A Distributed IP Multimedia Subsystem

Journal Club 2007-08 *Session #2*

Feb, 22th 2008

Xavier Milà

xavier[dot]mila[at]upf[dot]edu

Universitat Pompeu Fabra (UPF)

NeTSresearchgroup
Network Technologies and Strategies

Article Reference

Title: **A Distributed IP Multimedia Subsystem (IMS)**

[Author] M. Matuszewski, M.A. Garcia-Martin

[Appeared in] World of Wireless, Mobile and Multimedia Networks, 2007. WoWMoM 2007. IEEE International Symposium.

[Publisher] IEEE, Institute of Electrical and Electronics Engineers

[Publication date] 18-21 June 2007

[Digital Object identifier] 10.1109/WOWMOM.2007.4351728

[ISBN] 978-1-4244-0993-8

Introduction: IMS architecture (1)

- Home Subscriber Server (HSS) as an evolution of the GSM Home Location Register (HLR)
- HSS as a general repository for persistent user data (the central database)
  - Redundancy typically achieved by replicating the HSS data into a secondary HSS
  - The operator is forced to deploy new HSS units if the number of subscribers exceed the maximum limit.
  - a large HSS is typically costly for small networks.
- Subscriber Location Function (SLF): Diameter redirect server a single point of contact for Diameter clients. S-CSCF, I-CSCF, A
  - contains the range of addresses spaces that each HSS is allocated, it is locating the HSS that contains the user-related data.

Introduction: IMS architecture (2)

- Taking into account the previous constraints:
  - there is the possibility of *distributing the HSS* across different nodes which are configured in a distributed hash table (DHT) fashion.
    - Why DHTs? **they scale very well from 1 up to a very large number of nodes and allow for creating self configured networks with automatic replication capabilities**
- [Main Focus] to replace the IMS core network with self-organizing overlay network:
  - DHTs are able to react themselves to changes (fails or come
  - no operator intervention is required

Data Structure (1)

- DHT two basic operations:
  - PUT (key,value): stores the value of a given key in the DHT
  - GET (key) = value: returns the value of a given key which is already stored in the DHT.
- Values stored in the DHT node that is responsible for the key, re-distribution of the key space and of the storage.
- **What is a key in an IMS environment?**
  - each user allocated with
    - one or more *Private User Identities, IMPU* (e.g: Network Access identifiers) linked to one or more service profile and providing filter criteria, it de whether a request has to travel one or more AS.
    - and one or more *Public User Identities, IMPI* (e.g: SIP URI), are kn visible to users and are used to route SIP requests.

Data Structure (2)

- The 3 use cases for accessing the data:

1) [In real-time] An operator or a network node, knowing the IMPI, wants to access the user data to modify it.
   - to push the new filter criteria to the S-CSCF allocated to the user
2) [In real-time] A network node accesses the HSS to get the data associated to a given IMPU
   - for example during the registration attempt we want to obtain the registration status data (address of the S-CSCF, set of IMPIs, etc.)
3) [Not in real-time] The operator only knows partial information to start the search in the database (subscriber's name, family name, social security number, etc.)

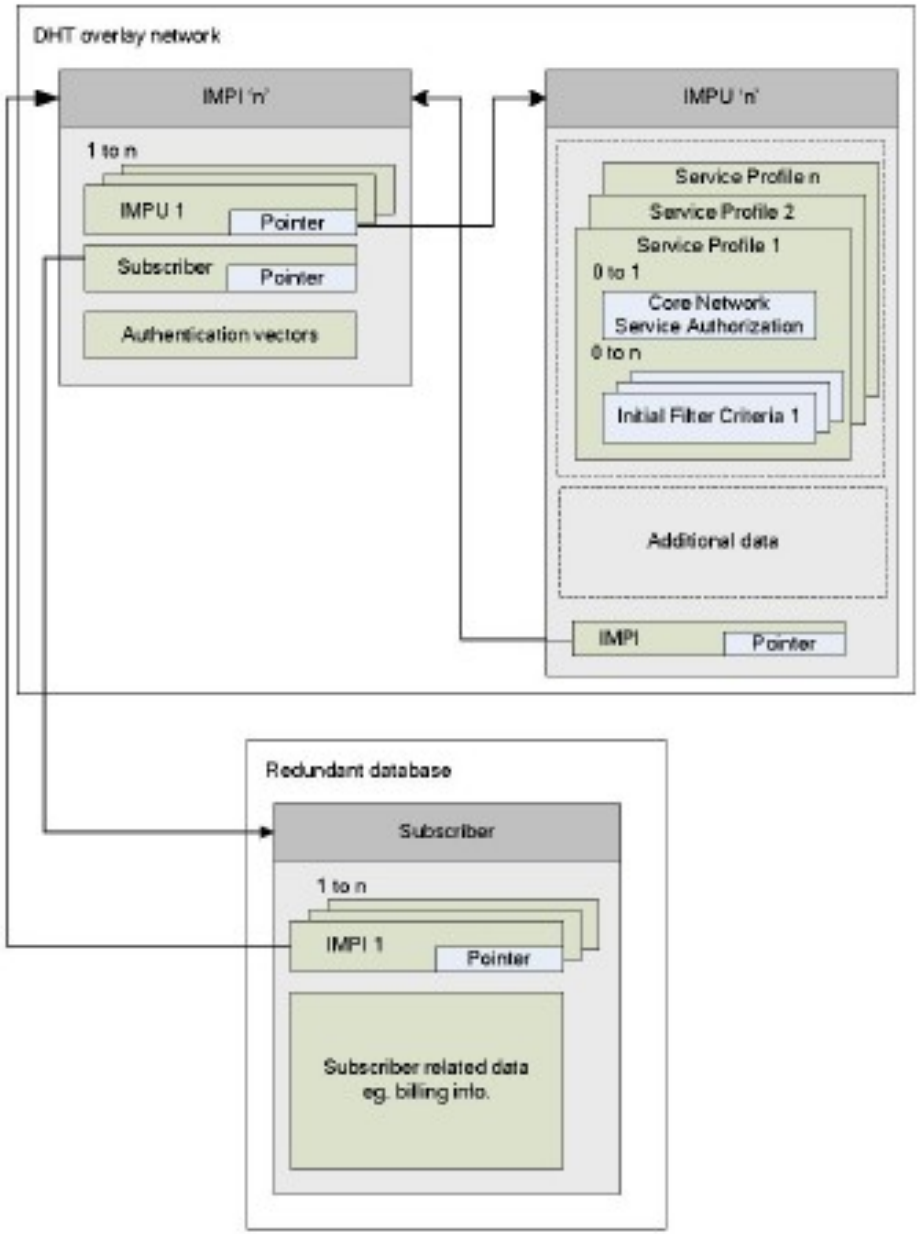
Not in real-time:

1) during operation and maintenance.
2) requires partial searches, “bad friends” of DHTs (require exact value)

Data Structure (3)

- Obtaining the keys for real-time traffic:
  - IMPI hashed to create a key composed by IMPU and authentication vectors,p.e.
  - IMPU hashed to create a key composed by IMPI, service profile (filter criteria).
- Obtaining the keys for non real-time traffic:
  - Each searchable string splitted into tokens and each token hashed.
- CONCLUSION regarding data:
  - *is better to continue with the current practice of storing the subscriber database in a single (redundant) database node.*
  - *At the operator's eye it will not be possible to determine which data is centrally stored and which one is stored in the DHT.*

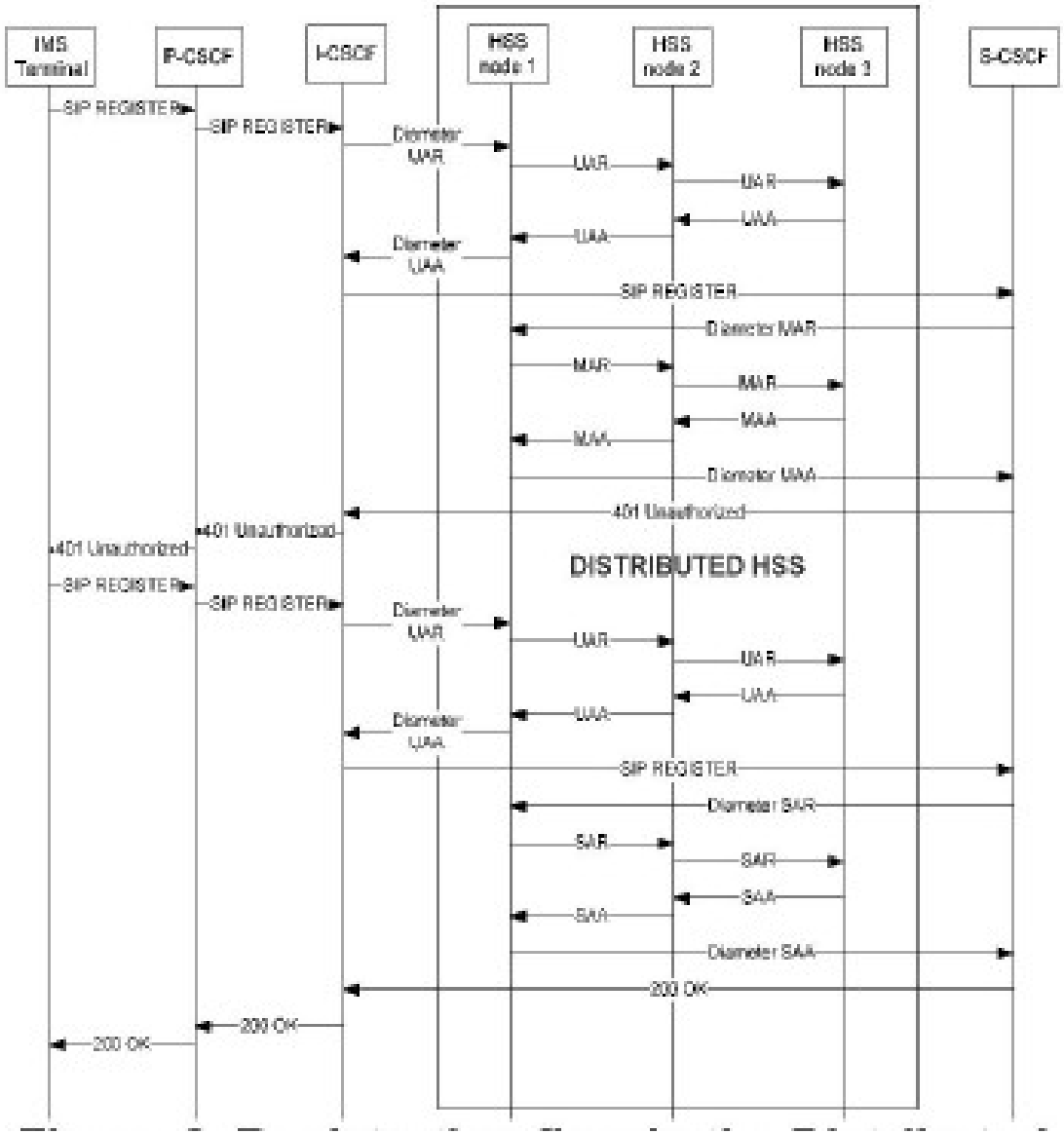
Distributed HSS overlay



Distributed HSS (HSS DHT)

- Data distributed across different HSS nodes
- Each HSS node have a pool of keys assigned and each key is stored in the closest successor responsible for that key (p.e.: with Chord algorithm)
- IMPIs and IMPUs share the same address space (not overlapping)
- The value pertaining to one key may contain ***pointers***:
  - to the HSS node that is storing the value of the IMPUs/IMPIs
  - to subscriber data stored in the subscriber data stored in the redundant database
  - Using pointers improves performance by removing multiple lookups for the same key, adding otherwise a bit more of complexity to keep pointers up to date.
- Data replicated for ensuring **ubiquitous** availability.
  - when a node fails another node automatically takes responsibility for the pc key-value pairs the failed node was responsible for.

Registration flow



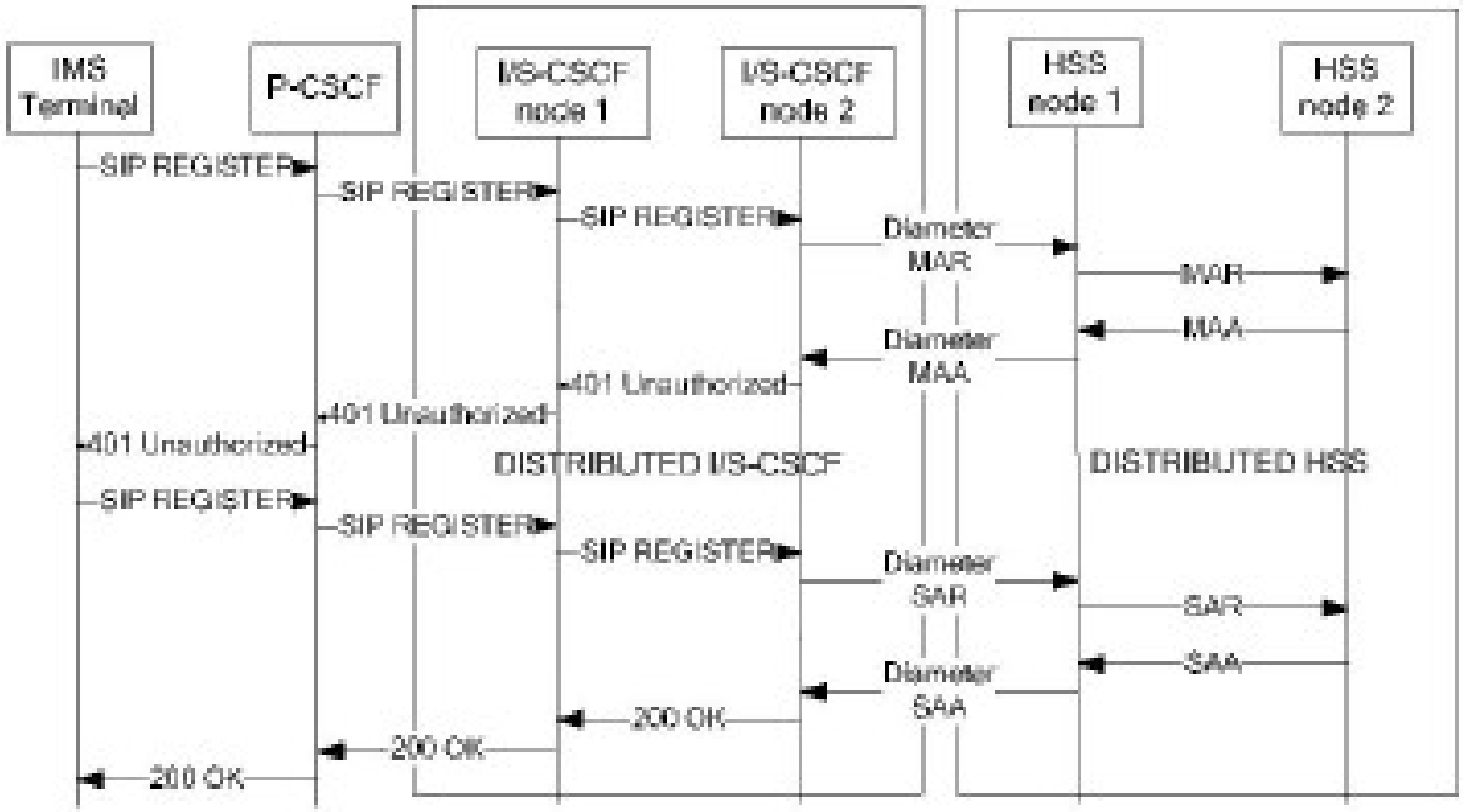
- S-CSCF serves the IMPU
- Diameter protocol for performing AAA (Authentication, Authorization and Accounting) functions.
- AKA (Authentication and key Agreement) can also be used with IMPI.
- Overlay -> HSS

Distributed I/S-CSCF (2nd DHT)

- Users with more than one allocated IMPU have their data spread across different I/S-CSCF nodes. There are, however, two main problems distributing this nodes:
  - First problem: *Only one node is actually authenticating the user.*
    - SOLUTION provided by DHT: If the first one is not capable to do it, a third party registration is required.
  - Second problem: *the standard IMS requires that all identities belonging to the same user are handled by the same S-CSCF*.
    - SOLUTION provided by DHT: restricting I/S-CSCF nodes to download a sigle authentication vector rather than downloading a bunch of vectors.
- Combining presence server and I/S-CSCF DHT node in a single node is good for handling all the SIP related data in a single node.

Merging both DHTs

- the number of Diameter messages is reduced because the DHT is able to find the S-CSCF that is serving the IMPU by itself.



Result: IMS DHT overlay

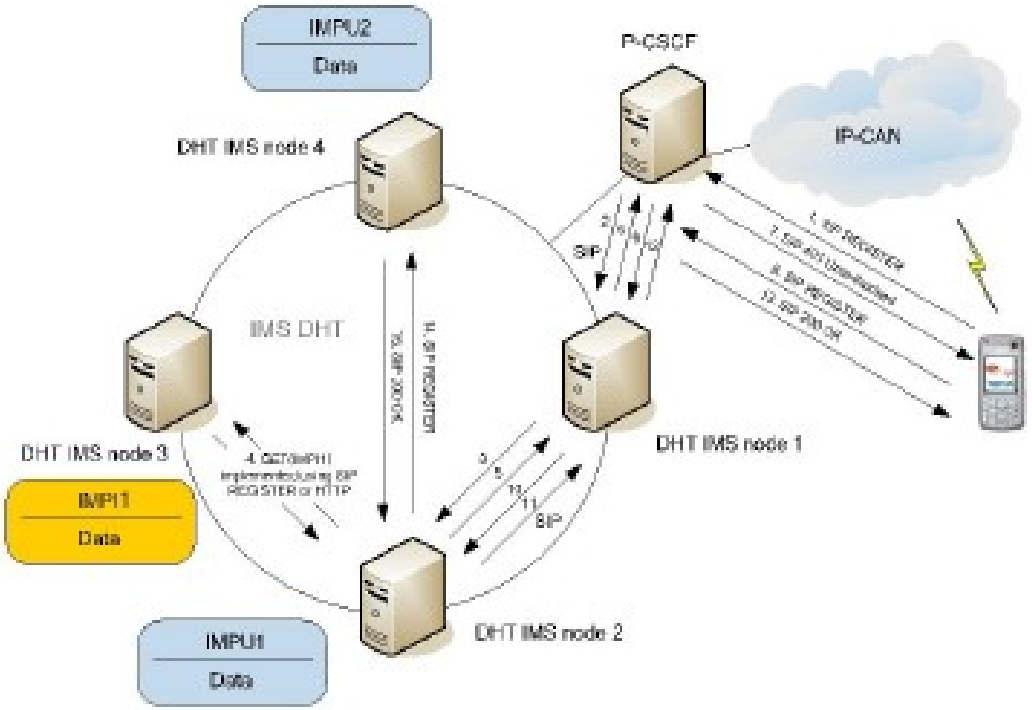


Figure 5. Registration in the IMS DHT overlay

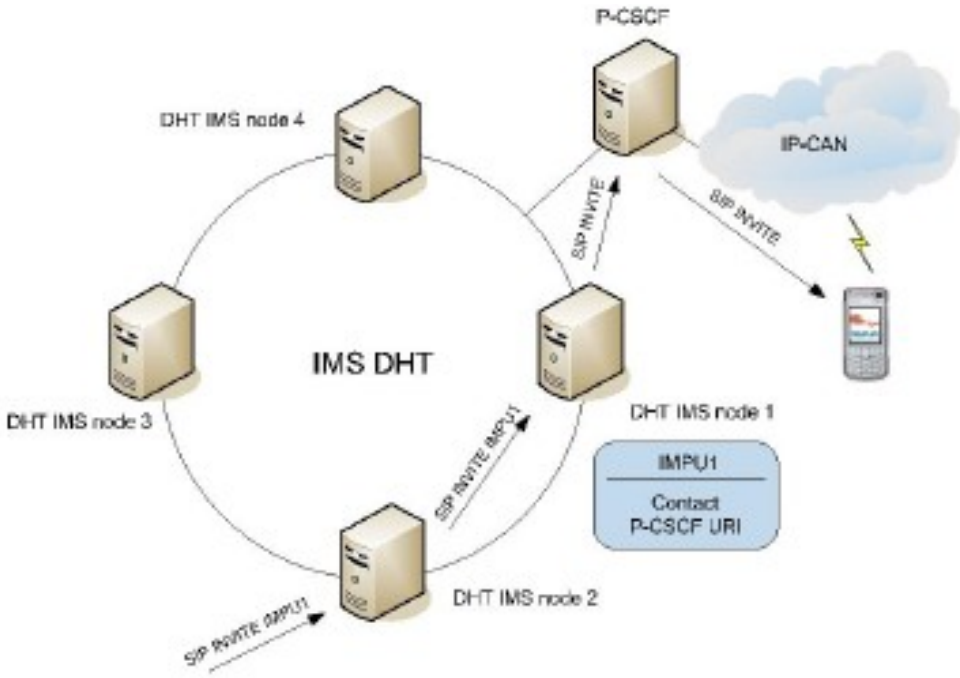


Figure 6. Incoming session attempt in the IMS DHT overlay

Authors Conclusions

- The overhead load depends on the used DHT algorithm
- there is no need for a Diameter protocol that allows CSCFs to download or query HSS-stored data.
- slightly higher number of messages for reasonably large DHT networks, the price to pay for having self-organization
- The robustness and self-organization properties of DHTs are able to significantly reduce the OPEX (operational costs)
- *a DHT composed of the combined enhanced HSS with I/S CSCF and presence server nodes is the best of the prese possible alternatives for the IMS.*