**Slide 1**

Hello, thank you all for joining to my jury. Today I will present my thesis, about a secure and seamless prepayment system for wireless mesh networks. The prepayment scheme is called SSPayWMN.

**Slide 2**

On this presentation, firstly I will give a brief introduction to my thesis. I will define the problem and propose a solution.

Then I will describe the building block of the system.

After that I will briefly explain our protocols and inform you about the simulation environment and client models.

Simulation results and performance evaluation will follow.

Finally we will discuss the success of SSPayWMN and I will give you the conclusions.

**Slide 3**

In e-payment systems clients generally put full or partial trust to service providers. However service providers may unintentionally overcharge their clients. We intended to provide a fair system for both clients and to the service providers.

There has been some research on e-payment systems. Rivest and Shamir, proposed the first prepayment for e-payment systems. It is called Pay-Word. Their system used elliptic curve cryptography for public key operations and hash chains for e-cash, which is the e-currency of the system. There have been extensive improvements on their work, like using RSA based signature. The improvements speeded up the system but they did not provide seamless service providing.

Some other related works provide seamless service providing; however they did not provide anonymity and untraceability.

SSPayWMN is proposed to tackle these problems. Providing a secure and seamless prepayment for wireless mesh networks, while providing privacy and untraceability to some extent. Moreover, support steady state performance with reasonable delays.

**Slide 4**

Our objectives are listed on this slide.

We intended to provide wide coverage since SSPayWMN is designed to provide service in metropolitan area.

Our system should be able to provide mobility support for clients and provide seamless connection without causing any interruption.

The system should provide anonymity and untraceability for the clients.

The system will provide mutual authentication. The client will be ensured that she is connected to the correct network.

Usage of hash tokens will provide two-way honesty. Overcharging will not be possible.

The system performance is evaluated using simulations conducted with network simulator 3 (a.k.a. ns-3).

**Slide 5**

Using the listed entities we have formed up the system.

There are mobile clients, access points that forms up the mesh backbone, gateways, several operator servers and a trusted third party server.

**Slide 6**

The clients will receive their services with the connection cards. The clients buy their connection cards from the trusted third party.

Trusted third party selects a random value and forms up a hash chain. Hash chains are formed by using the output of a hash algorithm as an input to another hash algorithm.

The count of hash operations determines the length of the hash chain.

We use the irreversibility property of hash chains. It is easy to find a hash output using the input but it is infeasible for otherwise.

Aliases will be used and changed frequently to provide anonymity and untraceability to some extent.

**Slide 7**

From now on I will explain the protocols of the system.

In this slide two protocols are depicted.

Initial Authorization and Reuse of a Connection Card.

Client encrypts the connection request using the trusted third party’s public key. Sends the request through the mesh backbone.

TTP will decrypt the packet and calculate SN.