ERICSSON

Challenges to Security in the Mobile Internet

Jari Arkko

Ericsson Research NomadicLab

ERICSSON

Outline

- The beginning
- Current challenges
- Future challenges
- Case studies
  - Case SRTP - Importance of efficiency
  - Case Mobile IPv6 - Importance of scalability
  - Case HIP - Insignificance of IP addresses
- Conclusions

ERICSSON

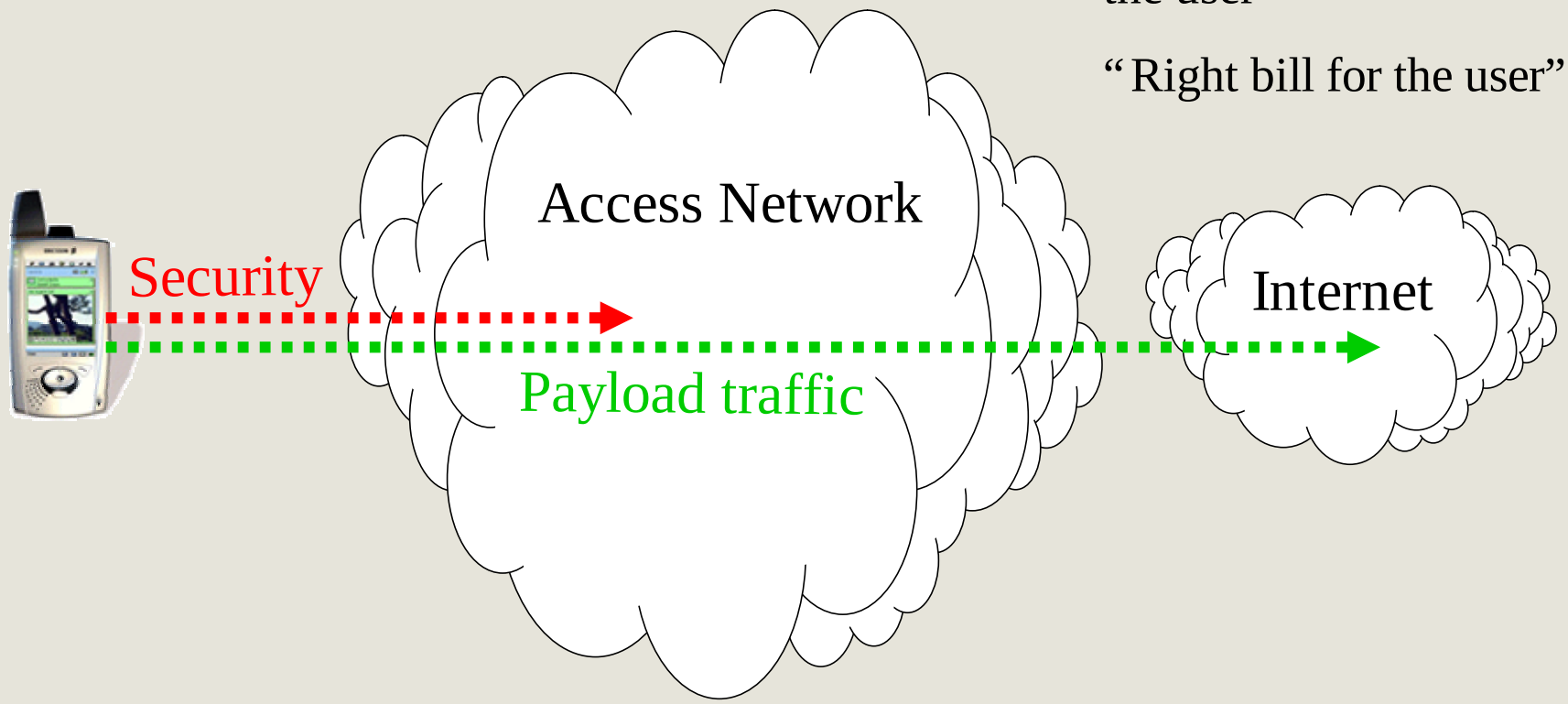
The Beginning

The First Attempts, Security Architecture

Provide access, and only it

Protect the operator from the user

"Right bill for the user"



2G, 2.5G, first WLANs

ERICSSON

Problems in this Architecture

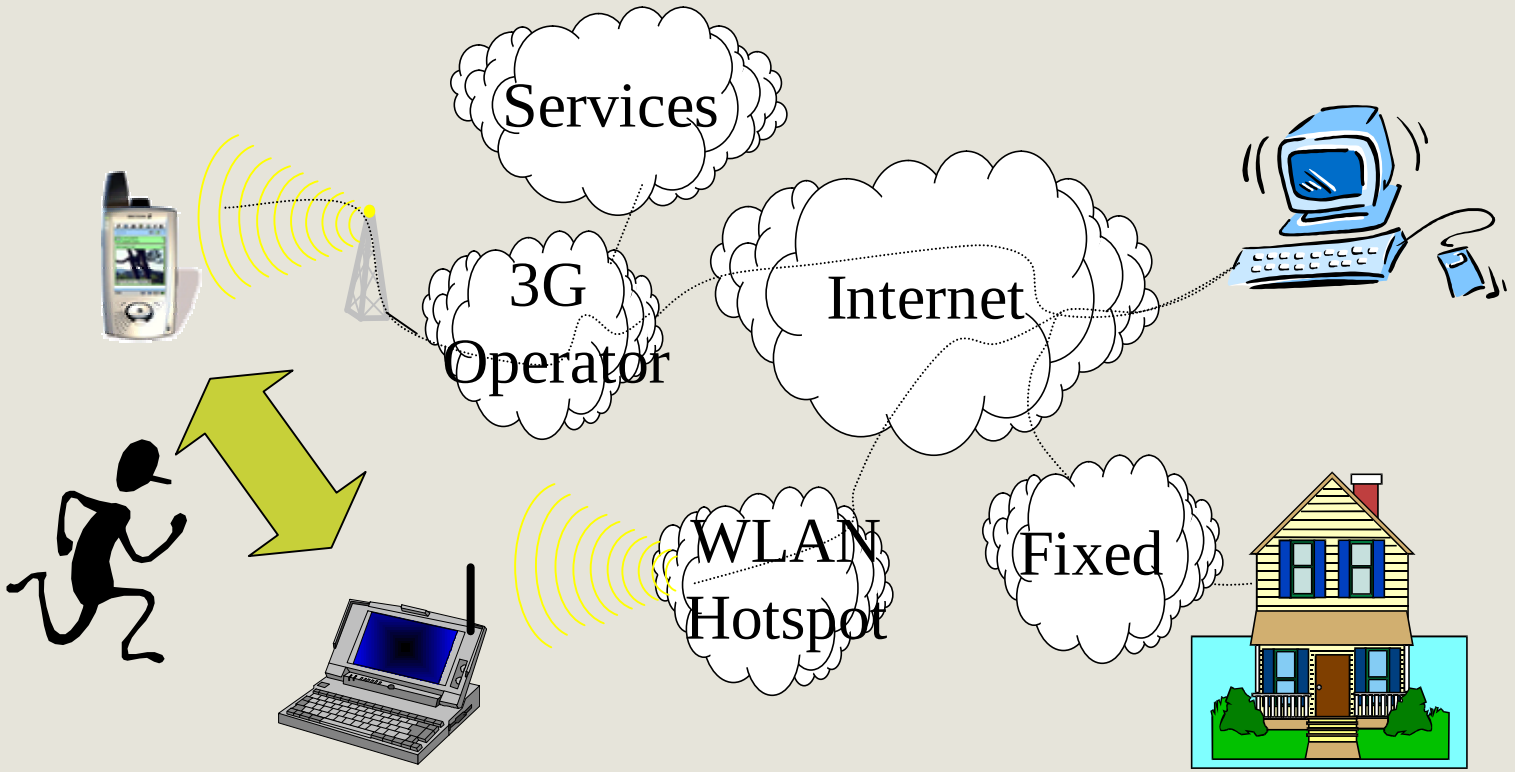
- Movements were impractical
  - Mobility only within one access network
  - Multiple access networks, multiple passwords
  - Tailored for a single device
- The provided security was not for services
  - Business implications
  - Practical implications for users
- Bad performance
  - Many of the Internet protocols not tailored for wireless
  - High RTT, small bandwidth, lossy & error-prone

ERICSSON

Current Challenges

ERICSSON

Current Architecture



Mobility, multi-access, services, improved security mechanisms

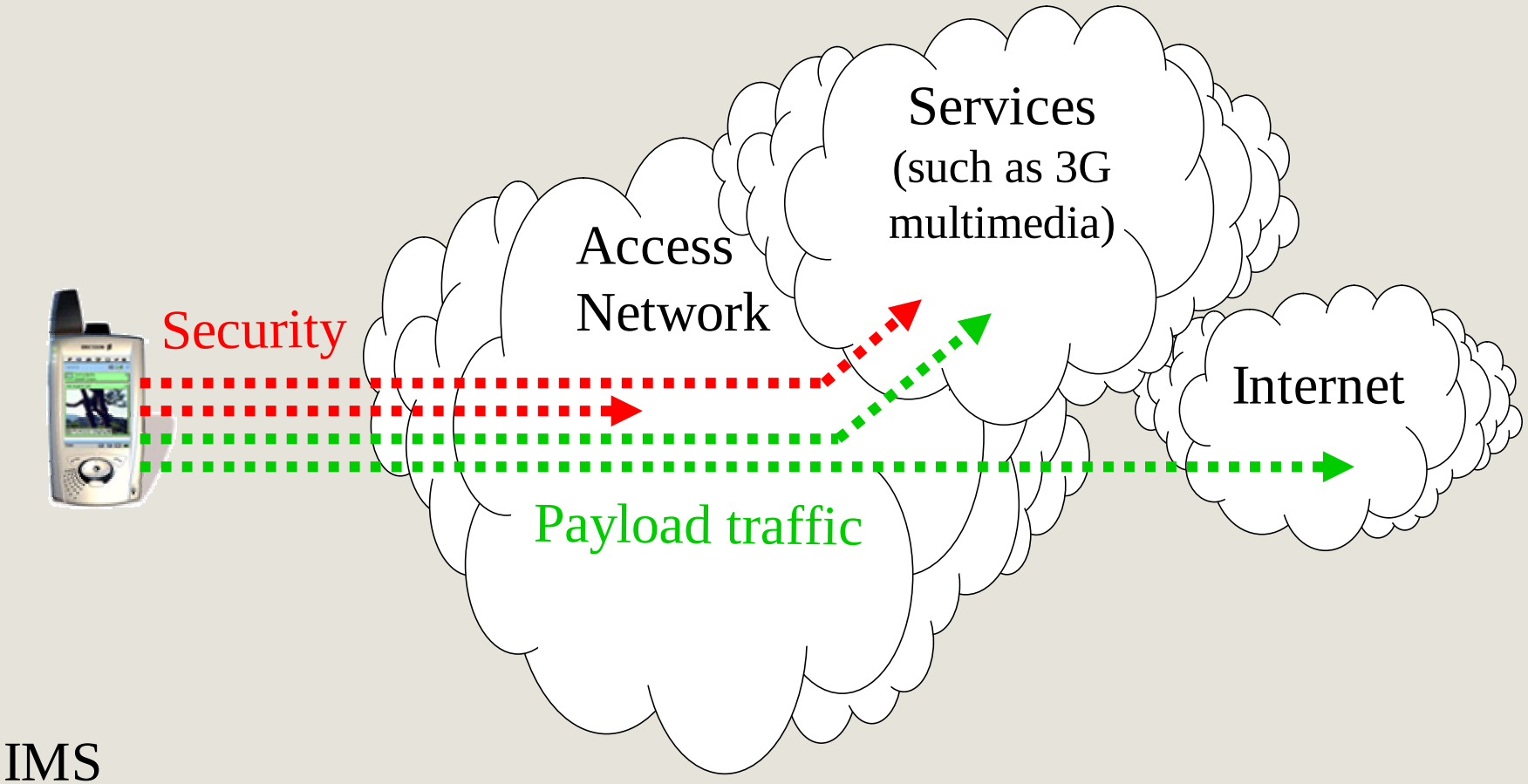
ERICSSON

What's New

- Include (some) services
- Basic mobility
- First solutions for multi-access
- Enhanced security mechanisms

ERICSSON

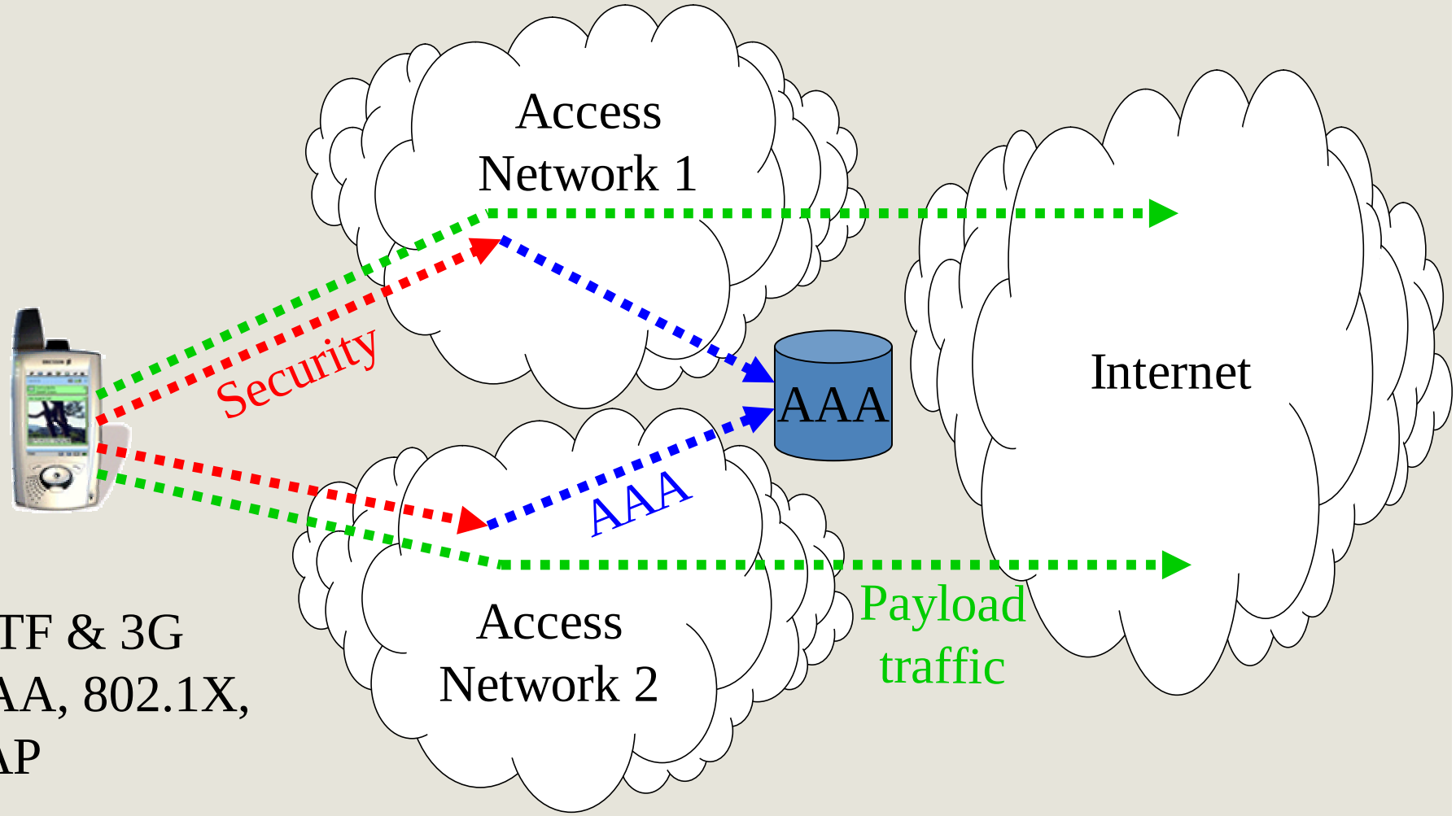
Security and Services



IMS

ERICSSON

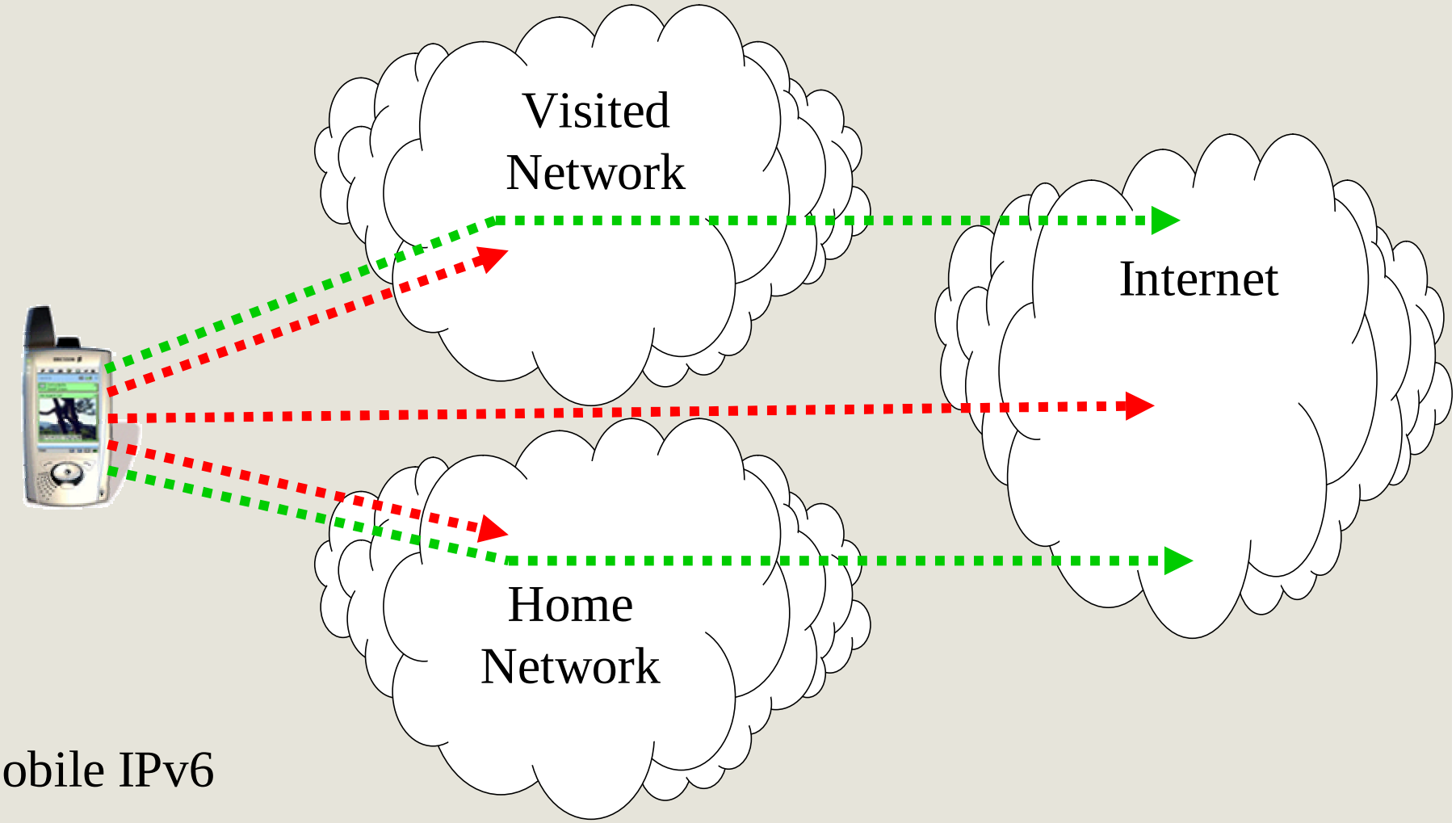
Security and Multi-Access



IETF & 3G
AAA, 802.1X,
EAP

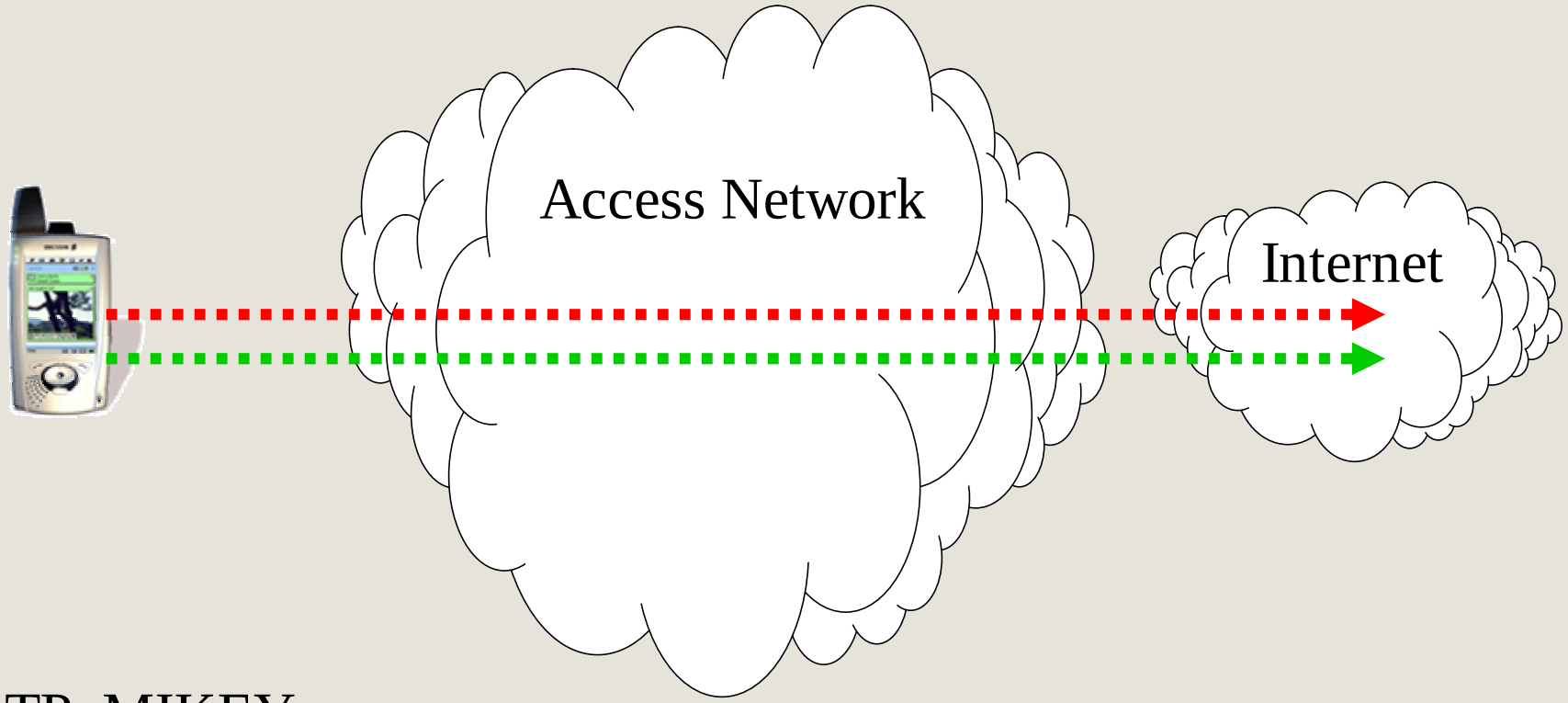
ERICSSON

Security and Mobility



Mobile IPv6

Improved Internet Security Solutions



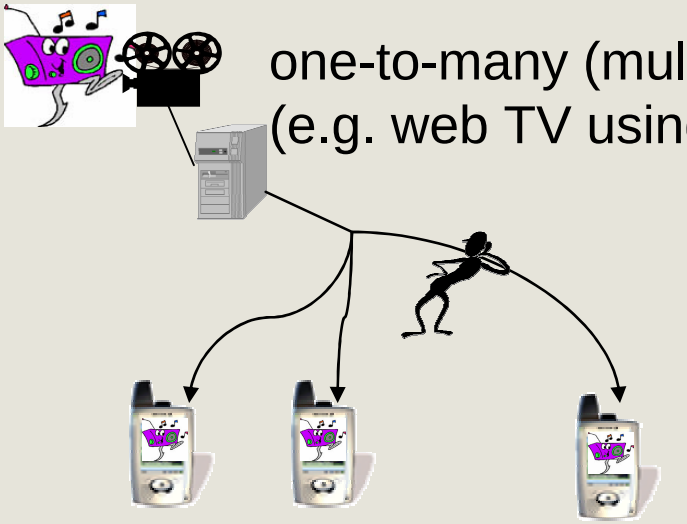
SRTP, MIKEY

ERICSSON

Case Study 1:
Importance of Efficiency
Importance of Wireless Considerations

Application: Multimedia Stream Protection

peer-to-peer communication (e.g. SIP call)



one-to-many (multicast)
(e.g. web TV using RTSP)

Requirements to Consider

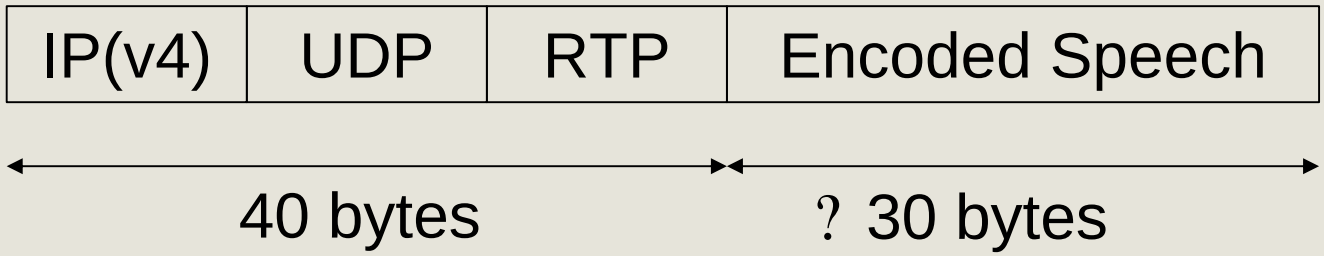
Wireless links can have

- Low bandwidth, high RTT
- Bit-errors
- Unequal Error Protection (UEP)

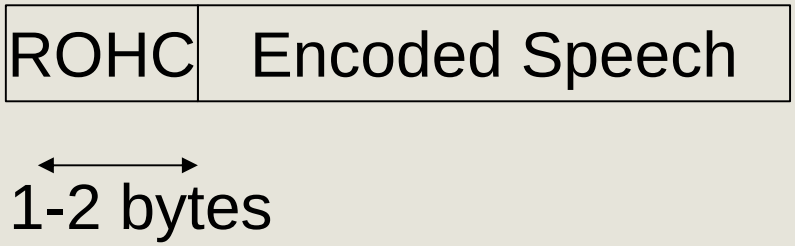
Most CODECS built to tolerate a few bit errors, but packet loss degrades speech quality

- Security processing should not increase size, bit-error rates, or packet loss rates
- Minimize # roundtrips for key-exchange

Typical VoIP Application



Header Compression (RFC 3095) needed for economy:



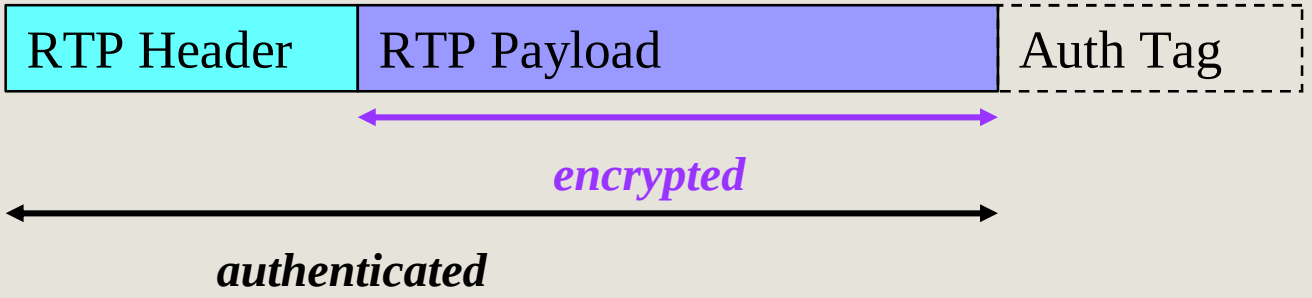
? Security processing must allow header compression

ERICSSON

Solution: SRTP

Secure RTP protocol (SRTP)

- AES -based stream cipher encryption
- Benefits:
  - Bit-error friendly
  - No expansion & allows header compression
  - Minimal key management roundtrips with MIKEY
- Bandwidth usage halved, no delays, good voice quality!



Secure Conversational Multimedia Example

v=0
o=bob 2891092897 2891092897 IN IP4 found
s=Cool stuff
e=bob@null.org
t=0 0
c=IN IP4 found.somewhere.com
a=key-mgmt:MIKEY skaoqDeMkdwRW278
m=audio 49030 RTP/SAVP 98
a=rtpmap:98 AMR/8000
m=video 52230 RTP/SAVP 31
a=rtpmap:31 H261/90000

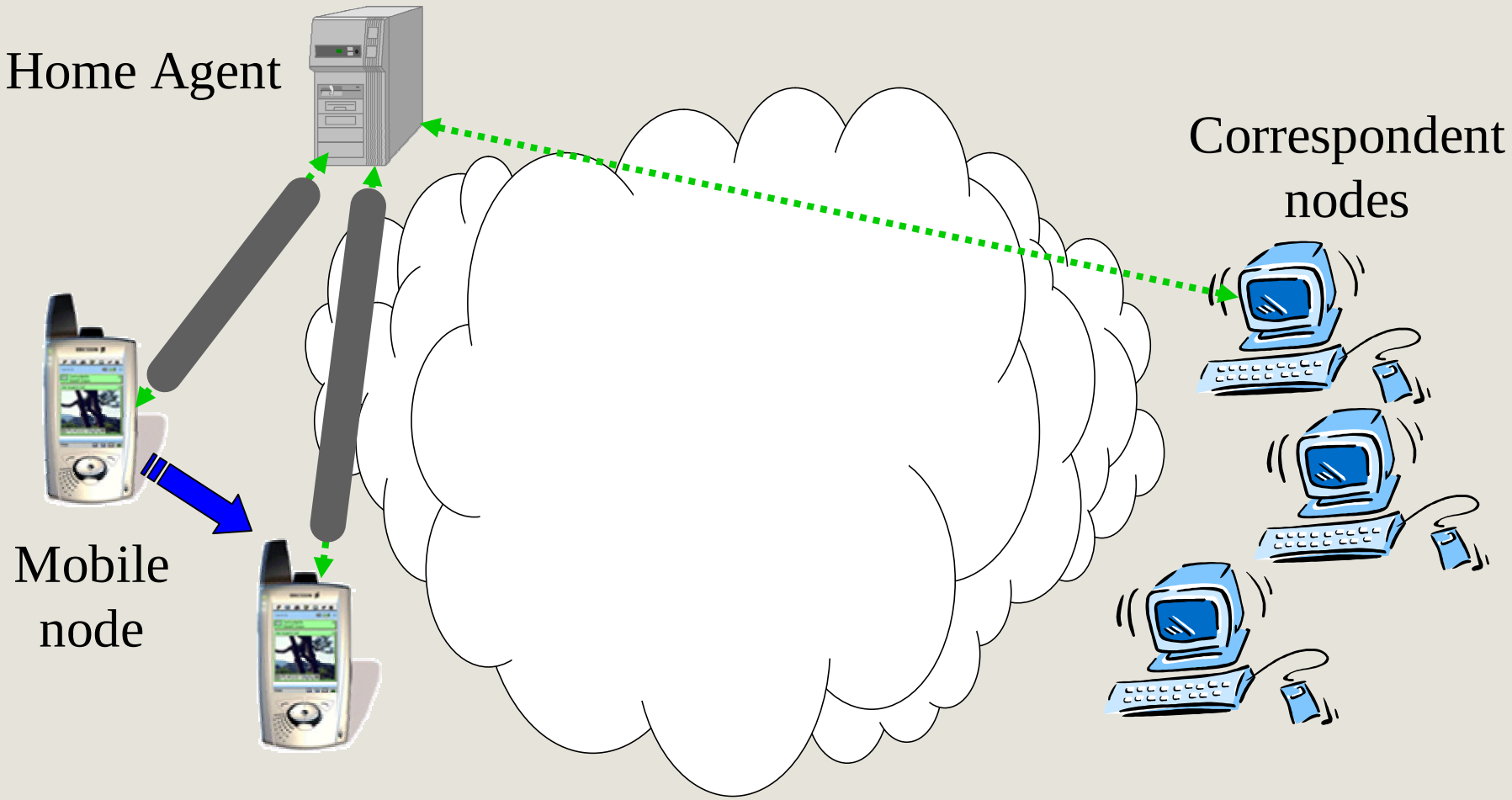
v=0
o=alice 2891092738 2891092738 IN IP4 lost.somewhere.com
s=Cool stuff
e=alice@w-land.org
t=0 0
c=IN IP4 lost.somewhere.com
a=key-mgmt:MIKEY uiSDF9sdhs727ghsd/dhsoKkdOokdo7eWsnDSJD...
m=audio 49000 RTP/SAVP 98
a=rtpmap:98 AMR/8000
m=video 52230 RTP/SAVP 31
a=rtpmap:31 H261/90000

ERICSSON

Case 2: Mobile IPv6 and the Importance of Scalable Security

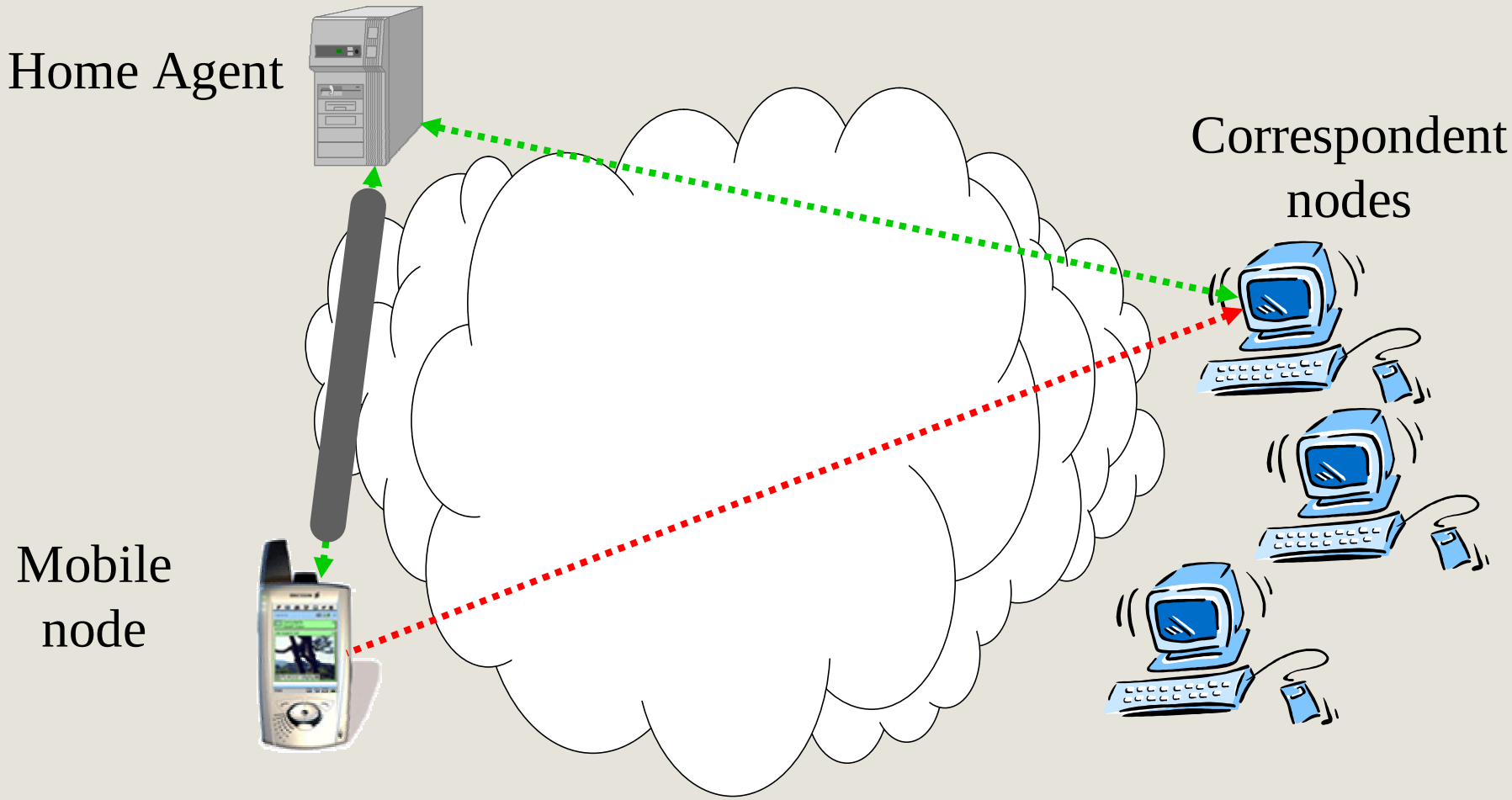
ERICSSON

Mobile IPv6



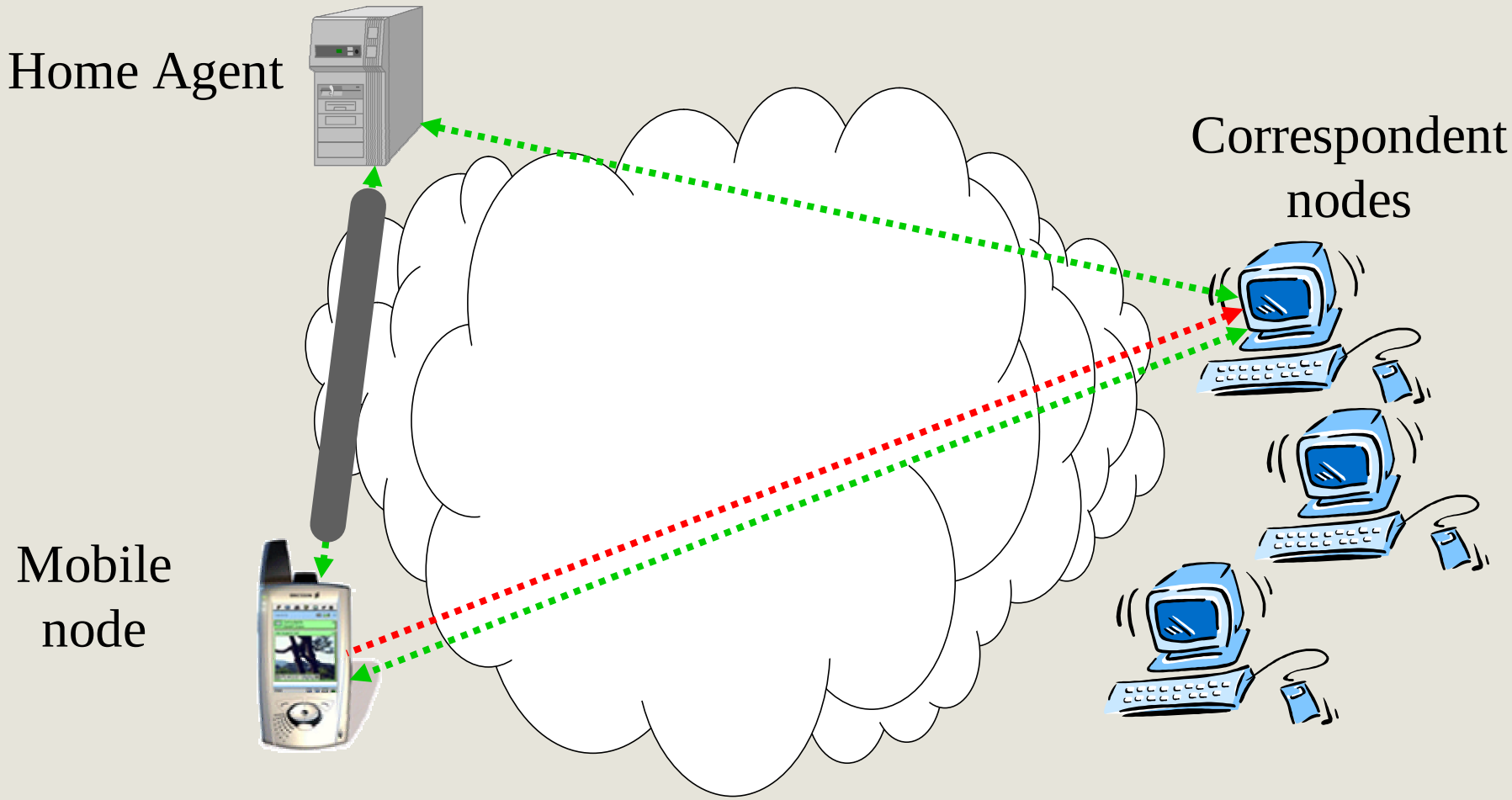
ERICSSON

Route Optimization



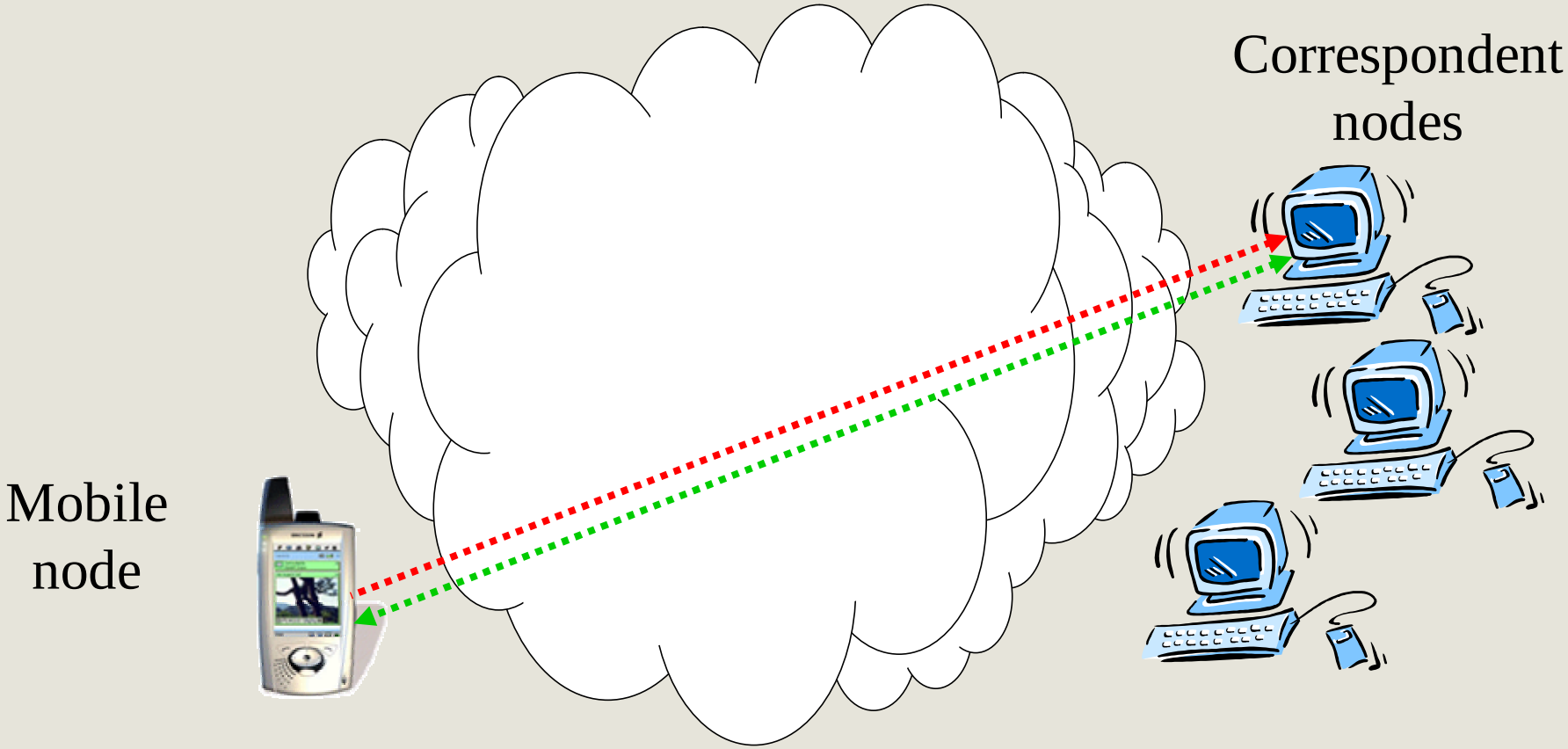
ERICSSON

Route Optimization



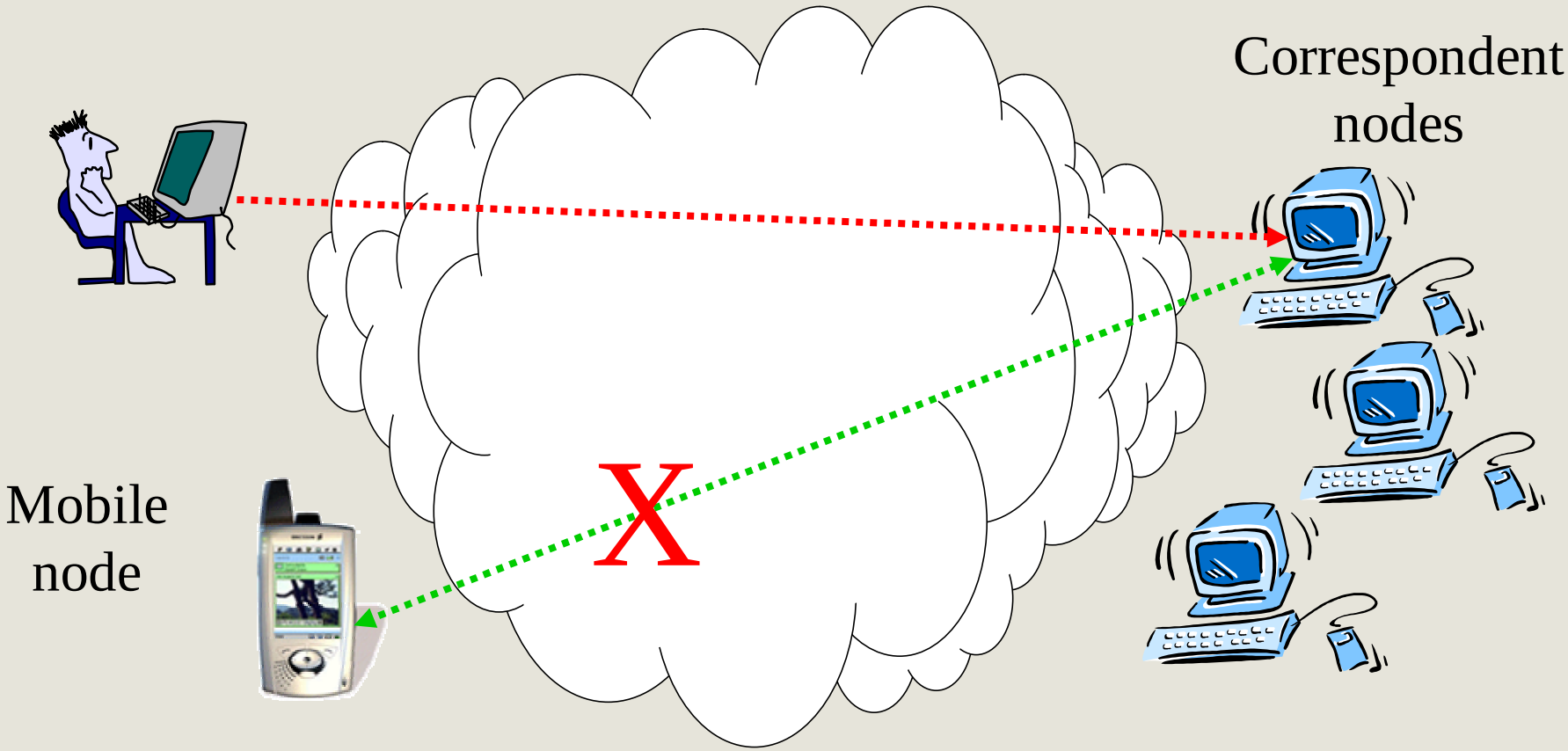
ERICSSON

Route Optimization



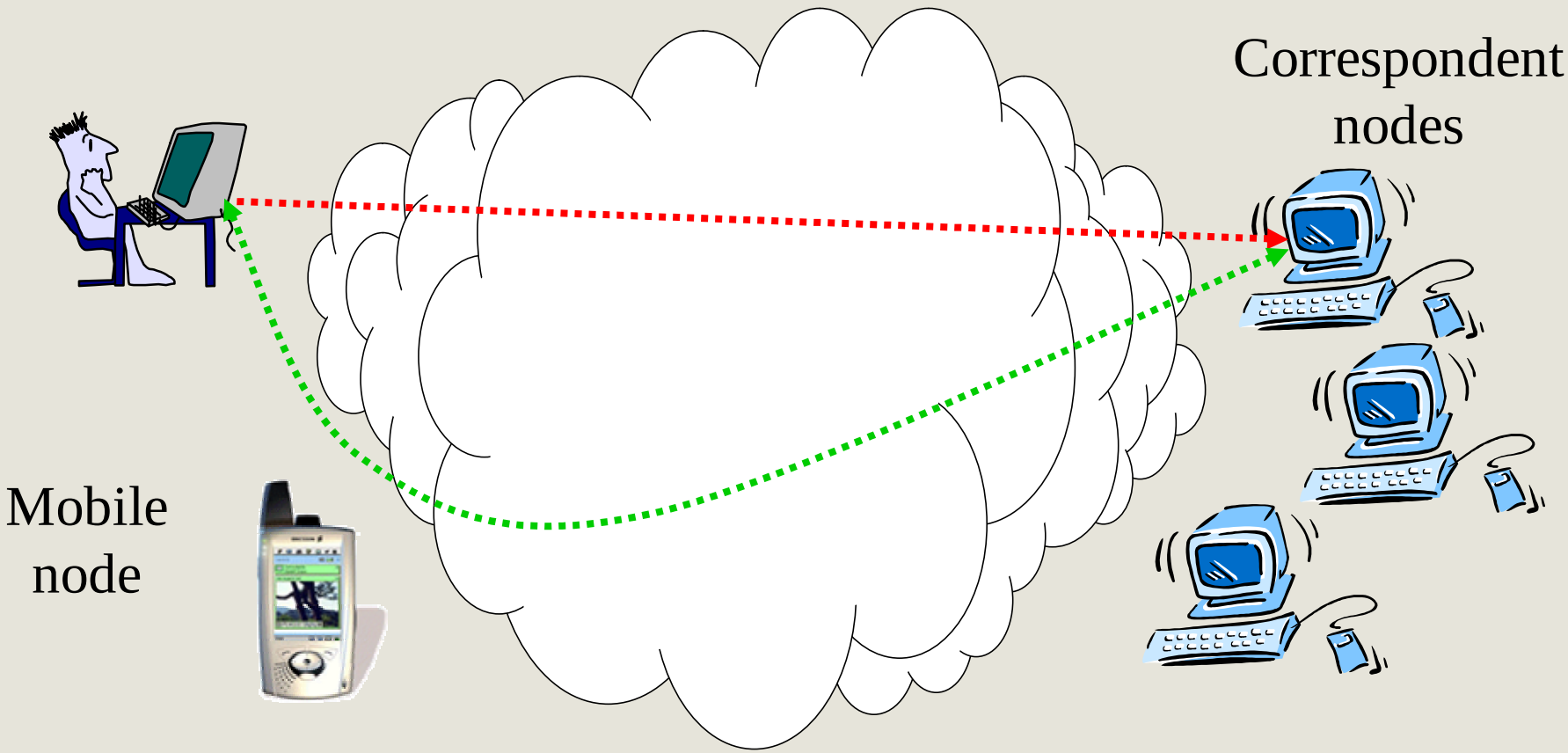
ERICSSON

Threats Involved in Route Optimization (1)



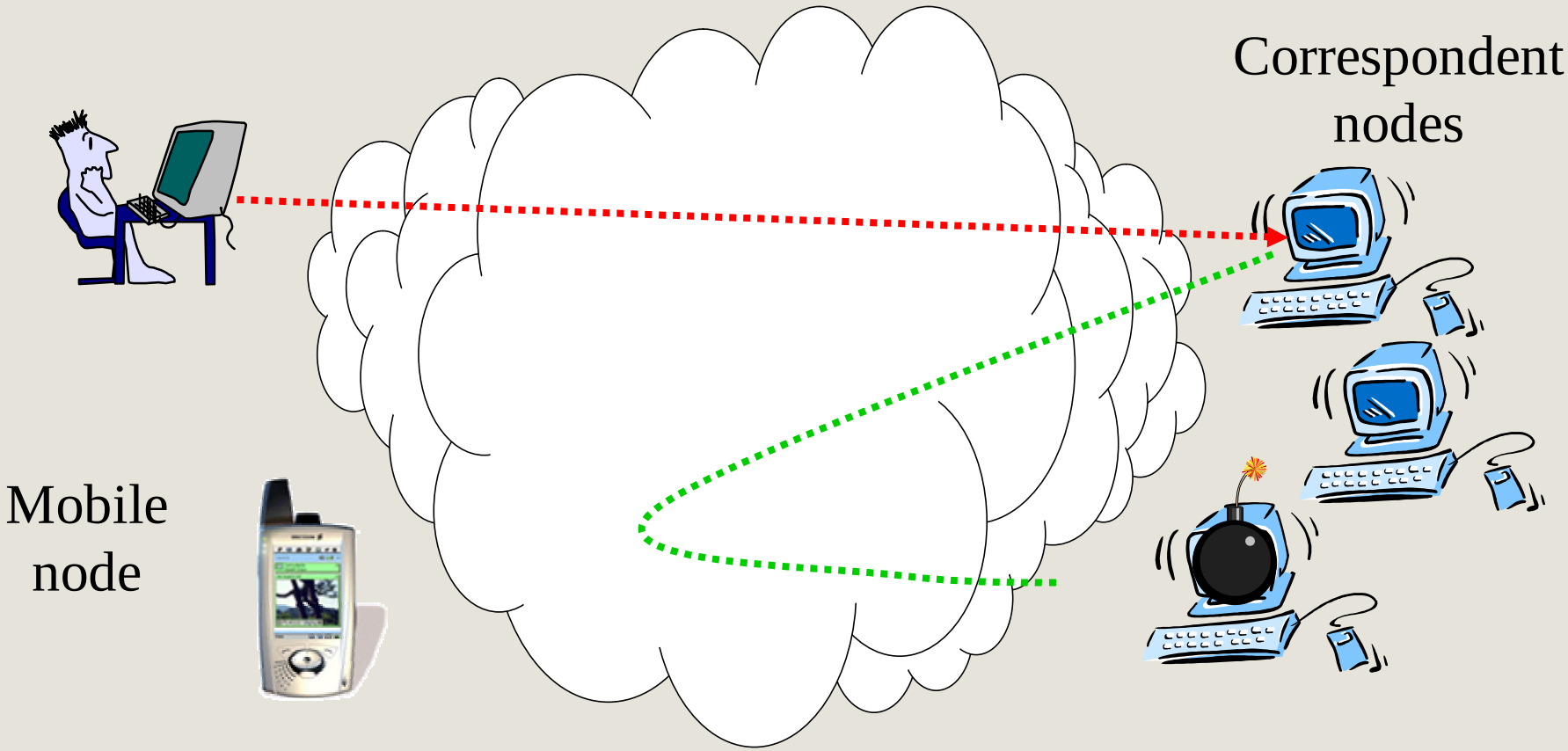
ERICSSON

Threats Involved in Route Optimization (2)



ERICSSON

Threats Involved in Route Optimization (3)



ERICSSON

Securing Route Optimization

- Clearly, security is needed.
- Approach #1: All signaling must be protected by a security association.
- Are we done?

ERICSSON

Problems with Approach #1

- Originally, our communications to peers did not require security associations

  (Sometimes SAs were not used, but not always)
- Then we added signaling for an *optimization*
- The end result is that we need SAs for all peers
- Very, very hard to establish global security between everyone
- Worse, it wouldn't show address ownership

? RO in very limited use or no security

ERICSSON

Approach #2: Zero-Configuration Security

- It turns out that one can test address ownership by sending messages to the addresses
- Needs a cryptographic exchange
- But no configuration, SAs, or infrastructure
- There are some remaining threats, but these exist in IPv6 even without mobility

ERICSSON

Lessons Learned - Scalability

- Deployment must be feasible
- Importance of function vs. cost
- Understand the threats

  Combat the threats, not more
- Understand what the mechanisms provide
  - For instance, authentication does not help authorization

ERICSSON

Lessons Learned - Other

- Design security along the rest of the design
  Risk major rework if not followed!

- Take in account threats to innocent third parties

ERICSSON

The Future of the Mobile Internet

ERICSSON

What's Next?

- Seamless operation and multi-everything
- Open business and technology model
- Many co-operating devices
- Communications without a controlling operator
- Protecting the user and availability of services

ERICSSON

Implications of the Future Scenario

- Mobility in different forms
- Peer-to-peer trust vs. user-to-operator trust
- End-to-end vs. hop-by-hop
- Co-operative vs. centralized solutions
- Deployment and scalability of security
- Hard outside, soft inside no longer sufficient
- Privacy

ERICSSON

Case 3: Host Identity Protocol (HIP) and the Insignificance of IP Addresses

ERICSSON

Some Interesting Network Functions

- End-host mobility
  - IP address changes to the location
- End-host multihoming
  - IP address changes when another interface used
- NAT traversal
  - IP address changes all by itself...
- IPv4 - IPv6 transition
  - IP address changes; this is like NAT but useful

ERICSSON

Network Functions, Continued

- Mobile networks
  - IP address changes to the router's address or prefix
- Location privacy
  - IP address changes from real to the public one
- Local mobility management
  - IP address changes (locally)
- Smooth handovers
  - IP address changes or there are simultaneously many

? See the pattern?

ERICSSON

IP Address = locator + endpoint identifier

- Addresses act also as endpoint IDs for TCP etc
- Does this make sense?
- Enter the Host Identity Protocol (HIP):
  - New layer
  - Hosts identified by public keys (or rather their hashes)
  - Sockets bound to host identifiers, not addresses
  - Dynamic binding to current IP address
- Mobility and multi-homing are duals of each other
- Most functions in our list become easier to solve
- Something to consider? Ongoing research…
  - Mailing list “hipsec” at lists.freeswan.org

ERICSSON

Conclusions

ERICSSON

Conclusions

- Security makes a big difference in quality of our protocol designs
- Key points to consider with new designs:
  - Design security at the same time as the function itself
  - Design security for the task at hand
  - Solutions need to be scalable and deployable
  - Consider the characteristics of solutions over wireless
  - Consider threats to third parties
  - Consider architectural changes when going gets tough

ERICSSON

ERICSSON

More Information

- IETF WGs: Mobile IP, Nemo, AVT, MSEC, EAP, AAA, PANA
- 3GPP WGs: SA2 (architecture) and SA3 (security)
- IEEE WGs: 802.1x and its newer versions
- Other: “hipsec” list at lists.freeswan.org