4. SIMULATIONS 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.

4.1. SIMULATION ENVIRONMENT

The simulations of SSPayWMN are conducted using ns-3. ns-3 is a widely used, popular and a free network simulator. ns-3 is a discrete event network simulator. It is mainly used in research and academia. The ns-3 project is still being developed by ns-3 users, since it is an open platform for developers. ns-3 supports 802.11s and wireless mesh networks and coding is done in C++ programming language.

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.

The network topology is hierarchical and WMN supports connections with other IEEE 802.11 protocols, 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 4.1. *Update Interval* determines the time value between two update packets that access point send to TTP.

Table 4.1: AP Specifications

AP-Gateway Connection bit rate	6-54 Mbps – Wi-Fi
AP-Gateway Distance	70 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.

1) Cryptographic Operations and Their Timings

Public Key Cryptography timings for access points and gateways are mentioned in [42]. For operator servers and TTP servers, timings from [43] are used. For mobile clients, performance values for iPhone 4 are computed using openssl.

Platform specifications are shown in Table 4.2, and RSA-2048 timings are shown in Table 4.3. For AES timings the values from [21] are used and they are shown in Table 4.4. Timings of hash algorithms are taken from [45] and they are presented in Table 4.5.

Table 4.2: Platform Specifications

	Gateway [42]	Linksys WRT54GS (AP) [42]	Server [43]	Client [44]
CPU Speed	2.08 GHz	200 MHz	Dual-core 64 bit 2.8 GHz	Not disclosed by Apple
CPU type	AMD Athlon XP 2800	Broadcom MIPS32	Intel Xeon	Arm Cortex-A8
RAM	512 MB	32 MB	-	-

Table 4.3: RSA-2048 Timings

	Gateway	Linksys WRT54GS	Server	Client
RSA Signing	47.3 ms	1529.0 ms	8.13 ms	120 ms
RSA Verification	1.3 ms	37.9 ms	0.32 ms	-

Table 4.4: AES-128 Timings

	Gateway	Linksys WRT54GS	Server	Client
Approximate AES-128 Timings per block	0.001 ms	0.01 ms	-	-

Table 4.5: SHA-256 Timings

	Gateway	Linksys WRT54GS	Server	Client
Approximate SHA-256 Timings per 256-bit block	-	0.02 ms	0.0002	0.008 ms

3.1. UNIT TEST RESULTS

Unit tests are simulation runs per standalone protocol behavior. In these tests there is only one user, and this user performs the same protocol every minute. These tests are done to ensure the robust behavior of modules of the system.

As discussed in Section 3, 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.

1) 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. End-to-end Two-way protocols consist of *Initial Authorization*, *Reuse-CC*, *Change Alias* and *Disconnection* protocols. Figure 4.1 presents 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.

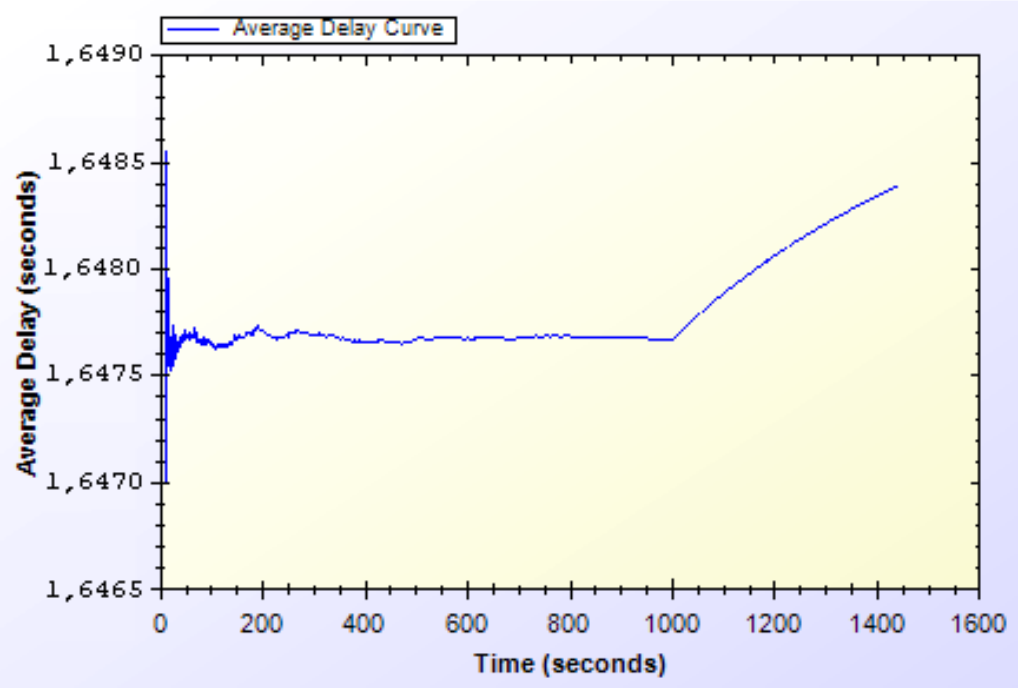

Figure 4.1. End-to-End Two-Way Protocols Unit Test Result

As shown in Figure 4.1, there is a delay that shows variation around 1.64 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.

2) 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 4.2, shows the average delay of the protocol versus time.

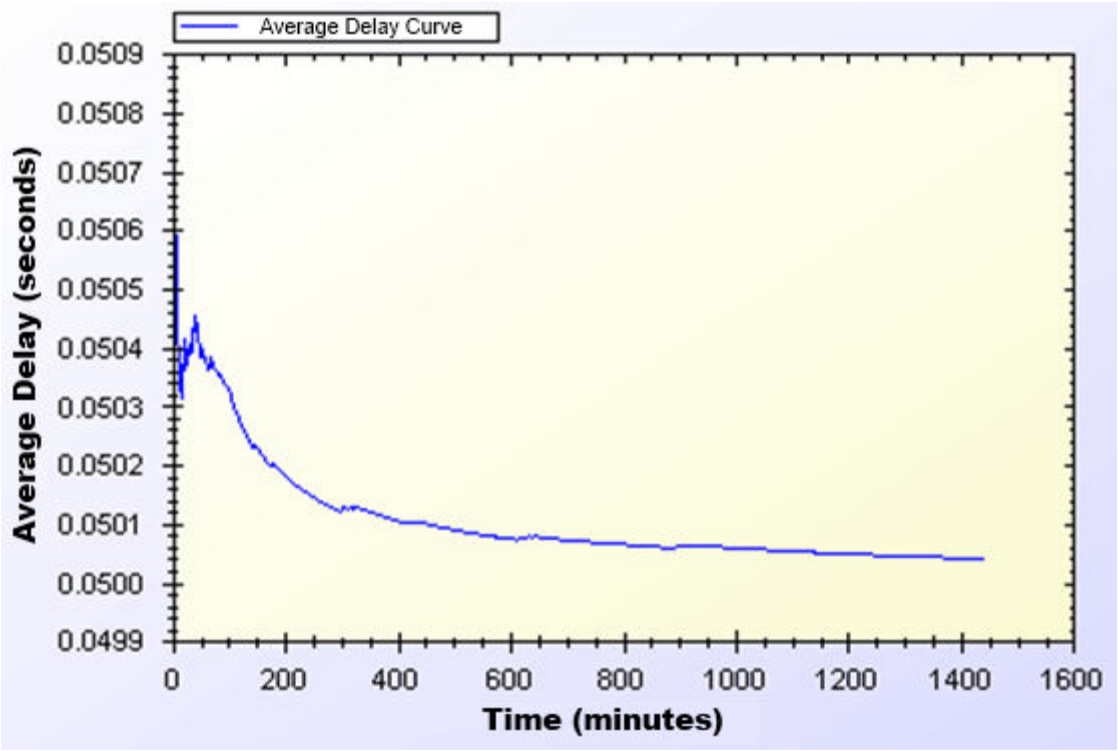

Figure 4.2. Access Point Authentication Protocol Unit Test Result

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.

3) 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 consist 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 4.3 presents the unit test result for *Seamless Mobility* and Roaming protocols.

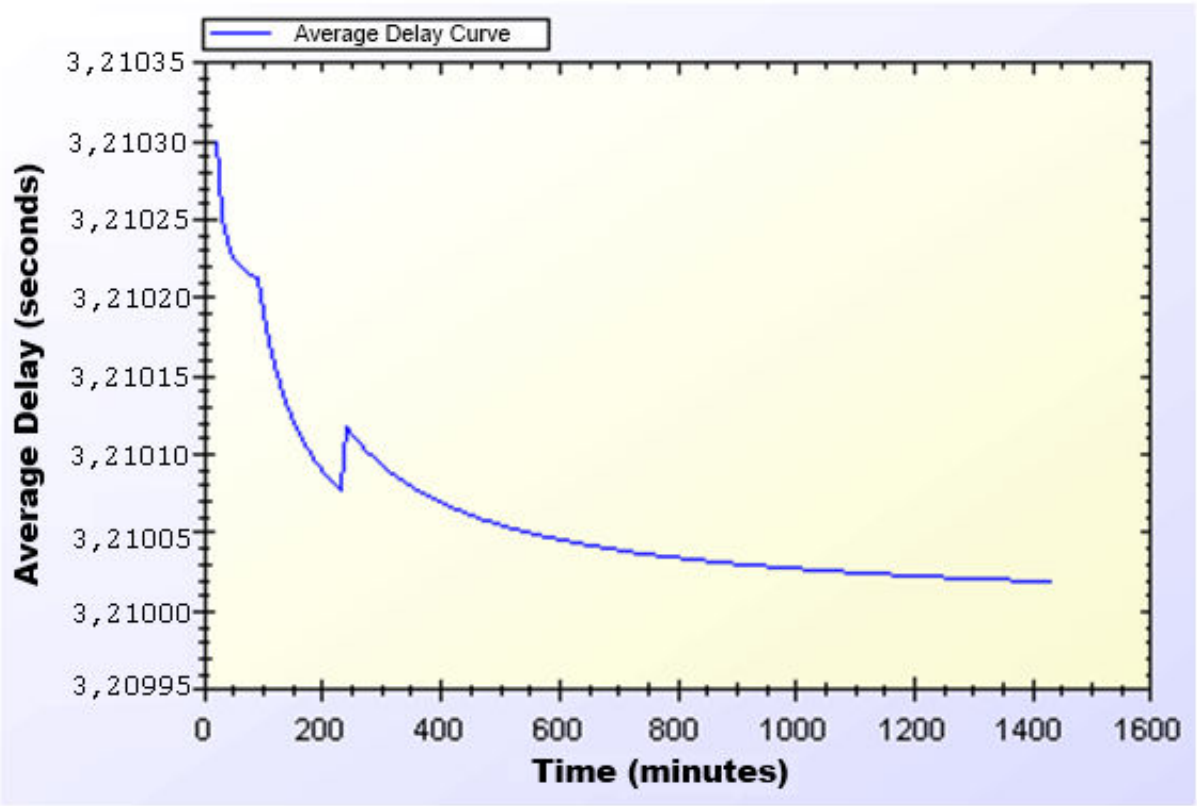

Figure 4.3. Seamless Mobility and Roaming Protocols Unit Test Result

In unit test for these protocols, 3.21 seconds of total delay for hash token transfer is observed. However the real network delay between service changes is approximately 0.15 second. Therefore seamless roaming and mobility is seamless to the clients. Similar to other protocols, there is a transitive period at the beginning of the simulations; however it reaches steady state in time.

4) 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 4.4 shows the unit test result for Packet Transfer protocol.

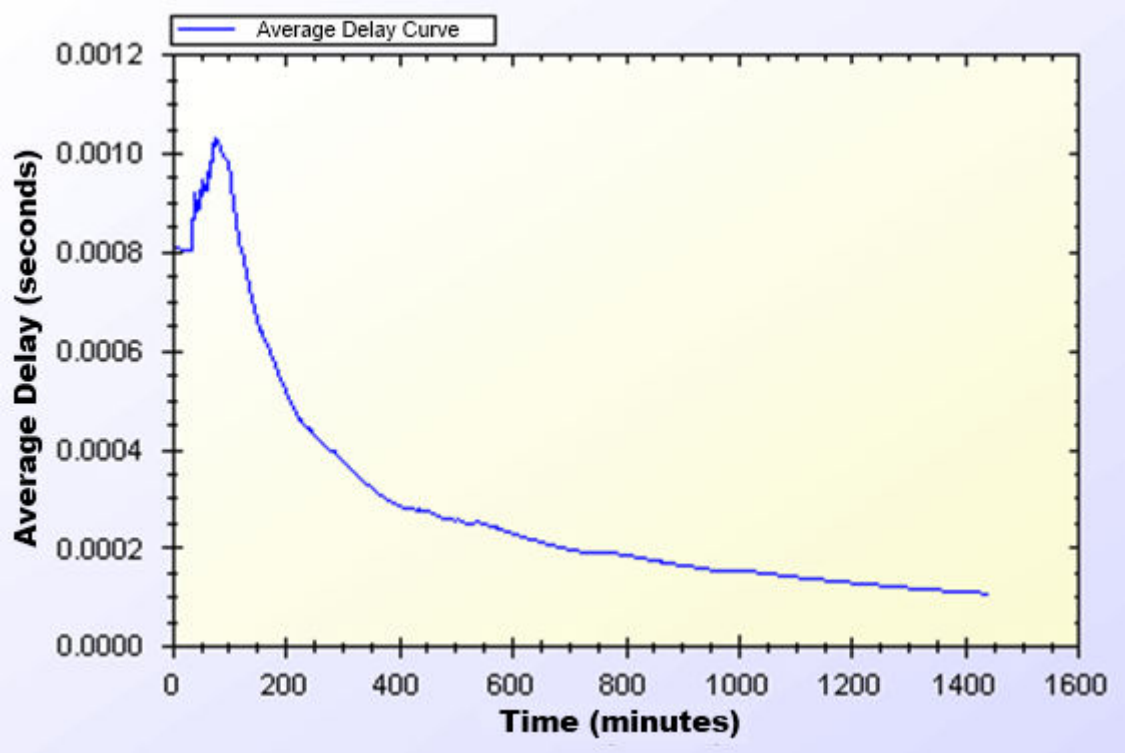

Figure 4.4. Packet Transfer Protocol Unit Test Result

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 4.4, at steady state, packets are received in a very short amount of time, which is around 0.0002 second.

5) 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 4.5 shows the average delay of *Update Packets* protocol over time.

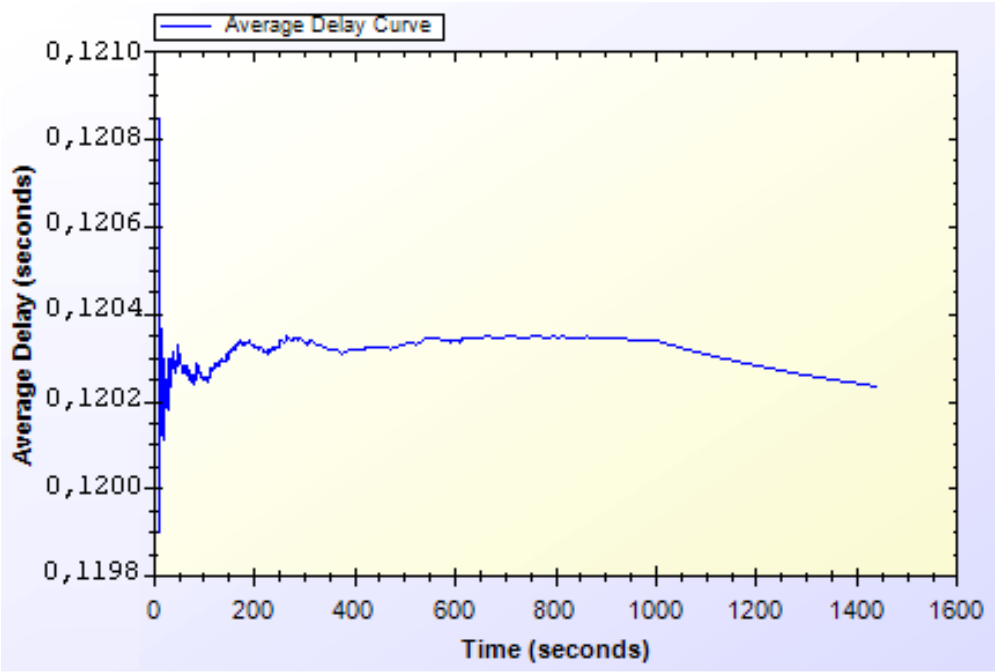

Figure 4.5. Update Packets Protocol Unit Test Result

In the simulation scenario, APs update operator once in every second. Our simulation showed that there is a 0.12 second maximum network delay for updating operator for the client usage.

4.2. USER MODELING AND MOBILITY IN REAL-LIFE SCENARIO

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.

1) User Actions

In real-life scenario simulations, network usage related actions are modeled using two-state Markov Chain as shown in Figure 4.6. 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.

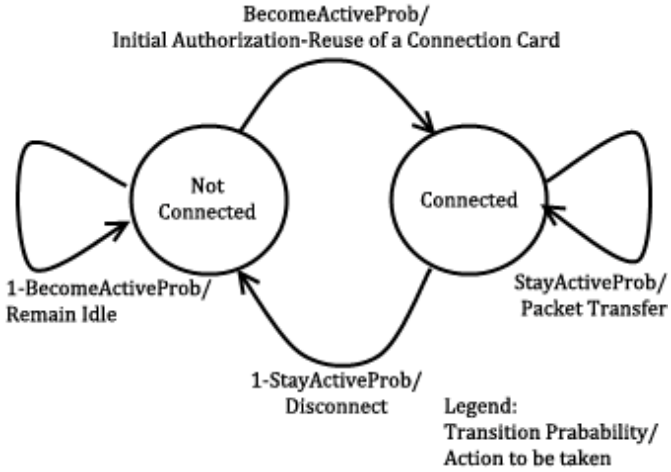

Figure 4.6. State Diagram of Clients

The initial state is *Not Connected*. In this state, the user switches to *Connected* state with the probability value of $BecomeActiveProb$. 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 $1 - BecomeActiveProb$.

While in *Connected* state, the user remains connected (i.e. stay in the same state) with the probability of $StayActiveProb$. 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 $1 - StayActiveProb$. This transition disconnects the user via *Disconnection* protocol.

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

$$T_{con} = \sum_{i=1}^{\infty}(1 - P_{SA}) \cdot i \cdot {P_{SA}}^{i-1} = (1 - P_{SA}) \sum_{i=1}^{\infty} i \cdot {P_{SA}}^{i-1} = \frac{1}{1-P_{SA}} \quad (1)$$

Where, P_{SA} denotes $StayActiveProb$.

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

$$T_{idle} = \sum_{i=1}^{\infty} P_{BA} \cdot i \cdot (1 - P_{BA})^{i-1} = P_{BA} \sum_{i=1}^{\infty} i \cdot (1 - P_{BA})^{i-1} = \frac{1}{1-(1-P_{BA})} = \frac{1}{P_{BA}} \quad (2)$$

Where, P_{BA} denotes $BecomeActiveProb$.

2) 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) morning (06:00 – 13:59), (ii) daytime (14:00 – 21:59), and (iii) evening (22:00 – 05:59).

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 evening 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 *evening* 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 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 the domestics get Internet service in an immobile way. These users are highly active at all times.

The parameters of $StayActiveProb$ and $BecomeActiveProb$ are determined based on the abovementioned discussion about the client type characteristics and the time slots. These values are given below. The triplet $\{x, y, z\}$ specify the probability values for morning, daytime and evening, respectively.

$$becomeActiveProb < Domestic > = \{0.40, 0.60, 0.60\};$$

$$becomeActiveProb < Student > = \{0.20, 0.20, 0.80\};$$

$$becomeActiveProb < Employee > = \{0.20, 0.99, 0.20\};$$

$$stayActiveProb < Domestic > = \{0.90, 0.98, 0.80\};$$

$$stayActiveProb < Student > = \{0.30, 0.20, 0.98\};$$

$$stayActiveProb < Employee > = \{0.30, 0.99, 0.20\};$$

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 $\frac{1}{1-(1-0.6)} = \frac{1}{0.6} = 1.67$ minutes between connections. Once connected, average connection time for this category is $\frac{1}{1-0.98} = \frac{1}{0.02} = 50$ minutes.

3) User Mobility and Timing

Real-time scenario covers Internet usage of 300 users in a 1-km^2 metropolitan area. The simulation time begins at 06:00 a.m. and lasts for 24 hours. Simulation time is divided into 3 parts considering morning, 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 4.7. 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 the closest to the client's current location.

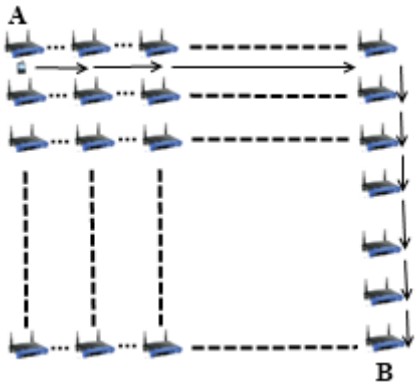

Figure 4.7. User Movement from A to B

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.

4.3. REAL-LIFE SCENARIO SIMULATION RESULTS

Real-life scenario consists of 300 mobile clients trying to get network service in a $1km^2$ metropolitan area. This scenario simulates an ordinary day with 24 hours. In these simulations clients have mobility patterns as mentioned before. Client's network usage

frequency is affected by their socio-economical status. In following sections we will give latency values for each protocol. Finally, we will explain the overall burden on the system caused by the system's protocol.

1) Simulation Results of Protocols

In this section, we will briefly explain each protocol's run time performance. The protocols are performed on a network with 435 network entities. We have 300 clients, 100 access points, 32 gateways, 2 operator servers and a server of the TTP. Every protocol in real-life simulations are executed simultaneously; therefore, real-life scenario simulation results have bigger latency values than unit tests.

In real-life simulations client models and mobility schemes are considered. The client roles and systematic mobility gave us realistic simulation results. In the beginning, every access point starts with 3 initial clients but then these clients move randomly in the metropolitan area and the initial setting do not remain as it was in the beginning.

The real-life scenario simulation results show that our protocols reach steady state in ordinary day usage.

Real-Life Scenario Simulation Result for Initial Authorization Protocol

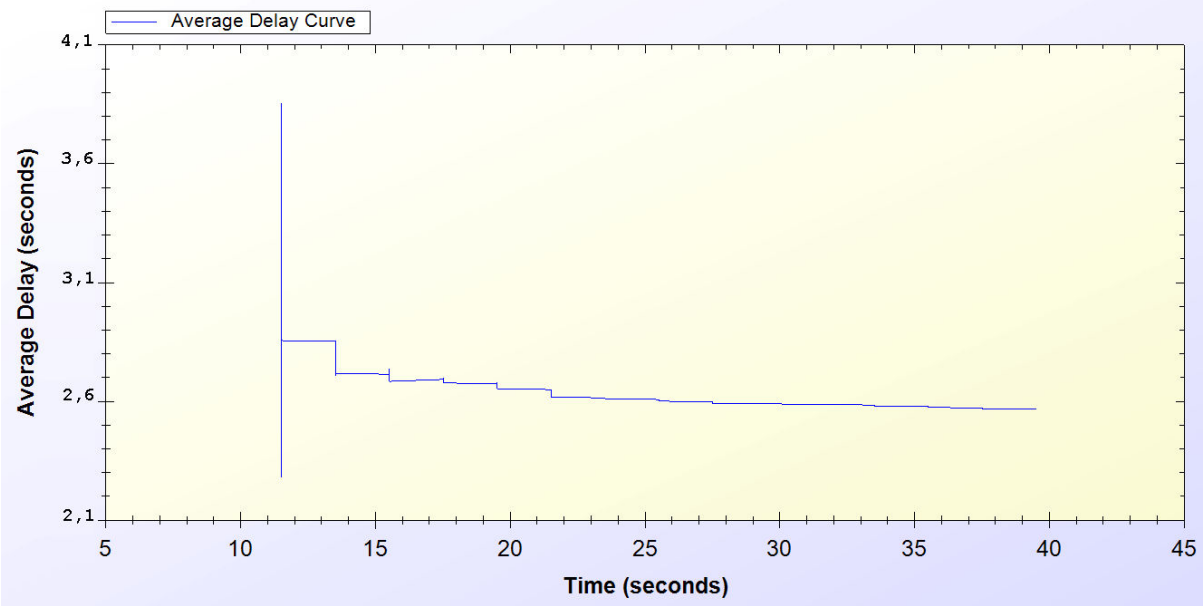

Figure 4.8. Real-life Simulation Result for Initial Authorization Protocol

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 4.8 indicates that, this process varies between 2.1 and 4 seconds. After 10 minutes it attains a balance and *Initial Authorization* protocol meets a delay of 2.6 second, which means when users open up their mobile device they would have Internet service after 2.6 second.

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

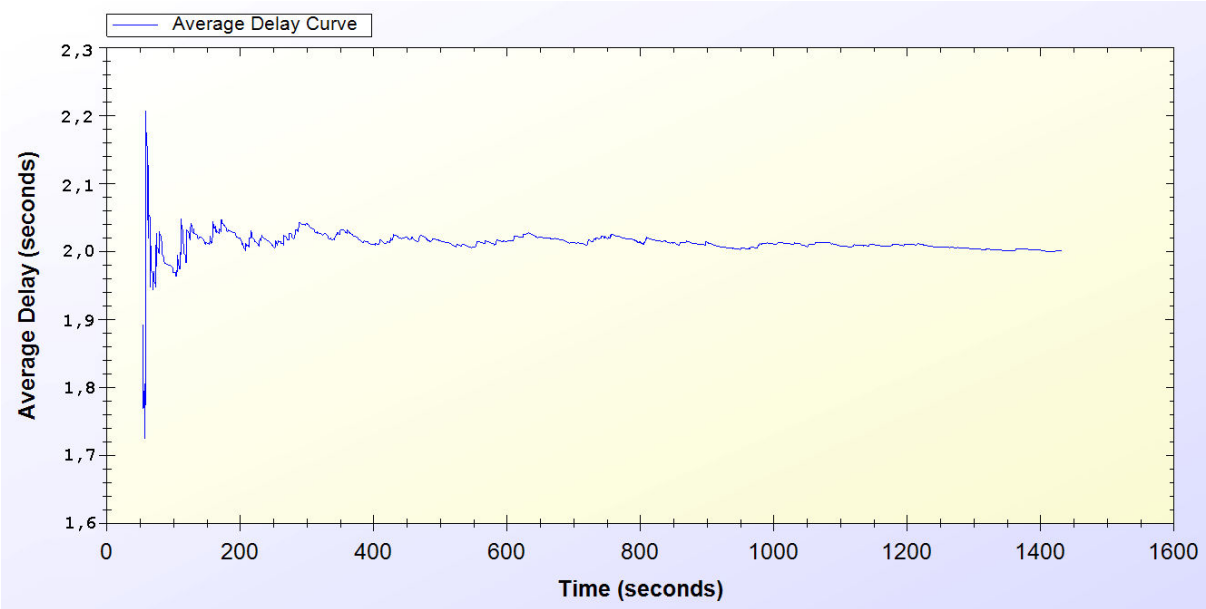

Figure 4.9. Real-Life Simulation Result for Reuse of a Connection Card Protocol

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 4.9, at the beginning of the protocol the delay changes between 1.7 and 2.2 seconds. After some time, the protocol achieves a steady state of 2.0 seconds.

Real-Life Scenario Simulation Result for Changing Alias

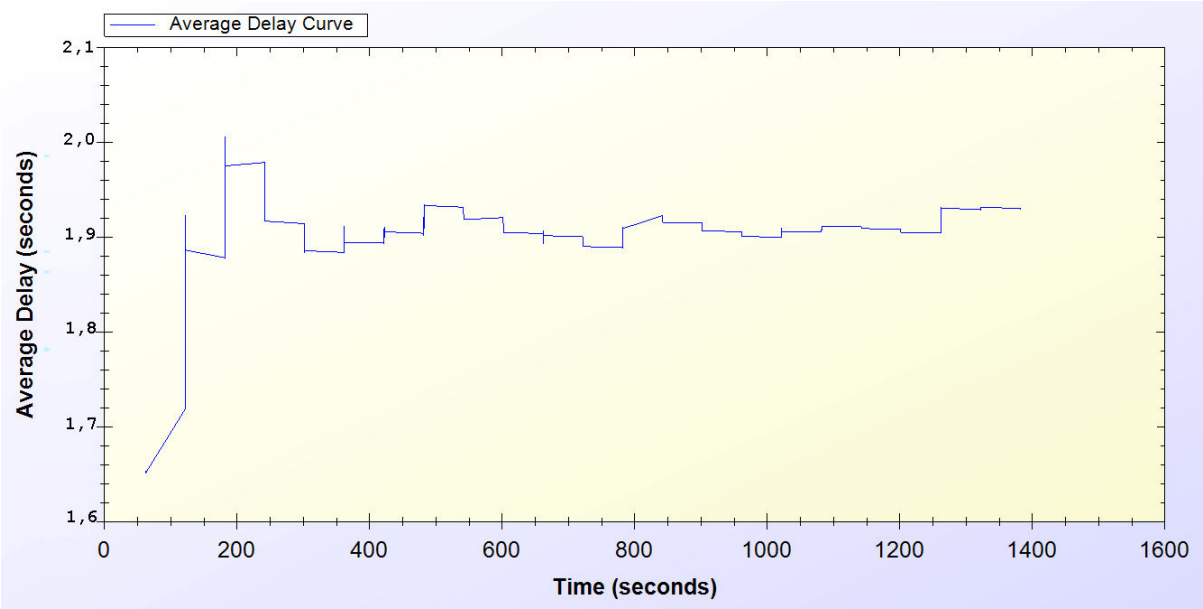

Figure 4.10. Real-Life Simulation Result for Changing Alias Protocol

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 4.10, at the beginning of the protocol the delay for the protocol varies between 1.7 and 2.0 seconds. The average delay for the protocol converges to 1.9 seconds after some initial deployment time.

Real-Life Scenario Simulation Result for Disconnection

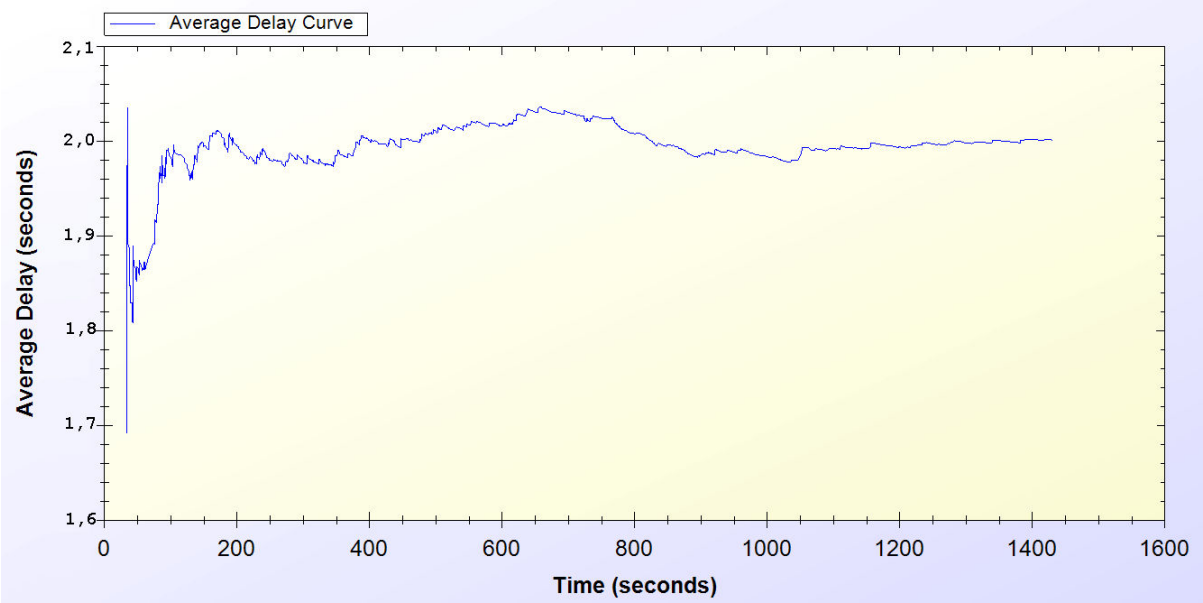

Figure 4.11. Real-Life Simulation Result for Disconnection Protocol

Disconnection protocol first appears around 30th minute and it is used through the entire time of the simulation. Figure 4.11 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

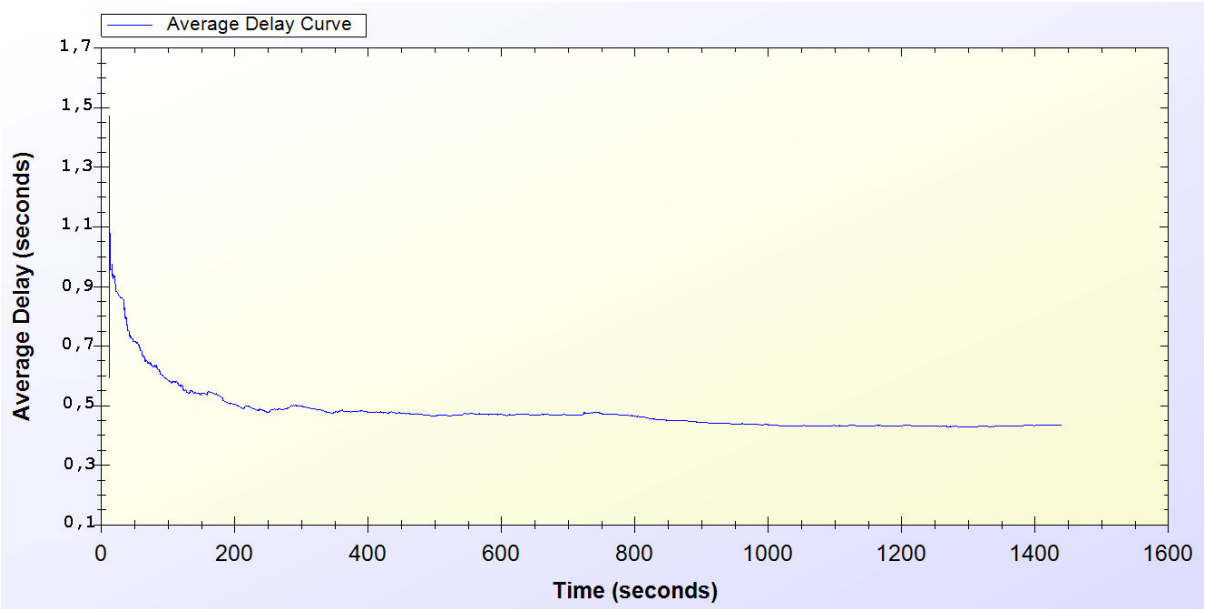

Figure 4.12. Real-Life Simulation Result for Update Packets

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 4.12, at the early stages of the protocol, the average delay value varies between 0.7 and 1.5 second but then after some time the protocol stabilized around 0.5 second.

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

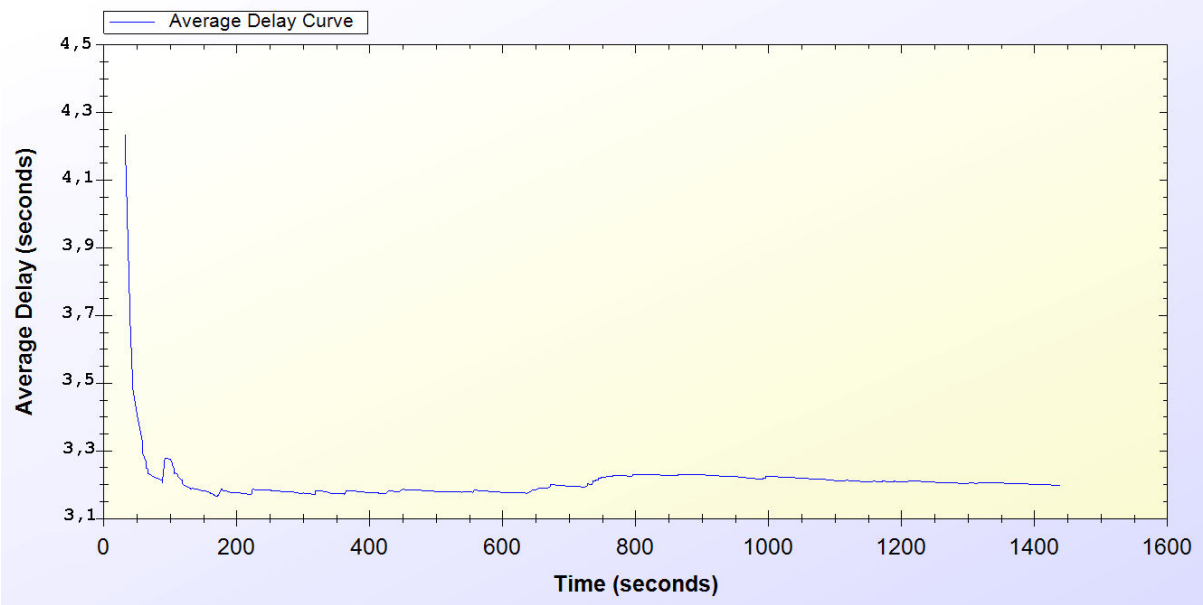

Figure 4.13. Real-Life Simulation Result for Seamless Mobility Protocol

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 4.13, it could be said that, *Seamless Mobility* protocol has an initial average delay that shows difference between 3.1 and 4.2 seconds. A user spends around 3.3 second to transfer the current hash token to the new access point. However, the client does not stop getting service from the old access point until she finishes all the handover process with the new access point. Therefore, *Seamless Mobility* protocol is seamless to the client.

Real-Life Scenario Simulation Result for Roaming Protocol

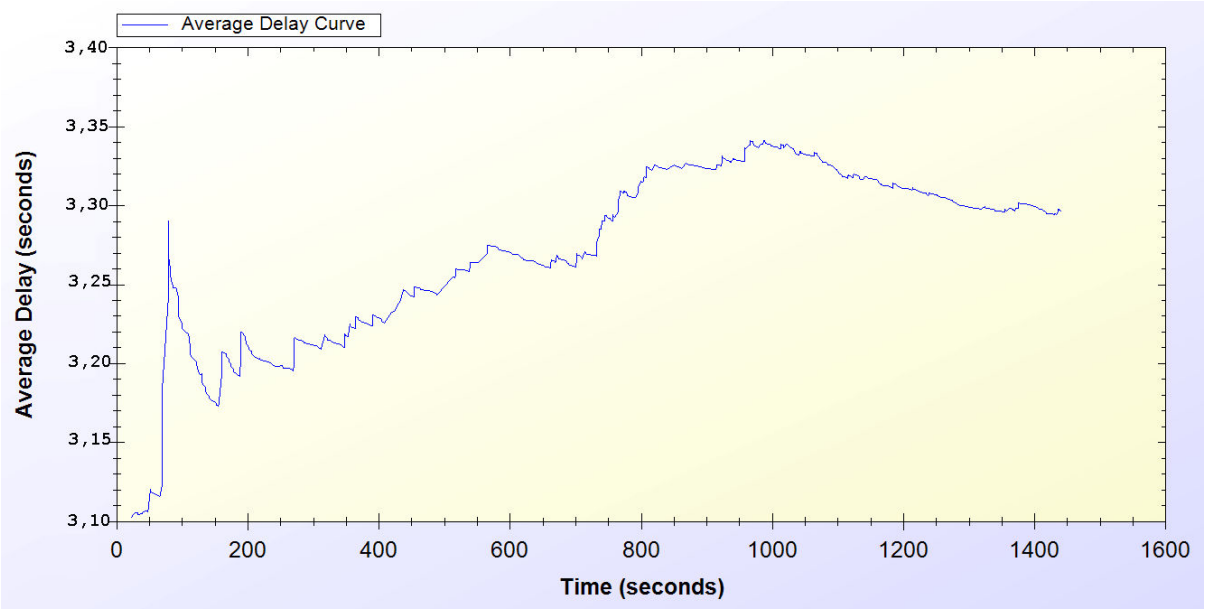

Figure 4.14. Real-Life Simulation Result for Roaming Protocol

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 3.1 and 3.3 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 3.3 second of delay.

As one can see on Figure 4.14, the results for *Roaming* protocol shows a boost until the middle of the simulation time but it decreases and achieves steady state.

This protocol is very similar with *Seamless Mobility* protocol, and the client does not stop getting service from the old access point until the protocol is over. Therefore, *Seamless Roaming* protocol is seamless to the client.

Real-Life Scenario Simulation Result for Packet Transfer

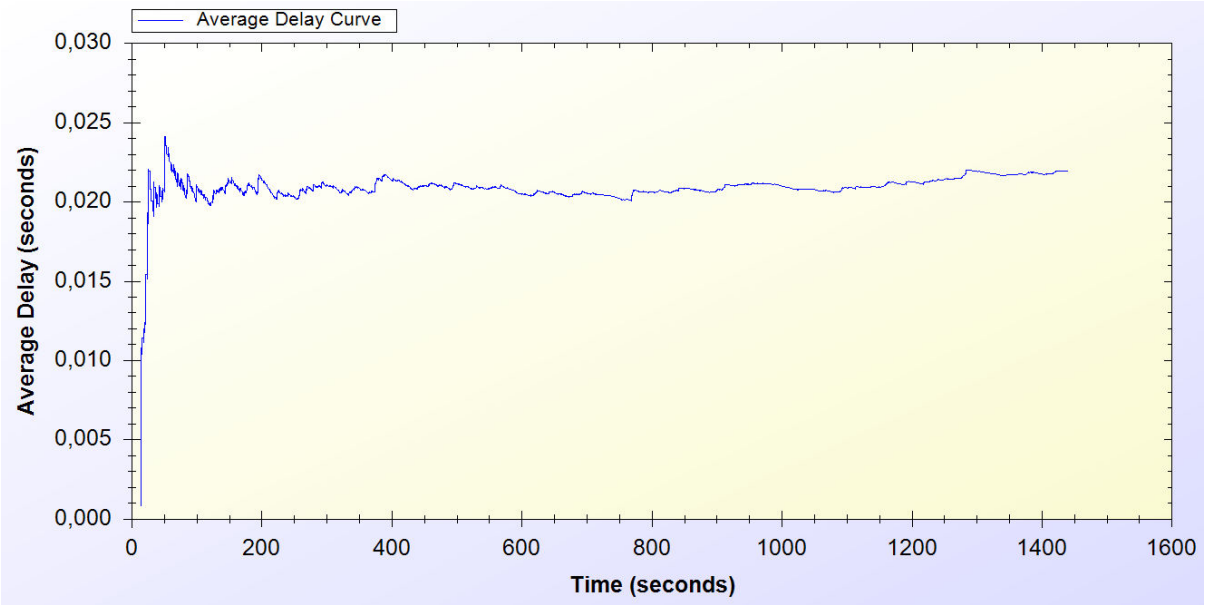

Figure 4.15. Real-Life Simulation Result for Packet Transfer Protocol

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

Figure 4.15 states that, at the beginning of the protocol the average delay value varies between 0.005 and 0.025 but then the protocol achieves steady state around 0.02 second of delay.

2) Overall Burden of the System

Real-life scenario simulation provided the results in Table 4.6. Charts on Figure 4.16 and Figure 4.17 are drawn exploiting the results in Table 4.6. 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 17 to 20 minutes of waiting.

Table 4.6: 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	2078 Minutes	958 Minutes	20 Minutes
Worker	101681 Minutes	1756 Minutes	1016 Minutes	17 Minutes
Non-Worker	105335 Minutes	1832 Minutes	1053 Minutes	18 Minutes

Difference between client types affects the system usage of the clients. The probabilistic values, which are mentioned in Section 4.2, determine the system usage frequency of the clients. As it is seen on Table 4.4, non-workers are the most active clients in the system. Workers and students follow non-workers in that sense. On Table 4.4, the simulation results are grouped into two subgroups, which are: Total Internet Usage and Average Internet Usage. In the real-life scenario simulation 100 clients exist in every group. Total Internet Usage means the overall sum of network usage of these 100 clients in a day. It could be seen that students in the system have used SSPayWMN for 95899 minutes in total. In average, every student receives 958 minutes of network service in a day. When we analyze the delay values we see that a client experiences a delay, which is approximately 1% of the total amount of received service.

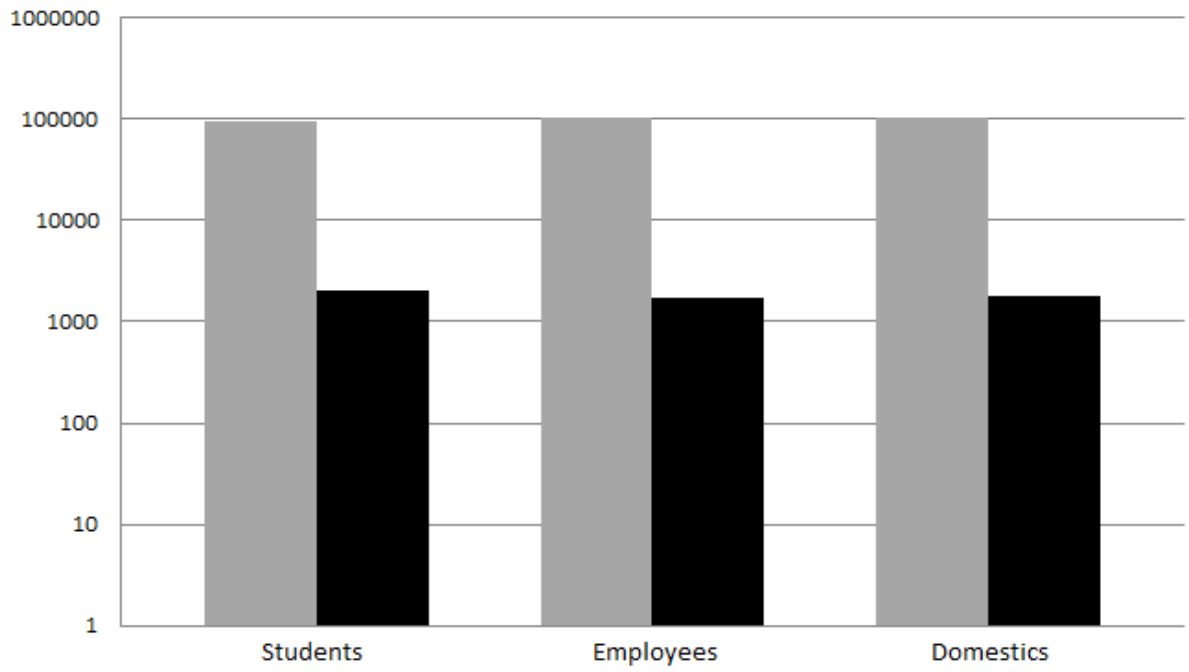

Figure 4.16. Total Amount of Service Usage Times for Client Types vs. Total Delays

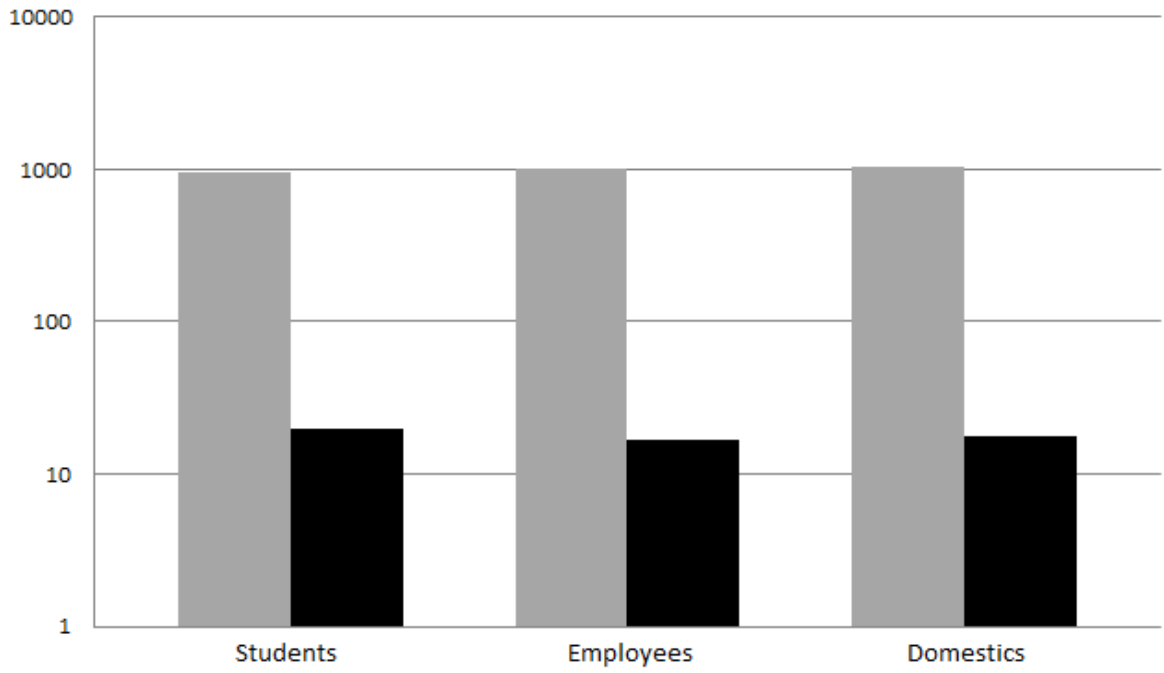

Figure 4.17. Average Service Usage Times for Client Types vs. Average Delays

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

Figure 4.8 and Figure 4.9 shows the overall results for real-life scenario simulation. Figure 4.8 shows comparison of minutes clients used as idle or active. Figure 4.9 shows the average value for the clients of the same group.