



Chapter 13

Location Privacy

- ❑ Security aspects of mobile communication
- ❑ Implicit addressing
- ❑ Pseudonyms
- ❑ Communication mixes

Security Aspects of Mobile Communication



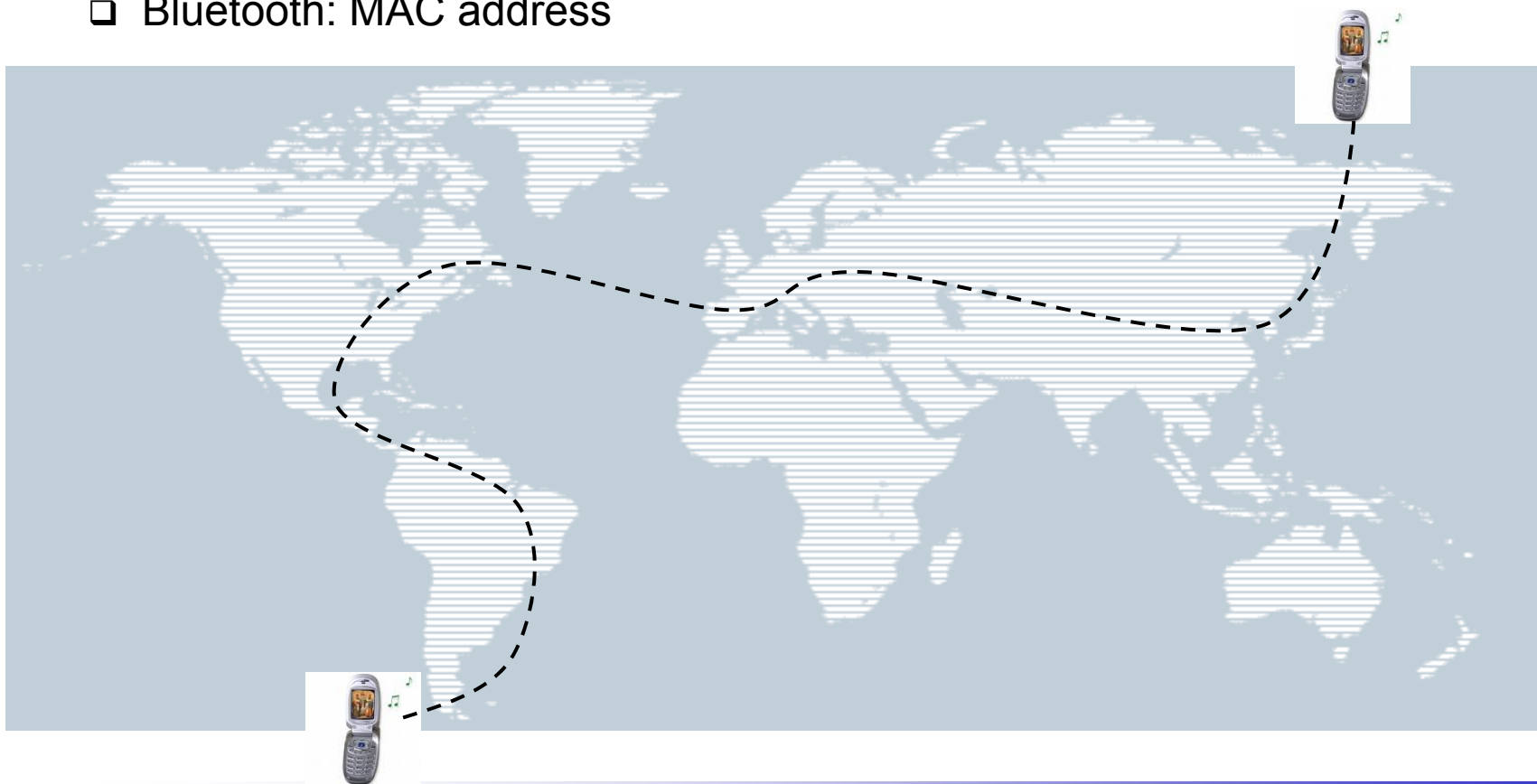
- ❑ Mobile communication faces all threats that does its fixed counterpart:
 - ❑ Masquerade, eavesdropping, authorization violation, loss / modification / forgery of transmitted information, repudiation of communication acts
 - ❑ Thus, similar measures like in fixed networks have to be taken
- ❑ However, there are specific issues arising out of mobility of users and/or devices:
 - ❑ Some already existing threats get more dangerous:
 - Wireless communications is more accessible for eavesdropping
 - The lack of a physical connection makes it easier to access services
 - ❑ Some new difficulties for realizing security services:
 - Authentication has to be re-established when the mobile device moves
 - Key management gets harder as peer identities can not be pre-determined
 - ❑ One completely new threat:
 - The location of a device / user becomes a more important information that is worthwhile to eavesdrop on and thus to protect

Location Privacy in Mobile Networks



❑ Identifier

- ❑ GSM/UMTS: IMEI
- ❑ WLAN: MAC Address
- ❑ Bluetooth: MAC address



Location Privacy in Mobile Networks



- ❑ There is no appropriate location privacy in today's mobile networks:
 - ❑ GSM / UMTS:
 - Active attackers can collect IMSIs on the air interface
 - Visited network's operators can partially track the location of users
 - Home network operators can fully track the location of users
 - However, at least communicating end systems can not learn about the location of a mobile device
 - ❑ Wireless LAN / IPv6:
 - No location privacy, as the (world-wide unique) MAC address is always included in the clear in every MAC frame
 - ❑ Mobile IP:
 - Standard Mobile IP: HA can fully / FA can partially track MNs
 - Mobile IP with AAA: no location privacy on air interface, foreign AAA infrastructure can partially / home AAA server can fully track MNs
 - Mobile IP with route optimization: even CNs can track an MN from everywhere around the world if the MN wishes to use the optimization

Location Privacy in Mobile Networks



- ❑ The basic location privacy design problem:
 - ❑ A mobile device should be reachable
 - ❑ No (single) entity in the network should be able to track the location of a mobile device
- ❑ Some fundamental approaches to this problem [Müller99a]:
 - ❑ *Broadcast of messages:*
 - Every message is sent to every possible receiver
 - If confidentiality is needed, the message is encrypted asymmetrically
 - This approach does not scale well for large networks / high load
 - ❑ *Temporary pseudonyms:*
 - Mobile devices use pseudonyms which are changed regularly
 - However, to be able to reach the mobile device this needs a mapping entity which can track the mobile's history of pseudonyms
 - ❑ *Mix networks:*
 - Messages are routed via various entities (mixes) and every entity can only learn a part of the message route

Addressing schemes



- ❑ Addressing schemes for location privacy with broadcast:
 - ❑ *Explicit addresses:*

Every entity that “sees” an explicit address is able to determine the addressed entity
 - ❑ *Implicit addresses:*

An implicit address does not identify a specific device or location, it just names an entity without any further meaning attached to the name

 - *Visible implicit addresses:*
 - Entities that see multiple occurrences of an address can check for equality
 - *Invisible implicit addresses:*
 - Only the addressed entity can check for equality of the address
 - This requires public key operations: $ImplAddr_A = \{r_B, r_A\}_{+K_A}$ where r_A is chosen by the addressed entity and r_B is a random value created by an entity B which wants to invisibly make reference to entity A



□ *Temporary Pseudonyms:*

- The location of a device A is no longer stored with its identification ID_A but with a changing pseudonym $P_A(t)$
 - Example: VLRs in GSM might just know and store the TMSI (which is kind of a temporary pseudonym)
- The mapping of an ID_A to the current pseudonym $P_A(t)$ is stored in a trustworthy device
 - Example: GSM HLRs might be realized as trustworthy devices
- When an incoming call has to be routed to the current location of device A :
 - The network provider of device A asks the trustworthy device for the current pseudonym $P_A(t)$
 - The network then routes the call to the current location of A by looking up the temporary pseudonym in a location database
 - It is important, that the entities that route a call can not learn about the original address of the call setup message (\rightarrow implicit addresses)
 - The use of mixes (see below) can provide additional protection against attacks from colluding network entities

Communication mixes



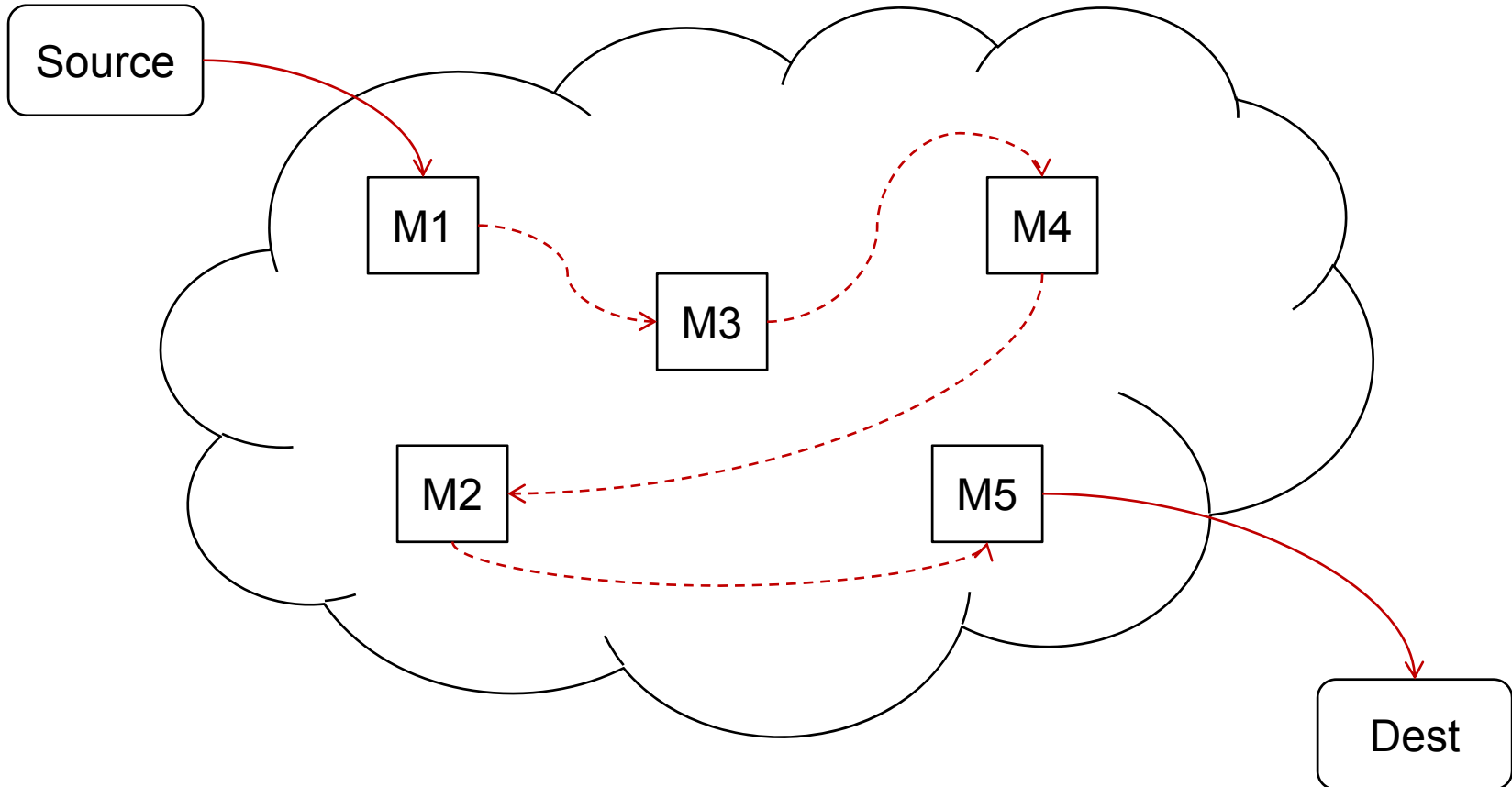
❑ *Communication mixes:*

- ❑ The concept was invented in 1981 by D. Chaum for untraceable email communication
- ❑ A *mix* hides the communication relations between senders and receivers:
 - It buffers incoming messages which are asymmetrically encrypted so that only the mix can decrypt them
 - It changes the “appearance” of messages by decrypting them
 - It changes the order of messages and relays them in batches
 - However, if the mix is compromised an attacker can learn “everything”
- ❑ Security can be increased by cascading mixes
- ❑ Example: A sends a message m to B via two mixes M1 and M2
 - $A \rightarrow M1: \{r_1, \{r_2, \{r_3, m\}_{+K_B}\}_{+K_{M2}}\}_{+K_{M1}}$
 - $M1 \rightarrow M2: \{r_2, \{r_3, m\}_{+K_B}\}_{+K_{M2}}$
 - $M2 \rightarrow B: \{r_3, m\}_{+K_B}$
 - It is important, that the mixes process “enough” messages

Communication mixes



$M1, \{M3, \{M4, \{M2, \{M5, \{Dest, \{Message\}_{+K_D}\}_{+K_{M_5}\}_{+K_{M_2}\}_{+K_{M_4}\}_{+K_{M_3}\}_{+K_{M_1}}$



Summary (what do I need to know)



- ❑ Security aspects of mobile communication
 - ❑ Same as for all other communication networks
 - ❑ PLUS location privacy issues

- ❑ Addressing schemes
 - ❑ Implicit addressing
 - ❑ Temporary pseudonyms

- ❑ Communication mixes
 - ❑ Chaum's mix

Additional References



- [Chaum81] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communications of the ACM*, vol. 24, pp. 84-88, 1981.
- [Chaum88] D. Chaum, "The Dining Philosophers Problem: Unconditional Sender and Receiver Untraceability," *Journal of Cryptology*, vol. 1 (1), pp. 65-75, 1988.
- [Müller99a] G. Müller, K. Rannenberg (Ed.). *Multilateral Security in Communications*. Addison-Wesley-Longman, 1999.