SECURITY IN MOBILE NETWORKS

Bharat Bhargava

CERIAS and Computer Sciences Departments
Purdue University, W. Lafayette, IN 47907
bb@cs.purdue.edu

Supported by CERIAS & NSF grants CCR-0001788 and CCR-9901712.

Mobile Computing Environment

- Vulnerable to failures, intrusion, and eavesdropping.
- Adhoc mobile systems has everything moving (hosts, base-stations, routers/agents, subnets, intranet).
- Need survivability from intentional and unintentional attacks.

Research Ideas

- Integrate ideas from Science and Engineering of security and fault-tolerance.

Examples:

- Need to provide access to information during failures
  $\leftrightarrow$ need to disallow access for unauthorized users.
  - Duplicate routers & functions, duplicate authentication functions, duplicate secrete session key database, secure database that provides public keys.
  - Auditing, logging, check-pointing, monitoring, intrusion detection, denial of service.
- **Adaptability**:
  - Adapt to timing, duration, severity, type of attack.
- **Election Protocols** – selection of back-up base station.

3

Deficiency in Mobile IP Authentication

- Authentication is through a home agent (HA).
  - If HA is out of service, mobile host will be homeless and not be able to communicate.

4

Deficiency in Mobile IP Key Management

- Data packets are encrypted before sending, and decrypted after receiving.
- Requires exchange of secret keys and public keys between sender and receiver.
- Mobile IP does not provide multi-cast session key management. Manual distribution implies N(N–1)/2 pairs of keys. Does not scale well.

5

Research Questions

- **Difficulty in initial authentication**.
  - How quickly a public key can be established without any prior knowledge between communicating parties?
- **Maintaining authentication**.
  - The session key and its life-time have to be made available to all other base stations in case MH moves across cells. Further complicates the problem of key distribution. Note session key information is not completely replicated in the database of base stations.
- **Hierarchical authentication of mobile base stations**.
  - Mobile base stations must authenticate one another. Need another centralized certificate authority. Both MH and base stations must trust the same security hierarchy.

6

- **Key agility**
  - Difficult to come up with a measure for how long the key can be retained.
- **Adaptive intrusion defection systems**
  - Detect possible break-ins of base station and fire wall reconfigurations.

7

Fault Tolerant Authentication in Mobile Computing

Bharat Bhargava
Sarat Babu Kamisetty
Sanjay Kumar Madria

CERIAS and Computer Sciences Department
Purdue University, W. Lafayette, IN 47907
bb@cs.purdue.edu

8

Objective

- To provide uninterrupted secure service to the mobile hosts when base station moves or fails.

9

Research Focus

- Fault-tolerant Authentication
- Group Key Management
- Adaptable, Re-configurable Software
- Experiments

10

Mobile IP Entities

- **Mobile Host (MH)** – which can change its point of attachment to the internet from one link to another.
- **Home Agent (HA)** – router on MH's home network which tunnels datagrams (packets of data) to MH when it is away from home.
- **Foreign Agent (FA)** – router on MH's visited network which provides routing services to the MH while registered.

11

Hardware Characteristics

- **Media** – Wireless media are inherently less secure.
- **Low power and limited computing resource** – motivation for making security an optional feature.
- **Bandwidth** – typically orders of magnitude less than wired bandwidth (motivation for reducing the overhead of the security scheme).

12

System Characteristics

- **Autonomy** – WAN, base stations and mobile hosts are governed by different entities.
- **Network Partitions** – Authentication requires communication with the home agent, which could be across the globe.
- **Clock Synchronization** – mobile hosts may travel across multiple time zones.

13

Application Characteristics

- **Location Privacy** – protecting the identity of the communicating entities (ex: Military Networks)
- **Mobility** – implies frequent upon handoffs
- **Secure Multicast** – one transmitter and many listeners (ex: Classrooms)

14

Fundamental Security Services

- **Authentication**
  - Provides assurance of a host's identity.
  - Provides a means to counter masquerade and replay attacks.
  - Can be applied to several aspects of multicast (ex: registration process).

15

Fundamental Security Services

- **Integrity**
  - Provides assurance that traffic is not altered during the transmission.
  - Lack of integrity services in IP can lead to spoofing attacks.
  - More crucial for applications involving key management than voice applications (easily detected).

16

Fundamental Security Services

- **Confidentiality**
  - Provides assurance that only authorized entities can decode and read the data.
  - Typically, encryption is used to achieve this.
  - Encryption can be applied at several layers of the protocol stack (ex: inherent in RTP, ESP for IP datagrams).

17

Fundamental Security Services

- **Other Services**
- **Non-repudiation –** recipient can prove that sender did sent the message in case sender denies it.
- **Access Control –** ensures that only authorized parties can access the resources.

18

Problem Description

- To ensure security and theft of resources (like bandwidth), all the packets originating inside the network should be authenticated.
- Typically, a Mobile Host sends a packet to its Home Agent along with the authentication information.

19

Problem Description (continued)

- If the Authentication is successful, Home Agent forwards the packet. Otherwise, packet is dropped.

20

Disadvantages of Typical Setup

- Home Agent becomes a single point of failure.
- Home agent becomes an attractive spot for attackers.
- Not scalable – large number of hosts overload the Home agent.

21

Research Goals

- Eliminate the single point of failure.
- Distribute the load and enhance scalability and survivability of the system.
- Failures – transparent to applications.
- Easy to implement, no manual setup.

22

Traditional Approaches

- Using a Proxy Server (or Backup) that takes up the responsibilities of the Base Station

Disadvantages

- Manual updating of the routing tables of the hosts necessary.
- Time consuming and hence smooth provision of service is not possible.

23

Traditional Approaches (continued)

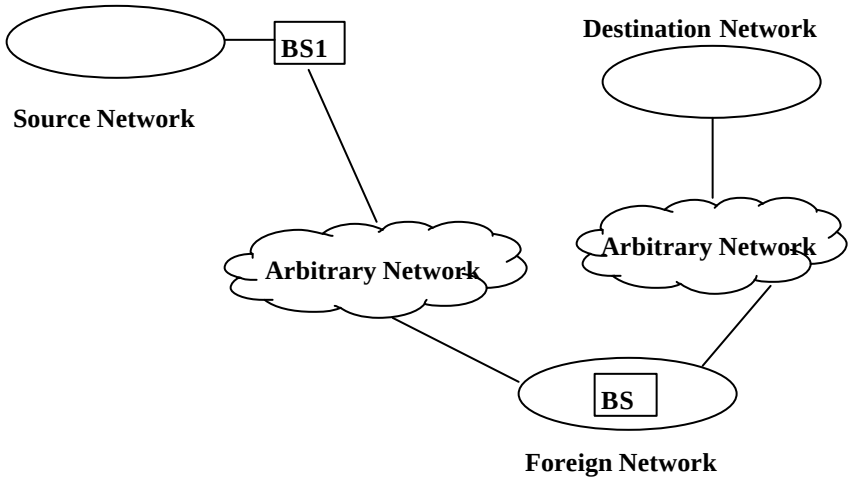
- Using a Second Base Station that forwards the packets to the actual Home Agent, using Mobile IP, which is now at a Foreign Network.

Disadvantages

- Communication Delays introduced makes this solution impractical.
- Introduces additional security threats as the packets now traverse long paths through Internet.

24

Proxy-Based Solution



25

Disadvantages

- Introduces additional security threats.
- Additional communication delays.
- Not transparent to applications.
- Manual set up – error prone.

26

Proposed Schemes

- We propose two schemes to solve the problem.
  - Virtual Home Agent
  - Hierarchical Authentication
- They differ in the architecture and the responsibilities that the Mobile Hosts and Base Stations (Agents) hold.

27

Authentication Using Virtual Home Agent

Entities in the proposed scheme

- Virtual Home Agent (VHA) is an abstract entity identified by a network address.
- Master Home Agent (MHA) is the physical entity that carries out the responsibilities of the VHA.

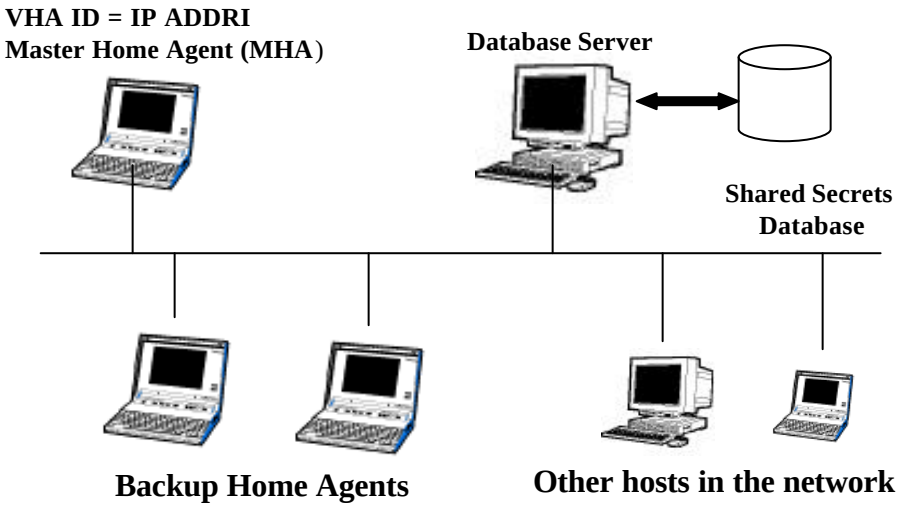
28

Authentication Using Virtual Home Agent

- Backup Home Agent (BHA) is the entity that backs up a VHA. When MHA fails, BHA having the highest priority becomes MHA.
- Shared Secrets Database Server is the entity that manages and processes the queries on the secret database.

29

Virtual Home Agent Scheme



30

Protocol Description

- All the MHAs and BHAs join a pre-configured multicast group.
- MHA and each BHA is assigned a priority that indicates its preference to become a MHA, when the current MHA fails.
- MHA has the highest priority at any given point of time

31

Protocol Description

- Periodically, MHA sends an advertisement packet to the configured multicast group.
- Purpose of this advertisement packet is to let the BHAs know that MHA is still alive.
- Time-to-live is set to 1 in each advertisement as they never have to be transmitted outside the network.

32

Protocol Description

- Advertisement Packet Format

VHA's ID	MHA's priority	Authentication Information

- VHA's ID indicates the VHA that this Agent is the Master for.
- MHA's priority is the priority of this MHA.
- Authentication Information is necessary to void the masquerading attacks (I.e., anybody posing as a Master after comprising it).

33

Protocol Description

- BHAs only listen for advertisements, they do not send the advertisements.
- If a BHA did not receive any advertisements for some period, it starts the Down Interval Timer, computed as follows:

Down Time Interval = 5*Advertisement Interval +

((*MHA's priority-BHA's priority)/MHA's priority*)

34

Protocol Description

- Down Interval Time takes care of packet losses (as it is at least 5 advertisement intervals).
- Down Interval Time is a function of BHA's configured priority (if the priority is more, Down Interval Time is less).

35

Protocol Description

- It is guaranteed that the Down Interval Timer of the BHA having the highest priority will expire first and that BHA transitions from BHA to MHA.
- This new MHA sends advertisements from now onwards.

36

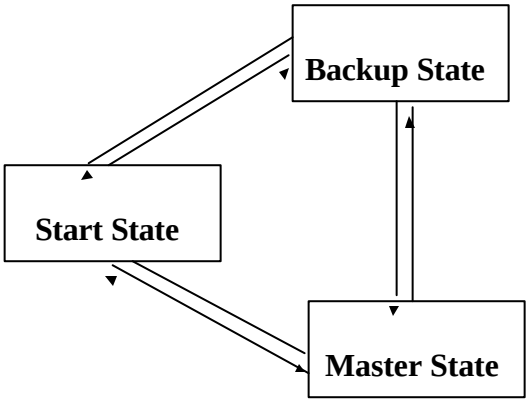
Protocol Description

Advantages of this Election Protocol

- No communication between the BHAs is required.
- There is no confusion about which BHA becomes MHA (only the one whose timer expires first).
- No additional security threats (like manipulating priorities of BHAs).

37

Protocol Description



State Transitions

38

Advantages of the Proposed Scheme

- Has only 3 states and hence the overhead of state maintenance is negligible.
- Very few tasks need to be performed in each state (outlined in the tech report).
- Flexible – there could be multiple VHAs in the same LAN and a MHA could be a BHA for another VHA, a BHA could be a BHA for more than one VHA at the same time.

39

Disadvantages of Virtual HA Solution

- Not scalable if every packet has to be authenticated
  - Ex: huge audio or video data
- BHA (Backup Home Agents) are idle most of the time (they just listen to MHA's advertisements.
- Central Database is still a single point of failure.

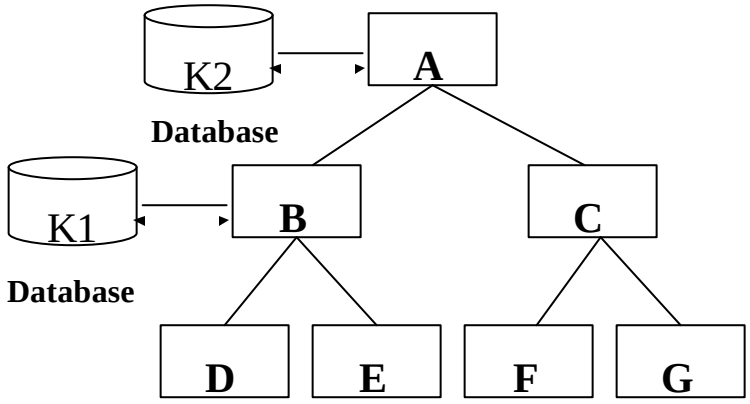
40

Hierarchical Authentication Scheme

- Multiple Home Agents in a LAN are organized in a hierarchy (like a tree data structure).
- A Mobile Host shares a key with each of the Agents above it in the tree (Multiple Keys).
- At any time, highest priority key is used for sending packets or obtaining any other kind of service.

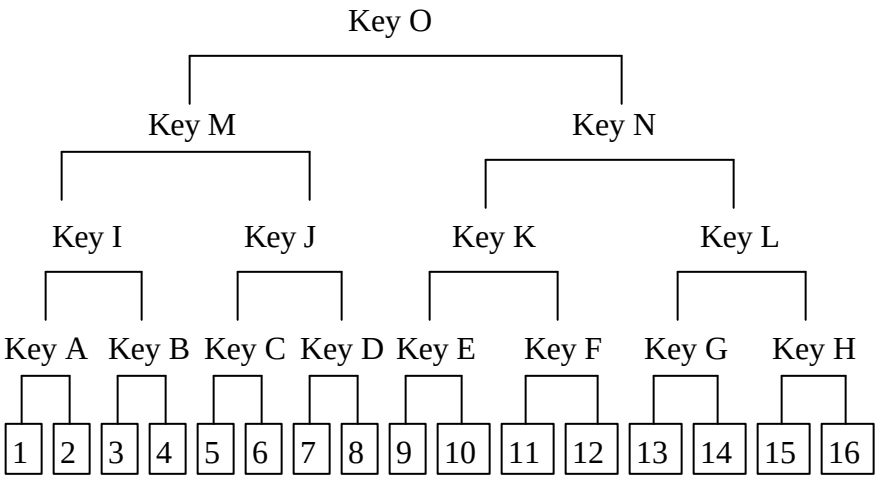
41

Hierarchical Authentication Scheme



42

Tree-Based Scheme



43

Hierarchical Authentication Scheme

Key Priority depends on several factors and computed as cumulative sum of weighted priorities of each factors:

Example Factors:

- Communication Delays
- Processing Speed of the Agents
- Key Usage
- Life Time of the Key

44

Hierarchical Authentication Scheme

- Hosts detect the Home Agent's failure or mobility when the Home Agent does not send an acknowledgement for a request.
- When the failure is detected, host reduces the priority of the current key and picks up the highest priority key to be used from now onwards.

45

VHA Scheme	**Hierarchical Scheme**
• Flat structure • Host has only one key • Failure is transparent to the user	• Tree structure • Number of keys depend on height of the tree. • Hosts should be aware of the failure of BS as which key to be used depends on the base station serving it.
• No Priority is assigned to the keys	• Each key has priority, the key with the highest priority is used for authentication.

46

Clusters to Achieve Scalable Fault Tolerant Authentication

- Front-End is the MHA.
- Back-Ends are BHAs.
- Each packet is digitally signed by the Mobile Host.
- Packets are forwarded to the MHA.
- Back-Ends verify the signatures.

47

Scalability Using Clusters

- **Cluster**
  - A group of servers.
  - Act as a single node (i.e., identified by a single IP address).
  - Gives the effect of parallel processor with a large main memory and secondary storage.
  - Largely scalable and efficient.
  - Deployed in service provider networks.

48

Cluster Architecture

- Client contacts the Front-End for a service.
- Front-End forwards the requests to a Back-End.
- Back-Ends serve/process the request.

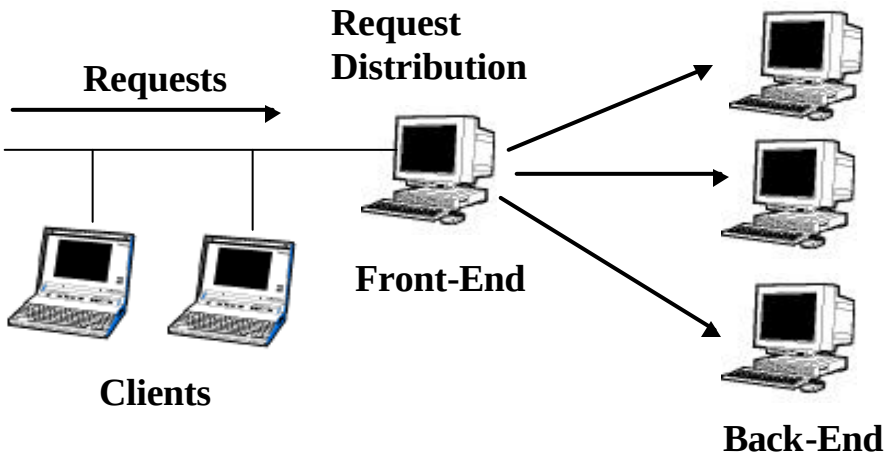
49

Front-End's Responsibilities

- Acts as a Request dispatcher or redirector.
- Does load balancing based on various factors.
- Keeps track of which Back-Ends are active.

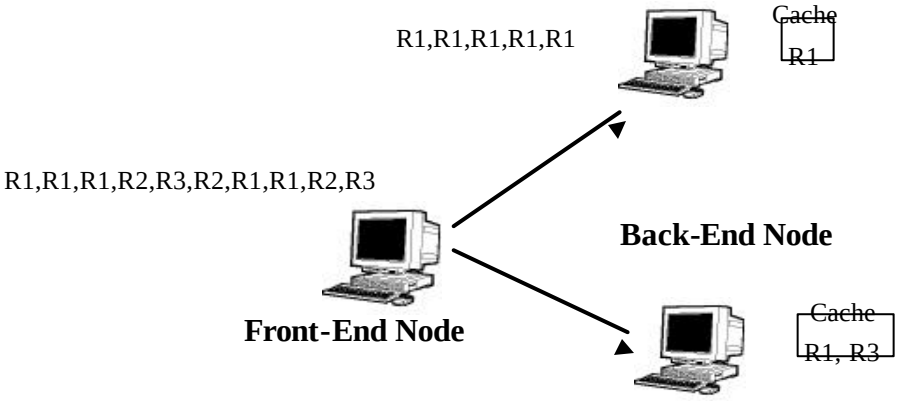
50

Cluster for Scalability



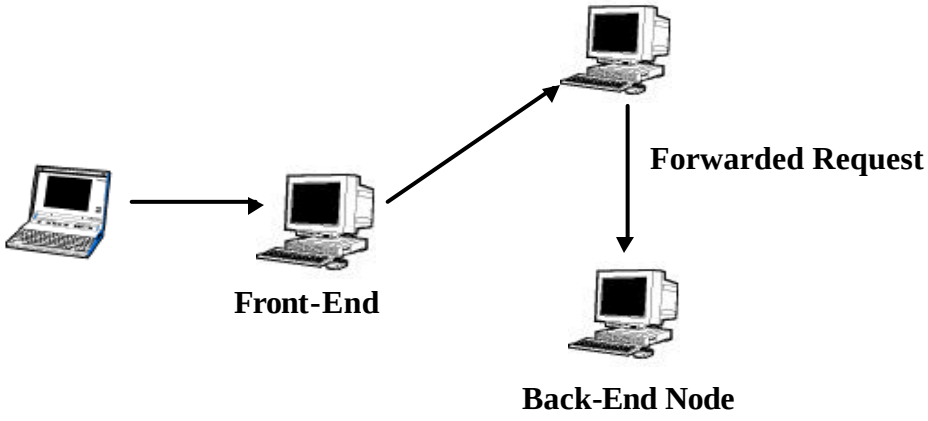
51

Locality-Aware Request Distribution



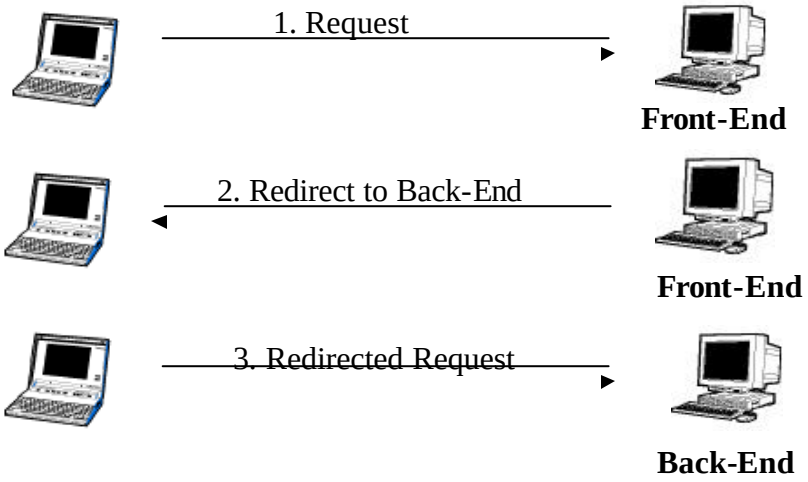
52

Back-End Forwarding



53

Request Redirection



54

Disadvantages of Redirection

- Introduces additional delays.
- Identities (i.e., addresses) of the Back-ends are exposed and thus poses a security risk.
- Poses an additional burden on clients or they might not handle redirects.

55

Request Distribution

- **Content Based Distribution**
  - Front-End takes into account the service requested to decide which Back-End is good (Ex: audio, video, text, etc.).
  - Increased performance.
  - Gives the flexibility of having different types of Back-End servers for different contents (Ex: audio, servers, video servers).

56

Request Distribution

- **Load Based Distribution**
  - Front-End does load balancing.
  - Front-End distributes the requests based on the current load of the Back-Ends.
  - Back-Ends report about their load periodically.
  - ***Front-End prefers minimally loaded Back-End.***
  - Useful when all the Back-Ends server similar requests (like only audio, only text).

57

Request Distribution

- **Locality Aware Distribution**
  - Front-End keeps a mapping of the Back-Ends and their cache contents.
  - When a request arrives, it maps the request to the cache contents.
  - Request if forwarded to that Back-End whose cache contents match the request.
- Useful for retrieving HTTP documents.

58

Conclusions and Future Work

- Flat-model and tree based schemes for fault-tolerant authentication in mobile environment.
- Cluster based enhancement.

59

Future Work

- Quantifying the priorities for each factor and computing the overall key priority as a weighted function of all these factors.
- Designing a adaptable database replication and partitioning scheme for secret key database that increases the system performance.
- Simulation of these approaches and obtaining performance statistics.

60

Experimental Evaluation

- Conducting experiments using *ns2* to:
  - study the performance of the proposed schemes
  - assess their reliability
  - devise suitable values for the parameters:
    - **VHA:** priority, ad interval, …
    - **Hierarchical:** priority, #of levels, tree structure, ….
    - **Both:** key distribution, key size, re-keying, replicating secret DB, ...

61

Experiments setup

- Different mobile environments by varying:
  - number of mobile hosts, number of home agents
  - number of groups/sub networks
  - mobility models
  - frequency of authentication requests
  - failure probability and movement behavior of home agents (base stations)
  - authentication scheme with different parameters
- Evaluate:
  - comm. overhead of each scheme
  - response time in case of failure
  - best parameters' values of each scheme

62