Host Identity Protocol (HIP): Connectivity, Mobility, Multi-homing, Security, and Privacy over IPv4 and IPv6 Networks

IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 12, NO. 2, SECOND QUARTER 2010

Authors:

Pekka Nikander, Andrei Gurtov, and Thomas R. Henderson

Speaker： Yu-Chan Lin

Outline

- Abstract
- Introduction
- Evolving Environments
- Fundamental Problems
- The HIP architecture and base exchange

Abstract

- HIP enhances the original Internet architecture by adding a name space used between the IP layer and the transport protocols.

- This new name space consists of cryptographic identifiers, thereby implementing the so-called identifier / locator split.

IETF : Internet Engineer Task Force

Abstract(cont.)

- Mobility, multi-homing, and baseline end-to-end security integrate neatly into the new architecture.

- This article provides an in-depth look at HIP, discussing its architecture, design, benefits, potential drawbacks, and ongoing work.

Introduction

- The Host Identity Protocol (HIP) and architecture, is a new piece of technology that may have a profound impact on how the Internet will evolve over the coming years.

- From a functional point of view, HIP integrates IP-layer mobility, multi-homing and multi-access, security, NAT traversal, and IPv4/v6 interoperability in a novel way.
  - Mobile IP、IPsec、ICE and Teredo.

NAT : Network Address Translation ； ICE : Interactive Connectivity Establishment
Ipsec ： IP Security

Introduction(cont.)

- From a technical point of view, the basic idea of HIP is to add a new name space to the TCP/IP stack. These names are used above the IP layer (IPv4 and IPv6), in the transport layer (TCP, UDP, SCTP, etc) and above.

- HIP provides new tools and functions for future network needs, including the ability to securely identify previously unknown hosts and the ability to securely delegate signaling rights between hosts and from hosts to other nodes.

Evolving Environments

- Ability to operate over all kinds of underlying networks, including ad hoc, commercial, and dedicated.
- Ability to survive in a partially hostile environment where some of the underlying networks may be only partially co-operating, competing, or even outright antagonistic to each other.
- Ability to support application, host, and sub-network level mobility and multi-access as primary design elements and not as extensions.
- Ability to support full location privacy, especially against any transit networks and other third parties.

Evolving Environments(cont.)

- HIP provide baseline protection for communication, including optional functionality to fully protect the identity of communicating parties from outsiders.

- They aim to provide a similar or higher level of flexibility than the original IP architecture did, allowing the protocols and mechanisms to be easily extended.

Fundamental Problems

- Loss of universal connectivity
- Poor support for mobility and multi-homing
- Problems with multicast
- Unwanted traffic

Fundamental Problems(cont.)

- Loss of universal connectivity
  - The largest problem all current ones is the loss of connectivity, caused by NATs, firewalls, and dynamic IP addresses.
  - The HIP architecture providing a new end-to-end naming invariant.

Fundamental Problems(cont.)

- Poor support for mobility and multi-homing
  - Effective mobility support requires a level of indirection, to map the mobile entitys stable name to its dynamic, changing location.
  - Effective multi-homing support requires a similar kind of indirection, allowing the unique name of a multi-accessible entity to be mapped to the multitude of locations where it is reachable.

Fundamental Problems(cont.)

- Problems with multicast
  - Certain applications, such as Internet TV, involve data transmission from one source to multiple destinations.
  - The network multicast is more efficient than the application multicast, because it can achieve ”one link – one packet” principle.
  - Application multicast is easily deployable while several issues hindered deployment of IP multicast.

Fundamental Problems(cont.)

- Problems with multicast(cont.)
  - Mobility of hosts participating to multicast is a largely unsolved problem. Especially, if the multicast source changes the IP address, the whole multicast tree needs to be reconstructed.
    - bidirectional tunnelling
    - authentication

Fundamental Problems(cont.)

- Unwanted traffic
  - An architectural approach where each recipient has an explicit name and where each potential sender can send packets to any recipient without the recipient's consent.
  - A business structure where the marginal cost of sending some more packets is very close to zero.

Fundamental Problems(cont.)

- Unwanted traffic(cont.)
  - The lack of laws, international treaties, and especially enforcement structures that would allow effective punishment of those engaging in illegal activity in the Internet.
  - The basic profit-seeking human nature, driving some people to unethical behaviour in the hopes for easy profits.

Fundamental Problems(cont.)

- Lack of authentication, privacy and accountability
  - While the Host Identity Protocol does not directly provide means to address the privacy and accountability problems.
  - Firstly, the use of cryptographic host identifiers as an integral part of connectivity, thereby providing automatic identity authentication.

Fundamental Problems(cont.)

- Lack of authentication, privacy and accountability(cont.)
  - Secondly, the separation of identities and locators makes it easier to hide the topological location of communicating parties.
  - Thirdly, there are a few privacy extensions to HIP that allow the identities of the communicating parties to be hidden from third parties.

The HIP architecture and base exchange

- Approach
  - Non-mutability - The source and destination identities sent are the identities received.
  - Location independence - The identities do not change during the course of an ”association”.
  - Reversibility - A return header can always be formed by reversing the source and destination identities.
  - Omnisciency - Each host knows what identities a peer host can use to send packets to it.

The HIP architecture and base exchange

- Basics

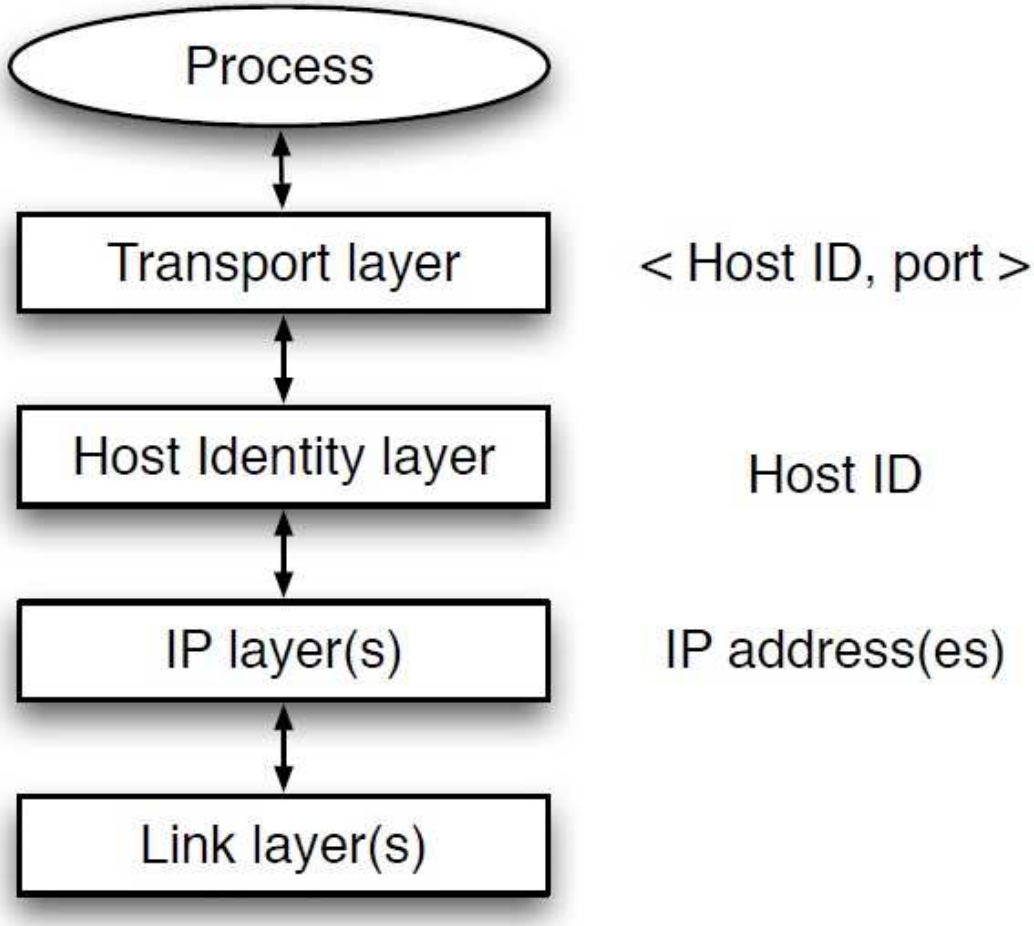


Fig. 1. Approximate location of the HIP sublayer within the TCP/IP stack.

The HIP architecture and base exchange

- Basics(cont.)
  - Diffie-Hellman
  - IPsec Encapsulated Security Payload (ESP) Security Association(SA)

The HIP architecture and base exchange

- HITs and LSIs
  - Host Identity Tags(HIT), According to the current specifications, a HIT looks like an IPv6 address with the special 28-bit prefix 2001:0010::/28, called Orchid.
  - Local Scope Identifiers(LSIs)

Protocols and packet formats

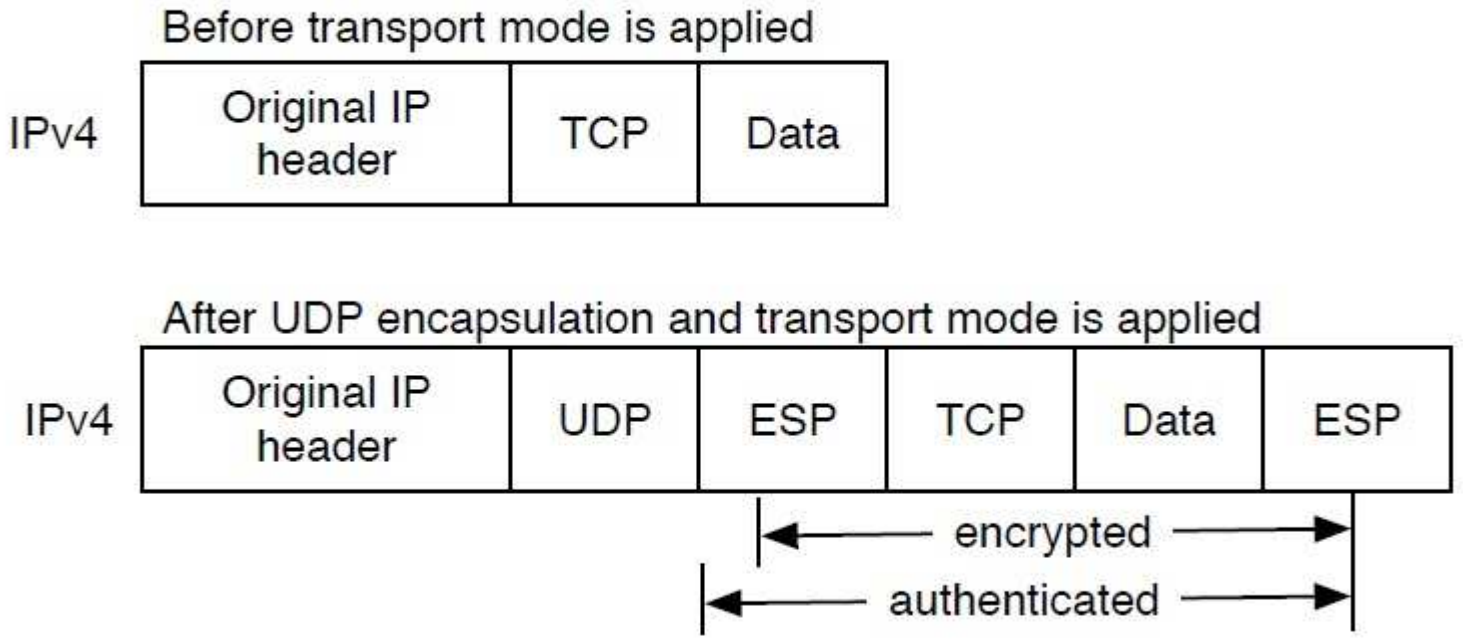


Fig. 2. IPsec NAT-Traversal.

Protocols and packet formats(cont.)

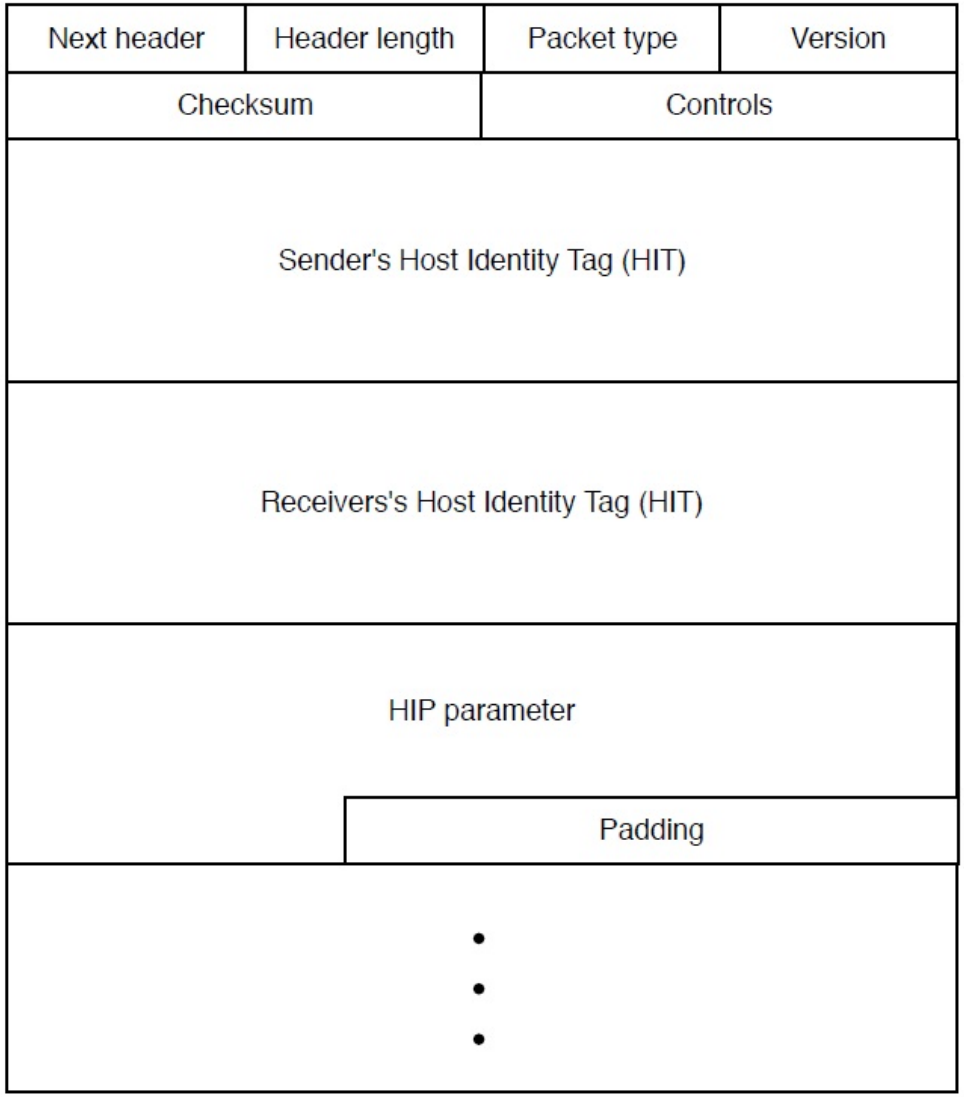


Fig. 3. HIP control packet format.

Protocols and packet formats(cont.)

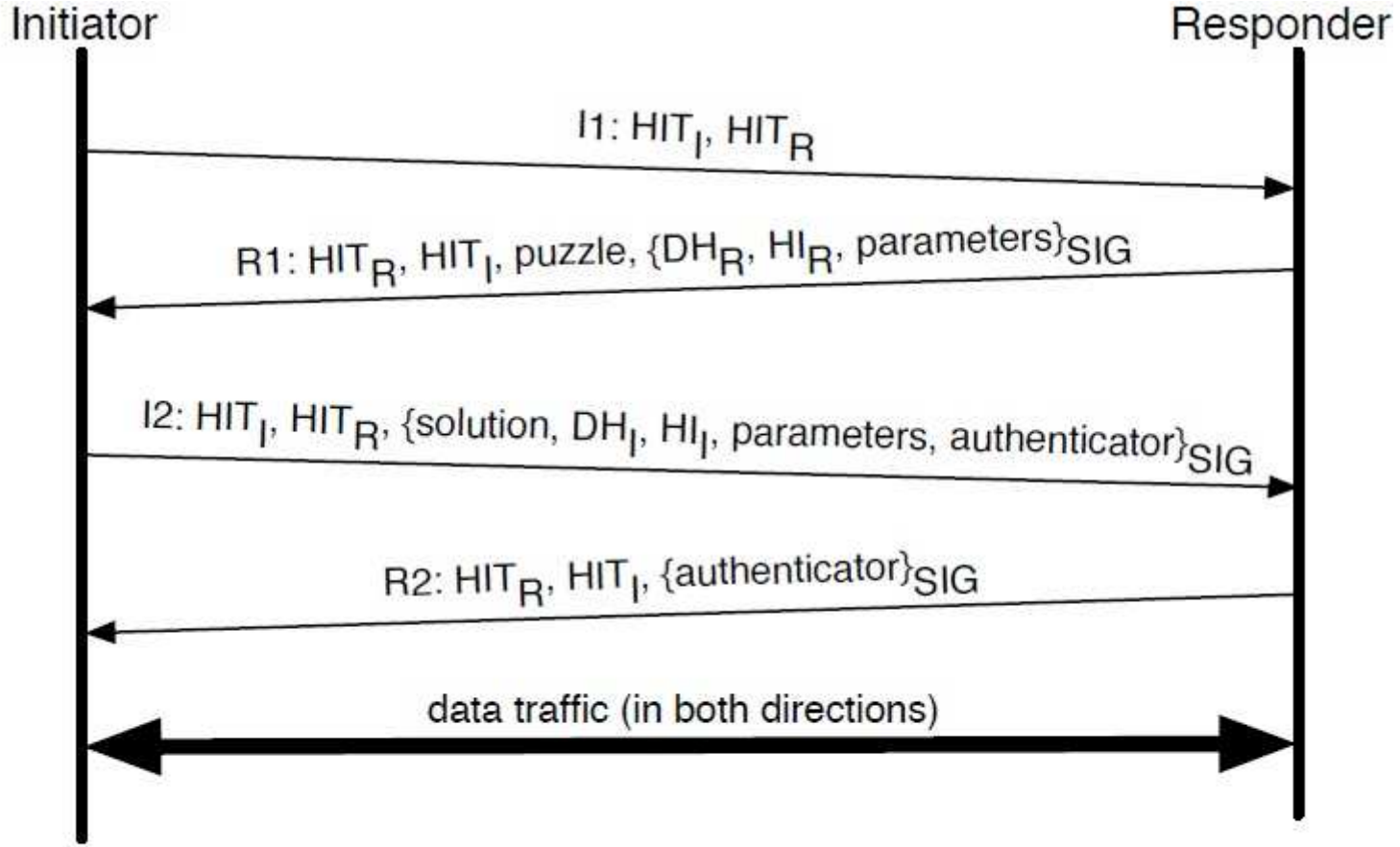
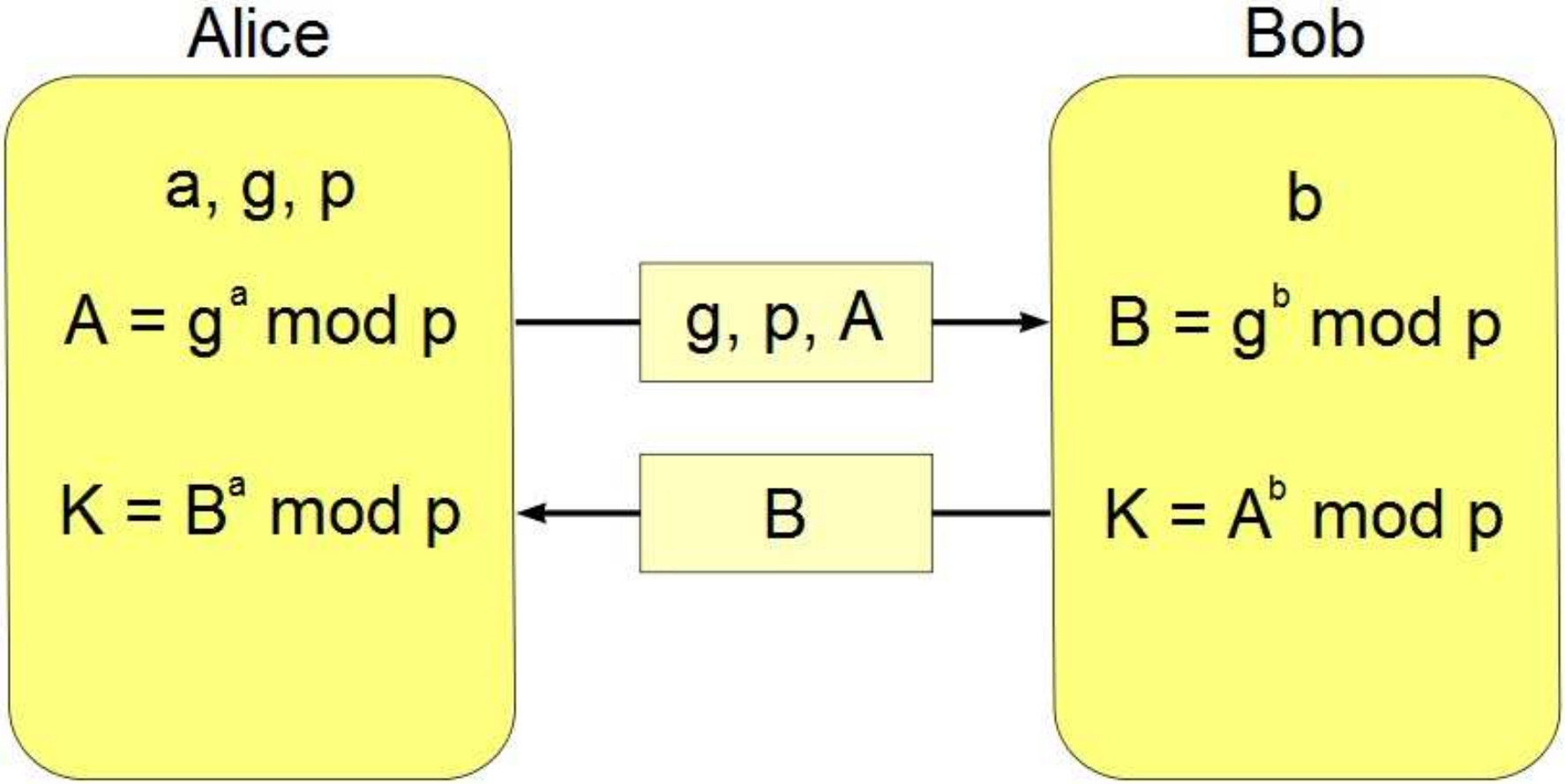


Fig. 4. HIP base exchange.

Diffie-Hellman



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

Thank you!

Q & A