Journal of Network and Computer Applications 50 (2015) 60–63

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Special issue on information-centric network architecture, protocols, algorithms and applications

Information Centric Networks (ICNs) are relatively a new paradigm of communications in Future Internet. ICNs strive to disseminate information regardless of its physical location. In other words, information can be accessed using its name rather than IP addresses, hence the information can be disassociated from its specific location. ICN is introduced mainly to address an increasing demand for highlight scalable, timely and efficient distribution of information. It will have a huge impact on the way we perceive communication systems, the design of future networking architectures, and in particular the trade-off we consider in the specifications of future protocols and the possibilities for new services. However, for the success and wide deployment of ICNs, a number of critical issues have to be addressed:

- Information naming and addressing: The IP-address is the predominant addressing scheme in the current Internet. With IP-addresses, a single number-space is used to define the host/device as well as its location. ICNs aim to identify information in a location-independent manner, hence, the need for a new addressing scheme.
- Network architecture and protocols: Despite its simplicity, the TCP/IP stack has been main protocol suit for communications in the Internet. It is arguable that without additional protocols, the TCP/IP will facilitate the unique features of the Future Internet such as the ICNs. However, the extra added functionalities to the TCP/IP might not come without side effect in terms of incompatibility and increasing the stack complexity.
- Resource management: One unique feature of ICNs is in-network caching of data contents. However, this feature will have a profound effect on network resources in terms of managing the storage capacity of all network nodes. Furthermore, to provide an efficient distribution of popular cached data raises challenges in terms of buffer management and caching policy.
- Power consumption and energy efficiency: There is a driving need for more energy-efficient network elements from the core to the access network. Considering the features of in-network storage and process of ICNs, there is a need for ICNs to trades-off between these features and energy consumption.
- Security: ICNs radicalize the communication and internetworking systems and consequently will bring about new security challenges in addition to current ones witness in the Internet. Research work in the area of security for ICNs is still in an early stage; there is a need for defining threat models and proposing security mechanisms.

The call of this special issue was aimed at collecting original papers that contribute on ICN architectures, algorithms, protocols, and applications, especially with an emphasis on real world problems and experimental investigations. The special issue call has attracted submission of 41 papers. However, only 11 papers have been accepted as the result rigorous review process; that is equal to a low acceptance rate of approximately 27%. The focused has always been on papers with outstanding contributions to one or more of the above topics in ICNs. Below we briefly describe the scope of each accepted paper.

A new information-centric network architecture called Network of Information (NetInf) has been developed in the context of the FP7 EU-funded 4WARD project. This architecture can significantly improve large scale information distribution. Furthermore, it supports future mobile networks in situations with intermittent and heterogeneous connectivity and connects the digital with the physical world to enable better user experience. However, NetInf is still in an early stage of implementation and its security is yet to be evaluated. The security concern of NetInf is a major factor for its wide-scale adoption. In their paper, “Challenges and Solutions for Secure Information Centric Networks: A Case Study of the NetInf Architecture”, Loo and Aiash, this issue use the X.805 security standard to analyze the security of the NetInf architecture. The analysis highlights the main source of threats and potential security services to tackle them. The paper also defines a threat model in form of possible attacks against the NetInf architecture and highlights potential security services.

While research efforts in the area of secure ICNs considers Information-Focus approaches where security measures are attached to data contents, in their paper “An Integrated Authentication and Authorization Approach for the Network of Information Architecture”, Aiash et al. argue that such measures are not enough on their own. Considering the Network of Information (NetInf) as an example of ICNs, the paper highlights Infrastructure-Security threats and demonstrates a new attack in the form of masquerading and content poisoning attacks through invalid data registration. To address the discovered attack, a new security protocol is proposed to identify and authenticate hosts before being able to access the NetInf system. Furthermore, a capabilities-based access policy has been introduced to mitigate the issue of unauthorized access to data objects. The proposed solutions have been formally verified using formal methods approach.

ICN is an approach to evolve the Internet infrastructure away from a host-centric paradigm based on perpetual connectivity and the end-to-end principle, to a network architecture in which the

http://dx.doi.org/10.1016/j.jnca.2014.11.003

focal point is “named information” (or content or data). In this paradigm, connectivity may well be intermittent, end-host and in-network storage can be capitalized upon transparently, as bits in the network and on storage devices have exactly the same value, mobility and multi access are the norm and anycast, multicast, and broadcast are natively supported. In their paper, “SIONA: Service and Information Oriented Network Architecture”, Ming et al. present a service and information based network architecture to fully optimize resources wherever they are. They describe SIONA's key design elements and illustrate how SIONA facilitates service-aware communication, name-based content delivery and mobility support, while keeping the network scalable and efficient. They implement Name-based Sockets (NBS) as a new transport application programming interface (API) for applications to use names instead of addresses. They develop a lightweight age-based cooperative caching scheme to improve content distribution in the network layer. They build an example system to show the feasibility and ease of use of SIONA. They conduct experiments in real networks to evaluate SIONA's transportation performance and perform a trace-based simulation to evaluate their caching scheme. Results show the advantage of the proposed approach compared with the existed solutions.

In ICN architectures, all network primitives involve named pieces of content: clients request content by name and servers respond with the corresponding content pieces. This allows the network to easily recognize requests for the same content and serve them via a single multicast transmission, so as to optimize content distribution. Even though all proposed ICN architectures support native multicast at the network layer, the unreliable service they provide is insufficient for applications requiring reliable information distribution, such as operating system patches and updates. In their paper, “A Reliable Multicast Transport Protocol for Information-Centric Networks”, Stais et al. propose a new transport layer protocol, RMTPSI, for the Publish/Subscribe Internet (PSI) ICN architecture, which can support either fully or partially reliable transmissions, depending on what each individual receiver deems appropriate. RMTPSI draws upon previous work on reliable multicast for IP networks, in particular on the well-known PGM protocol, using hierarchical feedback aggregation to avoid sender implosion with very large multicast groups. On the other hand, RMTPSI exploits the explicit routing scheme used by PSI to achieve not only native multicast for content distribution, but also reverse multicast for feedback reports. Finally, RMTPSI operates in rounds of transmissions and retransmissions, thus allowing each receiver to individually decide which level of reliability is sufficient for the application at hand. When used over a PSI network for reliable file transfers, RMTPSI is more efficient than PGM in the use of both downstream and upstream bandwidth, while offering similar download times.

Internet is suffering from severe data explosion problems due to introduction of new services which require Internet connection as well as increase in the number of content consumers. These problems give rise to the occurrence of redundant and bulk traffic while increasing the considerable burden on the network and content server. A content centric networking (CCN) is a newly emerging future network architecture that is designed to solve those problems by utilizing in-network caching and name-based packet forwarding functions. In order to provide efficient caching and content retrieval method, in their paper “Cache Capacity-aware Content Centric Networking under Flash Crowds”, Kim et al. investigate new caching and routing schemes that interact with each other to encompass cache management and cache-aware request forwarding. Their proposed selective caching scheme considers both content popularity and cache capacity, which makes popular contents to be probabilistically stored close to the content requester while maintaining cache diversity of routers on the path. During the content delivery, nodes that do not have chance to cache the contents in their cache maintain temporal information about the direction of the content has delivered. Then the node can re-route the following content request message toward the near CCN node according to the temporal information instead of forwarding the request toward content server. Compared with the well-known cache strategies in CCN, the proposal has several advantages, such as network load reduction, server load reduction, link stress reduction, and content retrieval time reduction.

Large attention is currently being devoted to data-centric networking, aiming to mitigate the mismatch between the host-based Internet architecture and the way users aim to share and access content-agnostic of content location. The aim is to devise a data-centric solution for the global Internet. However, no current framework is suitable for pervasive networking scenarios, encompassing a large number of wireless mobile devices, which can operate as sources, forwarders and destinations of data. In their paper, “Combining Data Naming and Context Awareness for Pervasive Networks”, Mendes et al. presents an Information and Context Oriented Networking framework (ICON) able to allow fast deployment and efficient operation of data-centric networking over pervasive networks, by combining social-aware forwarding, the capability to sense users' context, and the support of different naming schemes. Efficient data sharing is achieved by incorporating a social-aware opportunistic algorithm that does not require the usage of bread crumbs reverse paths, as done by data-centric networking approaches such as CCN and NDN. Besides the opportunistic forwarding property, ICON also fulfills other major requirement of pervasive systems: adaptation without disruption of operation. This goal is achieved by allowing modules to be replaced at runtime, by using dependency injection, and to be configured by a set of management rules. For data management, the used in-network caching is based on a simple LRU replacement policy, to show that a good network performance can be achieved with a simple caching implementation. As future work, cache entries may be removed based on the inference about their importance to neighbour devices.

Accurate and timely knowledge of network topology is essential for the achievement of efficient content delivery in ICN. However, due to the dynamics of information consumer and information provider mobility, fueled by massive proliferation of social media and by widespread use of portable user devices, design of a scalable topology management function is a challenging research problem. In their paper “Scalability of Information-Centric Networking using Mediated Topology Management”, Alzahrani et al. investigate the scalability of an ICN system that uses mediation between information providers and information consumers and is based on a publish/subscribe delivery mechanism. They estimate the workload of the mediated topology management function by extrapolating current IP traffic models for a typical national-scale network provider in the UK. It is demonstrated that the mediation workload is on a scale that is comparable to, or less than, that of current IP routing. At the same time, the considered ICN forwarding mechanism requires considerably smaller tables, compared to the current IP routing tables. It is also shown, that although the topology management function is termed a central function, it can be distributed among an arbitrary number of topology manager instances. Finally, the work shows that the scalability of the considered ICN system is not affected by additional security mechanisms. In particular, the incorporation of a security mechanism that mitigates against maliciously injected packets has been investigated. This mechanism is able to stop