Secure Mobile Systems

Professor Bharat Bhargava

Yi Lu, Ahsan Habib and Mohamed Hefeeda

{bb, yilu, habib, mhefeeda}@cs.purdue.edu

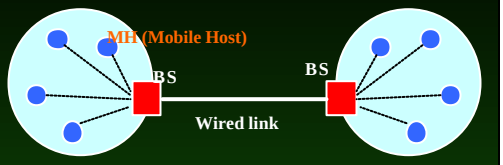
1

Wireless Networks

- Infrastructure-based architecture
  - – fixed base station => less flexible
  - – base station can be a single point of failure
  - + base station can enforce security policies for all in/out traffic
- Ad-Hoc architecture
  - + flexible
  - – less scalable
  - – no one enforces security policies

2

Infra-structure based networks



- Base Stations (BSs):
  - forward packets
  - authenticate roaming mobile hosts
- BSs can NOT move
- Why make them movable?
  - suitable for some environments, e.g. military
- Make the link wireless too
  - consequences ==>

3

Networks with movable Base Stations

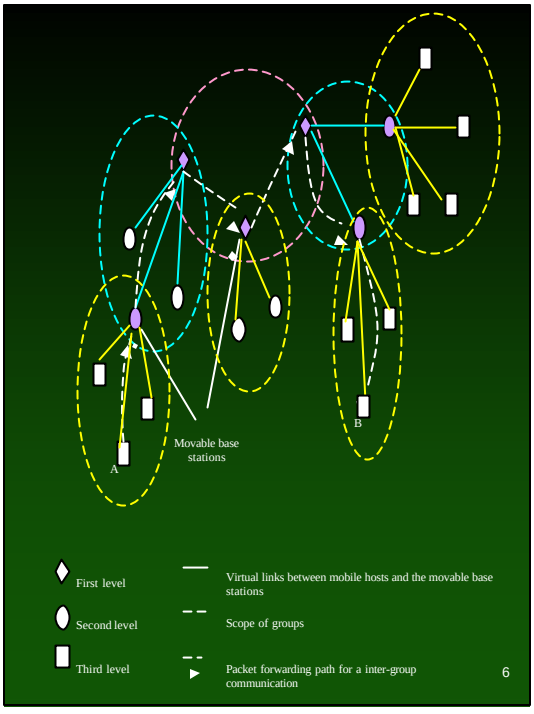
- Need new network architecture
- Need new routing protocols
- BS moves outside the communication range:
  - who forwards packets?
  - who authenticates roaming mobile hosts (MHs)?

4

Hierarchical architecture

- Mobile nodes are organized as groups (similar to subnets). Each group has
  - A movable base station
  - Mobile hosts
- Mobile hosts can directly communicate with other mobile hosts in the same group
- Inter-group communication via movable base stations

5



6

Security responsibilities of movable base stations

- Enforce security check for incoming/outgoing packets.
- Verify the identity of a mobile host in its group to foreign movable base stations.
- Grant the privilege of accessing group resources (eg, channel) to a visiting mobile host after verifying its identity.

7

Authentication

- Mobile Host moves to a foreign network
- Needs to authenticate/register itself to get the service
- Foreign Agent (base station) asks the Home Agent (base station) to verify Mobile Host
- If Home Agent is unavailable (down, moved from the net, …), then MH will be denied the service

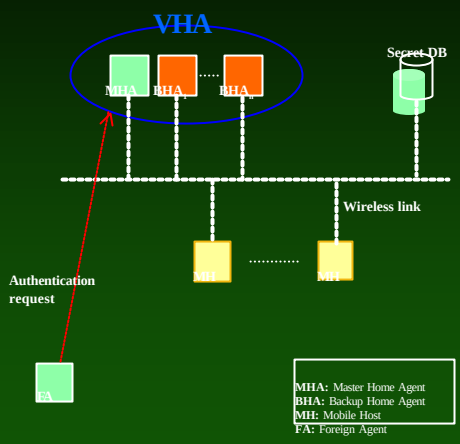
8

Fault-tolerant authentication

- Two proposed approaches to achieve fault tolerance:
  - Virtual Home Agent Scheme
  - Hierarchical Authentication Scheme

9

Virtual Home Agent (VHA)



10

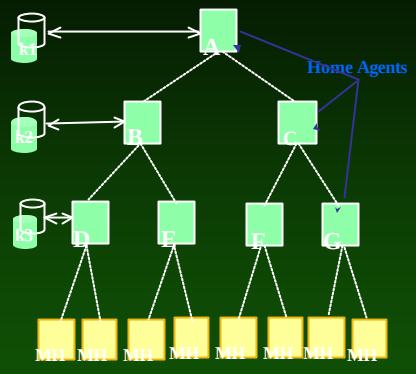
Virtual Home Agent (*contd.*)

- MHA *periodically* advertises "I'm alive" message
- If MHA fails (5 ads not received), an election takes place among the BHAs
- Simple scheme (no comm. over-head)
- The BHA whose timer expires first assumes the responsibilities of MHA

$$Timer_{BHA_i} = 5 * AD\_Interval + Priority_{BHA_i}$$

11

Hierarchical Authentication



(k1, A, Piro1)
(k2, B, Prio2)
(k3, D, Prio3)

12

Hierarchical Authentication (contd.)

- Each MH shares a key with every HA on the path from the leaf to the root
- Each key is assigned a priority (based on comm. delay, processing speed, lifetime, …)
- MH uses the key with the highest priority first
- If the associated HA fails (or the key priority changes), MH uses the second key and so on.

13

Experimental Evaluation

- Conducting experiments using *ns2* to:
  - compare speed of authentication
  - assess reliability of the schemes
  - devise suitable values for the parameters:
    - VHA: priority, ad interval, …
    - Hierarchical: priority, #of levels, tree structure, ….
    - Re-keying, size of the keys, ...

14