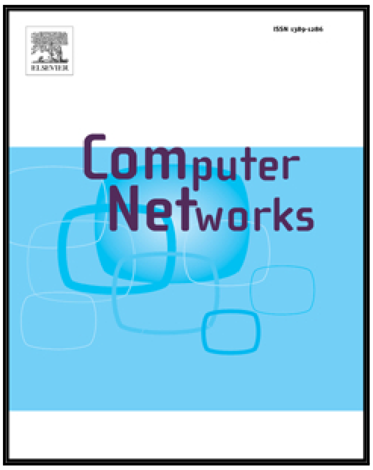
Accepted Manuscript



Up-to-date Key Retrieval for Information Centric Networking

Giulia Mauri, Giacomo Verticale

PII: S1389-1286(16)30366-8
DOI: 10.1016/j.comnet.2016.10.018
Reference: COMPNW 6041

To appear in: *Computer Networks*

Received date: 28 November 2015
Revised date: 23 June 2016
Accepted date: 31 October 2016

Up-to-date Key Retrieval for Information Centric Networking ☆

Giulia Mauri, Giacomo Verticale

Dipartimento di Elettronica, Informazione e Bioingegneria,
Politecnico di Milano,
Piazza Leonardo da Vinci, 32, Milano, Italy

Abstract

Information Centric Networking (ICN) leverages in-network caching to provide efficient data distribution and better performance by replicating contents in multiple nodes to bring content nearer the users. Since contents are stored and replicated into node caches, the content validity must be assured end-to-end. Each content object carries a digital signature to provide a proof of its integrity, authenticity, and provenance. However, the use of digital signatures requires a key management infrastructure to manage the key life cycle. To perform a proper signature verification, a node needs to know whether the signing key is valid or it has been revoked. This paper discusses how to retrieve up-to-date signing keys in the ICN scenario. In the usual public key infrastructure, the Certificate Revocation Lists (CRL) or the Online Certificate Status Protocol (OCSP) enable applications to obtain the revocation status of a certificate. However, the push-based distribution of Certificate Revocation Lists and the request/response paradigm of Online Certificate Status Protocol should be fit in the mechanism of named-data. We consider three possible approaches to distribute up-to-date keys in a similar way to the current CRL and OCSP. Then, we suggest a fourth protocol leveraging a set of distributed notaries, which naturally fits the ICN scenario. Finally, we evaluate the number and size of exchanged messages of each solution, and then we compare the methods considering the perceived latency by the end nodes and the throughput on the network links.

Keywords: Information Centric Networking, Named Data Networking, Digital Signature, Public Key Updating, Key Revocation, CRL, OCSP;

[☆] A preliminary version of this paper appears in G. Mauri, and G. Verticale, "Distributing Key Revocation Status in Named Data Networking", in *19th EUNICE Workshop on Advances in Communication Networking*, Aug. 2013.

Email addresses: giulia.mauri@polimi.it (Giulia Mauri), giacomo.verticale@polimi.it (Giacomo Verticale)