

Secure and Seamless Payment for Wireless Mesh Networks

Serhat Can Leloğlu, Can Yücel, Albert Levi

Sabancı 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. In this paper we propose a secure and seamless pre-payment system for Internet access through WMNs. The proposed system is called and will be mentioned as SSPayWMN. The system will be fair to both clients and to service providers. Since service providers intentionally or unintentionally may overcharge the clients, SSPayWMN offers cryptographic proofs for given Internet service. Additionally SSPayWMN protects clients' anonymity and provides unlinkability for the client actions. The implementation of the system is made on a network simulator and simulation results are presented in this paper. SSPayWMN has achieved remarkable results in the simulations, system protocols reached steady state in every simulation, which ensures the stability of the system.

Keywords—Wireless Mesh Networks, Cryptography, Payment Systems, Security, Network Simulation

I. INTRODUCTION

Wireless Mesh Networks [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 they do not need a centralized element, in that sense they are a subset of ad-hoc networks. Mesh nodes deliver packets from source to destination in a multi-hop manner, conclusively they extent network coverage. WMNs could support for both mesh purposes and also conventional Wi-Fi connections. WiMax [18], ZigBee [19] and 3G radio access [20] could also inter-connect with WMN structure.

There has been research for developing secure pre-payment systems for Internet access. In [8], the authors use a high-level approach for billing and propose architecture. Their focus is mostly its performance on a threshold based bandwidth management algorithm. In [9], 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 [8] 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 unlinkability. The proposed secure and seamless system will implement a prepaid billing scheme with simpler structures and trust models. Authentication, user and operator non-repudiation, settlement and especially user privacy is taken into consideration in the system design.

SSPayWMN employs some cryptographic primitives to ensure system security. The billing system counts on hash chains [10] and uses every element of the hash chain as a token, which buys time intervals with Internet service. SSPayWMN employs a Trusted Third Party (TTP), who ensures honest usage of the system by every party. The packets that are transmitted are either encrypted or transmitted on a secure line.

SSPayWMN is designed to reckon with real-life challenges such as stable Internet service during client mobility and rush hours. To estimate SSPayWMN performance, network simulations for the proposed system are executed. The simulations are divided into two groups. The former is unit tests, which simulate a unit of the system and check if it is fit to use. A unit in SSPayWMN corresponds to network protocols. The latter simulation group is called real-life scenario simulations. In these simulations the clients are selected considering human behaviour and they are grouped into different groups. Unit simulations provided considerable results and in all of the simulations SSPayWMN reached steady state performance. In real-life scenario simulation results the system reached steady state also, which ensures system stability.

The rest of the paper is organized as follows: First we give a brief overview for SSPayWMN and suggested network topology in Section 2. In Section 3 we explain the system protocols. Simulation environment is explained in Section 4 and unit test results are presented in Section 5. Discussion on system properties takes place in Section 6. Finally conclusion is given in Section 7.

II. 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.

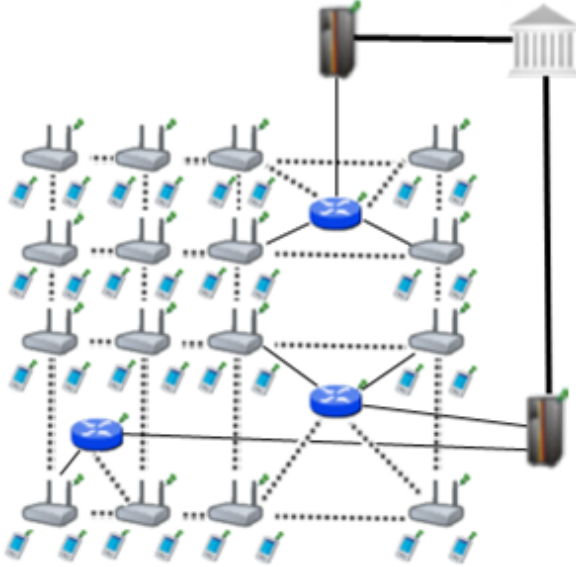


Figure 1. Network Topology

Connection between serving access points is wireless, and they use IEEE 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) [17].

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. This check is done in Change Alias protocol which will be mentioned in Section 3.

C. Notations

The symbols and operators used in this paper are listed below.

III. PROTOCOLS

There exist ten 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.

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.

A. End-to-End Two-Way Protocols

The main protocol in the system is the End-to-End Two-way protocols, which are also the most common ones in the system. The generic depiction is shown in Figure 2.

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.

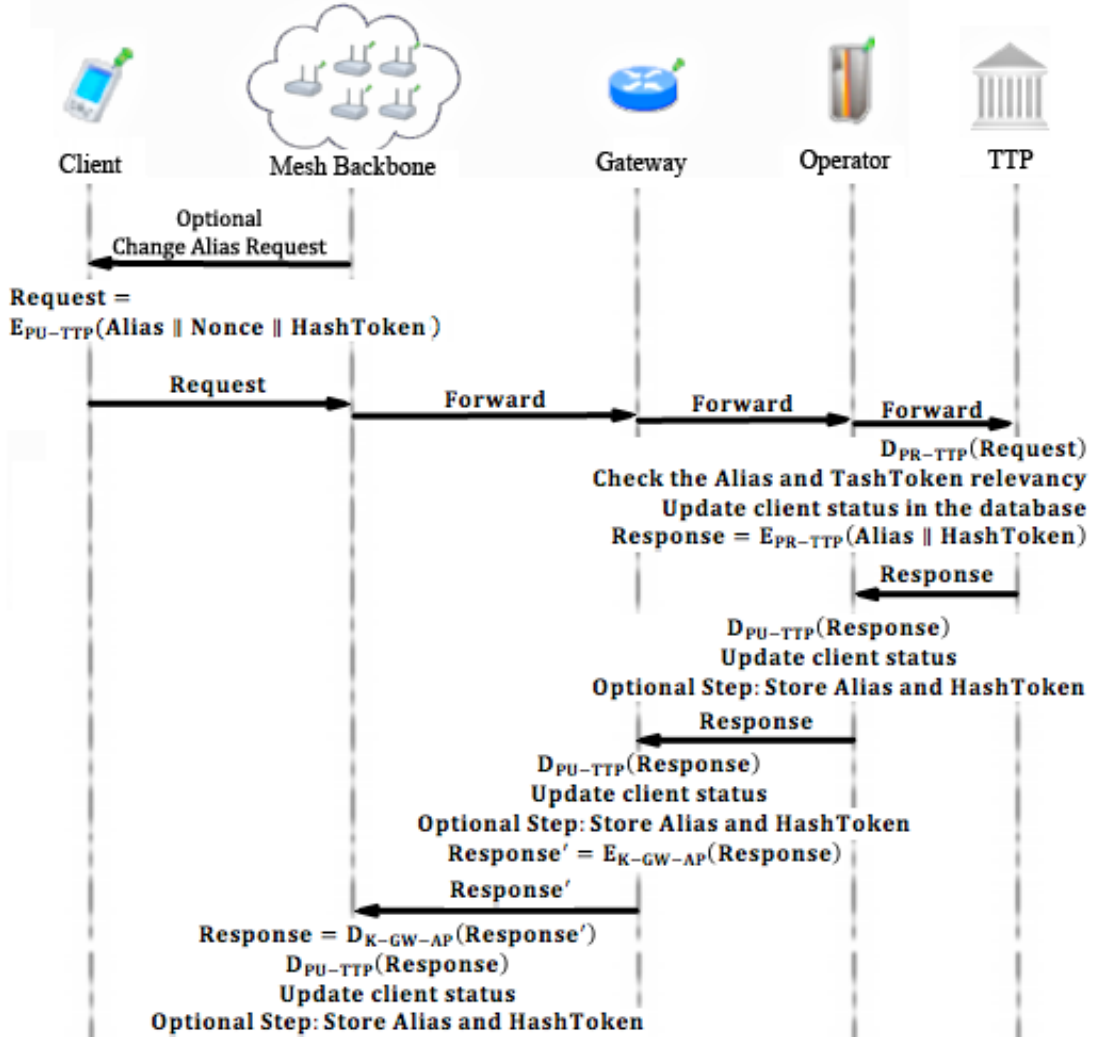


Figure 2. End-to-End Two-Way Protocol Flow

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. Protocol starts with client forming up a Connection request. Considering the generic depiction Figure 2 $Request = Connection Request$ in the case of Initial Authorization. Alias is calculated by taking the xor of Serial Number and a random nonce value as following $SN \oplus N_{CL} = Alias$. HashToken variable is H_0 . When TTP receives the Connection Request (CR) it decrypts it with its own private key and mark the client as connected in the database. In Initial Authorization protocol $Response = Connection Response$.

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 their hash token index. In Initial Authorization protocol the HashToken value is H_0 whereas in Reuse of a Connection Card protocol HashToken value is H_i where $i > 0$. In Initial Authorization and Reuse of a Connection Card protocols an new Alias is formed by performing an XOR operation of SN with a random nonce.

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. In Disconnection protocol $Request = Disconnection Request (DR)$. DR is formed as the same as a Connection Request the only difference is packet overhead which determines the packet's aim. There are 9 protocol that are used by the client, so 4-bit packet overhead is enough for this purpose. In Disconnection protocol client does not change its alias but uses the existing one. Therefore TTP could understand that the client with the particular alias wants to disconnect from the system.

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 by calculating $New Alias = SN \oplus Nonce'$ and send it to the TTP for signature. The overall process is called Change Alias protocol. In this protocol the optional the packet request step is executed unlike the other protocols. Every active client forms up a Change Alias Request (CAR). In the case of Change Alias protocol $Request = CAR$. When TTP receives the CAR and it decrypts the content using its private key. Checks the last used hash token, if it is equal to the hash token that resides in the CAR then TTP signs the new Alias and the HashToken. In this protocol TTP does not update client's status in the database because Change Alias protocol keeps a connected client connected, thus an update is not necessary.

B. Access Point Authentication

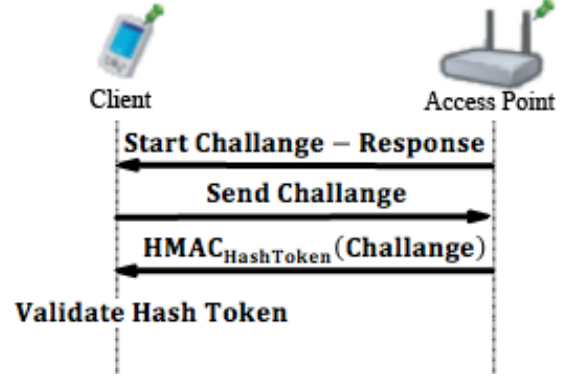


Figure 3. Access Point Authentication

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 an HMAC [16] 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. Distributing Access Point Public Keys

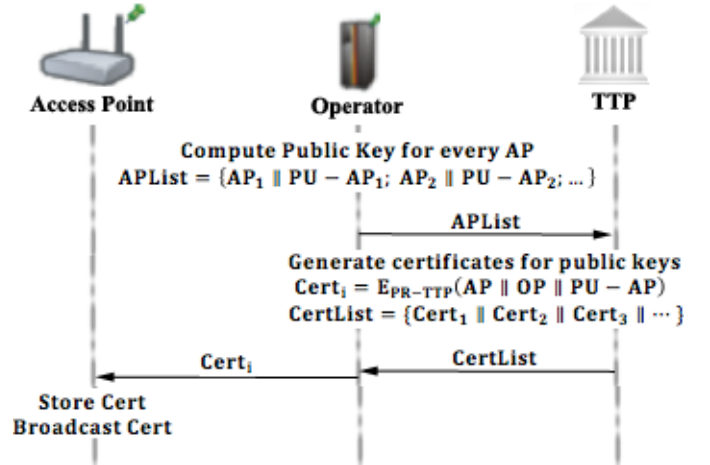


Figure 4. Distributing Access Point Public Keys

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 4, 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.

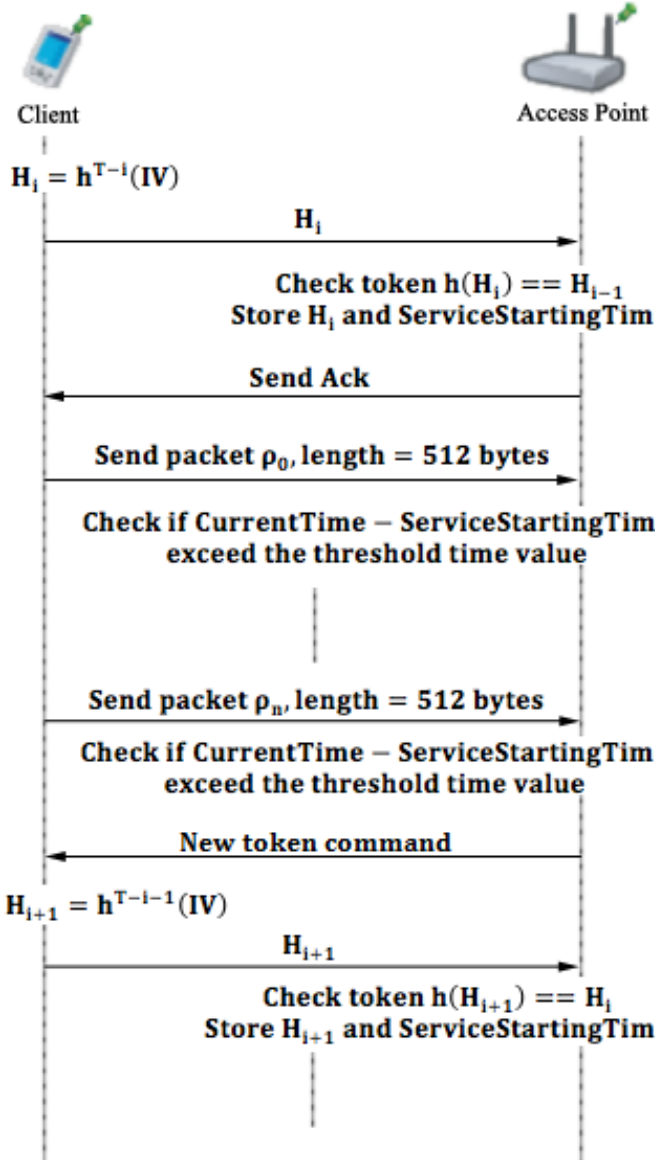


Figure 5. Packet Transfer

Packet Transfer protocol, shown in Figure 5, 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.

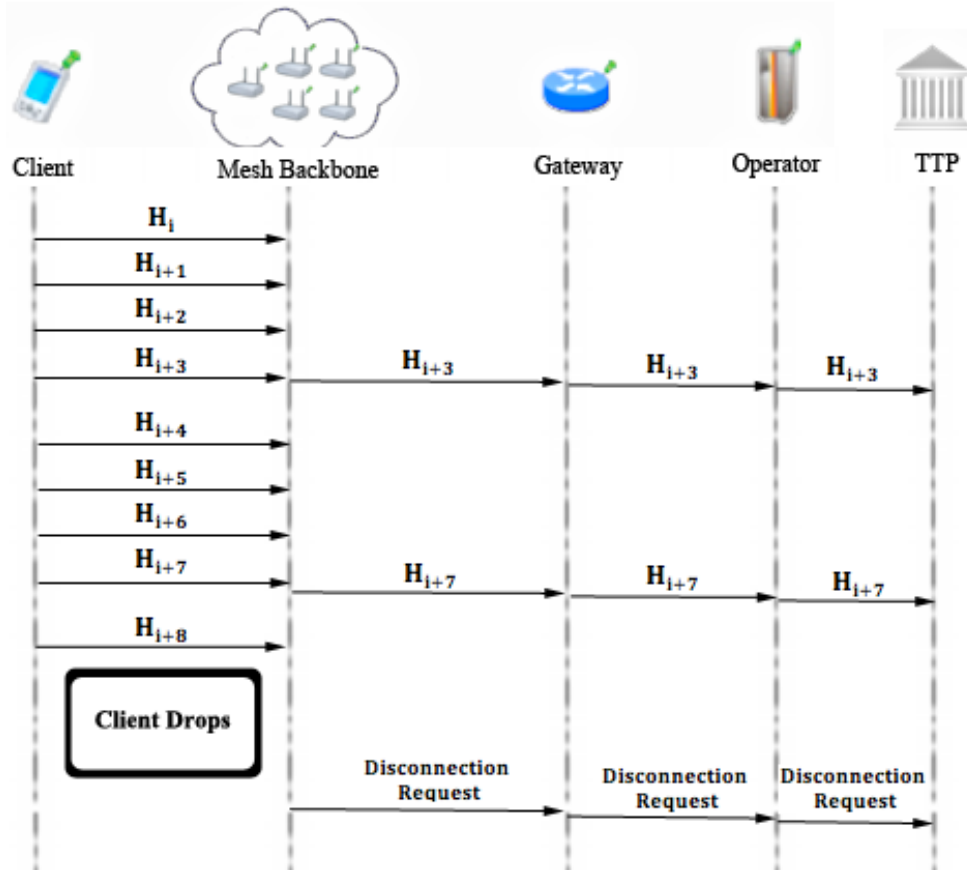


Figure 6. Update Packets

Update Packets protocol, shown in Figure 6, is used in case of an unexpected behaviour in network. If a client drops out of the network, operators and TTP needs to be informed that 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.

F. Seamless Mobility and Roaming (Payment Related)

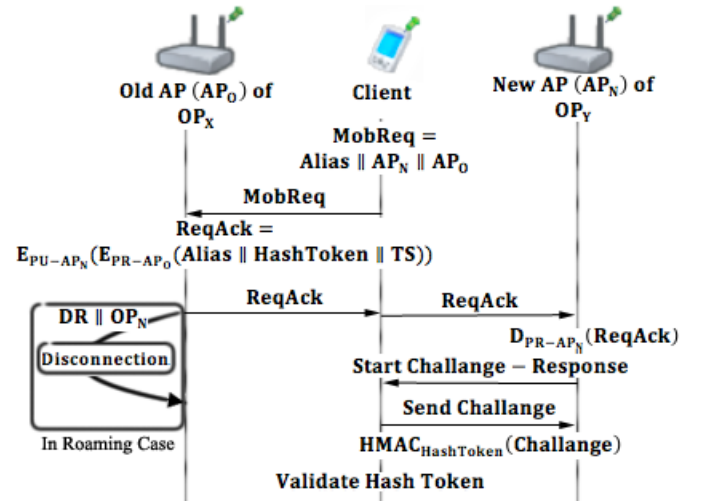


Figure 7. Seamless Mobility and Roaming

Seamless Mobility and *Roaming* protocols, shown in Figure 7, 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, then 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.

IV. SIMULATION ENVIRONMENT

The network topology is hierarchical and WMN supports connection with other IEEE 802.11 protocols [14, 15], clients communicate with TTP via APs, GWs and operators in sequence. Access points are connected to gateways with 6-54 Mbps Wi-Fi connection. Some important specifications about the APs are shown in Table 2. *Update Interval* determines the time value between two update packets that access point send to TTP.

TABLE II
AP Specifications

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

Public Key Operations and Their Timings

Public Key Cryptography timings for access points and gateways are mentioned in [11]. For operator servers and TTP servers, timings from [12] are used. For mobile clients, performance values from [13] are used.

Platform specifications are shown in Table 3, and RSA timings are shown in Table 4.

TABLE III
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 IIIV

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	-

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 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.

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.

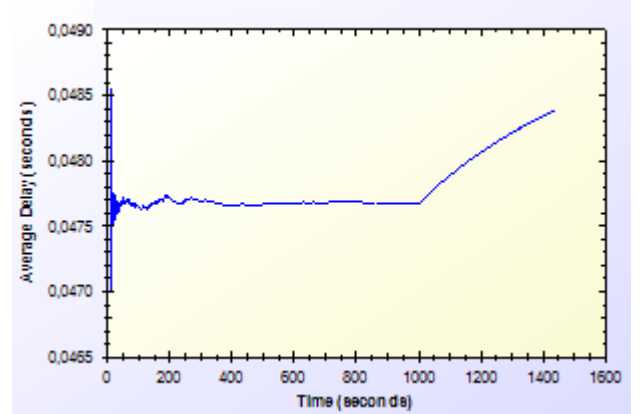


Figure 5. Unit Test Result for End-to-End Two-Way Protocols

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 Protocol

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.

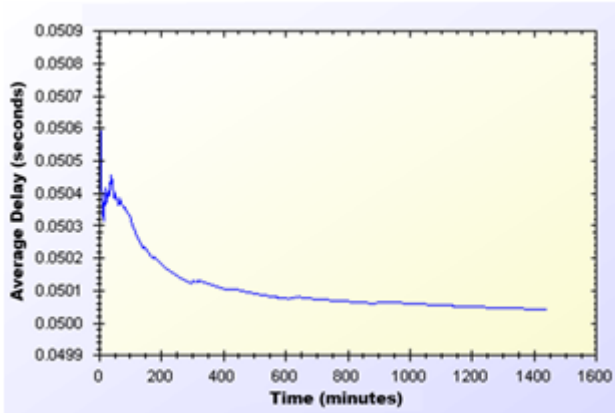


Figure 6. Unit Test Result for Access Point Authentication Protocol

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 Protocols

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.

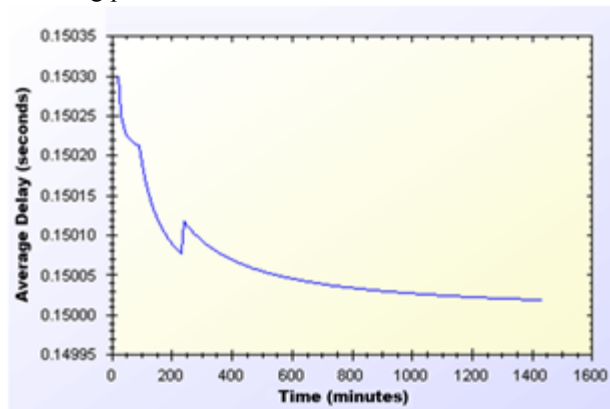


Figure 7. Unit Test Result for Seamless Mobility and Roaming Protocols

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 Protocol

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.

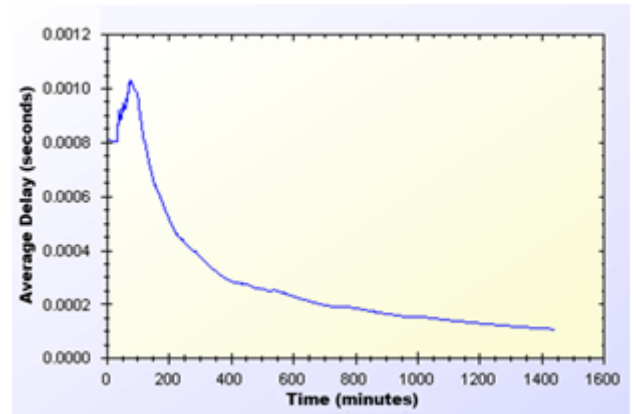


Figure 8. Unit Test Result for Packet Transfer Protocol

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 Protocol

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.

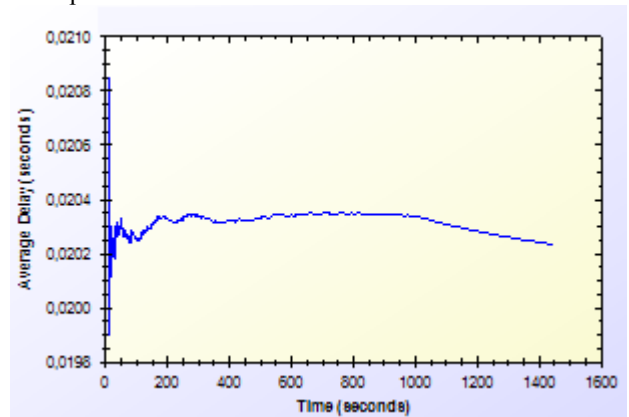


Figure 9. Unit Test Result for Update Packets Protocol

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.

VI. DISCUSSION

In this section the properties of SSPayWMN are discussed.

- *Seamless Roaming/Mobility*: Clients could continue getting service without an interruption in a case of handover.
- *Anonymity*: For legal purposes users must give their identities to Trusted Third Party (TTP) for getting connection cards. Therefore, as far as TTP keeps clients' identities secret, users can stay anonymous.
- *Mutual authentication*: Challenge-Response Protocol ensures mutual authentication between AP and the client.
- *No ultimate trust to operators*: Because of the one-way property of hash chains only the user could know the next element in the hash chain of tokens. Therefore without client giving the next element of the hash chain operator could not guess the element. The client could object to any type of over charge with cryptographic proofs.
- *Preventing double spending*: All the connection card information is stored in the TTP's database. TTP authorizes every token; it is not possible for client to use a token for a second time. Since TTP could not get the new token with a series of hash operations.
- *Unlinkability*: SSPayWMN provides unlinkability 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 system designer. In real-life scenario simulations the time period was 50 minutes.

VII. 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*
- [8] Zaghloul, S., Bziuk, W. and Jukan, A. "A scalable Billing Architecture for Future Wireless Mesh Backhauls", *IEEE ICC '08*.
- [9] 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.
- [10] Lamport, L. (1981) Password authentication with insecure communication, *Proceedings of Commun. ACM*, vol. 24, no. 11, pp. 770-772.
- [11] Efsthathiou, E., Frangoudis, P., and Polyzos, G. (2006) Stimulating Participation in Wireless Community Networks, *IEEE INFOCOM, 2006*, Barcelona, Spain.
- [12] 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>
- [13] 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
- [14] Intel Inc., Multi-Hop Mesh Networks—a new kind of Wi-Fi network.
- [15] 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>.
- [16] American Bankers Association, *Keyed Hash Message Authentication Code*, ANSI X9.71, Washington, D.C., 2000.
- [17] Chaum, D. (1982) Untraceable electronic mail, return addresses, and digital pseudonyms, *Communications of the ACM*, 4(2).
- [18] Vaughan-Nichols S.J., (2004) Achieving wireless broadband with WiMax, *IEEE Computer*, vol. 37, no.6, pp. 10-13
- [19] The ZigBee Alliance. Available from: <http://www.zigbee.org>.
- [20] 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