Authors: Albert Levi and Can Serhat Leloğlu

Contents

[1 Summary 2](#_Toc341537974)

[2 Introduction 2](#_Toc341537975)

[3 Network Topology 3](#_Toc341537976)

[4 User Modeling and Mobility 5](#_Toc341537977)

[4.1 User Actions 6](#_Toc341537978)

[4.2 Client Types 6](#_Toc341537979)

[4.3 Parameters 7](#_Toc341537980)

[4.4 User Mobility and Timing 8](#_Toc341537981)

[5 Results 9](#_Toc341537982)

[5.1 Overview 10](#_Toc341537983)

[5.2 Initial Authorization 11](#_Toc341537984)

[5.3 Reuse of a Connection Card 12](#_Toc341537985)

[5.4 Changing Alias 13](#_Toc341537986)

[5.5 Disconnection 13](#_Toc341537987)

[5.6 Update Packets 14](#_Toc341537988)

[5.7 Seamless Mobility in Home Operator 15](#_Toc341537989)

[5.8 Roaming 16](#_Toc341537990)

[5.9 Packet Transfer 17](#_Toc341537991)

[6 Conclusion 17](#_Toc341537992)

[References 18](#_Toc340937145)

# Summary

Wireless Mesh Network (WMN) technology is a multi-hop, high-speed networking technology for broadband wireless access. In this project, called SSPayWMN (Secure and Seamless Payment scheme for Wireless Mesh Networks), we design a secure and privacy-preserving prepaid payment scheme for broadband access using WMN technology. In the first WP of this second year, the developed protocols were tested in network simulator 3 (ns-3) as unit tests and performances were reported. In this deliverable, which includes the results obtained in the second WP of the second year of the project, we present the real life scenario results for SSPayWMN protocols. In these scenarios and corresponding tests, we model different types of users with different mobility and usage requirements changing in time of day basis, and consider various operators. As expected, the results obtained have more delay as compared to unit tests, but we achieved stable and affordable delay results.

# Introduction

In [1], we have briefly explained system and network requirements for SSPayWMN. In [2], we compared available network simulators and explained our decision for which network simulator to use. In [3], the design of the protocols are explained, and in [4] unit test results for the protocols, which are performed using network simulator 3 (ns-3), were presented. In this document we will present the results for the real-life scenario results for the designed protocols.

Unit tests [4] had been performed in order to understand the performance of our protocols under no stress. Real time scenarios, that are explained in this deliverable, show how our protocols would respond to any real time situation and how their performances are affected.

In the first half of the second year of the project we have implemented our protocols in network simulator 3 version 3.9 (ns-3). 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. We have improved ns-3 such that communication between mesh networks and other kinds of networks became possible. We also fixed a bug that was creating problems after 100th second of the mesh network simulation.

We have designed real life scenarios so that the simulation results reflect the most meaningful result. For these real life scenarios, we have grouped the clients into 3 groups. Group properties will be explained later in this deliverable. There is a probabilistic distribution for the client behavior based on the predefined group parameters and the simulated time of day so that we can model daily routines. Our clients are mobile so that their access points and/or operators change over time as well.

The rest of this deliverable is organized as follows. In Section 3, we give the network topology and design used in simulations. In Section 4, User modeling and mobility issues are explained. We give the simulation results in Section 5. Finally, Section 6 discusses and summarizes the conclusions reached by these analyses.

# Network Topology

SSPayWMN simulations are aimed to be close to real life situations. That understanding would ease the process, implementing SSPayWMN in real life. ns-3 is a successful network simulator but in order to get accurate results, a realistic network topology and user modeling need to be used. The former one, network topology, is going to be explained in this section.

In SSpayWMN, we have for different network entities in the construction of the network topology (other than the end users). These are shown in Table 1 (end users will be explained in Section 4).

|  |  |
| --- | --- |
| D:\My Documents\albert\tt proje\accessPoint.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. |
| D:\My Documents\albert\tt proje\gateway.png | Gateway (GW) that connects the mesh backbone to outer world and also to the operator's server |
| D:\My Documents\albert\tt proje\operator.png | Operator's server (OP). Keeps necessary logs and user info. |
| D:\My Documents\albert\tt proje\trustedThirdParty.png | Trusted Third Party (TTP). Payment related logs are mostly to be generated by the TTP. |

Table 1 System Entities

Simulations are done for a metropolitan area, where the blocks are located as a grid. Access Points (APs), which happen to be mesh routers at the same time, are located on a grid, which has 100 meters of step length. The area is a square one and is covered by 10x10 APs. Together with 50 meters of margin beyond the APs at the boundary, the coverage area becomes 1 km2. Figure 1 shows the mesh backbone topology.

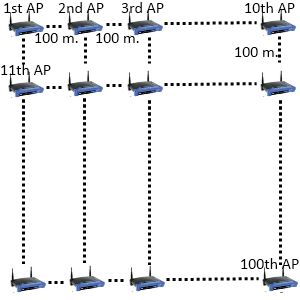


Figure 1. Mesh Backbone Topology

In the mesh backbone, the APs use 802.11s protocol and provide high-speed communication. Due to gird structure, every mesh neighbor with maximum four other mesh routers in four directions (north, south, east and west). Some mesh routers will be close to a gateway, which would lead us to have mesh routers with maximum five neighbors. On the other hand, the routers at the corners and the boundary of the region would have two or three neighbors as can be seen in Figure 1.

Gateways are located inside the mesh backbone. They will be accessible via mesh routers. We aim to make a mobile client to be able to communicate with a gateway through maximum 3 hops. This is necessary for increased speed and throughput, because mesh backbone is the most important and critical part of the network. Performance of wired and Wi-Fi technologies are proven to be efficient and fast. Communication between gateways and operators is wired. Mobile clients communicate with access points/mesh routers via Wi-Fi, so these parts of the network do not add a considerable overhead. Experience from the simulations showed that after 5 hops, mesh network could drop the packet or bring an unacceptable delay to packets. That is why we kept number of gateways high. More specifically we have 300 mobile clients, 100 access points, 50 gateways, 2 operators and 1 trusted third party in the topology. The entire topology is depicted in Figure 2.



Figure 2. Network Topology

# User Modeling and Mobility

In SSPayWMN, we intend 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 roaming behavior.

In our simulations, we define user types and model their corresponding behaviors. We define certain kinds of actions, 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 a two-state Markov Chain model, which will be described in Section 4.1. Roaming and handoff related actions are triggered by user mobility, which will be described in Section 4.3.

Three different user types are defined with different networking and mobility requirements. The differentiation among these types is provided by considering whether they are working, studying or domestic. These user types will be discussed in detail in Section 4.2.

## User Actions

In our simulations, network usage related actions are modeled using two-state Markov Chain as shown in Figure 3. 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.

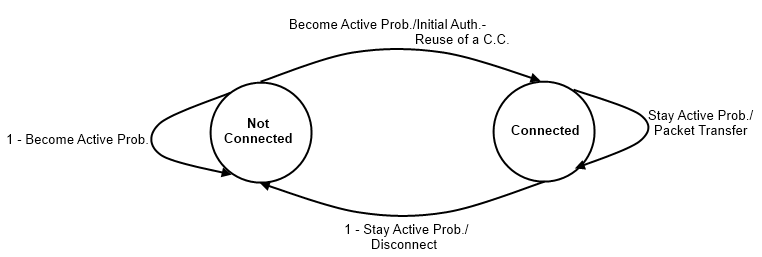


Figure 3. State Diagram of Clients

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

While in *Connected* state, the user stays connected (i.e. stay in the same state) with probability . This 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.

Eq. 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.

Eq. 2

where, denotes .

## Client Types

Three different user types are defined with different networking and mobility requirements. The differentiation among these types is provided by considering whether they are working, studying or domestic.

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. During the day and night, there is possibility to use network services, but this is relatively small. 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. it is possible for a student to go out with his/her friends and use “Seamless Mobility” and “Packet Transfer” protocols all the time.
* **Employees:** This kind of clients has routine lives. They are immobile and not so active during nights and evenings. 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 they 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 triplets specify the probability values for night, daytime and evening, respectively.

These values also determine the average connection duration and idle time by using Eqs. 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. We have divided the day 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, but every second in the simulation time stands for 1 minute in real life. In the simulations the night time begins at 00:00 a.m. and lasts until 07:59. Daytime period starts at 08:00 and finishes at 15:59. Evening starts at 16:00 and finishes at 23:59.

In our simulations clients are able to move from one location to another one. 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 his/her target destination (e.g. his/her home).

Considering user roles and their probabilities clients are assigned random movement times. Clients are also assigned a random target access point. The client moves from its current access point to the target access point on the grid. An example movement pattern is shown in Figure XXX. As a client goes on his/her way, if he/she needs to connect to Internet, he/she forms up a new connection with the access point, which is closest to client’s current location.

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. If there is an active connection during the movement of a client, he/she either handovers or roams. 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, then it means the client would perform *Seamless Mobility* protocol for handover. Otherwise, the client would run *Seamless Roaming* protocol. *Seamless Mobility* and Seamless *Roaming* protocols are explained in [3].

Clients are assigned uniformly distributed random speeds between 1 km/h to 6 km/h. The clients are assumed to move without a motor vehicle.

SORULAR:

* Active iken kullanim miktari ne kadar? Ne kadarda bir yeni token gonderiliyor?

# Results

Results for unit test simulations are available in [4], but the more important results are real-life scenario simulation results. Please note that there is randomness in the system. The actions of the clients are based on random numbers, but of course we define the chances they have to act in a particular way considering client type and time.

Charts for the results show the average delay for a particular protocol so far.

## Overview



Figure 3. Total Amount of Internet Usage Times for Client Types vs. Total Delays



Figure 4. Average Usage Times for Client Types vs. Average Delays

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

When we look at Figure 3 and Figure 4, we see the following results in the simulations.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Total Internet Usage Time | Total Internet Usage Delay | Average Internet Usage Time for a Client | Average Internet Usage Delay for a Client |
| Student | 95899,262599999 Minutes | 1698,9540999994 Minutes | 958,992625999999 Minutes | 16,9895409999945 Minutes |
| Worker | 101681,64  Minutes | 1316,3589999995 Minutes | 1016,8164  Minutes | 13,163589999995 Minutes |
| Non-Worker | 105335,0894 Minutes | 1456,1214999995 Minutes | 1053,350894 Minutes | 14,561214999995 Minutes |

Table 2. Simulation Results for Client Types

Final simulations gave the results in Table 2. Charts on Figure 3 and Figure 4 are drawn using the results in Table 2. Figure 3 explains the total amount of internet usage times for client types. These results show variance but it is not very distinctive between users. Figure 4 shows average internet usage times and delays. Considering the results it is very convenient that over 100 minutes of Internet service, workers have only waited for 1 minute. In average over 1000 minutes of Internet service need a delay of 13-16 minutes of waiting, which is considerable and satisfactory.

## Initial Authorization



Figure 5. Results 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. This means there will be users that are out of the system at the end of the first hour despite the high probability of getting active at the morning.

Simulation starts around the 10th minute of the morning. At the beginning there is a huge amount of users, trying to authenticate. Figure 5 show that, this process of the users varies between 0.6 and 2.5 seconds. After 10 minutes it achieves a balance and we have an *Initial Authorization* delay of 1 second, which means when a users opens up their mobile device they have internet service after 1 second.

## Reuse of a Connection Card



Figure 6. Results 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 SSPayWMN system. It starts around the 50th minute and used for the entire time of the simulation.

As seen on Figure 6, at the beginning of the protocol the delay changes between 0.1 and 0.6 second. After some time protocol achieves a balance and we have a 0.4 second of *Reuse of a Connection Card* protocol delay.

## Changing Alias



Figure 7. Results 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 7, at the beginning of the protocol the delay for the protocol varies between 0.1 and 0.4 seconds. After some time the average delay for the protocol achieves a balance and we have an average of 0.4 seconds for *Changing Alias* protocol.

## Disconnection



Figure 8. Results for Disconnection protocol

*Disconnection* protocol has prerequisite protocols, which are *Initial Authorization* or *Reuse of a Connection Card* protocols because a user needs to be in the system in order to disconnect from it.

*Disconnection* protocol first appears around 30th minute and it is used through the entire time of the simulation. Figure 8 shows that, at the beginning of the system *Disconnection* protocol delay varies between 0.1 and 0.5 second but through time the average delay achieves a balance around 0.4 second.

## Update Packets



Figure 9. Results for Update Packets protocol

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 9, at the beginning of the protocol, the average delay value varies between 0.6 and 1.4 second but then after some time the protocol achieves a balance around 0.4 second.

## Seamless Mobility in Home Operator



Figure 10. Results 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 10, it could be said that*, Seamless Mobility* protocol has an initial average delay that varies between 0.2 and 1.2 seconds. These results provide us a real seamless mobility property for the system. A user loses around 0.1 second to make a handover to the new access point. This amount of delay is a very reasonable amount of time that we think that a user would not understand that there is a handover process going on.

## Roaming



Figure 11. Results for Roaming protocol

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

*Roaming* protocol has a delay average that varies between 0.05 and 0.2 seconds. In our simulation 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 11, the results for *Roaming* protocol shows a boost until the middle of the simulation time but it decreases and achieves a balance at a reasonable amount of average delay, which was the aim for us at the beginning.

## Packet Transfer



Figure 12. Results for Packet Transfer protocol

*Packet Transfer* protocol is the mostly used protocol in the system. We had very good results for this protocol at unit tests and by looking at the *Packet Transfer* results for the real-life scenario simulations we still have reasonable average delay for the *Packet Transfer* protocol.

Figure 12 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.

# Conclusion

Uniform probability distribution model enables us to simulate real time scenarios in simulation environment, and gets results closer to real time situations.

There are different user types, as there are different types of clients in real life. There is also randomness at the system, so we have different outcomes for the same simulations as there is change in network traffic everyday despite the users are same. The average of those simulations would cover even the most unexpected situations and this attribute of the simulations will help us to handle every possible state of the system.

Our results show that the SSPayWMN system works in very reasonable amount of time. It is secure and fast. The simulation results are satisfactory indicating that the SSPayWMN works effectively and it is a respectable system.

**References**

*[1] Levi, Albert Leloğlu, Can Serhat Requirements Specification Document 16.08.2011*

*[2] Levi, Albert Leloğlu, Can Serhat Simulation Tools Comparison Document 25.10.2011*

*[3] Levi, Albert Leloğlu, Can Serhat Protocol Design Document 04.04.2012*

*[4] Levi, Albert Leloğlu, Can Serhat Unit Simulations Report 30.09.2012*