Registration and Session-Key Distribution in AAA for Mobile IP

Jae-Hoon Whang, Hong-Yeop Song

jhwhang@eve.yonsei.ac.kr

Coding & Information Theory Lab.
Department of Electrical and Electronic Engineering,
YONSEI UNIV.

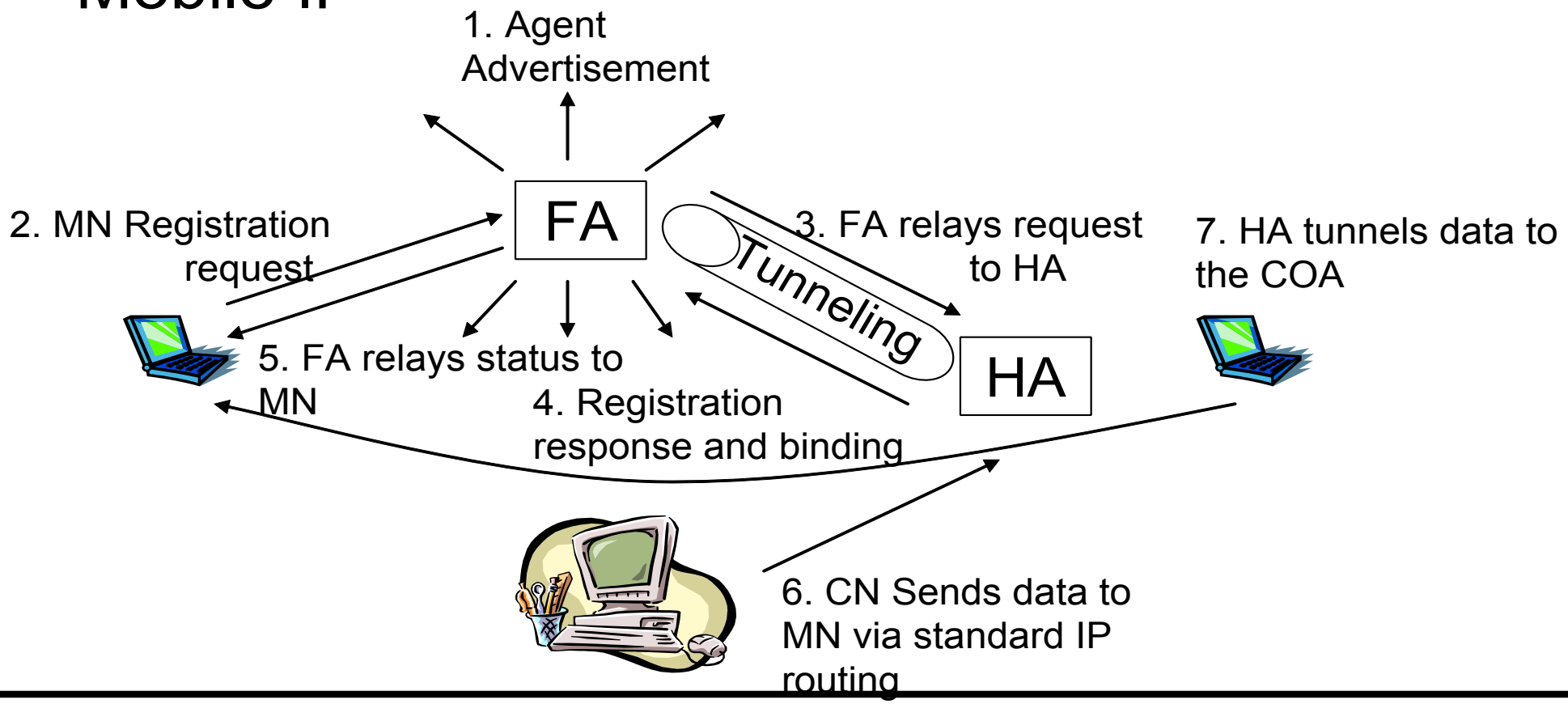
Contents

1. Introduction

- Mobile IP aims to support mobility within the internet.
- We'll mention the security aspect of Mobile IP,
- And propose a new registration and session-key distribution protocol using public-key cryptography.

2. Mobile IP and AAA

- Mobile IP

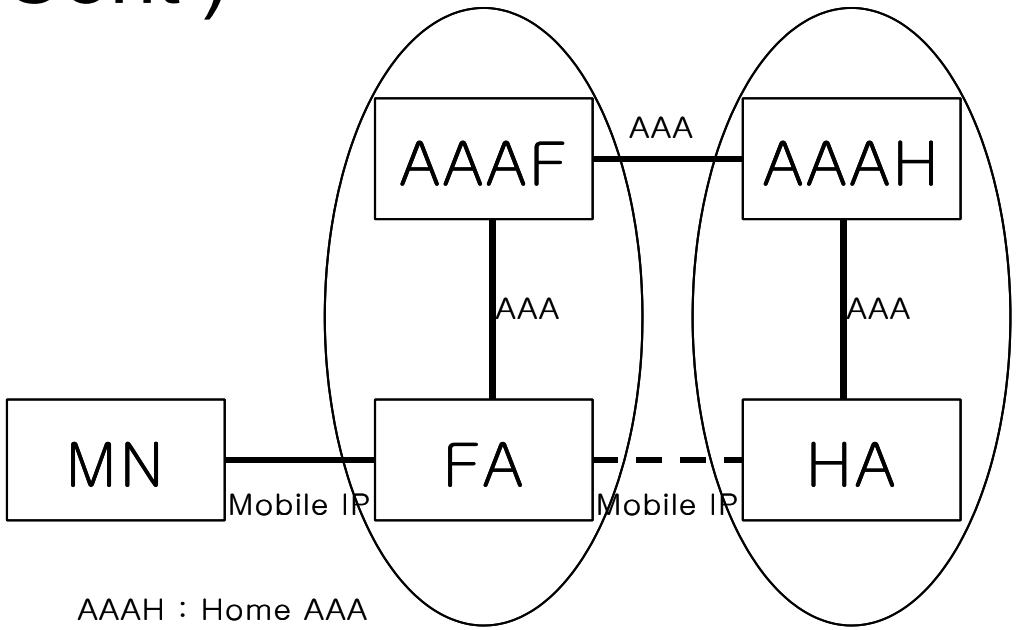


2. Mobile IP and AAA

- Authentication, Authorization and Accounting (**AAA**)
  - **Authentication** : validating the end user's identities prior to permitting them network access
  - **Authorization** : defines what right and services are allowed to the end user
  - **Accounting** : provides the methodology for collecting information about end user's resource consumption

2. Mobile IP and AAA

- Authentication, Authorization and Accounting (**AAA**) (Cont')



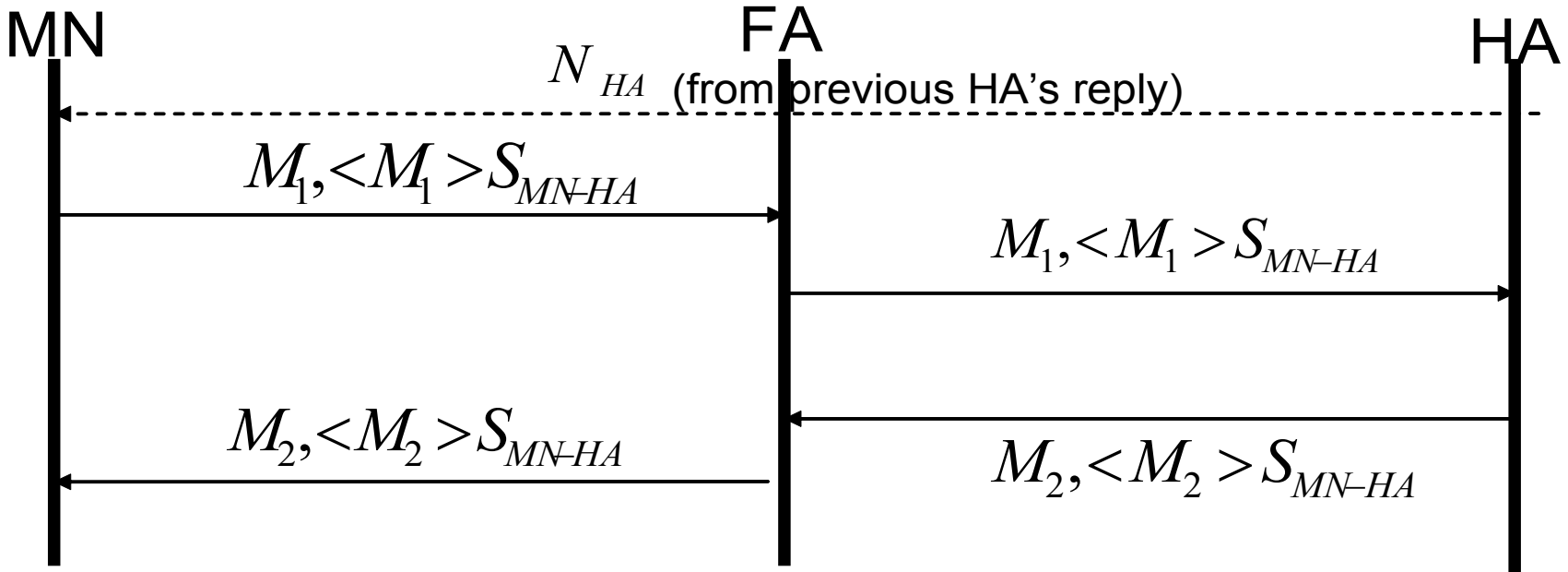
3. Conventional Registration Protocol and Replay Attack

- **Registration Protocol**

The following notations are used to represent message in protocol

- **M, N : concatenation of two messages M and N**
- **MN_{HM} : MN's home address**
- **MN_{COA} : MN's care-of-address**
- **HA_{id} : HA's IP address as its ID**
- **FA_{id} : FA's IP address as its ID**
- **N_{MN}, N_{HA} : nonce issued by MN and HA**
- **{M}K : encryption of message M under key K**
- **<M>K : MAC value of message M under key K**
- **S_{MN-HA} : shared secret key between MN and HA**
- **Req : a bit pattern indicating a request**
- **Rep : a bit pattern indicating a reply**
- **Result : a value of indicating result of the request**

3. Conventional Registration Protocol and Replay Attack



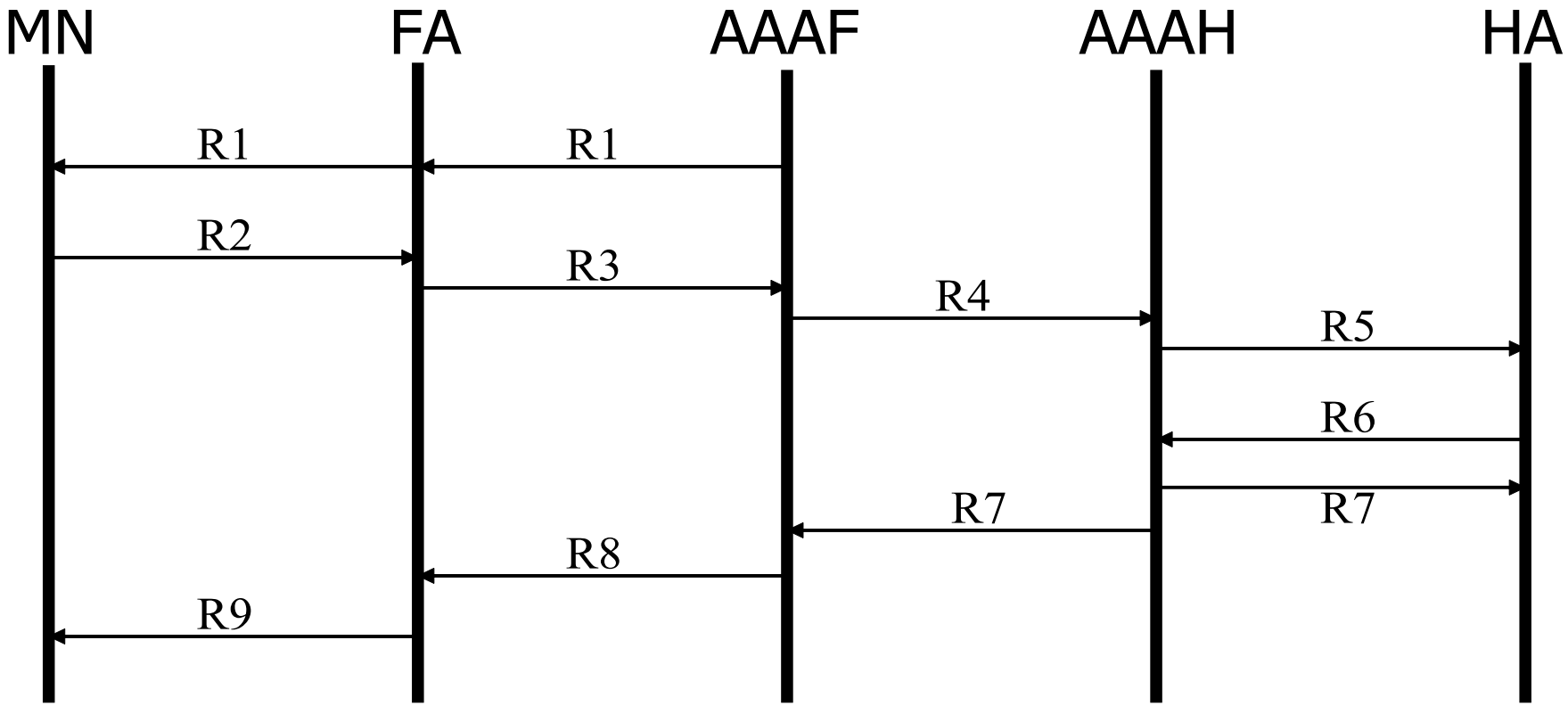
$$M_1 = \text{Req}, FA_{id}, HA_{id}, MN_{HM}, MN_{COA}, N_{HA}, N_{MN}$$

$$M_2 = \text{Rep}, \text{Result}, FA_{id}, HA_{id}, MN_{HM}, N'_{HA}, N_{MN}$$

4. Proposed Public-Key Based Registration and Session-Key Distribution

- Design principles
  - Minimize the computing power requirement as well as administration cost imposed on MN
  - Use mechanism for certificate retrieval and validation
  - Provide a secure session-key distribution
  - And we assume secure association(SA) between FA & AAAF, and HA & AAAH.

4. Proposed Public-Key Based Registration and Session-Key Distribution



4. Proposed Public-Key Based Registration and Session-Key Distribution

- **New notations are related to public-key operation and session-key**
  - $\mathbf{K_{AAAH}}$, $\mathbf{K_{AAAF}}$: public key of AAAH and AAAF, respectively;
  - $\mathbf{K^{-1}_{AAAH}}$, $\mathbf{K^{-1}_{AAAF}}$: private key of AAAH and AAAF, respectively;
  - $\mathbf{<<M>>K^{-1}_{A}}$: digital signature of message M generated using private key of A;
  - $\mathbf{Cert_{AAAH}}$, $\mathbf{Cert_{AAAF}}$: certificate of AAAH and AAAF, respectively;
  - **AD** : a bit pattern indicating an advertisement;
  - **Key-Req, Key-Rep** : bit patterns of session-key request and reply, respectively;
  - $\mathbf{S_{MN\text{-}AAAH}}$: shared secret key between MN and AAAH;
  - $\mathbf{S_{MN\text{-}FA}}$, $\mathbf{S_{MN\text{-}HA}}$, $\mathbf{S_{HA\text{-}FA}}$: session-keys generated by AAAH, shared by MN & FA, MN & HA, and HA & FA, respectively;

4. Proposed Public-Key Based Registration and Session-Key Distribution

- **The protocol**

  - **R1)** AAAF->FA->MN : A, $<<A>>K^{-1}_{AAAF}$, $Cert_{AAAF}$
    where A = AD, FA_{id}, $AAAF_{info}$

  - **R2)** MN->FA : C, $<C>S_{MN\text{-}AAAH}$
    where C = Req, N_{MN}, N_{AAAH}, MN_{HM}, HA_{id}, FA_{id}, $AAAF_{info}$, Key-Req, B
    B = A, $<<A>>K^{-1}_{AAAF}$, $Cert_{AAAF}$

  - **R3)** FA->AAAF : D
    where D = C, $<C>S_{MN\text{-}AAAH}$

4. Proposed Public-Key Based Registration and Session-Key Distribution

- **R4)** AAAF->AAAH : D, N_{AAAF}

- (upon receipt of R4)
  AAAH : validate <C>$S_{MN\text{-}AAAH}$ using $S_{MN\text{-}AAAH}$,
  check whether FA_{id} in B = FA_{id} in C,
  validate $Cert_{AAAF}$ based on existing PKI at AAAH,
  validate <<A>>K^{-1}_{AAAF} using authenticated K_{AAAF}.

- **R5)** AAAH->HA : Req, MN_{HM}

- **R6)** HA->AAAH : Rep, Result

4. Proposed Public-Key Based Registration and Session-Key Distribution

- **R7)** AAAH->HA : $S_{MN\text{-}HA}$, $S_{HA\text{-}FA}$
  AAAH->AAAF : F,<<F>>K^{-1}_{AAAH}, $Cert_{AAAH}$
  where F = E ,<E>$S_{MN\text{-}AAAH}$,N_{AAAF}, $S_{MN\text{-}FA}$, $S_{HA\text{-}FA}$, K_{AAAF}
  E = Rep, Result, N_{MN}, N'_{AAAH}, HA_{id}, FA_{id}, $AAAF_{info}$, $S_{MN\text{-}HA}$, Key-Rep

- (upon receipt of R7)
  AAAF : validate N_{AAAF},
  validate $Cert_{AAAF}$ based on existing PKI at AAAF,
  validate <<F>>K^{-1}_{AAAH} using authenticated K_{AAAH}

- **R8)** AAAF->FA : E, <E>$S_{MN\text{-}AAAH}$, $S_{MN\text{-}FA}$, $S_{HA\text{-}FA}$

4. Proposed Public-Key Based Registration and Session-Key Distribution

- **R9)** FA->MN : E, $<E>S_{MN\text{-}AAAH}$

- (upon receipt of R9)
  MN : validate $<E>S_{MN\text{-}AAAH}$ using $S_{MN\text{-}AAAH}$

5. Conclusion

- In this paper, we proposed a new protocol about public-key based registration and session-key distribution
- This protocol guarantees safe registration and provides the secure communication with session-key.
- MN still relies on the use of secret key so, can't provide the non-repudiation service.