are independent protocols and do not belong to any group. Distribution of Access Point Public Keys protocol is not implemented in the simulations and it is assumed to occur before the system deployment.

## Initial Authorization and Reuse of a Connection Card

Initial Authorization is the beginning for system usage. Whenever a client purchases new hash tokens from the TTP, she will need to authorize herself to TTP. Initial Authorization Protocol, shown in Figure 6.1, achieves mutual authentication and authorization of the user.

The clients may disconnect before using up all the credits in a connection card. *Reuse of a Connection Card* (Reuse-CC) protocol allows the clients to connect using the remaining credits in a card. Reuse-CC protocol does not differ extensively from *Initial Authorization* protocol. The main difference is instead of sending first hash token; the client sends whichever token is the next one. Alias will change before the protocol starts. Both protocols compute new aliases before sending the Connection Requests (). The crucial point here is that TTP should be able to update last hash value entry of the client in the database and associate it with the new alias.

In Figure 7.1, connection between client and serving access point () is Wi-Fi (IEEE 802.11b/g). The access point is a member of a mesh backbone and a particular access point is to be selected according to its transmission power. Since it is assumed that all access points have the same attributes, the serving access point is the closest access point to the client.

Macintosh HD:Users:canleloglu:Desktop:worddoc:thesisImages:protocolsInDetail:seqDiagram:pdf:initAuthReuse.pdf

Figure 2.2. Initial Authorization and Reuse-CC

Mobile clients introduce themselves to the operator using *Initial Authorization* protocol. in Initial Authorization protocol, in Reuse of a Connection Card protocol. TTP already knows mobile user’s serial number () and the first element, , of her hash chain. The mobile user does not want to reveal her to any adversary because that will be used all the time and it is sensitive information from security and privacy points of view. To achieve anonymity, the mobile client computes an alias and uses this value instead of . The mobile client will change her alias periodically as she continues to get service (Change Alias protocol will be explained later).

Initial Authorization and Reuse-CC steps are described below.

1. Client computes an alias using a nonce that she generated.
2. (The is assumed to have credits)
3. Client sends this to .
4. receives the connection request and relays the request through mesh backbone.
5. Gateway receives the and relays it to the operator.
6. Operator relays to TTP.
7. TTP receives the connection request () and decrypts it using its private key.
8. TTP checks alias' uniqueness within its database of users, it would make the client start over the protocol if alias is not unique.
9. It computes .
10. TTP checks and association. Store and
11. TTP computes
12. TTP sends to the Operator.
13. Operator receives and verifies the signature using public key of TTP.
14. The Operator gets and and stores these values. The value of is the client's alias until she changes it.
15. Operator sends to the gateway.
16. GW receives and verifies the signature using public key of TTP.
17. GW stores and .
18. GW uses the shared secret key with and calculates
19. GW sends to through mesh backbone.
20. receives and decrypts it using the shared secret key with GW.
    1. verifies the signature using public key of TTP.
    2. It calculates and and stores these values.

The wired links are secured however the communication between GW and APs are insecure; therefore the packets that are sent through this medium are encrypted with shared secret keys between GWs and APs.

## Access Point Authentication

After authentication processes of the client with the TTP, a second authentication step begins. Client and access point will mutually authenticate each other for safe communication; this protocol ensures the feature -Mutual Authentication- of SSPayWMN.

Figure 7.2 describes the protocol briefly.

Macintosh HD:Users:canleloglu:Desktop:worddoc:thesisImages:protocolsInDetail:seqDiagram:pdf:accessAuth.pdf

Figure 2.3. Access Point Authentication

1. sends a challenge request to the client, which started connection.
2. When client receives this challenge request:
   1. Client drops the packet if it is not the that she sent connection request.
   2. Client drops the packet if there was not any .

If (a) and (b) are 3 invalid then the client sends a 128-bit challenge to the .

1. takes the HMAC of this challenge, and uses relevant hash value (here , but it could be any if the authentication protocol runs after the Initial Authorization or Reuse-CC protocols) as the key of HMAC.

   2. sends to the client.
2. Client also takes the HMAC of the challenge and uses the stored hash value () as the key. Then it compares the result with the one that access point sent.

If it is authenticated, client starts to use access point to get Internet service.

## Packet Transfer

After mutual authentication of client and , the client starts to send packets as shown in Figure 7.3.

Macintosh HD:Users:canleloglu:Desktop:worddoc:thesisImages:protocolsInDetail:seqDiagram:pdf:packetTransfer.pdf

Figure 2.4. Packet Transfer

1. Client starts the session with the first hash token (in this case current has value is ) of the remaining hash chain.
2. receives , and updates client’s service starting time.
   1. Checks if
   2. If true sends acknowledgement () to client and updates currently used hash value as .
3. Client sends first 512-byte data packet .
4. If the client gets served for over the threshold value (5 minute interval is used in simulations) then the AP asks for the next hash token.
5. The steps between (1) and (4) are repeated as long as client gets Internet service.

## Changing Alias

Anonymity property is easily achieved by using aliases, but complicated part is achieving untraceability. The aliases should change on a basis that an adversary, who knows a certain client’s alias, could not be able to trace client’s activity on her home network, and also could not trace her movements among the operators or access points.

To be able to change alias in a safe way, client needs to communicate with TTP but interrupting TTP very often would slow down the entire operation due to extra delays caused. Therefore periodic changes of aliases are mandatory and these changes are achieved by making access points to ask all of the active clients for new aliases after a certain period of time. Attackers or access points themselves would know that aliases are changed but would not know the mapping between old aliases and the new ones. Such a protocol is also used in Mix Networks [28].

Simultaneous alias changes aim to prevent attacks that would aim to analyze network traffic of access points and examine connection requests. Enforcing alias change by the access points, a more generalized control over the clients is achieved. Attackers could not understand which client wanted to change her alias, because all the clients getting service from a particular access point have requested to change their aliases at that particular time.

The client should request changing alias, because client and the TTP should be the only parties who know association between an alias and a client’s SN.

Alias Change Timer is a local timer that runs on every Access Point. All of the timers are set roughly to the same time manually. System designer decides on the time value on which the access point will count down from (50 minutes of time period is used in simulations). The timer period is updateable by the TTP. TTP knows every access points’ public key, it could send new interval by encrypting the new value with the public keys of the access points. However, this process is not covered in simulations.

Macintosh HD:Users:canleloglu:Desktop:worddoc:thesisImages:protocolsInDetail:seqDiagram:pdf:changeAlias.pdf

Figure 2.5. Changing Alias

Changing Alias Protocol is shown in Figure 7.4 and described below.

1. Client continues to get service, in other words uses the *Packet Transfer* protocol.

When the Alias Change Timer countdown finishes, Access Points broadcast "Change Alias" command to all of their clients. The interval value is a system parameter; 50 minutes of interval value is used in the simulations.

1. Client receives "Change Alias" command.
2. Client computes a new alias by picking up a new random nonce N’CL and computing .
3. Client forms a Change Alias Request ()
4. The client sends the to .
5. receives and relays it to the GW via mesh backbone.
6. Gateway forwards to operator.
7. Operator forwards to TTP.
8. TTP receives Change Alias Request () and decrypts it using its private key.
9. TTP checks for new alias' uniqueness and starts over the protocol if not unique.
10. TTP computes .
11. It checks SN and association and stores and .
12. It computes .
13. TTP sends to operator.
14. Operator receives and verifies the signature using public key of TTP.
15. The operator receives and and stores these values.
16. Operator sends to the GW.
17. GW receives and verifies the signature using public key of TTP.
18. The GW receives and , and stores these values.
19. The GW encrypts the and calculates
20. GW sends to the .
21. receives and decrypts it as follows:
22. The verifies the signature using public key of TTP.
23. The reveals and and stores these values.

## Update Packets

In standard flow of the system, after authentication, access points handle the accounting. Because of the fact that access points keep the last alias and token of the client they are able to validate next token by performing hash operation to the token they kept and compare it with new coming hash token. However it is essential to send periodic updates to the TTP to provide stability in the system in the case of client drops.

Access points keep track of ongoing communications, after some time passed without update from a user it send disconnection request by itself. When access points broadcast change alias commands they delete all the record related to previous connections therefore they do not send unnecessary disconnection packets to TTP.

Macintosh HD:Users:canleloglu:Desktop:worddoc:thesisImages:protocolsInDetail:seqDiagram:pdf:updatePackets.pdf

Figure 2.6. Update Packets

Protocol design of Update Packets protocol is shown in Figure 7.5 and the details of the protocol are explained below.

1. After client sends the first token, the access point starts to count the time passed. After units of time (value of is a system parameter, 11 minutes of an time interval is used in simulations), access point encrypts the Alias and lastly used hash token using the public key of the TTP and sends this cipher text to the GW.
2. The GW receives the update packet and forwards it to TTP through related operator.
3. TTP receives the update packet and decrypts the packet using its private key. TTP updates the last token used by the client.
4. In a case of client drops from the network, access point concatenates the Alias, hash value and a time stamp and encrypts them with the public key of TTP. Sends it to TTP as a disconnection request from the client.

## Disconnection

To be able to run Reuse-CC, the client has to run a proper disconnection protocol. The Update Packets protocol brings stability to the system in case of a connection interruption, but the main assumption is that most of the users will be disconnecting from the operator using the disconnection protocol that we explain in this section and in Figure 7.6.



Figure 2.7. Disconnection

Disconnection protocol is described below.

1. Client forms a disconnection request

Client sends the packet to the .

1. relays to the mesh backbone, to make it reach to the GW.
2. GW receives and forwards the to the Operator.
3. Operator receives and forwards the to the TTP.
4. TTP receives the and . It checks the association between the and the hash token; if the association holds, then it computes a disconnection acknowledgement ().

TTP sends the to the Operator.

1. Operator receives , verifies the signature on it and marks client as disconnected.

Operator relays to GW.

1. GW receives , verifies the signature on it and marks client as disconnected.

It relays to the mesh backbone.

1. eventually gets the , verifies the signature on it and disconnects the particular client, which corresponds to the it received. Ideally access points are assumed to delete all information about the past connections for the sake of anonymity and untraceability. However if operators decide to trace user’s actions then they could do so for a limited time until the client changes it’s .

## Distributing Access Point Public Keys

Achieving seamless mobility in home operator and also to support seamless roaming, a public key distribution mechanism is integrated in SSPayWMN system.

In Figure 7.7, a generic model for public key distribution is shown. This protocol has two parts; one is certificate generation for access point public keys, the other one is distribution of the public keys. The part between operator and the TTP is offline. This part of the protocol runs during set-up, before the deployment of the access points in the field.

If an operator wants to add a new access points to the metropolitan area then it should perform the same protocol but his time only for the new access points.

Macintosh HD:Users:canleloglu:Desktop:worddoc:thesisImages:protocolsInDetail:seqDiagram:pdf:distributeAccessPublicKeys.pdf

Figure 2.8. Distributing Access Point Public Keys

Distributing Access Point Public Keys algorithm is described below.

1. Operator generates public/private key pairs for the access points in its mesh backbone and embeds these keys to them before the deployment.

* Operator forms an access point list (); which consists of access points and their corresponding public keys.
* Operator sends this list to the TTP through a secure channel or in offline manner.

1. TTP receives the and starts to generate certificates for every access point and public key pair.

* Certificates are formed as:
* TTP stores these certificates for distribution.
* Other protocols are employed (such as *Initial Authorization* or *Reuse-CC* protocols) of SSPayWMN for certificate distribution. Suppose an AP does not possess its certificate. In such a case whenever this access point gets a connection request it will concatenate a certificate request to the packet. When the TTP receives such a request, it concatenates corresponding certificate to the connection response. Then, TTP sends the connection response and together to the operator.

1. Operator receives the connection response and the certificate and relays these packets to the access point through gateway and mesh backbone.
2. Access point receives and stores its certificate and broadcasts it to the nearby access points.

## Seamless Mobility and Roaming (Payment Related)

*Seamless Mobility* and *Roaming* protocols are run whenever the client changes the serving access point. The running protocol is called *Seamless Mobility* if the new access point belongs to the same operator as the previous access point. If the operators differ, then the protocol is called *Seamless Roaming.*

Every access point has its public/private key pair and ability to broadcast it’s public key, seamless mobility in current operator and roaming could be handled in a seamless way without running the authorization process from scratch. As it is shown in Figure 6.8, client gets a signed handover ticket from its old access point and uses this signed ticket to maintain to get Internet service from a new access point.

Macintosh HD:Users:canleloglu:Desktop:worddoc:thesisImages:protocolsInDetail:seqDiagram:pdf:seamlessMobRoaming.pdf

Figure 2.9. Seamless Mobility (if X == Y) or Roaming (if X != Y)

Seamless Mobility and Roaming protocol is shown in Figure 7.8 and described below. In this protocol, the client would like to switch from its old operator () to a new one (). In this setting, is the last access point that the client got services from . , is the access point that the client would like to continue to get services in network.

1. Client sends a Mobility Request () to .
2. receives and forms a Roaming Acknowledgement ().

* sends to the client.
* consists of the mobility ticket that the client uses to get services from the . It is signed by and encrypted for .

1. If the new operator is different than the previous operator, then starts the disconnection protocol for the client after sending .

* This disconnection protocol runs in parallel with the roaming protocol. Thus it does not put an extra delay in roaming. Old operator () stores disconnection acknowledgement () to support its claim to get funds for the services that it provided until roaming occurs. TTP stores the information that this disconnection is due to a roaming to in order not to get confused when disconnects without a connection request reached to it.
* In this scheme, ’s signed ticket serves as a formal document, which represents the beginning of the session with .

1. Client receives and forwards it to the new operator ().
2. decrypts using its private key.

* reveals the signed ticket of the . sends this signed data to it’s affiliated operator to use it for collecting funds from TTP.
* verifies the signature over this signed ticket using ’s public key. Then, it checks in order to decide whether the ticket has expired or not.
* Then, starts a challenge-response protocol with the client.
* The rest of the protocol is the same as Access Point Authentication Protocol.

## Payment to the Operators (Settlement)

The settlement of the operators is similar with the settlement step in [38]. The purpose and the technique is the same, however the log design and TTP operations are different. Therefore, settlement step of SSPayWMN is altered but not completely changed.

In SSPayWMN, operators claim their money from the TTP by showing their service logs. A log proves a service that has been provided between a connection request and a disconnection request.

Operators store connection requests () of the clients; are formed in the Initial Authorization and Reuse of a Connection Card protocols. When a client makes a disconnection request, operator stores the disconnection request () as well. After receiving the , operator forms its log as follows.

stands for timestamp in the logs. are mandatory in the logs to make TTP’s job easier.

When TTP receives two consecutive logs from an operator:

1. TTP will sort the logs according to their value.
2. TTP first decrypts since it is encrypted with the public key of TTP. consists of , and the first hash token to be used to get service.

Consider

TTP decrypts it using its private key, and gets SN by the XOR operation:

Note that SN’s first token used is .

1. TTP decrypts the Signed Connection Response using its public key, and gets the alias and the hash token. TTP compares the values with the ones in connection request. If they match, then the log is marked as valid.
2. The abovementioned log is only a service starter; operator needs to show service-ending log to claim its money from the TTP.

Service ending log naturally has a larger value; therefore this log comes later in the sorted list of logs.

TTP takes the ending log and decrypts using its private key.

TTP gets , and the hash token from the decrypted . TTP makes the XOR operation: and gets the . Note that used is the hash token came with the to end the service.

1. TTP takes the Signed Disconnection Response and decrypts it using its public key. TTP gets the alias and the hash token from it, and compares the values with the ones came with the . If the values match, TTP considers the log as a valid service-ending log.
2. After validating the logs, TTP performs the hash operation over service ending hash token until it reaches the service starter hash token. TTP counts these hash operations. This count is mapped to funds for the provided service.

However the misusage of the logs should be reckoned with. Consider the situation of a client:

* Gets service from her home operator between and
* Gets service from a foreign operator between and
* Gets service from her home operator between and

In this type of situation home operator has two and , whereas foreign operator has a and . Home operator has the following logs:

The home operator has served between and and also has served between and . Home operator would want to take the money for serving between and . It could pretend that it has served the client between and by not sending and . Since indicates that client is disconnected from the operator at and suggests that the client started to get service from the operator at . Sending only and results TTP to think that the home operator has served the client between and . This way operator would want money for serving 30 hash tokens.

Abovementioned situation suggests that there should be another operator, which has served between and . Second operator would have two logs as follows.

Foreign operator proves that it has served between and by showing the signed and .

TTP would see that it has already paid home operator for service to that particular client between and . This means that home operator has tricked TTP to pay more.

In the proposed system TTP is the one who has the authority, it pays operators their money. If the TTP finds an operator misbehaving it could give a penalty to the operator and do not pay for future services, or there could be several other kinds of penalties, since TTP has the proof it could bring the subject to the court as well.

# sımulatıons of sspaywmn

In this section we will explain the simulation environment and properties of system entities in the implementation. Then timings of cryptographic operations on different system entities will be explained. Unit test results and comments on independent protocol performances will follow. Then we will present the client models and mobility scheme. The overview of real-life scenario simulation results will be given. Finally, every real-life scenario simulation result for protocols will be shown and explained.

## 3.1. SIMULATION ENVIRONMENT

The network topology is hierarchical and WMN supports connections with other IEEE 802.11 protocols [2, 3], clients communicate with TTP via access points, GWs and operators in sequence. Access points are connected to gateways with 6-54 Mbps Wi-Fi connection. Some important specifications about the access points are shown in Table 9.1. *Update Interval* determines the time value between two update packets that access point send to TTP.

The simulator was run on a computer with 2.4 GHz Intel Core 2 Duo, 2 GB 1067 MHz DDR3, Apple MacBook OSX v10.6.8.

Table 3.1: AP Specifications

|  |  |
| --- | --- |
| AP-Gateway Connection bit rate | 6-54 Mbps – Wi-Fi |
| AP-Gateway Distance | 100 m |
| Service Duration per token | 5 minutes |
| Update Interval | 11 minutes |

The network consists of 32 gateways and 100 access points. In unit simulation there is only one mobile client whereas in real-life scenario simulations there are 300 mobile clients.

## Cryptographic Operations and Their Timings

Public Key Cryptography timings for access points and gateways are mentioned in [33]. For operator servers and TTP servers, timings from [34] are used. For mobile clients, performance values from [35] are used. For AES timings the values from [36] are used, which results a 0.00004 second of delay for AES-128 on Linksys WRT54GS. The same value is used for gateways as well. Timings of hash algorithms are taken from [37] which are considerably lower than symmetric key encryption delay.

Platform specifications are shown in Table 9.2, and RSA-2048 timings are shown in Table 9.3.

Table 3.2: Platform Specifications

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Gateway [11] | Linksys WRT54GS (AP) [11] | Server [12] | Client [13] |
| CPU Speed | 2.08 GHz | 200 MHz | Dual-core 64 bit 2.8 GHz | 3.2 GHz |
| CPU type | AMD Athlon XP 2800 | Broadcom MIPS32 | Intel Xeon | Celeron D 351 |
| RAM | 512 MB | 32 MB | - | - |

Table 3.3: RSA-2048 Timings

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Gateway [11] | Linksys WRT54GS [11] | Server [12] | Client [13] |
| RSA Signing | 1.3 ms | 37.9 ms | 8.13 ms | 1.8 ms |
| RSA Verification | 47.3 ms | 1529.0 ms | 0.32 ms | - |

## 3.1. UNIT TEST RESULTS

Unit tests cover protocol behavior under low pressure. In these tests there is only one user, and this user performs the same protocol every minute. These tests are done to ensure that modules of the system are fit for use.

As discussed earlier some protocols show similarity considering packet sizes, cryptographic operations and packet routes. Since there would be no difference between unit tests of protocols that are in the same group, there is one result chart for a particular group of protocols.

## Unit Test Result for End-to-End Two-Way Protocols

Unit tests for end-to-end two-way protocols consist of a user, running the same protocol every minute. Charts present the average delay of packet delivery over time. In this simulation the user sends the packet to a serving access point and the packet hops 2 times in the mesh backbone until it reaches the gateway. Gateway forwards the packet to operator and operator transmits the packet to TTP. TTP processes this packet and sends it back to the client through the same route.

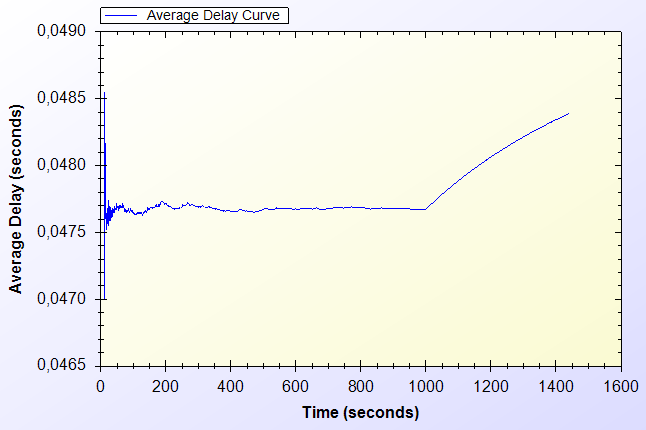


Figure 3.1. End-to-End Two-Way Protocols Unit Test Result

As shown in Figure 10.1, there is a delay that shows variation around 0.04 second. This unstable behavior is caused by different initial packet delays. System needs some packets to set up paths between mesh nodes. The performance stabilizes in time. Average delay shows a peak by the end however the difference between highest and lowest values of the results is inconsiderable.

## Unit Test Result for Access Point Authentication

*Access Point Authentication* protocol consists of a challenge-response protocol. It contains two HMAC operations.

Unit test for this protocol contains a user, trying to run access point authentication protocol with a serving access point every minute. The resulting chart, presented on Figure 10.2, shows the average delay of the protocol versus time.



Figure 3.2. Access Point Authentication Protocol Unit Test Result

Average delay of access point authentication converges to 0.05 second in the steady state. The initial delay values are higher than the later ones, because nodes need some time to establish and see who is around. At the time of initial deployment, wireless nodes send and receive beacons and perform operations using them.

## Unit Test Result for Seamless Mobility and Roaming

*Seamless Mobility* and *Seamless Roaming* protocols have the same behavior since client sends and receives same length of packets. Thus, they are grouped together for unit tests.

Unit test for *Seamless Mobility* and *Seamless Roaming* protocols consists of a client changes serving access point every minute. Client is located in between two access points and these access points are both eligible for service. Since these protocols must be seamless to the user it is important to get reasonable delays for these protocols.

Figure 10.3 presents the unit test result for *Seamless Mobility* and Roaming protocols.



Figure 3.3. Seamless Mobility and Roaming Protocols Unit Test Result

In unit test for these protocols, a 0.15 second of network delay for access point change is observed. Similar to other protocols, there is a transitive period at the beginning of the simulations, however it reaches steady state in time and gains balance.

## Unit Test Result for Packet Transfer

*Packet Transfer* is the mostly used protocol in the system. It is crucial to have small amount of network delay for this protocol because of it’s often use. Unit test scenario of *Packet Transfer* protocol is that a client sends a 512-byte packet every minute.

Figure 10.4 shows the unit test result for Packet Transfer protocol.



Figure 3.4. Packet Transfer Protocol Unit Test Result

Unit test gave a higher average delay value at the early parts of the simulation but expectedly it reaches a balance through time. As seen on Figure 10.4, at steady state, packets are received in a very short amount of time, which is around 0.0002 second.

## Unit Test Result for Update Packets

*Update Packets* protocol takes place between AP and TTP. In this simulation access point updates the user info stored at operator. Figure 10.5 shows the average delay of *Update Packets* protocol over time.

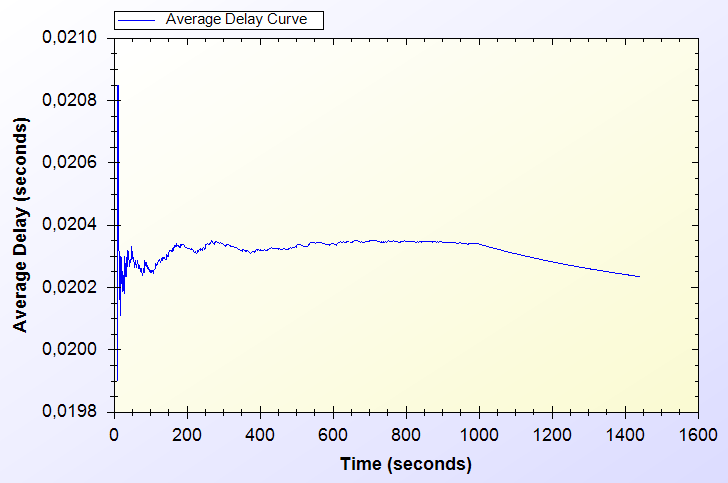


Figure 3.5. Update Packets Protocol Unit Test Result

In the simulation scenario, APs update operator once in every second. Our simulation showed that there is a 0.02 second maximum network delay for updating operator for the client usage.

## USER MODELING AND MOBILITY

The proposed system intends to serve a variety of users (a.k.a. network clients). Network clients differ in their network usage frequency with respect to time of day, their mobility patterns and frequency of usage.

Certain kinds of actions are defined, such as authorization (initial or reuse of a connection card), disconnection, packet transfer (network usage), payment related roaming and payment related AP handover. All of these actions are triggered as a result of a random event. Connection and network usage related actions are triggered according to a two-state Markov Chain model [8]. Roaming and handoff related actions are triggered by user mobility.

## User Actions

In real-life scenario simulations, network usage related actions are modeled using two-state Markov Chain as shown in Figure 11.1. There are two states that a user could be in: *Connected* and *Not Connected*. State transitions or staying in the same state triggers some actions as described below.



Figure 3.6. State Diagram of Clients

The initial state is *Not Connected*. In this state, the user switches to *Connected* state with the probability value of . This state transition triggers *Initial Authorization* (if the CC is used for the first time) or *Reuse of a Connection Card* protocol (if the connection has been used before). In this way, the user starts consuming the network and getting the service. While in *Not Connected* state, the user stays in the same state with probability value of .

While in *Connected* state, the user remains connected (i.e. stay in the same state) with the probability of . Staying connected triggers *Packet Transfer* protocol. In other words, the user continues to get service via the currently connected AP. In *Connected* state, transition to *Not Connected* state occurs with probability of. This transition disconnects the user via *Disconnection* protocol.

In this 2-state Markov chain model, the average connection duration, , is calculated as the expected value of staying in *Connected* state, as given below.

(1)

Where, denotes .

The expected value of staying in *Not Connected* state is the average idle time for a user between two connections. This value, , is calculated as follows.

(2)

Where, denotes .

## Client Types

Three different user types are outlined with different networking and mobility requirements. Considering whether they are working, studying or domestic provides the differentiation among user types.

The network usage within one day has been modeled in three time slots: (i) night (00:00 – 07:59), (ii) daytime (08:00 – 15:59), and (iii) evening (16:00 – 23:59).

User types are described as follows:

* **Students:** This kind of clients uses network services mostly in the evening when they return back from school. Their possibility to use network services during morning and night is relatively small comparing to mid-day time. Thus, the probabilities for being active are higher for evening. Students are assumed to be mobile at the beginning and end of the *daytime* slot since they go to their school. Until the end of the *night* slot, students would more likely to get service in their homes in an immobile way.
* **Employees:** This kind of clients has routine lives. They are immobile and not so active during nights. However, during the daytime, they are very active and use network services at their work places. Moreover, they are mobile as they commute to/from work from/to home at the beginning and end of the working times.
* **Domestics:** This type of users does not work outside and spend their time at home. Usually the domestics get Internet service in an immobile way. These users are highly active at all times.

The parameters of and are determined based on the abovementioned discussion about the client type characteristics and the time slots. These values are given below. The triplet specify the probability values for night, daytime and evening, respectively.

These values also determine the average connection duration and idle time by using Eq. 1 and 2. For example, a domestic client remains idle during daytime for minutes between connections. Once connected, average connection time for this category is minutes.

## User Mobility and Timing

Real-time scenario covers Internet usage of 300 users in a 1-km2 metropolitan area. The simulations time begins at 00:00 a.m. and lasts for 24 hours. Simulation time is divided into 3 parts considering night, daytime and evening. Every part of the day has different statistical values for client behaviors.

Simulations are run for 1440 seconds, however every second in the simulation stands for 1 minute in real life.

In real-life scenario simulations clients are able to move from one location to another. The time and direction of their movement is selected at random but probabilities are affected by user roles. For example, when school is over, a student is most likely to move towards her target destination (e.g. her home).

Clients are assigned a random target access point. Every one of 100 access points has 3 initial clients. The client moves from its current access point to the target access point on the grid. An example movement pattern is shown in Figure 11.2. As a client moves from access point A to the access points B, if she needs to connect to the Internet, she forms up a new connection with the access point, which is closest to client’s current location.



Figure 3.7. User Movement from A to B

In real-life scenario simulations, there are two operators and they have same amount of access points. In current simulations, each operator has 50 access points. The client executes handover or roaming if there is an active connection during movement between access points. In such a case, depending on the new access point’s affiliated operator, user’s movement triggers either *Seamless Mobility* or *Roaming* protocols. If new access point’s affiliated operator is same as the one that client currently uses, and then it means the client would perform *Seamless Mobility* protocol for handover. Otherwise, the client would run *Seamless Roaming* protocol.

Clients are assigned uniformly distributed random speeds between 2 km/h to 6 km/h. The clients are assumed to move without a motor vehicle.

## SIMULATION RESULTS FOR REAL-LIFE SCENARIO

Results for unit test simulations are described before; however the most significant results are real-life scenario simulation results. Despite the randomness of the system, users’ actions are highly related to their group and current simulation time.

Charts for the results display the average delay for a particular protocol.

## Overview

Final simulations provided the results in Table 12.1. Charts on Figure 12.1 and Figure 12.2 are drawn exploiting the results in Table 12.1. Considering the results it could be calculated that over 100 minutes of Internet service, workers have only waited for 1 minute for system delays. In average, over 1000 minutes of Internet service needs a delay of 13 to 16 minutes of waiting.

Table 3.4: Simulation Results for Client Types

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Total Internet Usage Time | Total Internet Usage Delay | Average Internet Usage Time for a Client | Average Internet Usage Delay for a Client |
| Student | 95899 Minutes | 1698 Minutes | 958 Minutes | 16 Minutes |
| Worker | 101681  Minutes | 1316 Minutes | 1016  Minutes | 13 Minutes |
| Non-Worker | 105335 Minutes | 1456 Minutes | 1053 Minutes | 14 Minutes |



Figure 3.8. Total Amount of Service Usage Times for Client Types vs. Total Delays



Figure 3.9. Average Service Usage Times for Client Types vs. Average Delays

As described before the clients are grouped into 3 groups. The client roles and probabilistic values affect their behavior in the system, which results difference between overall values of the simulations.

Figure 12.1 and Figure 12.2 shows the overall results for real-life scenario simulation. Figure 12.1 shows comparison of minutes clients used as idle or active. Figure 12.2 shows the average value for the clients of the same group.

## Real-Life Scenario Simulation Result for Initial Authorization



Figure 3.10. Real-life Simulation Result for Initial Authorization Protocol

*Initial Authorization* protocol is used at the beginning of the service for each user. As it is seen on the chart every one of the 300 users are authenticated at the end of 40th minute.

Simulation starts around the 10th minute in the morning. At the beginning there is a huge amount of users, trying to authenticate. Figure 12.3 indicates that, this process varies between 0.6 and 2.5 seconds. After 10 minutes it attains a balance and *Initial Authorization* protocol meets a delay of 1 second, which means when users open up their mobile device they would have Internet service after 1 second.

## Real-Life Scenario Simulation Result for Reuse of a Connection Card Protocol



Figure 3.11. Real-Life Simulation Result for Reuse of a Connection Card Protocol

*Reuse of a Connection Card* protocol is used after disconnecting from the system. As it is seen it is a highly used protocol in the system. It starts around the 50th minute and used for the entire time of the simulation.

As seen on Figure 12.4, at the beginning of the protocol the delay changes between 0.1 and 0.6 second. After some time protocol achieves a balance and a 0.4 second of network delay is observed.

## Real-Life Scenario Simulation Result for Changing Alias



Figure 3.12. Real-Life Simulation Result for Changing Alias Protocol

Every active client uses *Changing Alias* protocol in the system in every 50 minutes. The protocol is first used at 50th minute and it is used entire time of the simulation.

As one can see on Figure 12.5, at the beginning of the protocol the delay for the protocol varies between 0.1 and 0.4 seconds. The average delay for the protocol converges to 0.4 seconds after some initial deployment time.

## Real-Life Scenario Simulation Result for Disconnection



Figure 3.13. Real-Life Simulation Result for Disconnection Protocol

*Disconnection* protocol first appears around 30th minute and it is used through the entire time of the simulation. Figure 12.6 shows that, at the beginning of the system Disconnection protocol average delay vary between 0.1 and 0.5 second but through time the average delay meets 0.4 second.

## Real-Life Scenario Simulation Result for Update Packets



Figure 3.14. Real-Life Simulation Result for Update Packets

*Update Packets* protocol is an end-to-end one-way protocol. It is expected to get lower delay values for this one. Only access points use *Update Packets* protocol and they send packets to TTP. The packets are sent every 10 minutes.

As it is seen on Figure 12.7, at the early stages of the protocol, the average delay value varies between 0.6 and 1.4 second but then after some time the protocol stabilized around 0.4 second.

## Real-Life Scenario Simulation Result for Seamless Mobility in Home Operator Protocol



Figure 3.15. Real-Life Simulation Result for Seamless Mobility Protocol

*Seamless Mobility* protocol is used when a handover happens between access points. If these access points are belonging to the same operator then it means the client is using *Seamless Mobility* protocol.

By looking at Figure 12.8, it could be said that*, Seamless Mobility* protocol has an initial average delay that shows difference between 0.2 and 1.2 seconds. A user loses around 0.1 second to make a handover to the new access point.

## Real-Life Scenario Simulation Result for Roaming Protocol



Figure 3.16. Real-Life Simulation Result for Roaming Protocol

*Roaming* protocol is used when a handover happens between access points. If these access points are belongings of different operators then it means the client is using *Roaming* protocol.

*Roaming* protocol has an average delay that varies between 0.05 and 0.2 seconds. There are 2 operators so a client has a %50 chances to make a *Seamless Mobility* or *Roaming* protocols. After some time protocol reaches a balance around 0.2 second of delay.

As one can see on Figure 12.9, the results for *Roaming* protocol shows a boost until the middle of the simulation time but it decreases and achieves a balance

## Real-Life Scenario Simulation Result for Packet Transfer



Figure 3.17. Real-Life Simulation Result for Packet Transfer Protocol

*Packet Transfer* protocol is the mostly used protocol in the system.

Figure 12.10 states that, at the beginning of the protocol the average delay value varies between 0.005 and 0.025 but then the protocol achieves a balance around 0.02 second.

# discussion

In Section 4 the requirements for a secure and seamless pre-payment scheme were discussed. In this section the success of the proposed system on meeting the requirements and simulation results are discussed.

Wide Coverage: Every access point could serve within a 100 meters radius. It is proven that with 100 access points, 1 km2 area is covered for Internet service.

Seamless Connection and Roaming: Users are able to switch between access points no matter what operator they belong to. The delays are low enough to maintain current connection without any interruption.

Roaming/mobility: Reuse of a connection card is possible after attempting first connection. Roaming is supported, when our protocol is implemented in participating *AP*s, and tokens are valid.

Anonymity: For legal purposes users must give their identities to connection card issuer (*TTP*) for getting connection cards. Therefore, as far as *TTP* keeps clients’ identities secret, users can stay anonymous. However, every action of the client is completed using their aliases.

Mutual authentication: Initial Authorization and Reuse-CC protocols ensure the authentication of the user. TTP signs the acknowledgement values and a handshake protocol is run between the serving access point and the client. These processes ensure mutual Authentication.

Two-way honesty: Since the tokens are issued by *TTP*, only the *TTP* and connection cardholder knows all the tokens that are related with a specific connection card. Hence whenever a Client sends a new token, it is not possible for him to say, “I did not use it”. Since *TTP* is a trusted third party, in the roaming phase, operators cannot say that they provided service for non-used tokens.

Preventing double spending: Clients could not pay with a hash token, which is not related to previous tokens. Since all the clients have different *Initial Value* forthe beginning of their hash chain an upcoming token could not be another client’s hash token.

Untraceability: Our protocol provides untraceability by changing aliases periodically. Clients are traceable between the times they change their aliases nonetheless they could not be related to future actions after the alias change. The period of time to change the aliases is a choice of the designer.

Performance: The performance of the system is tested using ns-3. Both unit tests and real-life scenario results are obtained. In both simulations system protocols achieved a steady state performance. Achieving stable performance is significant because it represents the system behavior in rush situations and long run.

# Conclusion

In this thesis we have proposed a secure and seamless pre-payment scheme for network service. The system uses outputs of hash operations in reverse manner to use irreversibility property of hash functions. Fast computation of hash algorithms ensures a fast and secure system for Internet service pre-payment.

In unit tests, standalone performances of the protocols under trivial usage scenarios are analyzed. Unit tests set an example for how the system will behave in empty hours. In this way, the first proof-of-concept implementation of the system is provided and showed that the designed protocols reach steady state.

In real-life scenario simulations we have tested the proposed scheme using complex scenarios with realistic client types and movement patterns. Expected behavior of SSPayWMN is took form after these simulations since they are most close-to-real-life simulations of all the SSPayWMN simulations performed before.

Uniform probability distribution model enabled us to simulate real time scenarios in simulation environment, and gets results closer to real time situations. Different client types are used to make simulations closer to real-life. There is also randomness in the system, so different outcomes could occur for the same simulation.

Unit tests and real-life scenario simulation results show that the proposed system is a considerable and an effective pre-payment system.

# References

1. Akyildiz, I. F., Wang, X., and Wang, W. (2005) Wireless mesh networks: a survey, *Computer Networks and ISDN Systems*, 47(4): 445-487.
2. Intel Inc., Multi-Hop Mesh Networks—a new kind of Wi-Fi network.
3. J. Walker, Wi-Fi mesh networks, the path to mobile ad-hoc. Available from [http://www.wi-fitechnology.com/ Wi-Fi\_Reports\_and\_Papers/Mesh\_Networks\_References.html](http://www.wi-fitechnology.com/%20Wi-Fi_Reports_and_Papers/Mesh_Networks_References.html).
4. Vaughan-Nichols S.J., (2004) Achieving wireless broadband with WiMax, *IEEE Computer*, vol. 37, no.6, pp. 10-13.
5. The ZigBee Alliance. Available from: <http://www.zigbee.org>.
6. Network Simulator 3 (ns-3) <http://www.nsnam.org>
7. Trappe, W. Washington, L. C. Introduction to Cryptography with Coding Theory, Second Edition, pp. 218-220
8. Oligeri, G. Chessa, S. Giunta, G. Loss Tolerant Video Streaming Authentication in Heterogeneous Wireless Networks, Computer Communications, 34(11): 1307-1315, 2011.
9. American Bankers Association, *Keyed Hash Message Authentication Code*, ANSI X9.71, Washington, D.C., 2000
10. H. Krawczyk, M. Bellare, and R. Canetti, *HMAC: Keyed-Hashing for Message Authentication*, Internet Engineering Task Force, Request for Comments (RFC) 2104, and February 1997.
11. FIPS PUB 46-3 (1999) Data Encryption Standard (DES), <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>
12. FIPS PUB 197 (2001) Announcing the Advanced Encryption Standard (AES), <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
13. Biryukov A. and Kushilevitz E. (1998). Improved Cryptanalysis of RC5. *EUROCRYPT* 1998.
14. Bruce Schneier (1993) Description of a New Variable –Length Key, 64 bit Block Cipher (Blowfish), <http://www.schneier.com/paper-blowfish-fse.html>
15. Robshaw, M. J. B. (1995) Stream ciphers, RSA Laboratories Technical Report.
16. W. Stallings, Cryptography and Network Security: Principles and Practices, 3rd edition, Prentice Hall, NJ, 2003.
17. Managed File Transfer and Network Solutions, <http://www.jscape.com/blog/bid/82975/Which-Works-Best-for-Encrypted-File-Transfers-RSA-or-DSA>
18. Coleridge, R. (1996) The Cryptography API, or How To Keep A Secret, *Microsoft Security Technical Articles*, <http://msdn.microsoft.com/en-us/library/ms867086.aspx>
19. Koblitz, N. (1987). "Elliptic curve cryptosystems". *Mathematics of Computation* 48 (177): 203–209.
20. FIPS PUB 186-3 (1994) Digital Signature Standard (DSS) - CSRC, http://csrc.nist.gov/publications/fips/fips186-3/fips\_186-3.pdf
21. Elgamal, T. (1985) A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, *IEEE Transactions on Information Theory*, <http://caislab.kaist.ac.kr/lecture/2010/spring/cs548/basic/B02.pdf>
22. Rivest, R., Shamir, A., and Adleman, L. (1978) A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*,21(2): 120–126.
23. FIPS 180-3 (2008) Secure Hash Standard (SHS), <http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf>
24. RFC 1321 (1992) The MD5 Message Digest Algorithm, <http://tools.ietf.org/pdf/rfc1321.pdf>
25. Joseph D. Camp and Edward W. Knightly The IEEE 802.11s Extended Service Set Mesh Networking Standard
26. Kai Yang, Jian-feng Ma, Zi-hui Miao (2009) Hybrid routing protocol for wireless mesh network, Computational Intelligence and Security – CIS ’09
27. Ethernet Prototype Circuit Board, Smithsonian National Museum of American History, Retrieved 2007-09-02.
28. Chaum, D. (1982) Untraceable electronic mail, return addresses, and digital pseudonyms, *Communications of the ACM, 4(2)*.
29. Rao, Y.S.; Wing-Cheong Yeung; Kripalani, A., "Third-generation (3G) radio access standards," *Communication Technology Proceedings, 2000. WCC - ICCT 2000 International Conference on*, vol.2, no., pp.1017-1023 vol.2, 2000  
    doi: 10.1109/ICCT.2000.890849
30. Zaghloul, S., Bziuk, W. and Jukan, A. "A scalable Billing Architecture for Future Wireless Mesh Backhauls", IEEE ICC ’08.
31. Zhang, Y. and Fang, Y., "A secure authentication and billing architecture for wireless mesh networks", Wireless Networks, vol.13, no. 5, pp. 663-678, October 2007.
32. Lamport, L. (1981) Password authentication with insecure communication, *Proceedings of Commun. ACM,* vol. 24, no. 11,pp. 770-772.
33. Efstathiou, E., Frangoudis,P., and Polyzos,G. (2006) Stimulating Participation in Wireless Community Networks, *IEEE INFOCOM, 2006,* Barcelona*,* Spain.
34. Deng, L., and Kuzmanovic, A., (2009) A feeder-carrier-based internet user accountability service, *Northwestern University Technical Report,* <http://networks.cs.northwestern.edu/susinet/TR-09-12.pdf>
35. Yakovyna, V., Fedasyuk, D., Seniv M., Bilas O. (2007) The performance testing of RSA algorithm software realization, *CAD Systems in Microelectronics*, *CADSM ’07*, pp. 390-392, Polyana, UKRAINE.
36. B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson Performance Comparison of the AES Submissions, Proc. Second AES Candidate Conference, NIST, March 1999, 15-34.
37. Crypto++ 5.6.0 Benchmarks: <http://www.cryptopp.com/benchmarks.html>
38. Yucel, C. (2010). A Secure Prepaid Micropayment Scheme for Wireless Mesh Networks (Unpublished master’s thesis). Sabanci University, Istanbul, TR.
39. David B. Johnson and David A. Maltz. Dynamic source routing in ad hoc wirelees networks. In Mobile Computing, edited by Tomasz Imielinski and Hank Korth chapter 5, pages 153-181. Kluwer Academic Publishers, 1996.
40. OMNET++ Discrete Event Simulator, <http://www.omnetpp.org>
41. P. Crescenzi, M. Di Ianni, A. Marino, G. Rossi, and P. Vocca. Spatial Node Distribution of Manhattan Path Based Random Waypoint Mobility Models with Applications. In Sirocco 2009, to appear.
42. Tiwari, A., Sanyal, S., Abraham, A., Knapskog, J. S. & Sanyal, S., “A Multi-factor Security Protocol for Wireless Payment-Secure Web Authentication Using Mobile Devices”, IADIS International Conference Applied Computing, pp.160-167, 2007.
43. Ronald L. Rivest and Adi Shamir, "Pay-word and MicroMint: Two simple micropayment schemes", International Journal of Network Security, volume 2, No. 2, pp 81-90, 2001.
44. Mohammad A. Al-Fayoumi, Sattar J. Aboud, Mustafa Ahmad Al-Fayoumi, Daniyal AlgHazzawi, (2010) Efficient E-Payment Protocol Using Hash Chain, EMCIS2010 Proceedings Accepted Refereed Papers, 2010, 12-13 April, Le Royal Méridien Abu Dhabi
45. Chien H, Jan J and Tseng Y, "RSA-based partially blind signature with low computation", Proceeding of the International Conference in Parallel and Distributed Systems, pp. 385–389, 2001.
46. O’Mahony, D., Tewari, H. and Peirce, M. Electronic Payment Systems. Artech House, Inc, 1997.
47. Praneetha R. Bayyapu, Manik Lal Das (2008) An Improved and Efficient Micro-Payment Scheme, available at [www.jtaer.com](http://www.jtaer.com) DOI: 10.4067/S0718-18762009000100008
48. Hwang, M. S. and Sung, P. C. A study of micro-payment based on one-way hash chain. International Journal of Network Security, vol. 2, no. 2, pp 81-90, 2006.
49. N. Koblitz. Elliptic Curve Cryptosystems. Mathematics of Computation, vol. 48, pp. 203-209, 1987.
50. Y. Y. Chen, J. K. Jan, and C. L. Chen, “A fair and secure mobile billing system,” Computer Networks, Vol. 48, 2005, pp. 517-524.
51. Shiqun Li, Guilin Wang, Jianying Zhou, Kefei Chen (2007) Undeniable Mobile Billing Schemes, European Public Key Infrastructure Workshop - EUROPKI, pp. 338-345, 2007.
52. Ji Qi, Yi Zhao, Xingming Wang, Jaeho Choi, "Security Authentication and an Undeniable Billing Protocol for WMNs," cyberc, pp.266-269, 2010 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2010.
53. G. Bertoni, J. Daemen, M. Peeters and G. Van Assche, The KeccakSHA-3 submission, 2011.
54. Miller, V. (1985). "Use of elliptic curves in cryptography". CRYPTO 85: 417–426.