A Quantitative Study of Authentication and QoS in Wireless IP Networks

Wei Liang Wenye Wang

IEEE Infocom 2005

2006/11/10

Presented by L.K. Chien

Outline

- Introduction
- Challenge/Response Authentication
- Handoff authentication
- QoS metrics
- Security levels
- Quantitative model
- Results
- Conclusion
- Discussion

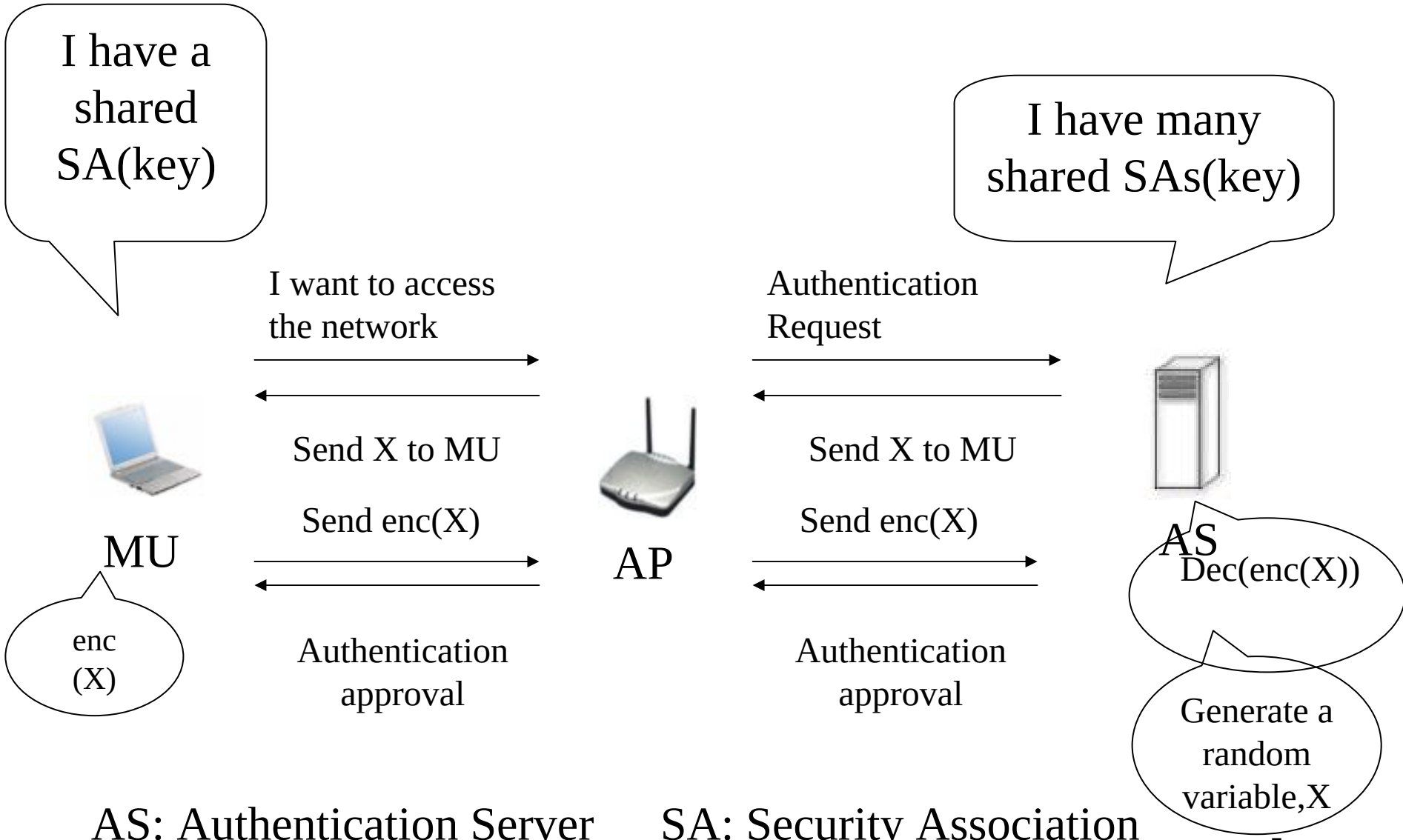
Introduction

- We need secure and high-quality communications in public access wireless IP networks.
- If we increase security level, then the QoS will decrease, and vice versa.
- Is there a quantitative model to find a numerical result to scale the security level and QoS?

Challenge/Response Authentication(CRA)

- The client and server both know the function for encryption/decryption.
- We use a shared security association (SA) to identify the mobile user (MU).
- Shared SA is a trust relationship with parameters (keys…).

Challenge/Response Authentication(CRA)



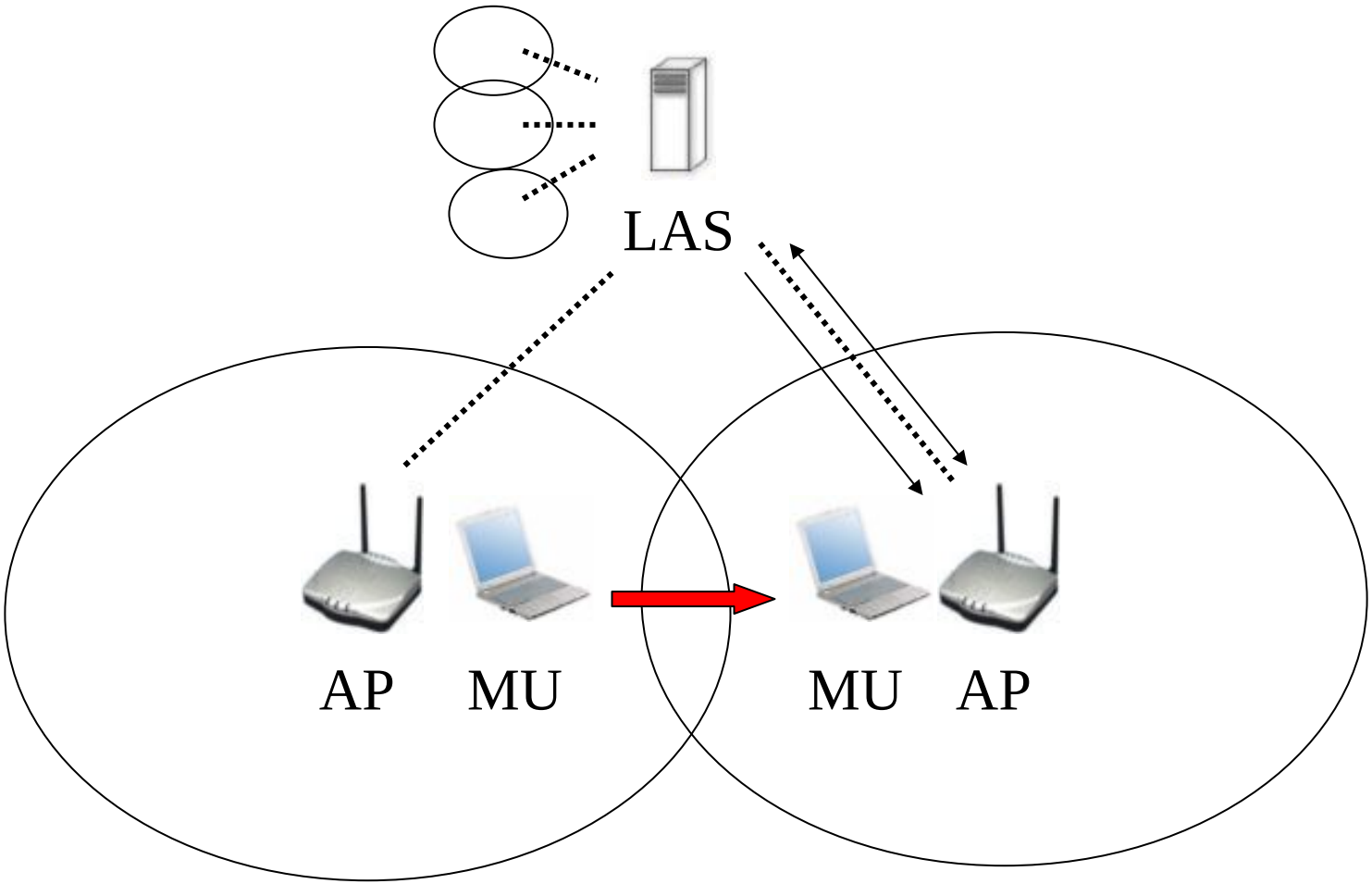
AS: Authentication Server SA: Security Association

Handoff Authentication

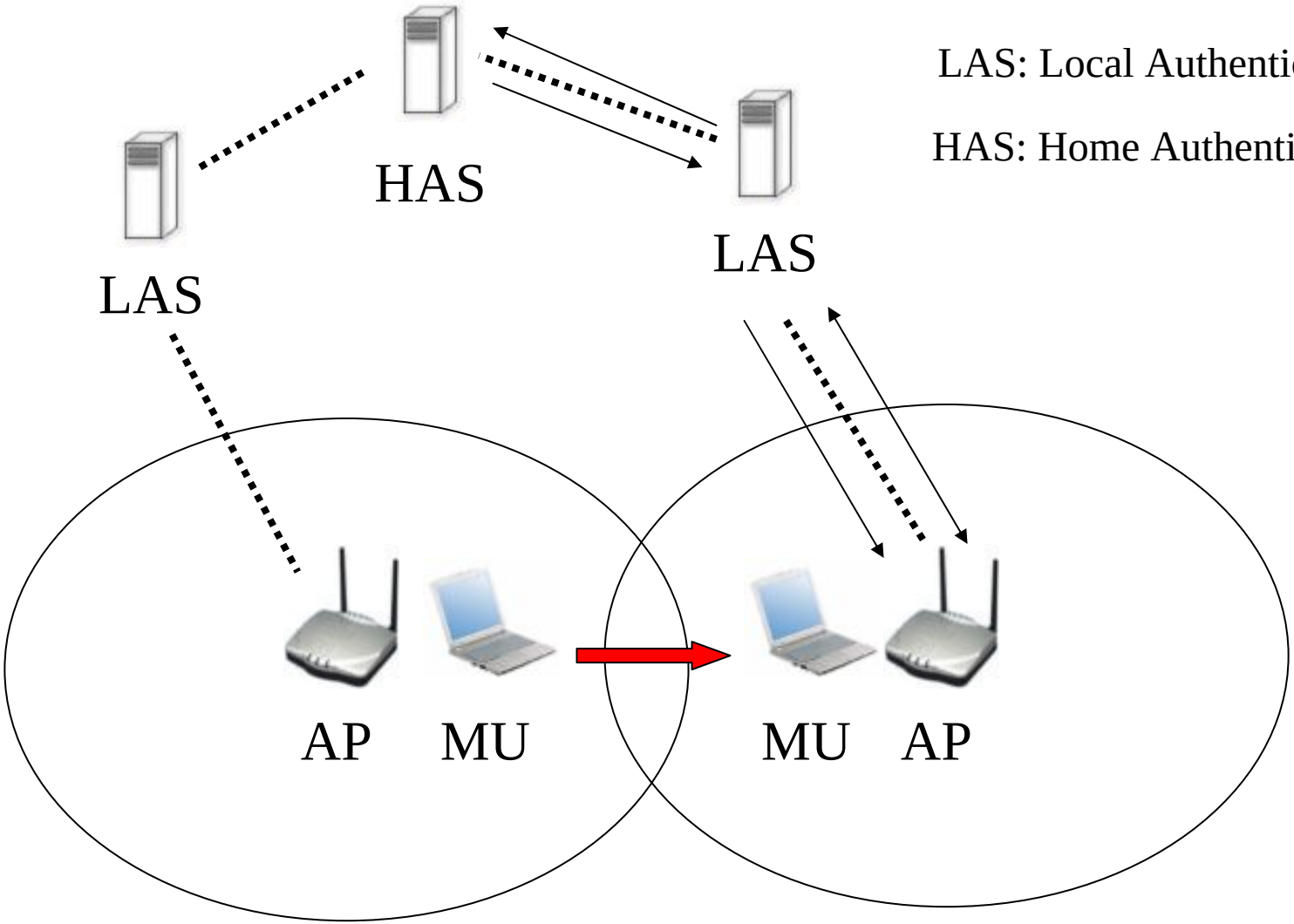
- Intra-domain handoff authentication
- Session authentication
- Inter-domain handoff authentication

Intra-domain handoff authentication

LAS: Local Authentication Server



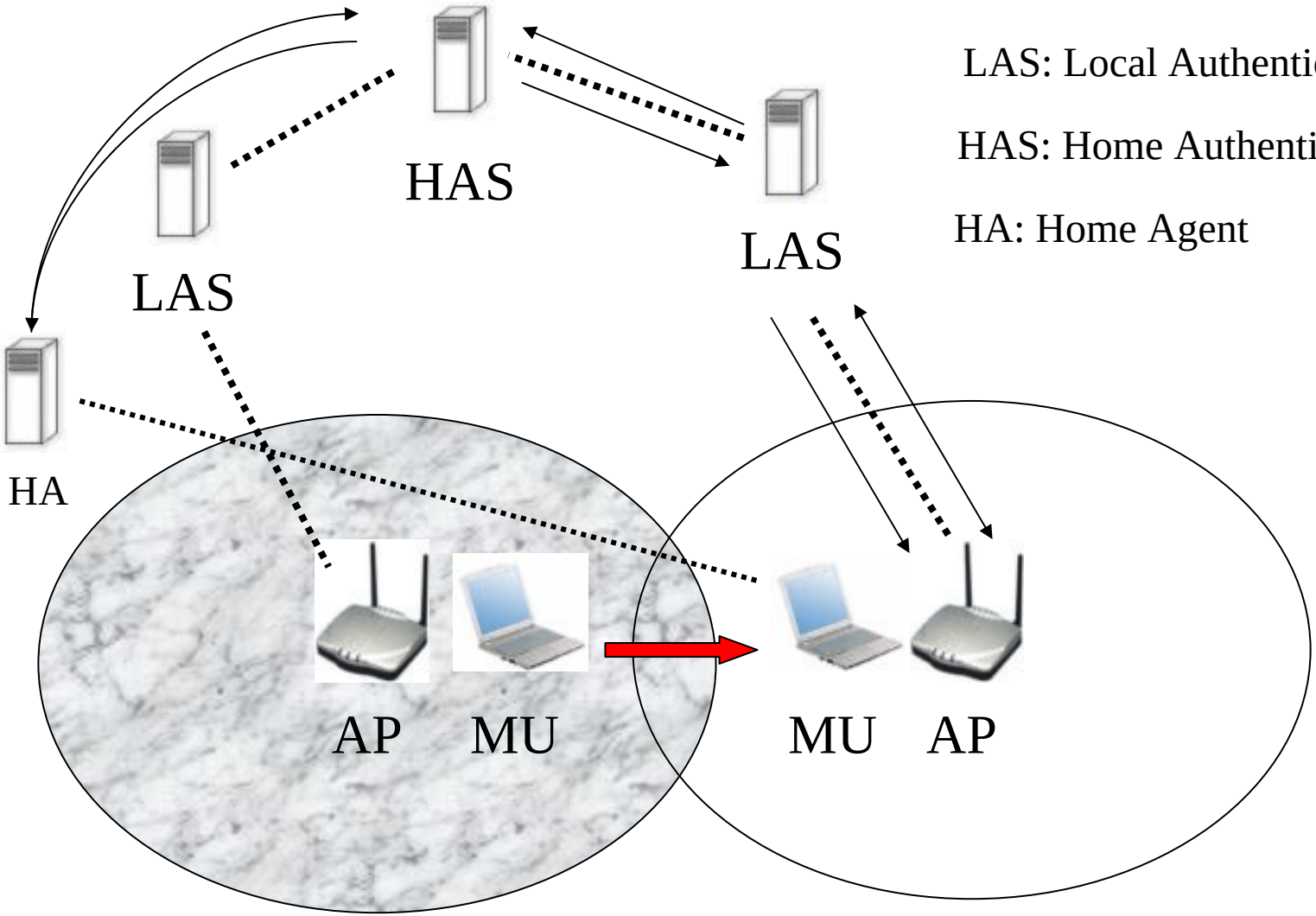
Session authentication



LAS: Local Authentication Server

HAS: Home Authentication Server

Inter-domain handoff authentication

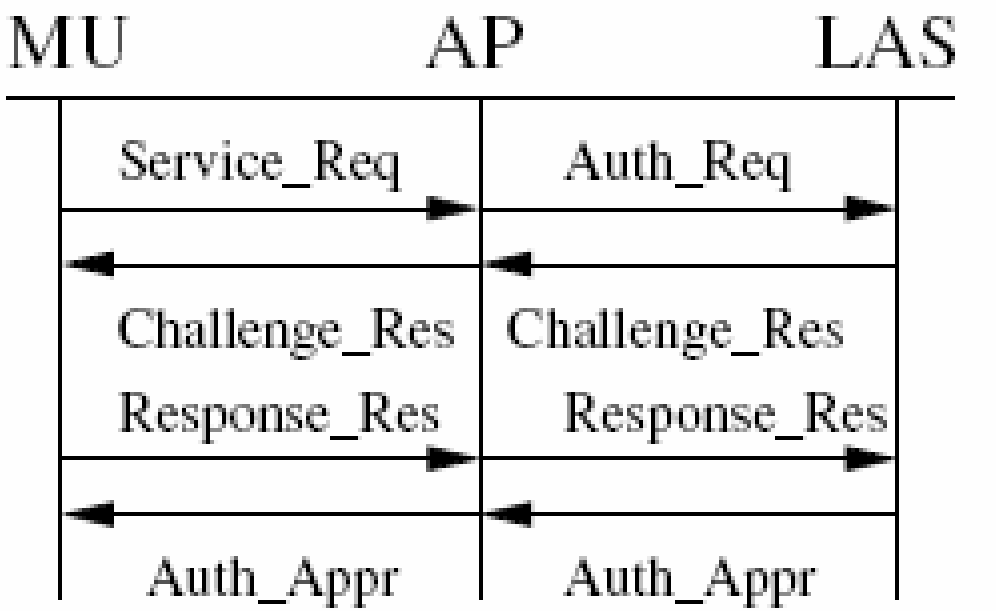


LAS: Local Authentication Server

HAS: Home Authentication Server

HA: Home Agent

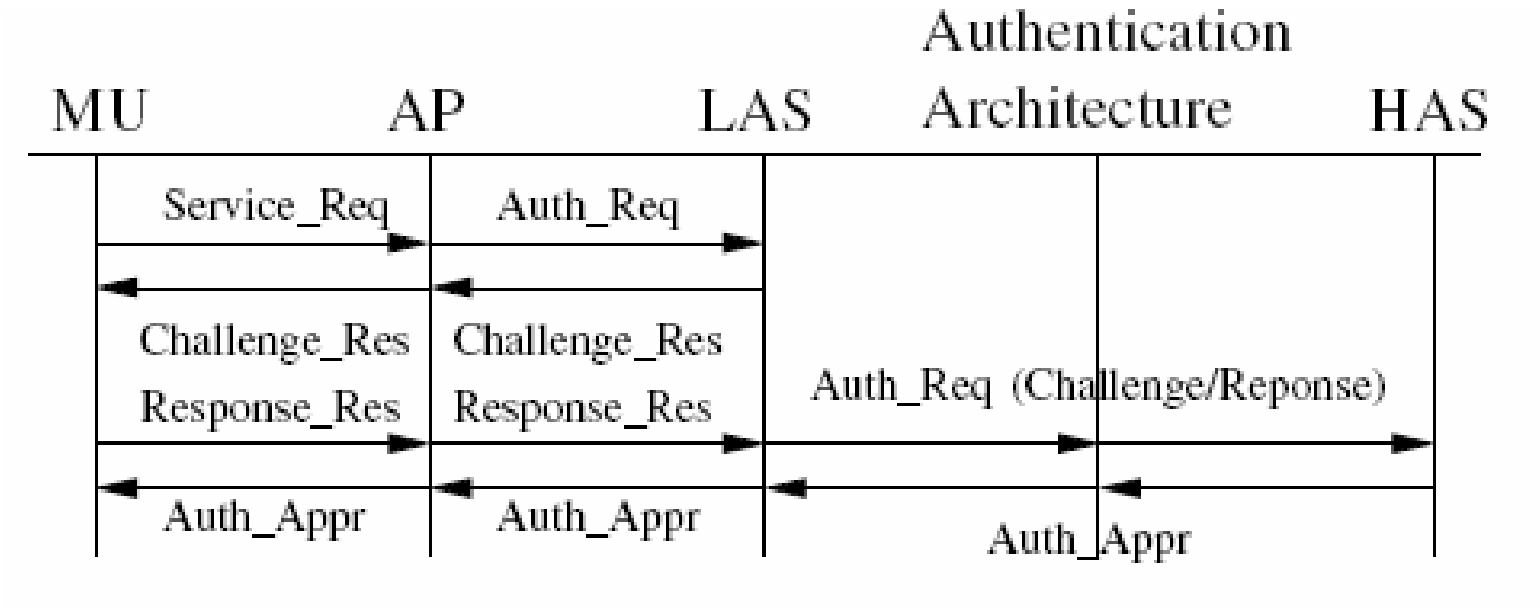
The diagrams of 3 handoff authentications



A. Intra–domain Handoff Authentication

LAS: Local Authentication Server HAS: Home Authentication Server HA: Home Agent AP: Access Point MU: Mobie User

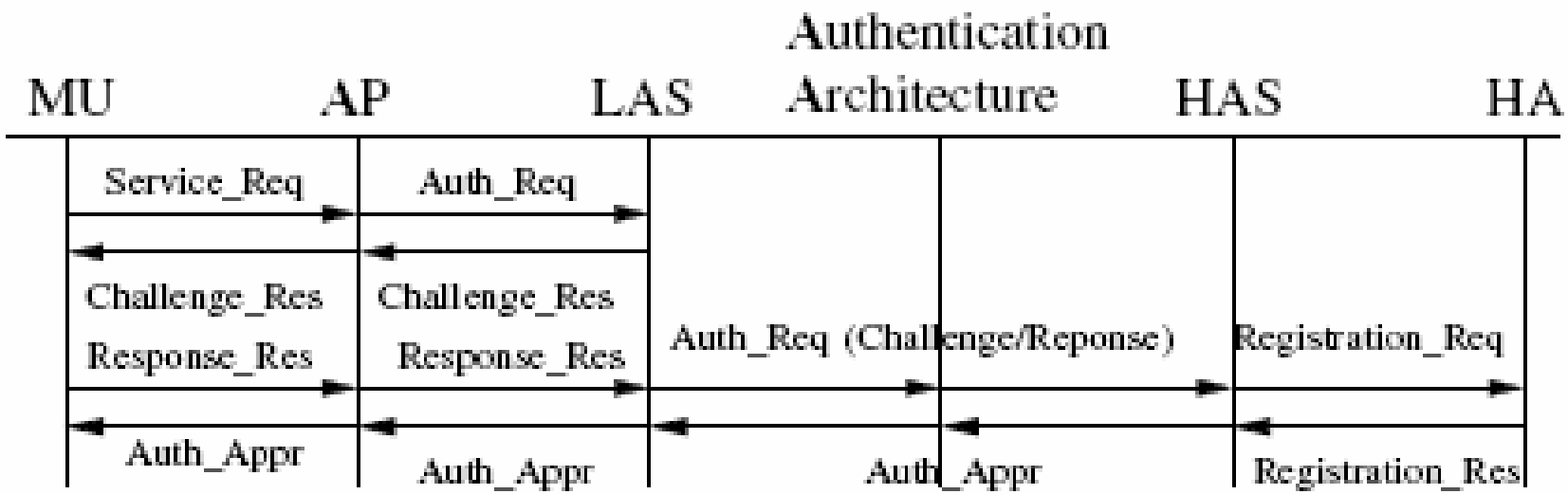
The diagrams of 3 handoff authentications



B. Session Authentication

LAS: Local Authentication Server HAS: Home Authentication Server HA: Home Agent AP: Access Point MU: Mobie User

The diagrams of 3 handoff authentications



C. Inter–domain Handoff Authentication

LAS: Local Authentication Server HAS: Home Authentication Server HA: Home Agent AP: Access Point MU: Mobie User

QoS Metrics

- Authentication delay :
  - The interval of MU sends *service_request* and receives *authentication_approval*.
- Call dropping probability :
  - The probability of connection loss due to too long authentication delay or authentication failure.

Security levels

- Security level 1:
  - If the MU sends a *service_request*, the AP just checks the resource availability, then the MU can access the network or not.

Security levels

- Security level 2:
  - When the MU sends a *service_request*, the AP asks for the MU's MAC address, and AP relays the MAC address to the LAS. If the MAC address is in the LAS's list (or HAS's one), the *authentication_approval* will be sent to the MU.

Security levels

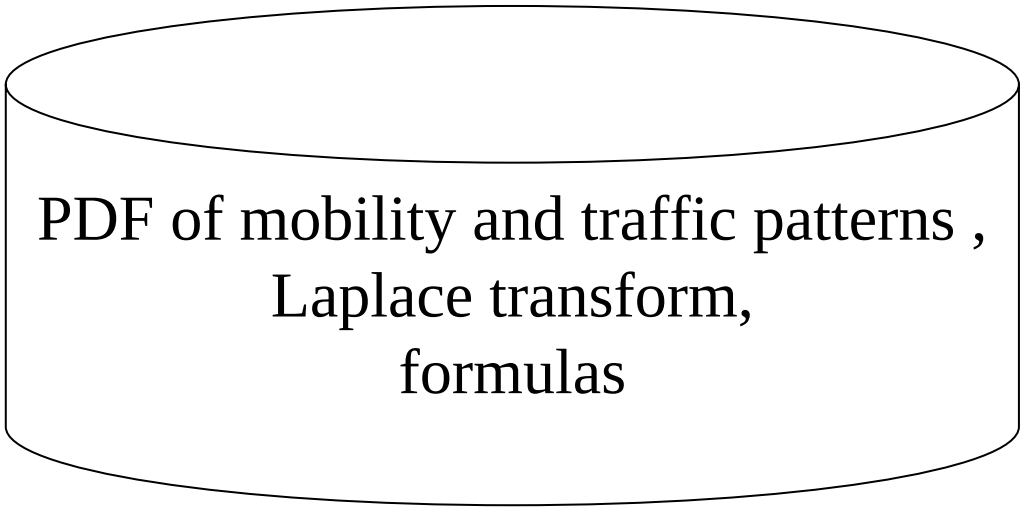
- Security level 3:
  - When the MU sends a *service_request*, the AP sends a *authentication_request* to the LAS. The Challenge/Response Authentication is used.
  - The MU is identified as a legal user after the CRA, however, the data transmissions are not encrypted. It means that there is no data integrity and secrecy.

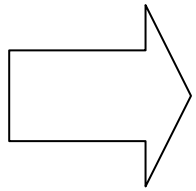
Security levels

- Security level 4:
  - It’s similar to level 3, and the difference is that the keys are generated, encrypted, and transmitted to the MU, HA.
  - The keys are used to encrypt the data of communication in order to protect data integrity and secrecy.

Quantitative model

Security level,
average arrival rate, service rate, residence time,
other parameters.





Numerical results

Numerical Results

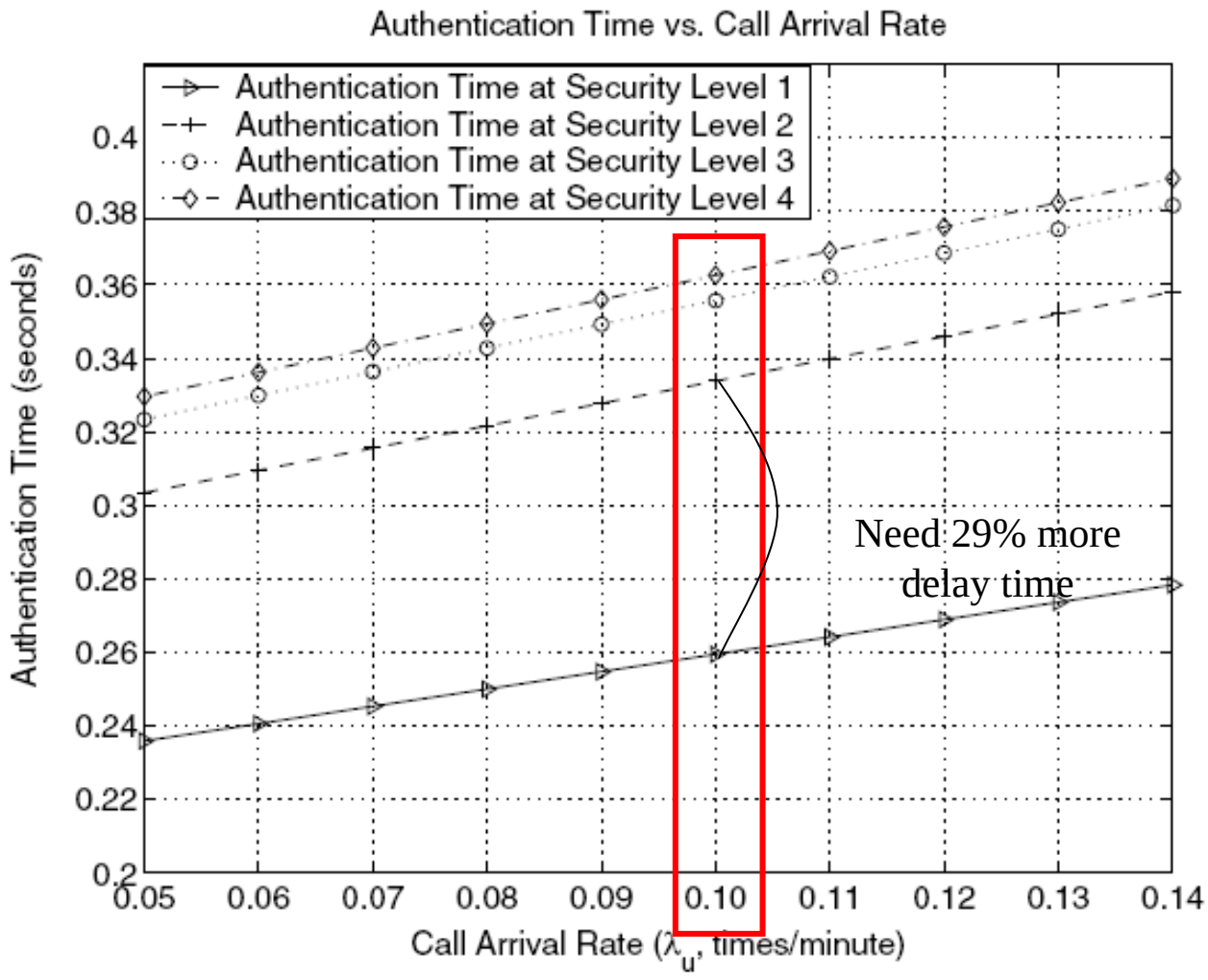
- We assume that M/M/1 queues are used at AP, LAS, HAS, and HA.
- Parameters

PARAMETERS FOR EVALUATION ON QOS METRICS

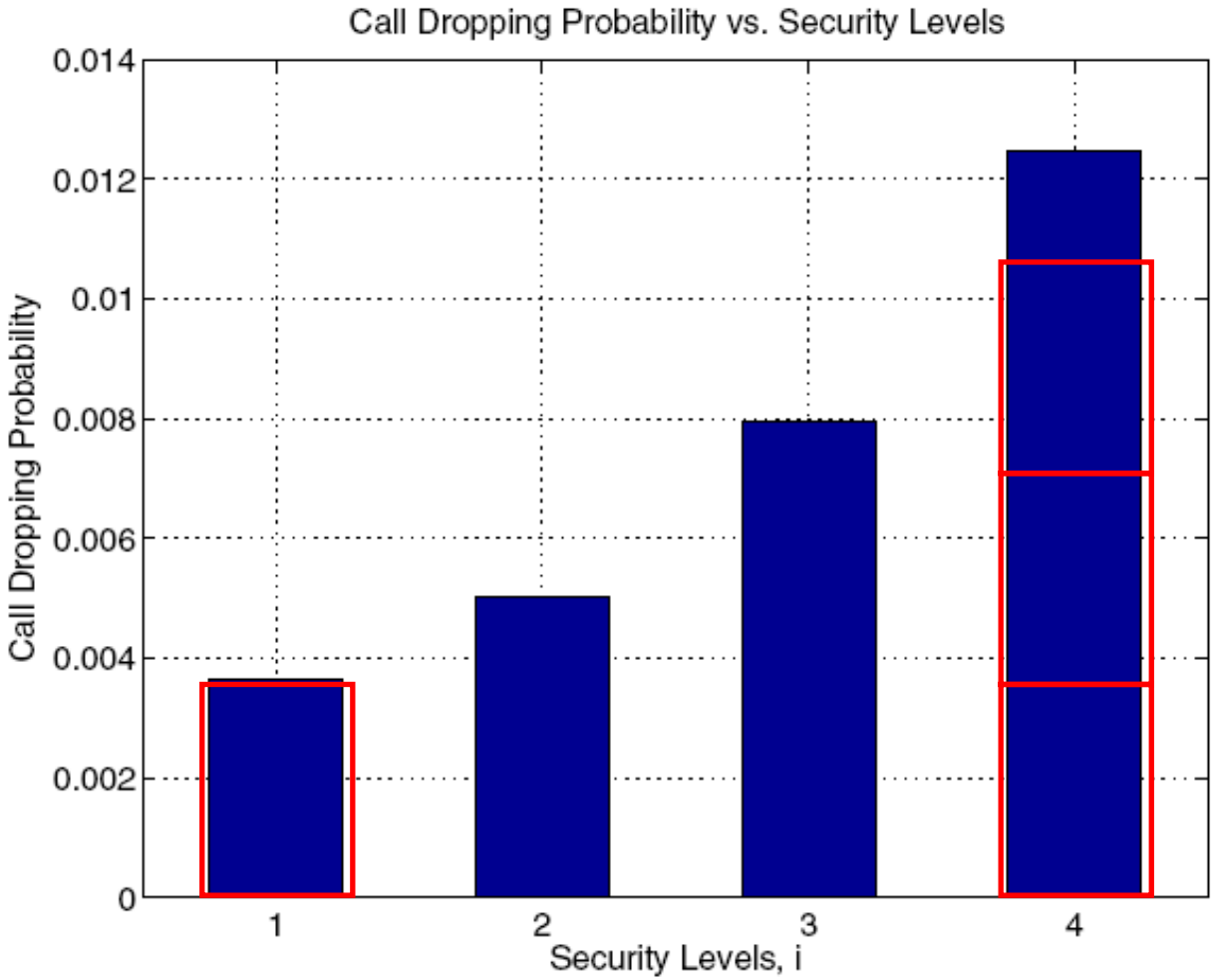
Parameters for Authentication Delay						
T_{th}	T_{pr}	T_{tr}	T_{ed}	T_g	M	N_h
3s	40 μs	20ms	2ms	2ms	120	10

Parameters for Random Variables				
λ_u	η	γ	μ_r	ξ
0.1 min^{-1}	0.3 min^{-1}	225	1/15 min^{-1}	15 sec^{-1}

Numerical Results



Numerical Results



Conclusion

- The contribution of this paper is that the authors proposed a quantitative model to analyze the impact of authentication on security and QoS.
- Their study was the first work on providing a quantitative analysis on security and QoS.

Discussion

- What is the mechanism of SA delivery?
- Is it necessary to encrypt the data on transmission after authentication in WiFi and WiMAX networks?