

Using Host Identity Protocol in Ad Hoc Access Networks

Mikko Särelä

Helsinki University of Technology

Introduction

- Ad hoc networks
- Host Identity Protocol (HIP)
- HIP in ad hoc access networks
- Summary

Ad Hoc Networks

- Dynamic networks with no fixed infrastructure
- Links often short lived, i.e. decisions must be based on local information
- Routing mostly based on flat topology and reactive route creation
- Conceptually ad hoc network routing operates using identities
- Fixed networks currently use IP addresses both as addresses and identities
- This difference is the main problem for using ad hoc networks as access networks

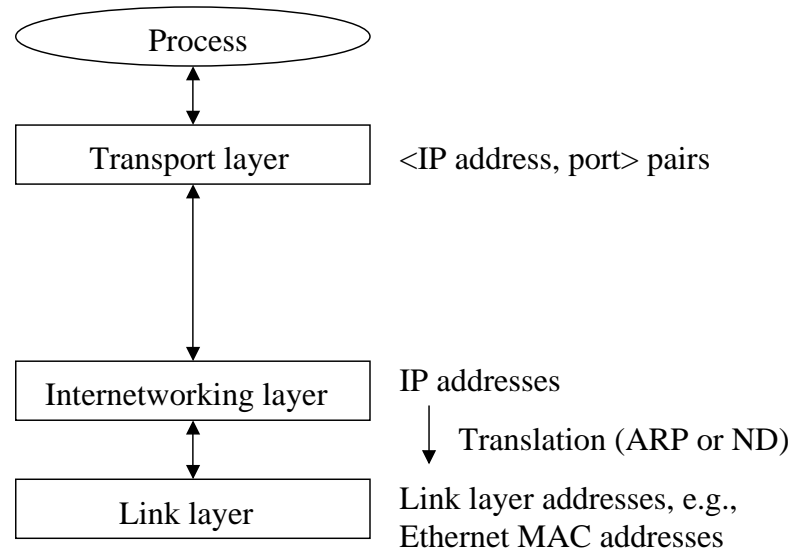
Host Identity Protocol

- A new Host Identity Layer between Internetworking and Transport layers.
- Introduces a new cryptographically secure Host Identity namespace.
- Transport connections will then operate using Host Identities, rather than IP addresses, to denote end points.

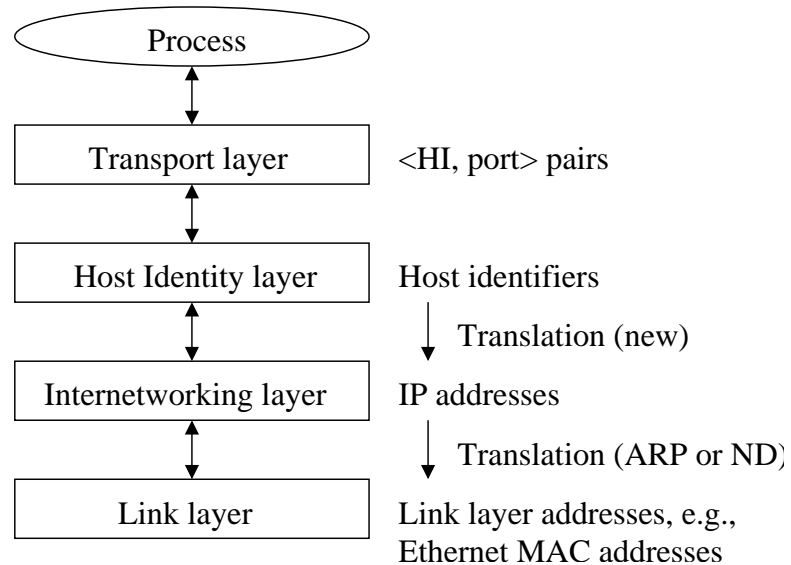
Host Identity Protocol

- A Host identity is a public/private key pair.

The current Internetworking architecture:



The new proposed architecture:

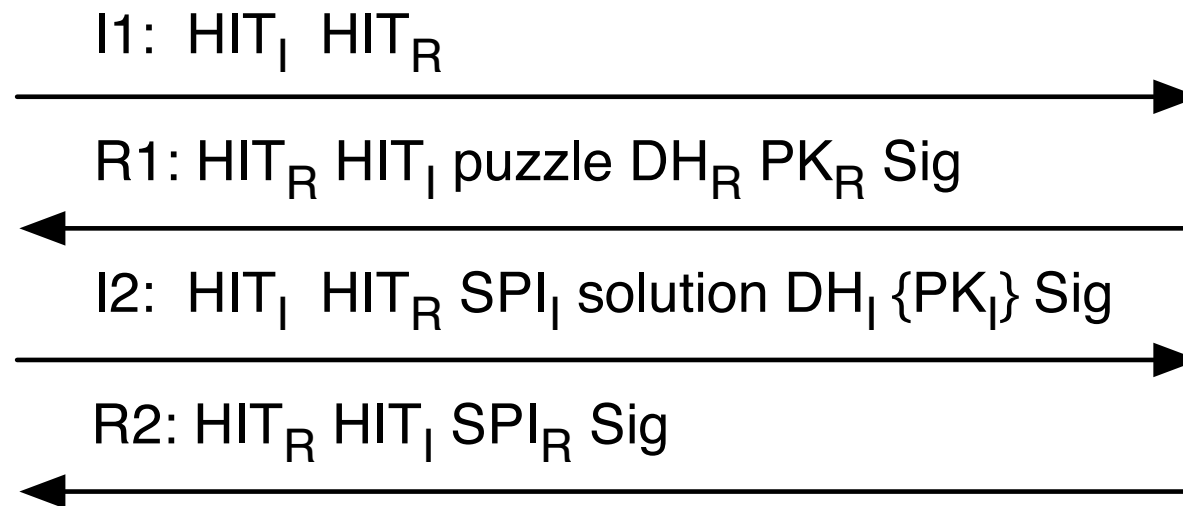


HIP Base Exchange

- Consists of 2-round trip Diffie-Hellman key exchange
- Host Identity Tag (HIT) 128 bit cryptographic hash of Host Identity

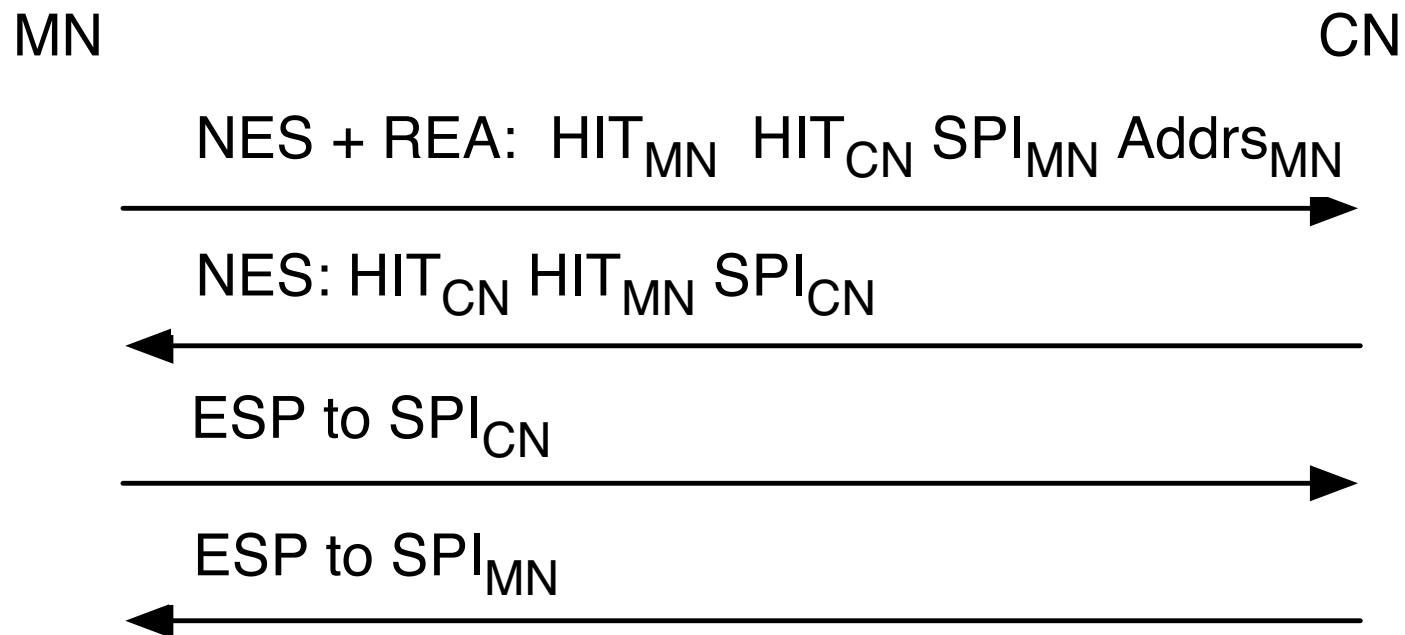
Initiator

Responder



HIP Re-addressing Protocol

- Allows a host to inform peer of current IP addresses they have
- Since the first packet is authenticated, the last 3 packets are optional based on the level of trust in networks

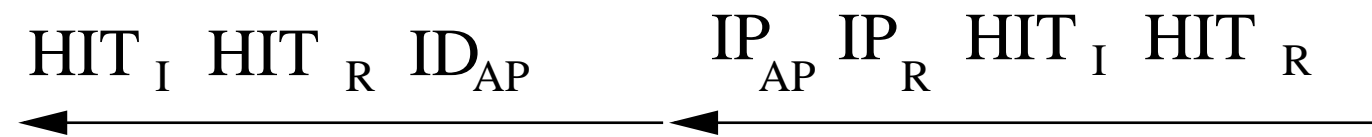


HIP with ad hoc access networks

- Two possible solutions: In both access point (AP) acts as a NAT box for the ad hoc node (MN). Thus MN does not need to obtain a globally routable IP address.
- MN needs to upkeep a route to AP and possibly add itself to a Rendezvous Server identity database.
- Either MN will find out the CN's IP address and use it,
- or MN only knows the identity, and AP will handle identity to IP address translation.

Changes to Base Exchange Packets in AP

Initiator Access Point Responder

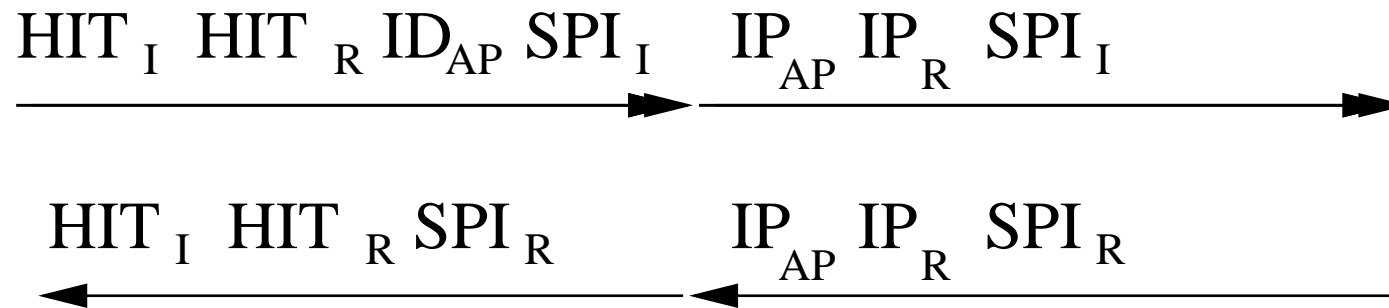


Changes to Packets in AP

Initiator

Access Point

Responder



Lazy Access Point Switching

- Lazy switch of AP means that the MN starts sending packets through a new AP before starting REA with CN.
- To enable this in the latter case, the AP may send a context to the MN. This context can contain the IP address of the previous AP, necessary information for IP address to identity translation and possibly other information for accounting, authorization, etc.

Summary

- IP is mainly based on hierarchical stable addressing, which works poorly in dynamic ad hoc networks.
- HIP can be used to help ad hoc network nodes to gain connectivity to fixed networks while allowing ad hoc networks to operate their routing based on cryptographically strong identifiers.
- It does not require them to obtain and update globally routable IP addresses as Mobile IP does.
- It is possible to allow ad hoc network nodes to communicate completely based on identifiers even with nodes within fixed network. This requires AP to act as a NAT box.
- Lazy switch of AP is easier, if ad hoc network nodes know the IP address of their fixed network peer.