A Key Management Scheme for Content Centric Networks

Sarmad Ullah Khan, Thibault Cholez*, Thomas Engel*, Luciano Lavagno
Electronics and Telecommunication Department, Politecnico di Torino, Italy
***SnT, University of Luxembourg, Luxembourg**

Introduction to CCN

A new way to look at networking:

- **Content Centric Networking (CCN) :** proposal for an alternative paradigm to the current architecture of computer networks mainly based on TCP/IP.
- **Goal :** democratize Content Distribution and re-design the Internet by placing content, and not machines, at its core.

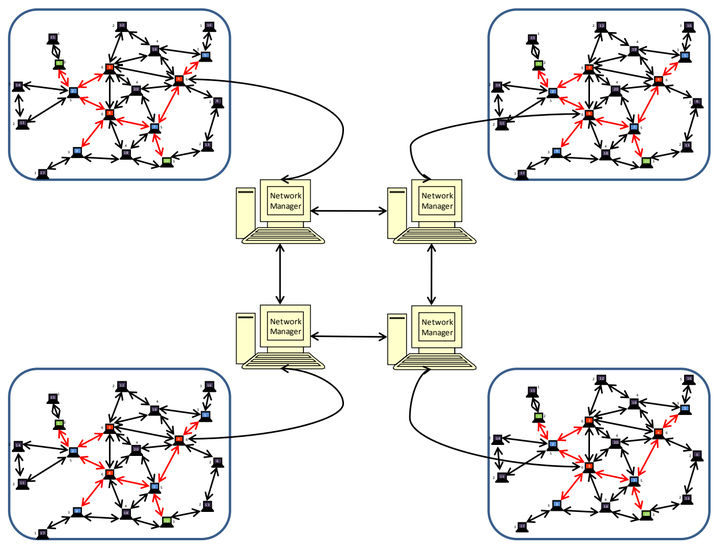
Key principles of Information Centric Networking:

- Named Data are better abstraction than named hosts : data as a name, not a location (data is directly addressed at the network level, not the computer storing it)
- Pull based model : consumer broadcast Interests in the network, Data are returned in response
- Anybody with the data can answer : all data are self-sufficient and authenticated
- Rely on replication and caching : data storage is proven heaper than bandwidth

Security:

- **Current Internet :** no built-in security mechanisms
  - No security of transported data : VPN, IPSec, SSL, etc. secure the conversation not the transmitted content (ex : spam in mailboxes despite secure connections)
  - Pay to get certificates
- **CCN :** digital signature in the core of CCN security, encryption for privacy
  - Trust in the content not in the way we got it : content is signed by the initial provider and bind to its name:

    Signature (Name; Content; SignInfo)
  - Open evidence based security, data provenance (traceability) can be checked
  - Request based routing, no classical DoS



Virtual network organization

Components:

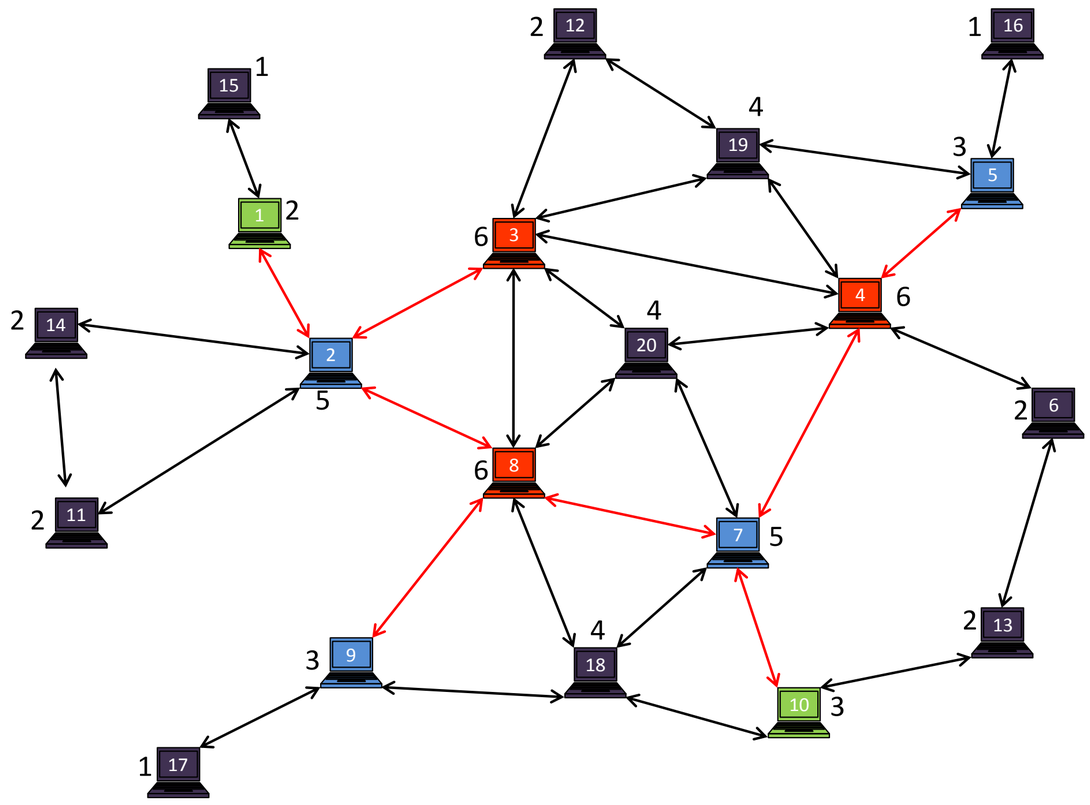
1. Network Manager
2. Key Holding Nodes
3. Normal Nodes

Performance Evaluation:

1. ccnSim

Security Validation:

1. AVISPA



A node with highest number of connections with neighboring nodes is selected as Key Holding Node (KHN)

Main/1st Level KHN

3rd Level KHN

2nd Level KHN

End nodes / Normal Nodes

Problem statement

- Every content must be authenticated at the Internet scale: How to design a distributed, efficient and secure key management?
- Encryption keys must be linked to content providers
- No key management scheme defined for CCN yet

Contribution

- A scalable distribution of keys to certify contents
- A mechanism that can also **certify the encryption keys**
- A secure mechanism to protect keys and contents from attackers
- Make both the content and the key dependent on each other

Key Ideas

- Distributed Key Holding Nodes for scalability and resilience
- Key shares to check authenticity and integrity of the key
- Keep the relationship between the content and the network of its provider: NeTwork Public Share (NTPS) and NoDe Public Share (NDPS)

Algorithm

Each node in the network is assigned a random number generator, a one way Hash function (H), a share generation function (f) and a natural number group generator G (G can be, for example, a prime number). NDRN and NTPS are sent on join by Network Manager.
Each network manager is also assigned a fixed random number (NMRN) assigned by the network owner, a random number generator, a one way Hash function (H), a share generation function (f) and a group generator G.

$K_{plc} = P_1 + P_2$

$P_1 = f(NTPS + Content)$

$P_2 = f(NDPS + P_1)$

$NTPS = f(NMRN; node\ ID; RN)$

$NDPS = f(NDRN; RN; NTPS)$

$K_{prt} = K_{plc}^{-1} \bmod G$

$X = Hash(P_1)$; $Y = Hash(P_2)$; $Z = Hash(K_{plc})$

$A = g^X$; $B = g^Y$; $C = g^Z$

Data packet = (Content; A;B;Z)
KHNs Have = (P_1; P_2;C;Z;NDPS)

KHNs send (NDPS;NTPS;C) to the key share requesting nodes

Evaluation

Scheme	Geant Topology (s)	Level3 Topology (s)	Tiger Topology (s)	dtelecom Topology (s)
PKI	0.009	0.020	0.003	0.0133
OUR	0.004	0.018	0.002	0.0131

Average time taken to retrieve a key for a content in different topologies

Technique	Summary
OFMC	SAFE
CL-AtSe	SAFE

Avispa simulation results

Acknowledgements: This work was partially supported by the European FP7 projects BUTLER (contract no: 287901) and IoT6 (contract no: 288445)