Wireless Mobile & Multimedia Networking

7COM1076

Mobile IP 3

Dr Tazeen Syed

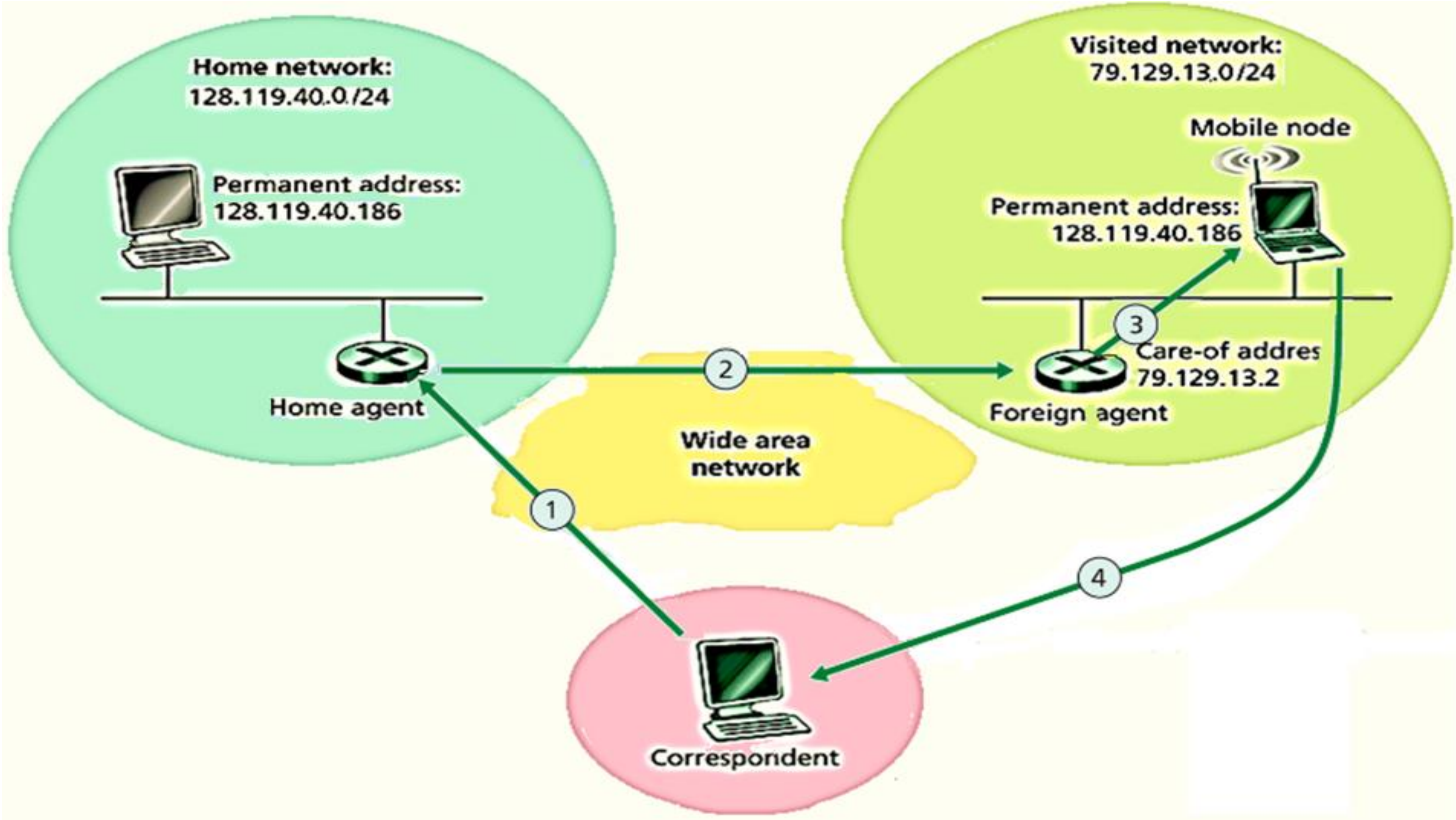
t.s.syed@herts.ac.uk

School of Physics Engineering and Computer Science (SPECS)

Outline

- ❑ **Route Optimization**
  - ➢ Routing to mobile node
  - ➢ Triangle Routing Problem
  - ➢ Route optimisation by implementing location cache
  - ➢ Foreign Agent Handoff
  - ➢ Improved handoff
- ❑ **Security in Mobile IP**
  - ➢ Denial of Service Attack
  - ➢ Replay Attack
  - ➢ Using MD5 during registration
  - ➢ Mobile IP Authentication
  - ➢ Replay Attack - Solution

Routing to Mobile Node

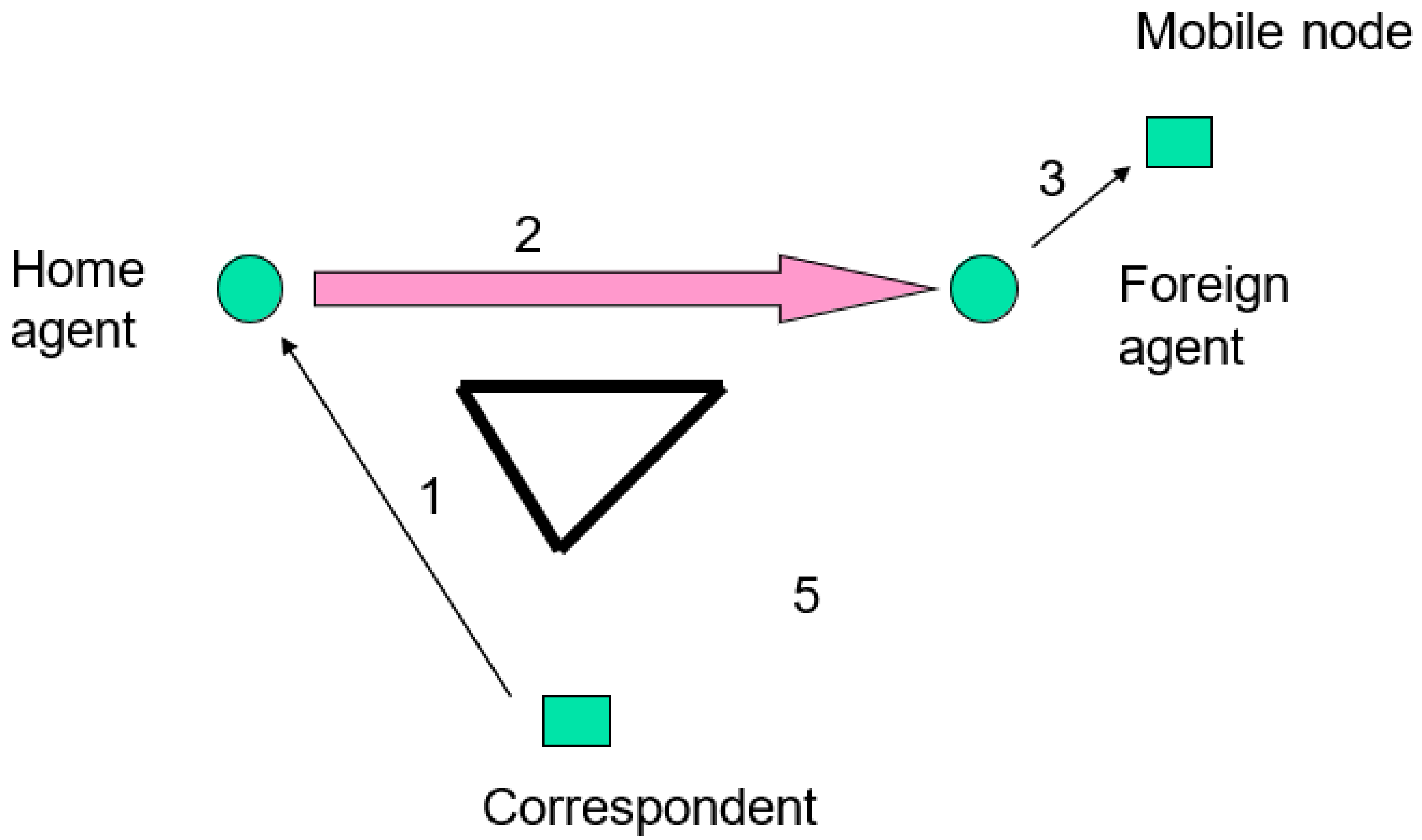


Triangle Routing problem

- Packets from correspondent travel to home agent first, and then to foreign agent.
- A triangle is formed among correspondent node, home agent, and foreign agent.
- High latency and network load

- Solution:
  - Avoid routing through home agent
  - Home agent gives COA of mobile node to correspondent node
  - Sender learns the current location of mobile host
  - Correspondent node does direct tunneling to this location

Triangle Routing problem



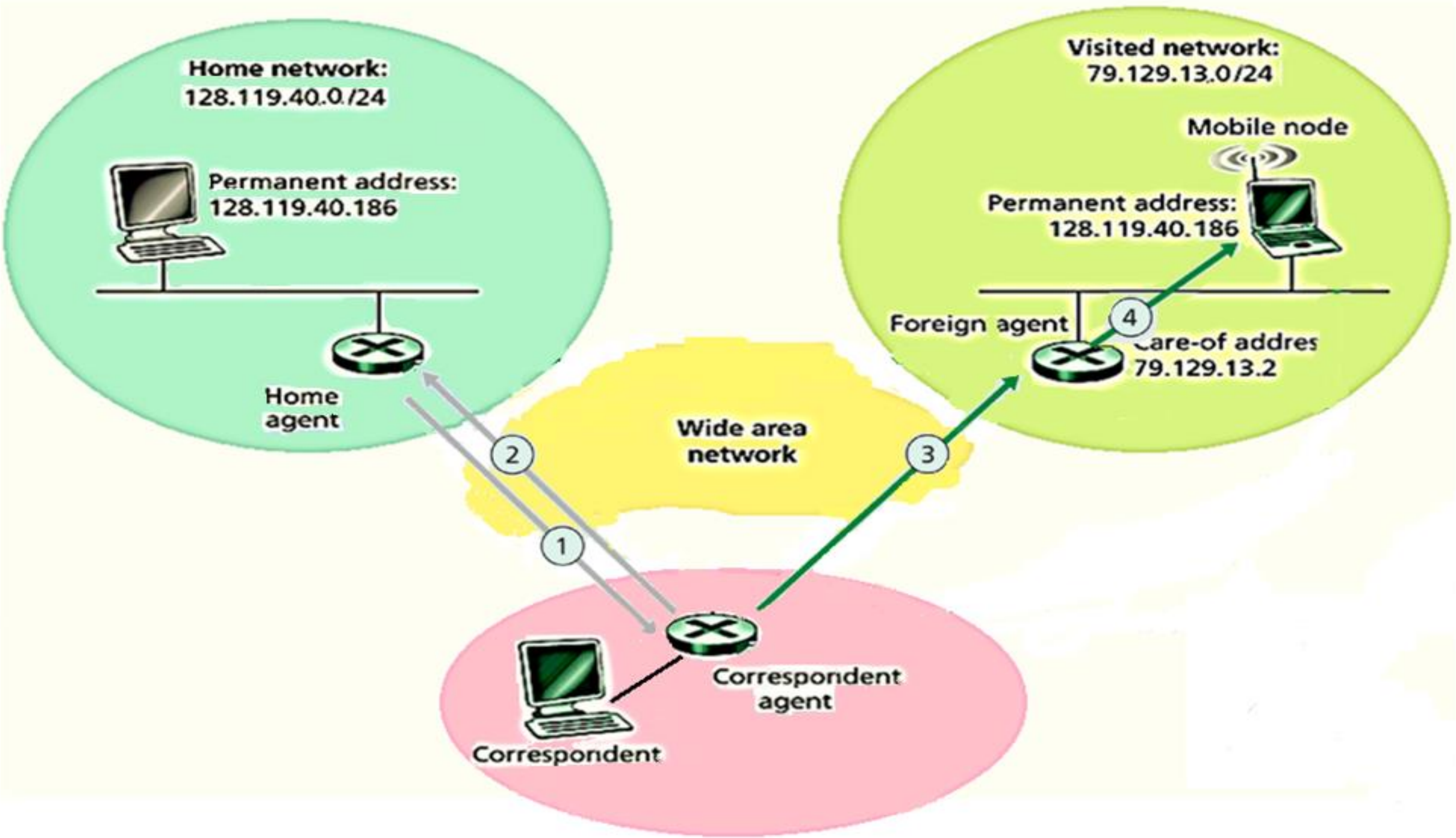
Triangle Routing problem - Solution

❑ Location Caching at a Correspondent

- By using *location caching* at the correspondent
  1. Correspondent learns mobile node’s COA from the home agent.
  2. Correspondent forwards packets to foreign agent by using *tunnelling*
  3. Foreign agent forwards the packets to the mobile node

- Disadvantage:
  1. Transparency of node mobility is lost.
  2. The correspondent is informed of the mobile host’s current mobility binding.

Route Optimisation by implementing location cache



Reverse tunneling

- In this process, foreign agent will forward packets through tunneling to home agent
- Home agent forwards it to correspondent node.

Foreign Agent handoff

- Handoff

1. It is a process of a mobile node moving from one foreign network to another foreign network.

2. You can say a mobile host is handed off from one foreign agent to another foreign agent.

Foreign Agent handoff

- How does mobile IP handle handoff?

1. The basic Mobile IP protocol does not notify the old foreign agent that the MN has moved out of its network.

2. Home agent realises that mobile node has moved to a new foreign network after receiving the registration request message from MN.

3. Home agent now tunnels the new packets of mobile node to the new care-of-address

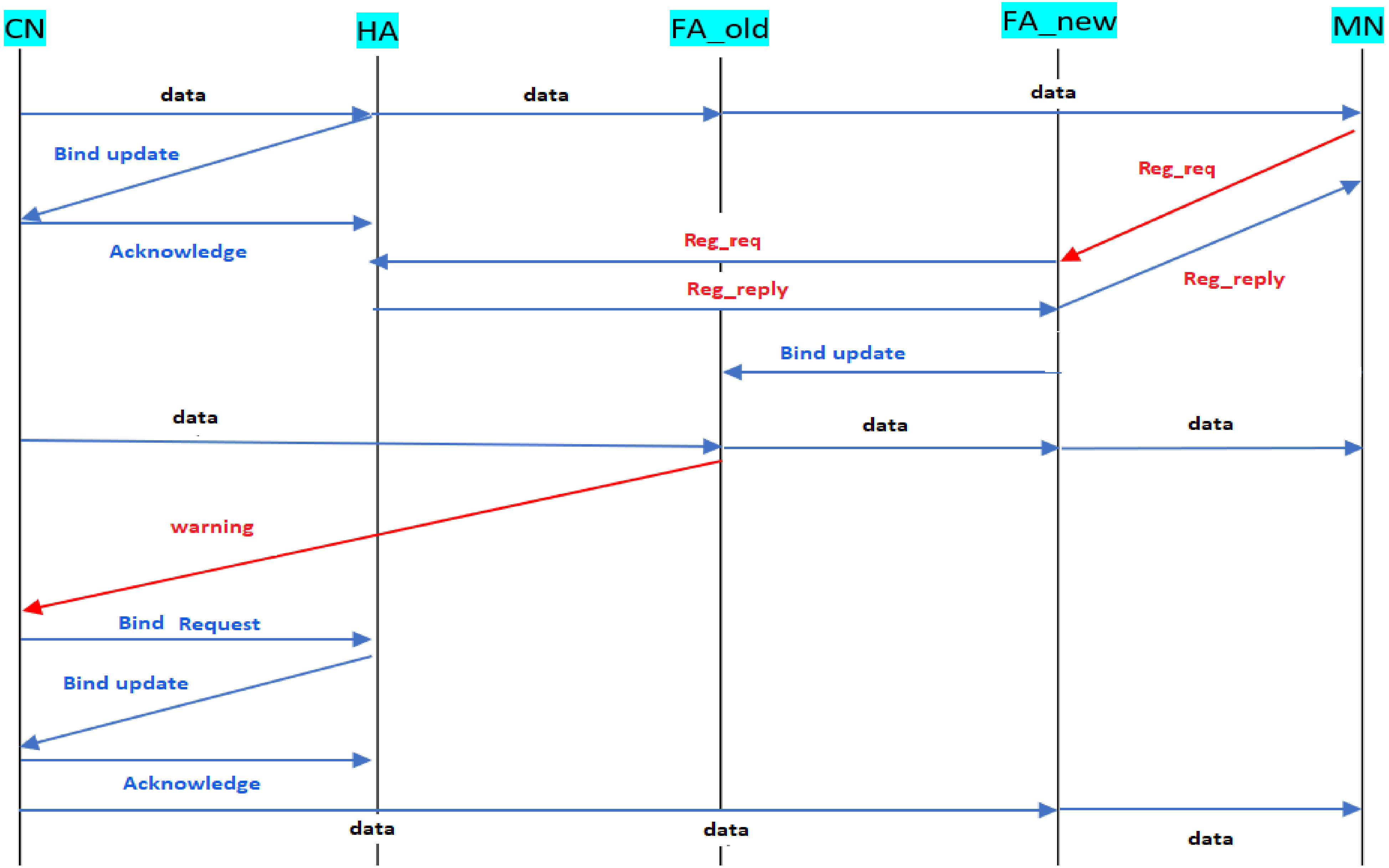
4. Any packets already been tunneled to old care-of-address is lost and assumed to be retransmitted by higher-protocols if needed.

Improved Handoff

- The basic idea is to let the previous foreign agent know where the mobile host has moved to, i.e., the new binding of the mobile host.

- Process
  1. The mobile host sends a *binding update* to the previous foreign agent after it moves to a new foreign agent.
  2. The previous foreign agent then forwards the packets tunneled to it by the home agent to the new care-of address instead of dropping these packets.

Improved Handoff



Security in Mobile IP

Network security in Mobile IP is essential. Compromise in security may lead to undesirable consequences such as:

- Denial of service (DOS) attack
- Replay attack
- Unauthorised access
- Unreliability

Security in Mobile IP

- **Denial of service (DOS) attack**

  An attacker overflows access server. This is possible because the sensitive IP addresses of the HA and the MN are not hidden in the registration messages.

- **Replay attack**

  An attacker records and replays the registration request message after a mobile node already leaves a foreign network.

- **Masquerade**

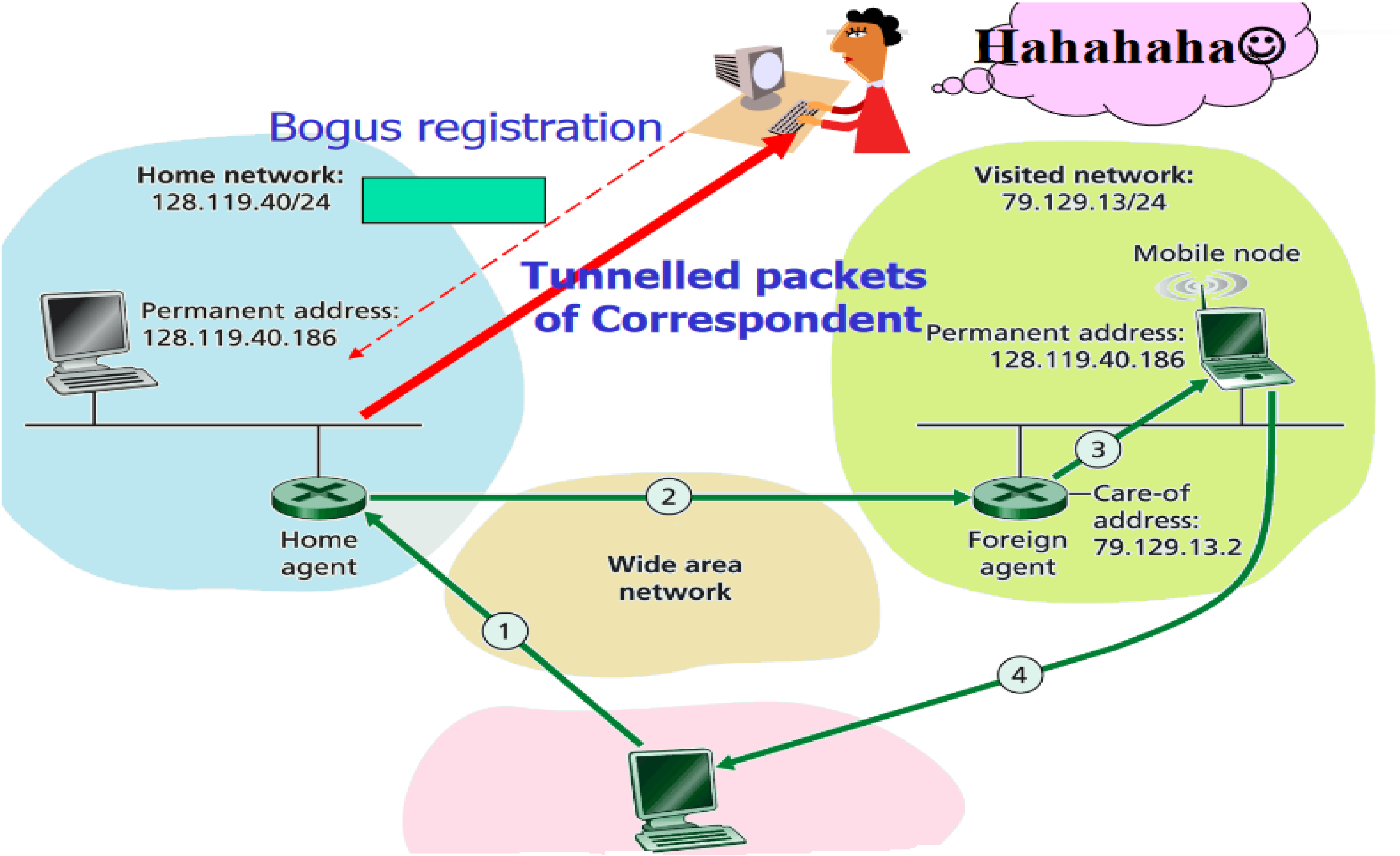
  During registration process, an attacker could masquerade as a foreign agent and get all the data of mobile hosts to be diverted to him.

Security in Mobile IP

- ❑ Hacker sends fake or bogus registration message to home agent, using his own address as the care-of address of a mobile node
- ❑ All packets sent by a correspondent could be tunneled by home agent directly to the hacker

Security in Mobile IP

Bogus registration



Security attacks – Solutions

Security can be maintained by using authentication and integrity during registration

Authentication in security means the process of deciding whether a principle is the one he claims to be. Provide authentication between a mobile node and its home agent, so that hacker cannot claims that he is the mobile node.

- E.g., whether this registration really comes from the mobile node that it claims to be.

Integrity in security means the information has not been changed by a third party during its transmission from the sender to the receiver

Security Extension of Mobile IP Registration Message

- **Security Parameter Index**
  Identifies a security context between a pair of nodes. This security context is configured so that the two nodes share a secret key and parameters relevant to this association.

- **Authenticator**
  A code used to authenticate the message. The sender inserts this code into the message using a shared secret key. The receiver uses the code to ensure that the message has not been altered

Security in Mobile IP

However, authentication with FA is normally problematic because foreign agent typically belongs to a different network. There will be many restrictions and firewalls etc.

Using MD5 during Registration

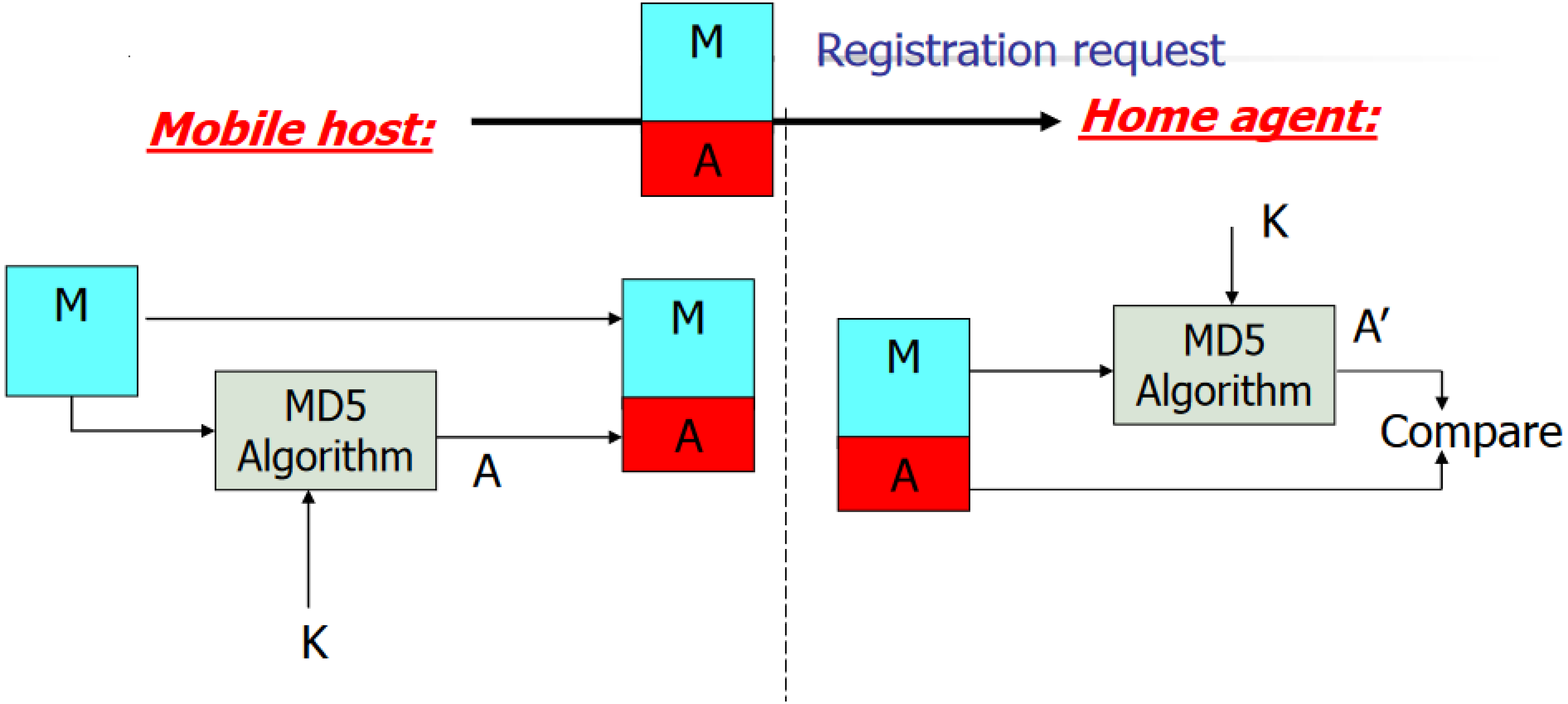
- Mobile IP supports MD5 *Message-Digest Algorithm* (RFC 1321) that provides secret-key authentication and integrity checking
  - Secret key is a secret that is only known to a pair of communication party.
  - MD5 algorithm takes a message as input, applying the secret key, calculating an authenticator based on the message and the key.
- A mobile node and its home agent share a secret key (probably assigned to both while the mobile node is at home).

Using MD5 during Registration

M : Registration request / reply message

A : Authenticator code

K : The secret key shared between MN and HA



Mobile IP Authentication

1. During registration, the mobile node takes the critical information of the registration fields including chosen care-of address and calculates an authenticator by MD5 algorithm using the secret key it shares with the home agent.

2. When home agent receives the registration request message, it is able to calculate an authenticator by MD5 algorithm using the same secret key.

3. The home agent then compares the authenticator, it calculates locally with the one carried in the registration request message

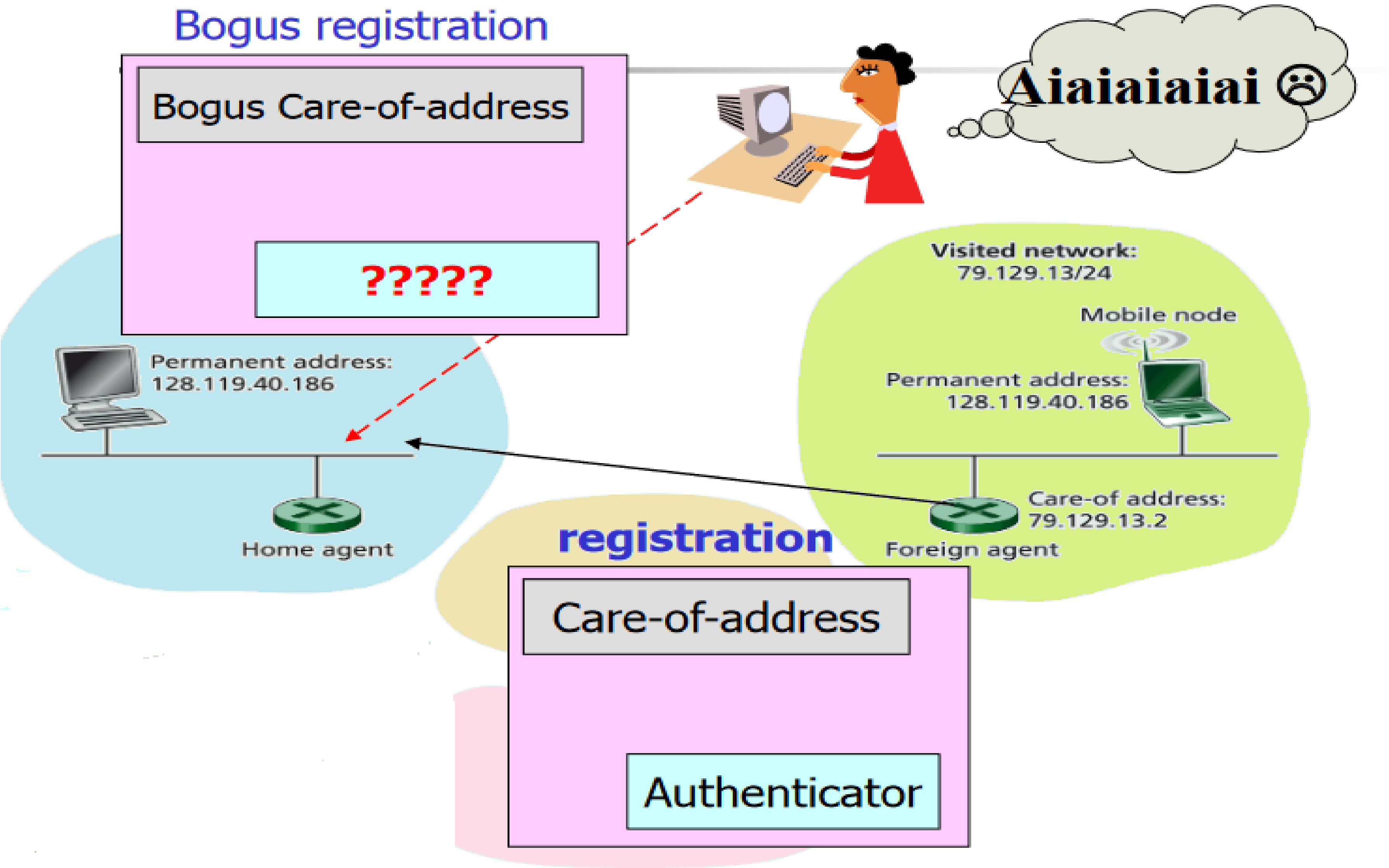
Mobile IP Authentication (cont.)

4. If they match, the home agent concludes that this request is sent from the mobile node (authentication) and nobody else has changed the message since it was sent (integrity).

5. If not, the home agent ignores the registration request.

6. The home agent sends registration reply message, also with an authenticator based on the key and the important fields of the reply message.

Authentication is used during Registration



Replay Attack

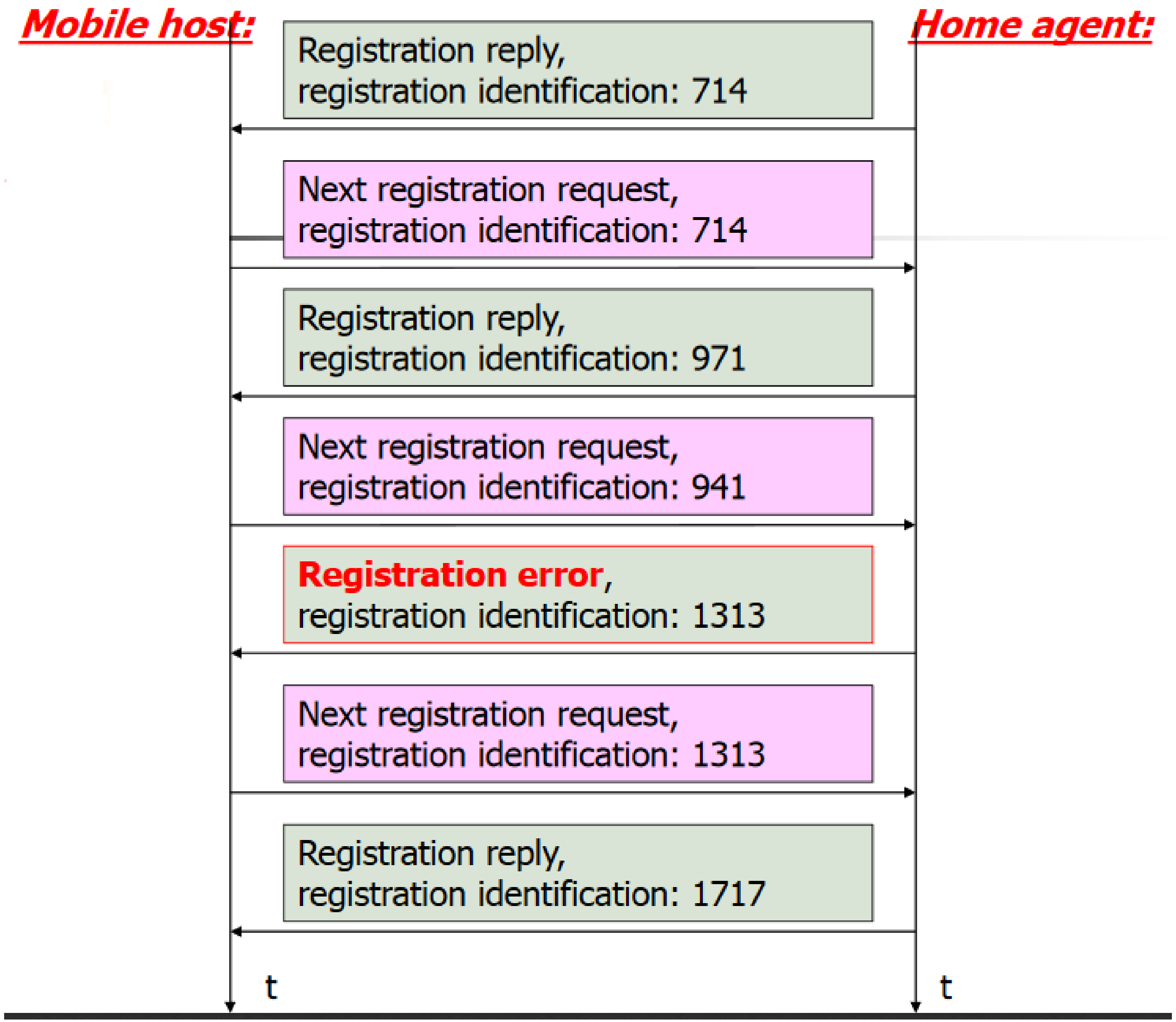
- Hacker may replay old registration messages of a mobile host, so that the home agent of the mobile node will forward the packets addressed to the mobile node to hacker. The mobile node is thereby effectively cut from the network.

Replay Attack : Solution

- Provide freshness in the mobile node registration process by including a nonce or timestamp.

- The registration identification field in the registration request message and registration reply message is defined for this purpose.

  - The 64-bit registration identification acts like a sequence number.
  - It serves to match a received registration reply with a registration request.



Mobile host:

Home agent:

Registration reply,
registration identification: 714

Next registration request,
registration identification: 714

Registration reply,
registration identification: 971

Next registration request,
registration identification: 941

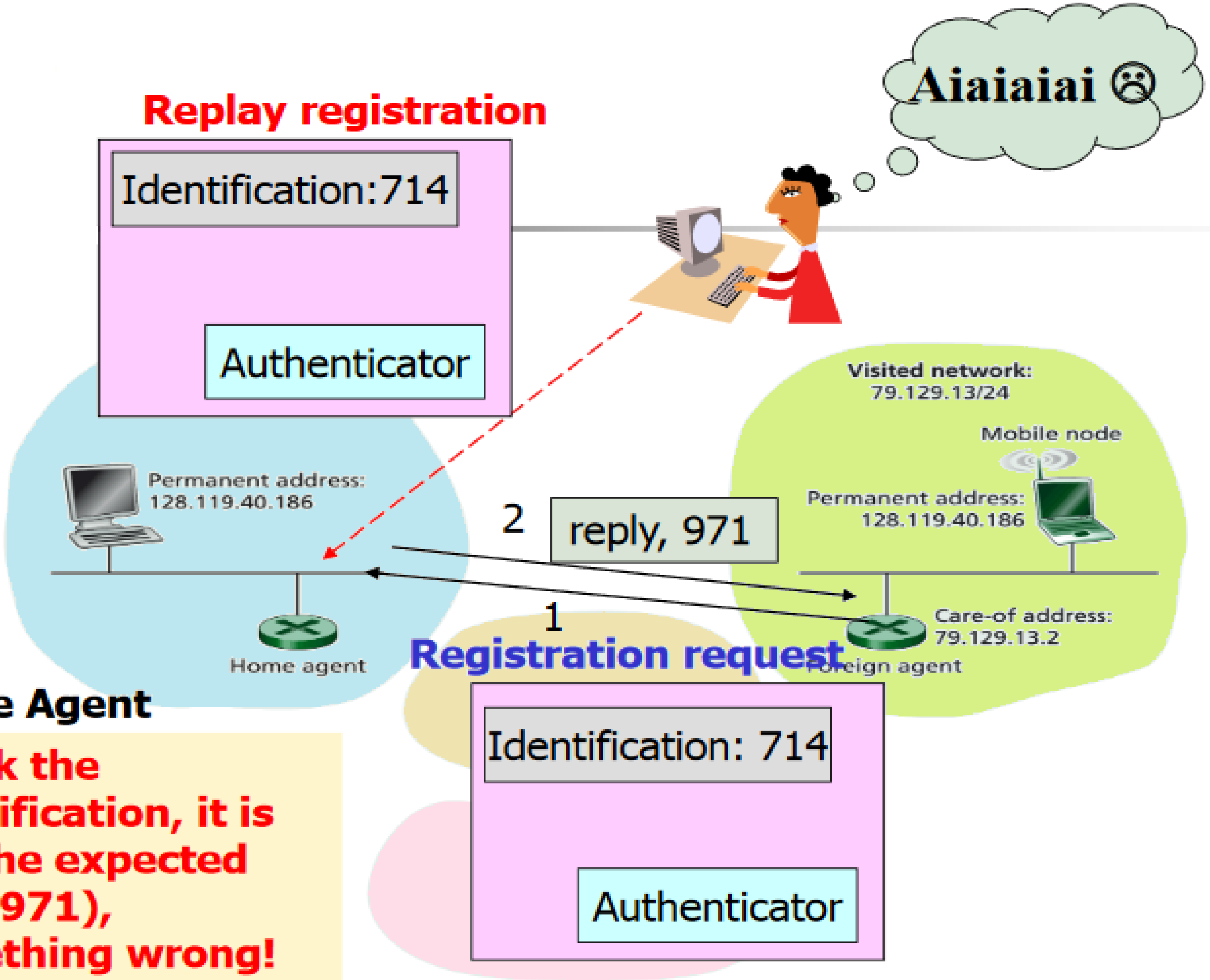
Registration error,
registration identification: 1313

Next registration request,
registration identification: 1313

Registration reply,
registration identification: 1717

t

t



Replay registration

Identification:714

Authenticator

Aiaiaiai ☹

2 reply, 971

1 Registration request

Identification: 714

Authenticator

Home Agent

Check the identification, it is not the expected one (971), something wrong!

Thank you

Any Questions?

t.s.syed@herts.ac.uk