Extending GONE with a DHT to improve end-to-end availability

Christian Dickmann
Advanced Topic in Internet Research
University of Göttingen, Jul. 2006
Outline

• Introduction
• Background
  – Gist Overlay Network Extension (GONE)
  – Distributed Hash Tables (DHTs)
• Motivation
• Solution approach
• Security considerations
• Conclusion
Introduction

• Todays internet faces alot of problems (availability, reliability, security, mobility, etc.)
• GONE is an overlay solution to (some of) these problems

• Distributed Hash Tables (DHTs) are recently studied by the research community and provide efficient distributed databases

• This presentation studies the use of DHT in GONE to improve availability of end-to-end communication
GONE Background (1)

• GONE is an path-coupled overlay network built upon GIST
  – GONE capable routers on the IP-path are discovered by GIST
• GONE maintains SCTP connections between GONE capable routers
  – Add support for multihoming and mobility to the „network layer“
• GONE utilizes capability concept
  – Not discussed in this work
GONE background (2)
GONE background (3)
DHT background (1)

• DHTs provide simple lookup service
  – Map key to value

• Interesting properties:
  – Peer-to-peer, no infrastructure, self organizing
  – Able to handle permanent joins and leaves (churn)
  – Fast lookup (log N), moderate state (log N)

• Popular DHTs include Chord, Pastry, Tapestry, CAN
Motivation of this work

• GONE is limited to (IP-)path-coupled overlay
  – Only multiple routes between GONE routers are utilized by SCTP (multihoming of GONE routers)

• Studies indicate, that a reasonable percentage of recoverable route/link failures can be recovered using „one-hop source routing“ (i.e. One off-path forwarder)

• Lookup of available off-path forwarders is non-trivial

• Idea: Build a DHT for lookup of off-path forwarders and extend GONE with „one-hop indirection“
One-hop indirection scenario

Internet core

AR 3
AR 1
AR 2
Outline

• Introduction
• Background
• Motivation
• Solution approach
  – Build a DHT in GONE
  – Store „Forwarder Advertisements“ in the DHT
  – Extend GIST to support one-hop indirection
• Security considerations
• Conclusion
Build a DHT in GONE (1)

• Which nodes should comprise the DHT?
  – 3 types of GONE nodes: end-hosts, access router, core router
  – Only routers are reasonable forwarders
  – Including end-hosts increases nodes in DHT significantly ➞ scalability problem
Build a DHT in GONE (2)

• How to form the DHT?
  – Requirements: Self-organized, autonomous
  – On node startup, the node creates a new DHT only including itself as a member
  – When router A meets router B, their DHTs are joined
  – Should $DHT_A$ join $DHT_B$ or the other way round?
    • $DHT_A$ joins $DHT_B$ for security reasons!

• Note: This approach requires efficient joins of two DHTs. Problem not well studied in the research community!
Build a DHT in GONE (3)
Build a DHT in GONE (3)
If a path between two GONE routers fails, an appropriate forwarder needs to be found.

Idea: GONE routers advertise their SCTP associations in the DHT. This is called „Forwarding Advertisement“ (FA).

FA is given by 4-tupel (Local-Node-Host-Ident, Peer-Host-Ident, Last-Updated-Time, FA lifetime).

FA is stored with Peer-Host-Ident as key.
• Example of operation:
  – Assume failure between GONE node A and B
  – A searches the DHT for key: Host-Ident-of-B
  – DHT provides a set of nodes advertising their connection to B
  – Set is ordered by some metric (e.g. Last-Updated-Time, Topological position, Bandwidth, Rating-system or some other metric)
  – Top most FAs in the set are tried as forwarders
  – If a forwarder is found, the traffic is now rerouted
  – Once the original path is available again, the traffic is switched back to that path
Extend GIST with one-hop indirection

- GIST is flexible regarding the message-routing-method (MRM) used to determine GIST nodes
- Default MRM is path-coupled (PC-MRM)
  - GIST finds nodes on the IP path
- A new one-hop-indirection MRM (OHI-MRM) needs to be defined
- Details are studied in the seminar report, out of scope today
Extend GIST with one-hop indirection
Outline

• Introduction
• Background
• Motivation
• Solution approach

• Security considerations
  – DHT security consideration
  – Integrity of Forwarding Advertisements
  – False-Friend-Attack

• Conclusion
DHT security consideration

• Anyone is allowed to join the DHT
• Malicious users can join DHT and e.g. delay or reroute queries, thus interrupt or slow down DHT operation
• Not studied in detail, as no particular DHT is studied here
Integrity of FAs (1)

• Hijack-Attack:
  – Insert a FA, and act as GONE forwarder, but perform a „off-path Man-in-the-Middle attack“
  – Indirection traffic could be encrypted or end-to-end encryption could be strongly advised

• Bogus-FA-Attack:
  – Insert a lot of bogus FAs in the DHT to make it unlikely, that a node is able to find a forwarder
  – The metric of ordering FAs could be extended to do validity checks and some trust relationship (if a router is known to be a bad forwarder, it gets a low score)
Integrity of FAs (2)

• Flood-Attack:
  – Node B inserts a lot of FAs advertising A as a forwarder, thus A is flooded
  – FA can be cryptographically protected to ensure that an FA advertising A is only issued by A (e.g. using the HIT)
  – Introduces processing overhead and is therefore interfering with the Bogus-FA-Attack
False-Friend-Attack

• False-Friend-Attack:
  – In GONE/GIST, signaling traffic is protected by a random SessionID
  – GONE forwarders learn Session IDs
    ➔ Later in time, they can use the SessionID and claim to be a forwarder again
  – Original nodes can exchange secret and change it when a forwarder learned the SessionID, but the original path is available again
    ➔ Only during the failure, the forwarder has the knowledge needed
Outline

• Introduction
• Background
• Motivation
• Solution approach
• Security considerations
• Conclusion
Conclusion (1)

- GONE is an on-path overlay network
- DHTs can be used as a scalable, efficient distributed database
- Studies indicate, that one-hop indirection is often sufficient to repair end-to-end availability in case of a recoverable failure

- This presentation showed:
  - How GONE can be extended to support one-hop indirection
  - How a DHT can be build and used to search for available GONE forwarders to be used with the one-hop-indirection
Conclusion (2)

• Summary of proposed solution:
  – DHT is build autonomously. Whenever DHT clouds meet, they join together
  – GONE routers issue Forwarding Advertisements for the connections they maintain in the DHT
  – A router experiencing a failure can search the DHT for these FAs and use the one-hop-indirection MRM to bypass the failure

• Summary of security considerations:
  – Hijack-Attack: „off-path Man-in-the-Middle attack“
  – Bogus-FA-Attack: Bogus FAs to render DHT useless
  – Flood-Attack: Flood a node by inserting false FAs
  – False-Friend-Attack: Forwarders learn SID and abuse it
Thank you for your attention!

Questions ?