Secure and Seamless Payment for Wireless Mesh Networks

Serhat Can Leloğlu, Can Yücel, Albert Levi

Sabanci University, Turkey
canleloglu@sabanciuniv.edu
canyucel@sabanciuniv.edu
levi@sabanciuniv.edu

Abstract— **Wireless Mesh Network (WMN) technology is a multi-hop high-speed networking technology for broadband network access. Compared to base stations, WMNs are easy to deploy and cost-effective systems. Building a secure payment system over WMNs is highly desirable since it provides network access to mobile or stationary clients. In this paper a secure and seamless way of pre-payment for Internet access is proposed additionally network simulations for this system are shown.**

Keywords⸺**Wireless Mesh Networks, Cryptography, Payment Systems, Security, Network Simulation**

I. INTRODUCTION

Wireless Mesh Networks [1] are often used for service providing; moreover a secure system built using WMNs should support user identification, authentication as well as authorization and accounting.

Commonly payment systems service providers do not fully trust clients, but in reality service providers –intentionally or not- may over charge the clients or charge for services that they did not provide. It is proven that using native cryptographic algorithms, every action could have an undeniable cryptographic proof so thatthe client could not get service without payment and service providers could not charge without serving.

The secure and seamless pre-payment system presented in this paper, has the properties such as wide-coverage, seamless mobility and roaming, anonymity, mutual authentication, two-way honesty, preventing double spending and unlinkability. Ten protocols are designed for actions of the system entities, and these protocols are tested using network simulator 3 [2]. The designed system had formidable results in unit tests and the results are explained in this paper too.

II. CRYPTOGRAPHIC NOTES

The designed protocols are formed by the usage of some cryptographic primitives such as public key cryptosystems and hash functions forms up the designed protocol. 2048-bit RSA [3] is employed for public key encryption-decryption and signature purposes. AES-128 [4] is utilized for symmetric key cryptography and SHA-256 [4, 5] is used as a hash algorithm in the system. HMAC [5, 6] algorithm is used for challenge-response protocols.

III. GENERAL OVERVIEW OF PROPOSED SCHEME AND SYSTEM ENTITIES

The proposed system is a secure pre-payment infrastructure for WMNs that also considers users' privacy and fairness. In this infrastructure there are mobile phones or laptops as clients, as well as tools that are used for service providing. Table 1 gives a list of system entities that function in the proposed system.

TABLE I
SYSTEM ENTITIES

	Mobile user (client)
	Access Point (AP). From now on in this document, it is called as AP, but please note that it also has routing capability.
	Mesh backbone
	Gateway (GW) that connects the mesh backbone to outer world and also to the operator's server
	Operator's server (OP). Keeps necessary logs and user info.
	Trusted Third Party (TTP). Payment related logs are mostly to be generated by the TTP.

Figure 1 shows the topology of the network and connections between entities.
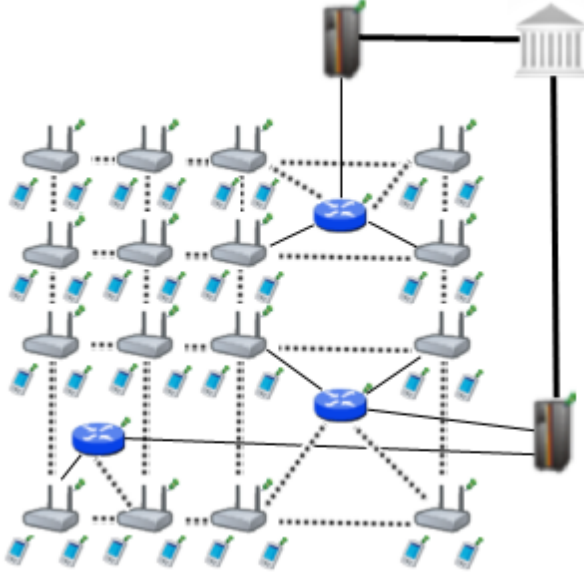
Figure 1. Network Topology

Connection between serving access points is wireless, and they use 802.11s protocol [6]. 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) [7], which is a hybrid routing protocol, which has routing tables.

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

A. Connection Card Structure

A Connection Card (CC) is the main deed that clients buy from operators and use to get Internet service. CCs include credits as tokens. Hash tokens are generated using hash chains as discussed below. CCs also have unique Serial Numbers (SN), which are to be used for alias computation later.

Tokens for getting Internet service are basically links in a hash chain. For each set of tokens, the operator picks on a random Initialization Vector (IV) and takes hashes of it several times. The number of hash operations is actually the number of tokens in a set.

$$H_0 = h(H_1) = h^{99}(IV)$$

$$H_1 = h(H_2) = h^{98}(IV)$$

…

$$H_{98} = h(H_{99}) = h^2(IV)$$

$$H_{99} = h(IV)$$

H_0 is the first token to be used, then tokens are used in increasing order by token index. In this manner, one-way property of hash algorithms is exploited such that an attacker cannot learn the next token even if she knows the previous tokens.

B. Alias Computation

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

The serial number (SN) of the CC, 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 N_{CL}.
2. Perform XOR operation with SN and his nonce, $SN \oplus N_{CL} = Alias$
3. Client will use this alias whenever his identity is required.

One may argue that this kind of alias computation would run a risk of producing same alias for several users.However making TTP to check the proposed alias to be a unique one solves this problem.

IV. PROTOCOLS

There existten protocols to make the system work. These protocols define packet transfers and routes. Cryptographic primitives and the way they are used are also explained in the protocol designs.

Some protocols show similarity e.g. *Initial Authorization* and *Reuse of a Connection Card*. The only difference between these two protocols is their hash token index. *Initial Authorization* uses the very first hash token while *Reuse of a Connection* Card using the other hash tokens on the hash chain. This kind of similar protocols will be explained simultaneously.

A. End-to-End Two-Way Protocols

The main protocol in the system is the End-to-End Two-wayprotocols, which are also the most common ones in the system.

The protocols classified as End-to-End Two-way are *Initial Authorization, Reuse of a Connection Card, Disconnection, Change Alias* protocols. These protocols transmit equally sized packets from client to TTP. TTP executes the same cryptographic operations on the packet and forwards the packet to the client. In these protocols client performs an encryption over a 384-bit packet using RSA-2048 and sends it to the TTP. TTP decrypts this cipher using RSA-2048 private key then signs 256-bit data using RSA-2048 private key. TTP sends this signed data to GW through the operator. GW encrypts the response with the symmetric key between itself and the target AP and sends it to the target AP through mesh backbone.
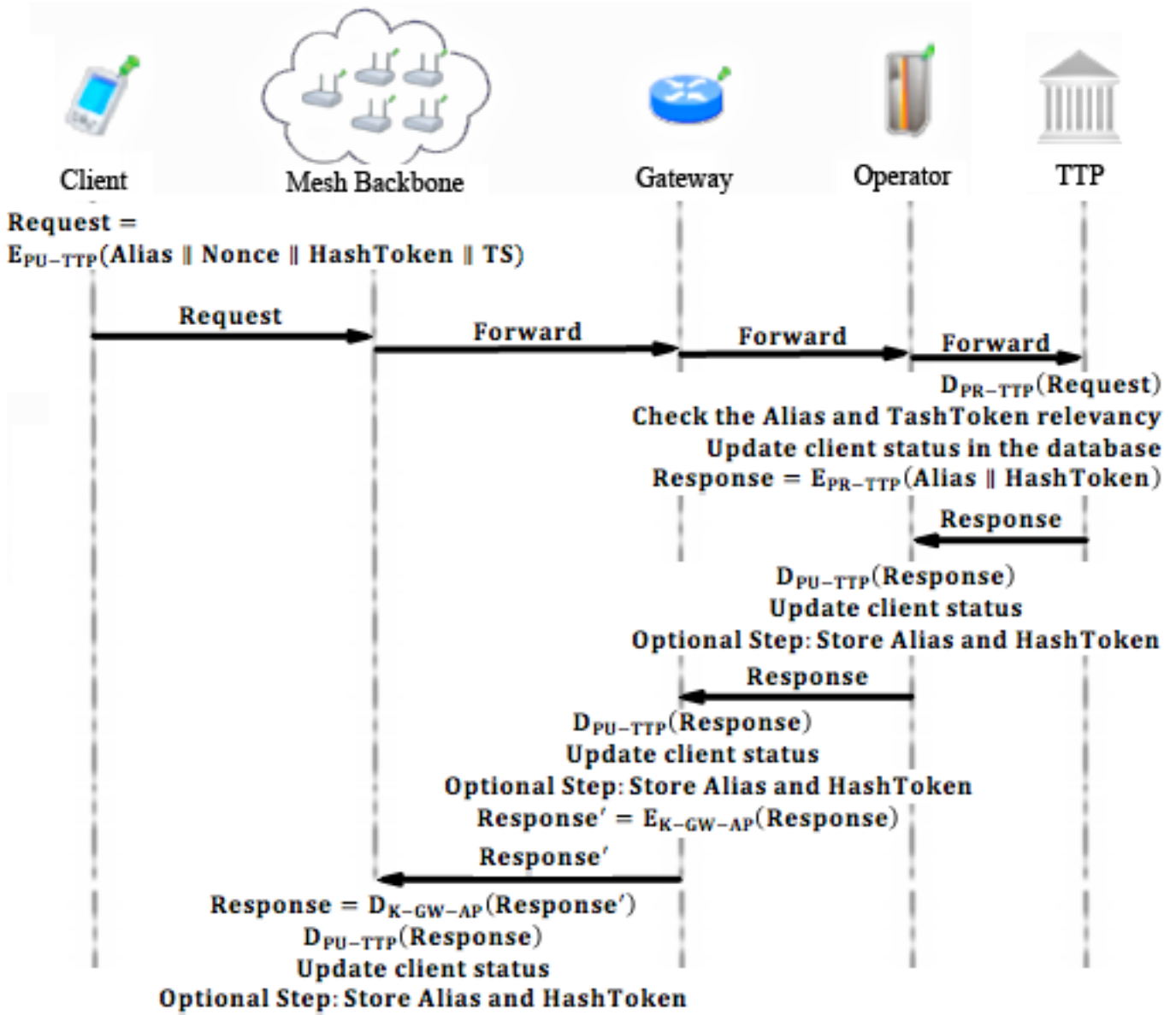
Request =
$$E_{PU-TTP}(Alias \parallel Nonce \parallel HashToken \parallel TS)$$

Client   Mesh Backbone   Gateway   Operator   TTP

Request → Forward → Forward → Forward →

$$D_{PR-TTP}(Request)$$

Check the Alias and TashToken relevancy
Update client status in the database
$$Response = E_{PR-TTP}(Alias \parallel HashToken)$$

← Response

$$D_{PU-TTP}(Response)$$
Update client status
Optional Step: Store Alias and HashToken

← Response

$$D_{PU-TTP}(Response)$$
Update client status
Optional Step: Store Alias and HashToken
$$Response' = E_{K-GW-AP}(Response)$$

← Response'

$$Response = D_{K-GW-AP}(Response')$$
$$D_{PU-TTP}(Response)$$
Update client status
Optional Step: Store Alias and HashToken

Figure 2. End-to-End Two-Way Protocol Flow

Initial Authorization is the first protocol that a client uses in the system in order to get authorized. It is used only once by a particular user.

Reuse of a Connection Card protocol is used when a user does not finish the tokens in a connection card and would like to use the remaining tokens at a later time. Initial Authorization and Reuse of a Connection Card protocols only differ in theirhash token index.

The initial time of the session for a user is stored when a user performs one of the two previously mentioned two protocols. Disconnection protocol yields the ending time of the session. In this way, the TTP learns the amount of time that the user got served. This information is used for settlement purposes.

One of the privacy preserving features of the proposed system is that access points ask every user to change their aliases from time to time. When received such a command from the access point, clients compute aliases and send it to the TTP for signature. The overall process is called Change Alias protocol.
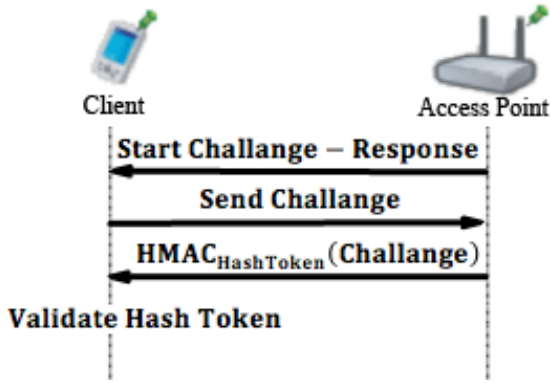
B. *Access Point Authentication*

Figure 3. Access Point Authentication

Access Point Authentication, which is shown in Figure 3, takes place between a mobile client and an access point. It is a challenge-response type of protocol to authenticate the access point to the client.

Access Point Authentication starts with the serving access point by sending a request to the client. Client sends a 128-bit challenge to the access point. Access Point performs anHMAC operation on this challenge using the last hash token as a key. Client performs the same operation and compares two results. If they match, the access point is verified as authenticated.
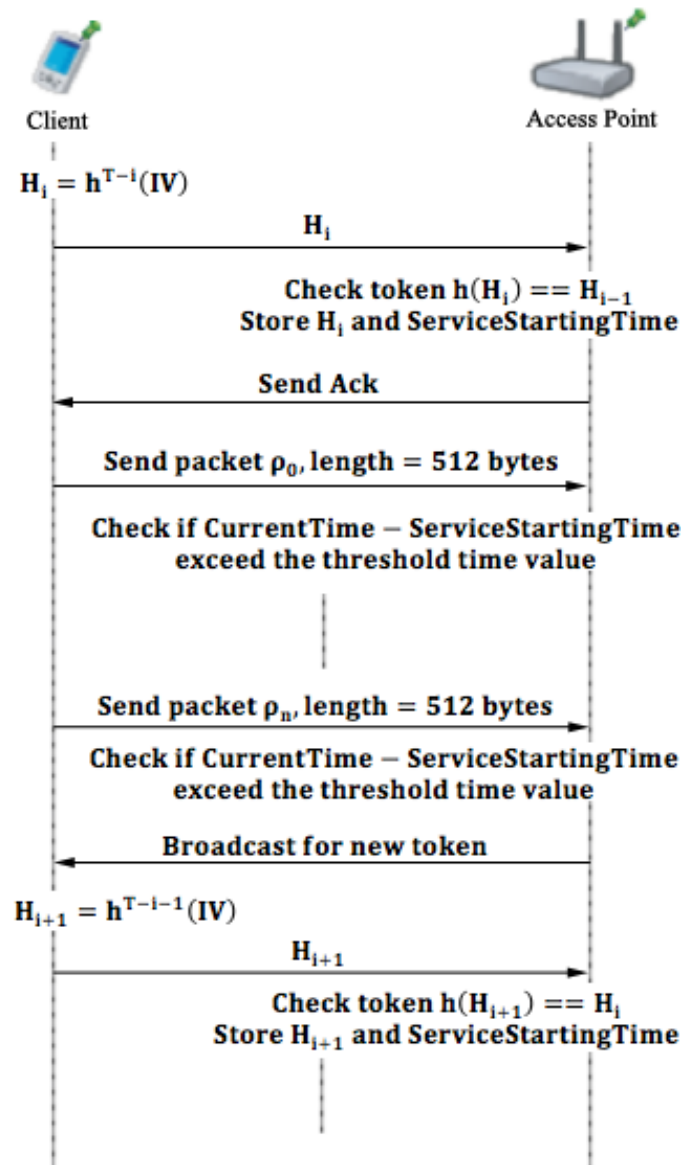
C. *Packet Transfer*

Figure 4. Packet Transfer

Packet Transfer protocol, shown in Figure 4, protocol is the simplest and the most commonly used protocol among others. It is the main service access protocol that uses tokens one by one. One token of the hash chain is sent from client to AP and the client starts to use the broadband access service. Usage is charged in time basis. Every five minutes client sends a new hash token to continue to get Internet service. When a user sends a hash token it means that she already has paid for the service and in case of disconnection the protocol is called after e.g. 2 minutes, user could not get a refund for the remaining 3 minutes.

The time measurement happens between access point and client. The access point does decrementing from 5 minutes. If client tries to get service after 5 minutes, access point sends a request to client to make her to send a new hash token.

D. *Update Packets*
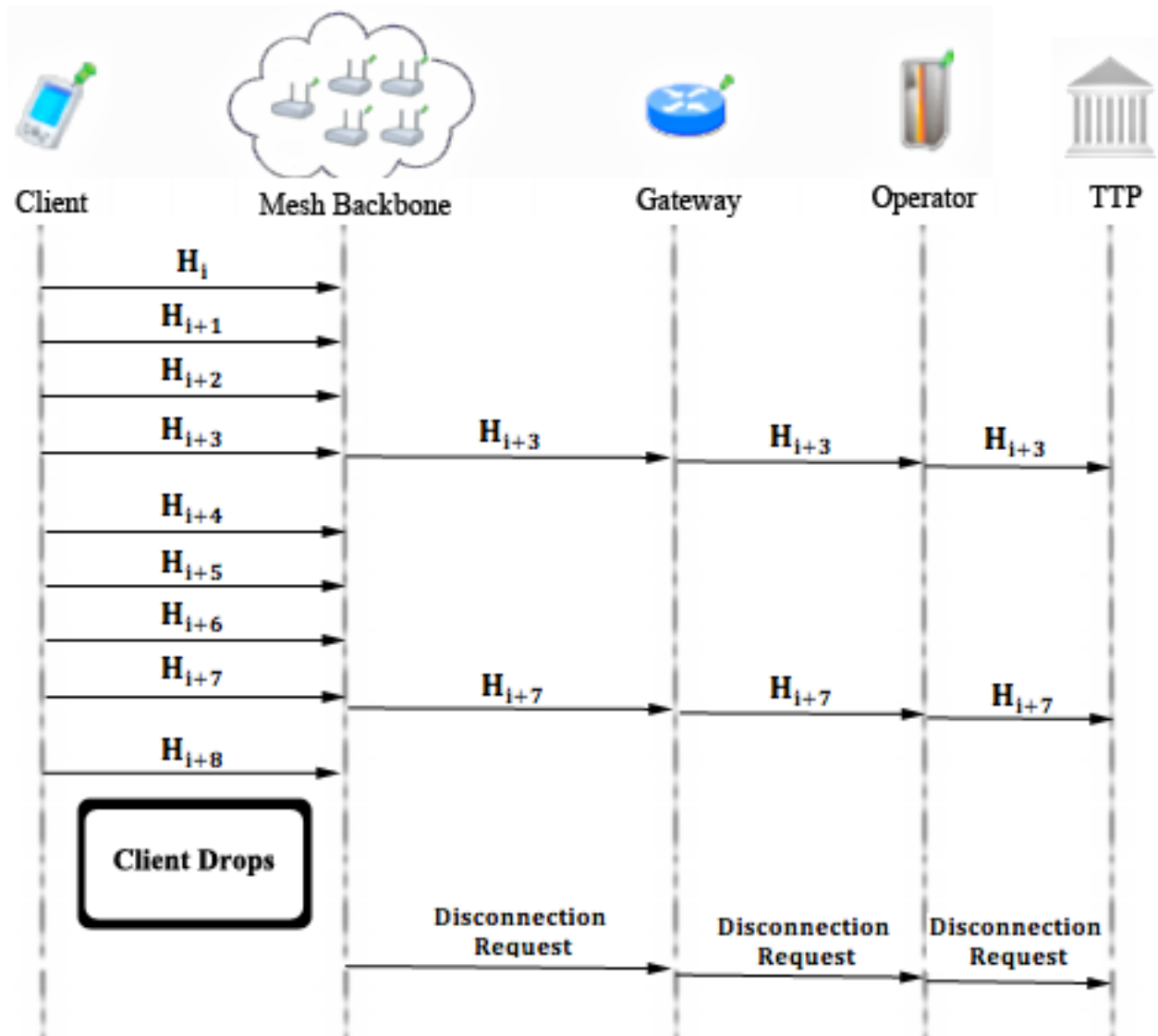
Figure 5. Update Packets

Update Packets protocol, shown in Figure 5, is used in case of an unexpected behaviour in network. If a client drops out of the network, operators and TTP needs tobe informedthat this client is not active anymore. In order to handle this unexpected behaviour, the access points periodically update operators using Update Packets protocol.

In this protocol, client sends concatenation of 128-bit alias and 128-bit hash token to the operator. Operators update TTP in case of a drop. This protocol is a one way end-to-end protocol.

E. *Seamless Mobility and Roaming (Payment Related)*
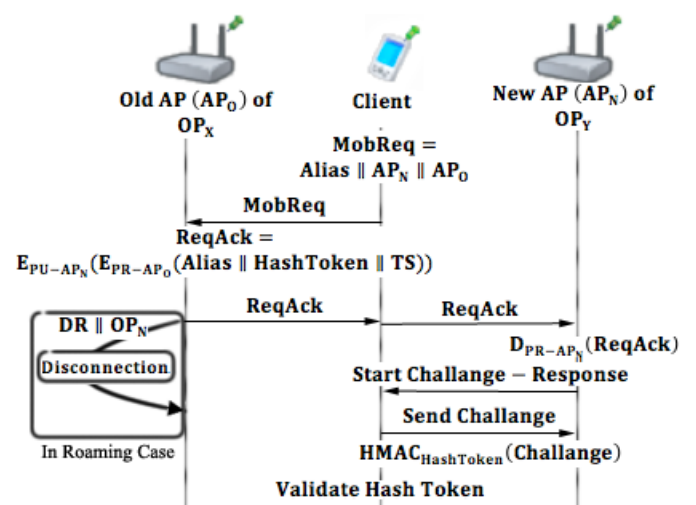
Seamless Mobility and *Roaming* protocols, shown in Figure 6, are run whenever the client changes the serving access point. The running protocol is called *Seamless Mobility* if the new access point belongs to the same operator as the previous access point. If the operators differ, then the protocol is called *Seamless Roaming.*

In these two protocols client sends a 384-bit request packet to the old access point. The old access point receives this packet and performs an encryption on it using RSA-2048, than signs this cipher text using RSA-2048 private key. The old access point sends this packet to client and the client relays it to the new access point. New access point decrypts the packet using RSA-2048 private key and verifies the signature using RSA-2048 public key.

Finally the new access point and the client run a *Challenge-Response Protocol* to authenticate the new access point.

If the running protocol is *Seamless Roaming*, then receiving break-off request from the client triggers the old access point to send a disconnection request to the TTP. This part of the protocol is not implemented in the unit test because it runs in background.

F. *Distributing Access Point Public Keys*
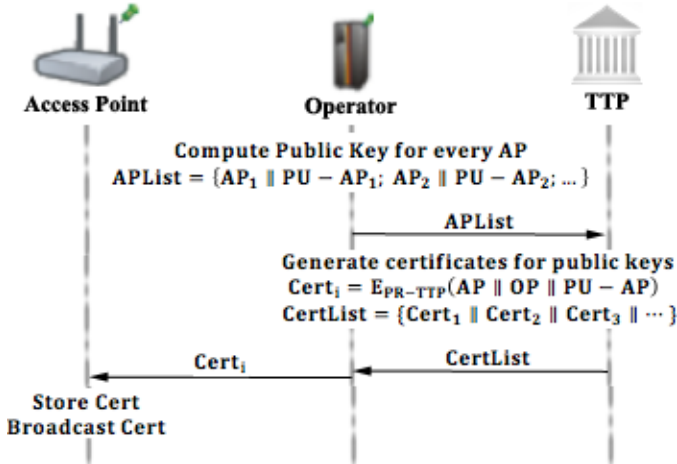
Figure 7. Distributing Access Point Public Keys

A public key distribution mechanism is placed within the system in order to achieve *Seamless Mobility* in home operator and also to support *Seamless Roaming.*

In Figure 7, a generic model for public key distribution is shown. This protocol has two parts; one is certificate generation for the access point public keys, second is distribution of the public keys. The part between operator and the TTP is offline; it runs during the set-up, before the deployment of the access points in the field.

V. UNIT TEST RESULTS

Unit tests cover protocol behaviours 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 systemare 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.

A. *Results 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 8 gives the result for unit test of end-to-end two-way protocols.
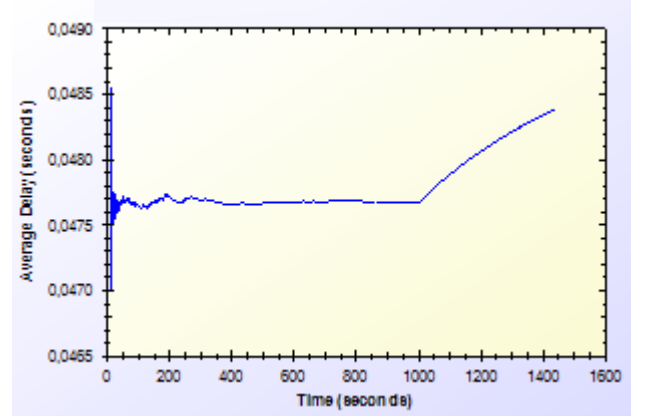
Figure 8. Unit Test Result for End-to-End Two-Way Protocols

As shown in Figure 8, there is a delay that shows variation around 0.04 second. This unstable behaviour 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.

B. *Results 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 9, shows the average delay of the protocol versus time.
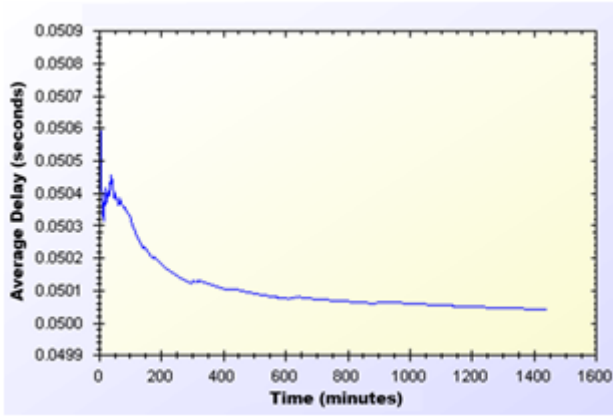
Figure 9. Unit Test Result for Access Point Authentication Protocol

As shown in Figure 9, 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.

C. *Results for Seamless Mobility and Roaming*

Seamless Mobility and *Seamless Roaming* protocols have the same behaviour 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 presents the unit test result for Seamless Mobility and Roaming protocols.
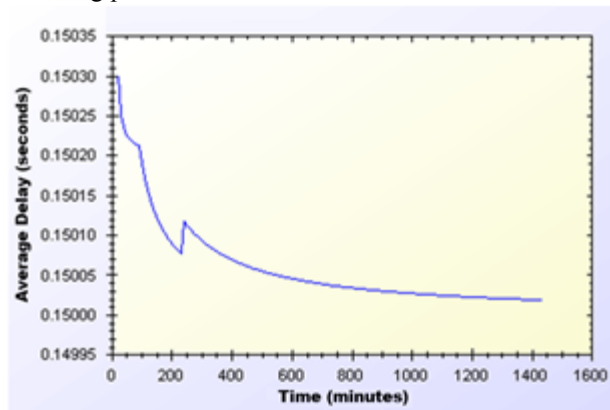

Figure 10. Unit Test Result for Seamless Mobility and Roaming Protocols

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.

D. *Results 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. Packet transfer unit test scenario is that a client sends a 512-byte packet every minute.

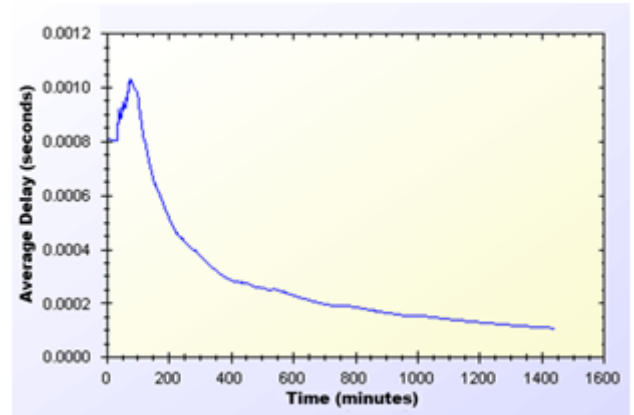Figure 11 shows the unit test result for Packet Transfer protocol.

Figure 11. Unit Test Result for Packet Transfer Protocol

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

E. *Results 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 12 shows the average delay of Update Packets protocol over time.
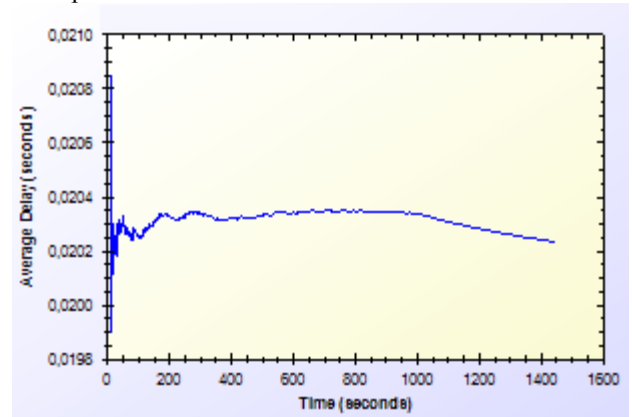

Figure 12. Unit Test Result for Update Packets Protocol

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

VI. CONCLUSION

In unit tests, standalone performances of the protocols under trivial usage scenarios are analysed. The 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 it is demonstrated that the designed protocols reach steady state and reasonable performance in time.

The results are significant since the actual usage of the system is a combination of these protocols. Unit tests 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]   Network Simulator 3 Official Web Site: http://www.nsnam.org/
[3]   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
[4]   FIPS PUB 197 (2001) Announcing the Advanced Encryption Standard (AES), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[5]   Trappe, W., and Washington, L. (2006) Introduction to cryptography with coding theory, *Person Education, Inc*
[6]   Joseph D. Camp and Edward W. Knightly The IEEE 802.11s Extended Service Set Mesh Networking Standard
[7]   Kai Yang, Jian-feng Ma, Zi-hui Miao (2009) Hybrid routing protocol for wireless mesh network, Computational Intelligence and Security – CIS '09