
Vers de nouvelles architectures de type P4P



Marguerite Fayçal & Ahmed Serhrouchni

Forum ATENA – 30 octobre 2008

Contents

- Statement of the problem
 - Related work
 - Background
 - CAP: A Context-Aware P2P System
 - Conclusion
-

Contents

- Statement of the problem
- Related work
- Background
- CAP: A Context-Aware P2P System
- Conclusion

The problem

- P2P and IP networks do not match up
 - A single overlay hop involve multiple IP hops
 - Some suppositions of DHTs
 - Uniformity of location
 - Uniformity of resources
- A financial matter
 - buying and selling network capacities
 - terms of agreements between ISPs (Volume of traffic; max network BW; different costs; security & routing policies; dynamic configurations; etc.)
 - impact on clients
 - Quality of media streaming...
- A security problem
 - Fake objects
 - Communication Tracking
 - Clustering resources (virtual community; provider-oriented services)

Contents

- Statement of the problem
- Related work
- Background
- CAP: A Context-Aware P2P System
- Conclusion

Some existing architectural solutions

- Plethora
 - Two-layer system; local overlays according to AS
- Hieras
 - Multi-layer system based on link latency to landmark nodes
- Oracle Service
 - A service for ranking queries
- P4P (Provider Portal for P2P)
 - A kind of CDN (*iTracker*) applied to file-sharing network

Contents

- Statement of the problem
- Related work
- **Background**
- CAP: A Context-Aware P2P System
- Conclusion

Background - HMAC

- HMAC (keyed-Hash Message Authentication Code)
 - RFC 2104 : guarantee integrity between sender and receiver
 - $HMAC(h, k, m) = h(k \oplus opad, h(k \oplus ipad, m))$
 - $opad = 0x36$ (64 times) $ipad = 0x5C$ (64 times)
 - \oplus = bitwise XOR $'$ = concatenation
 - **Does not affect DHT's principle or existing P2P systems**

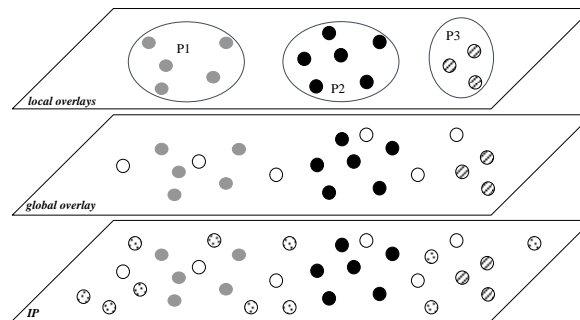
Contents

- Statement of the problem
- Related work
- Background
- CAP: A Context-Aware P2P System
- Conclusion

CAP: A Context-Aware P2P System (1)

- HKey \Rightarrow virtual DHT = VDHT
 - Simple HKey
 - Compound HKey = $h(HKey_1, \dots, HKey_n)$ } \Rightarrow 1 secondary layer
 - Derived HKey = dHkey
 - n ones \Rightarrow n secondary overlays
 - Profile (e.g. bootstrap node)
 - Examples:
 - Zone Identifier (AS Id; domain name; etc.)
 - group key (secret or not)
 - QoS parameter (min available BW, battery power, image quality, etc.)
 - Localization (network or real distance; country; etc.)
 - File type (".ram"; ".gif"; etc.)
 - File language or topic (metadata)

System overview



M. Fayçal & A. Serhrouchni

Vers de nouvelles architectures de type P4P

Forum ATENA

CAP: A Context-Aware P2P System (2)

- Routing mechanism
 - The same at each level, but with different identifiers and DHTs
 - Identifiers are computed first
 - searching the local overlay first
 - according to the preferences in the profile, in case of dHKey
 - caching at the local overlay
 - guarantee of contextual data retrieval
- Failures/disconnections
 - treated in the same way but independently at each level

M. Fayçal & A. Serhrouchni

Vers de nouvelles architectures de type P4P

Forum ATENA

CAP: A Context-Aware P2P System (3)

■ Join procedure

- Global overlay first, then local ones, after a *zone_table_request()*
- zone table = zTable
 - identifies a local overlay according to the profile
 - stored on a *rendezvous point* in the global overlay

Zone ID	Zone label	Largest nodeID	2 nd largest nodeID	2 nd smallest nodeID	Smallest nodeID
---------	------------	----------------	--------------------------------	---------------------------------	-----------------

- Zone Id = h (HKey) Zone Label = "HKey" (for conflict avoidance)
 - NodeIDs are in the global overlay
 - if zTable exists, then 'join(newid_{local}, HKey)'
 - if zTable does not exist:
 - zTable created and cached on the rendezvous point
 - Creation of the local overlay
- Comparison with the nodeIDs in the zTable

Contents

- Statement of the problem
- Related work
- Key derivation technique
- NETWORK Provider Oriented P2P System
- Conclusion

CAP - summary

- Context-awareness
 - Guarantee a data retrieval from the *zone* where it has been found
- Configurable
 - Identifiers computed with HMAC, based on HKey (simple; complex)
 - new virtual overlays (with VDHT) labeled HKey
- Extensible
 - *derived* HKey \Rightarrow multiple secondary overlays
- Independent of the initially implemented P2P routing protocol
- Message latencies are alleviated
- Lookup time are enhanced
- Caching mechanism
 - An advantage to less popular data

Thank you
Questions?

