Information-centric Routing for Opportunistic Wireless Networks

Paulo Mendes
COPELABS, University Lusofona
paulo.mendes@ulusofona.pt

Rute C. Sofia
COPELABS, University Lusofona
rute.sofia@ulusofona.pt

Jose Soares
COPELABS, University Lusofona
jose.soares@ulusofona.pt

Vassilis Tsaoussidis
Democritus University of Thrace
vtsaousi@ee.duth.gr

Sotiris Diamantopoulos
Democritus University of Thrace
diamantopoulos.sotiris@gmail.com

Christos-Alexandros Sarros
Democritus University of Thrace
csarros@ee.duth.gr

ABSTRACT

This poster describes DABBER, a protocol developed to extend the reach of Named Data Networking into wireless environments. Our key contribution lies in the fact that DABBER supports communication in opportunistic wireless environments by relying on data reachability metrics that take into consideration availability and centrality of adjacent nodes, as well as the availability of different data sources. The poster provides an overview to the DABBER architecture, and of the available open-source implementation.

CCS CONCEPTS

• **Networks → Routing protocols**;

ACM Reference Format:
Paulo Mendes, Rute C. Sofia, Jose Soares, Vassilis Tsaoussidis, Sotiris Diamantopoulos, and Christos-Alexandros Sarros. 2018. Information-centric Routing for Opportunistic Wireless Networks. In *5th ACM Conference on Information-Centric Networking (ICN '18), September 21–23, 2018, Boston, MA, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3267955.3269011

1 INTRODUCTION

In networking scenarios with an increasing number of wireless systems, there are two networking paradigms highly correlated to the efficiency of pervasive data sharing: Information-Centric Networking (ICN), and opportunistic wireless networking. The latter refers to multi-hop wireless networks where finding an end-to-end path between any pair of nodes at any moment in time may be a challenge.

Combining opportunistic networking with ICN frameworks, such as Named-Data Networking (NDN), is relevant to extend the applicability of ICN to novel scenarios, such as affordable pervasive access, low cost extension of access networks, edge computing, and vehicular networks.

The Data reAchaBility BasEd Routing (DABBER) protocol [5] has been developed in this context. One of the key requirements to support end-to-end ICN communication is, in our opinion, interoperability [1]. Therefore, DABBER takes into consideration the routing being deployed within ICN networks, while considering new principles related with data reachability aspects, as well as contextual-awareness about network operation [6] to ensure adaptation to wireless environments.

ACM ICN'18, September 21–23, 2018, Boston,MA,USA

ACM ISBN 978-1-4503-5959-7/18/09.
https://doi.org/10.1145/3267955.3269011

2 DABBER ARCHITECTURE

The four major considerations driving the design of DABBER are: i) opportunistic networking is agnostic of the complete network topology; ii) network flooding must be avoided; iii) selecting the best set of neighbors to transmit Interest packets may not be efficient if based only on inter-contact times and contact duration; iv) interoperability should be achieved towards routing protocols in fixed ICN networks.

In terms of fixed networks, a well known NDN routing solution is the Named Data Link State Routing Protocol (NLSR) [3]. DABBER has therefore been designed to be compatible with NLSR, by considering the same message format and data structures, such as the Forwarding Information Based (FIB) and Routing Information Base (RIB), used by the NDN Forwarding Daemon (NFD). DABBER relies on ChronoSync [8] to exchange routing information among neighbors, ensuring the needed interoperability between DABBER mobile devices and NLSR edge routers. However, since DABBER only requires the dissemination of Prefix LSAs, it ignores Adjacency LSA passed by NLSR routers. Another difference towards NSLR is that DABBER does not compute shortest paths: the path cost metric of NLSR is replaced with a data reachability cost metric, reducing the impact that topological changes would have on routing stability.

A DABBER implementation is available on Google Play [1] and GitHub [2]. DABBER has been tested in emergency scenarios with intermittent connectivity based on a novel NDN instant messenger, Oi! [4, 7], and by exploiting Wi-Fi direct connectivity, based on a new NDN Android branch called NDN-OPP [[2], which code is also available on GitHub [3].

2.1 Naming Aspects

DABBER makes use of NDN hierarchical naming scheme to identify each wireless node. This strategy is similar to the one used by NLSR. In wireless networks, a hierarchical naming scheme identify the operator and home network of each node. Based on the operation of mobile networks, the following semantics is used: */<network>/<operator>/<home>/<node>*, where *<network>* represents

[1] https://play.google.com/store/apps/details?id=pt.ulusofona.copelabs.ndn
[2] https://github.com/COPELABS-SITI/ndn-opp/tree/dabber
[3] https://github.com/COPELABS-SITI/ndn-opp

the international transit network allowing roaming services; <*operator*> refers to the mobile operator; <*home*> is the node home network; <*node*> is the mobile device. The hierarchical name is used to implement the trust model described in section 2.3.

2.2 Next Hop Computation and Data Reachability Metrics

To support the forwarding of Interest packets, DABBER considers that there is a set of potential next-hops via which a Name Prefix N can be reached with a certain cost k: this cost represents the probability of reaching a data object identified by N via a certain neighbor, and is related to the time validity of the Name Prefix announced by that neighbor, as well as the capacity of such neighbor to forward the Interest packet. The validity of a Name Prefix is set by the data source as an integer that represents the expiration date of the data.

DABBER relies on four different categories of weights to select the best set of neighbors to reach data related to each Name Prefix in opportunistic wireless environments.

From a node perspective, it considers node availability (A) and node centrality (C). While A provides a measure of the internal status of a node (e.g., low battery, low storage), C provides a measure of the external (neighborhood) status.

From a link perspective, it considers node similarity (I) that measures the clustering similarity between nodes.

DABBER considers also a path weight cost (T) to measure the availability of different data sources. Such path cost is based on the validity of disseminated Name Prefixes, and on time-to-completion measurements (time lapse between forwarding of an Interest packet and receiving the respective data packet).

DABBER gathers periodic information about A, C, and I weights via internal communication with a software-based agent that runs in background in wireless devices, the Contextual Manager (CM) [6]. The CM seamlessly captures wireless network smart data and computes costs of different node aspects, such as the neighborhood status and usage of internal resources.

2.3 Security Considerations

DABBER routing messages are carried in NDN data packets containing a signature. Hence, DABBER can verify the signature of each routing message to ensure that it was generated by the claimed origin node. For this propose, DABBER makes use of a trust model for routing to verify the keys used to sign the routing messages, based on the hierarchical name structure (c.f. section 2.1).

With this hierarchical trust model, one can establish a chain of keys to authenticate LSAs. Since keys must be retrieved in order to verify routing updates, DABBER allows each node to retrieve keys from its neighbors. This means that a DABBER node uses the NDN Interest/Data exchange process, with Interests of the type /<network>/broadcast/KEYS, to gathers keys from its direct neighbors. In case a neighbor does not have the requested key, the neighbor can further query its neighbors for such key.

3 DABBER OPERATION

The DABBER operation is illustrated in Figure 1. The Name Prefix Manager acts as the interface towards the Chronosync, from which it receives notifications when a neighbor updates a Name Prefix LSA. The Name Prefix Manager then determines if the updated LSA should be retrieved. The Name Prefix Manager is also used to notify the Chronosync when local LSAs are updated.

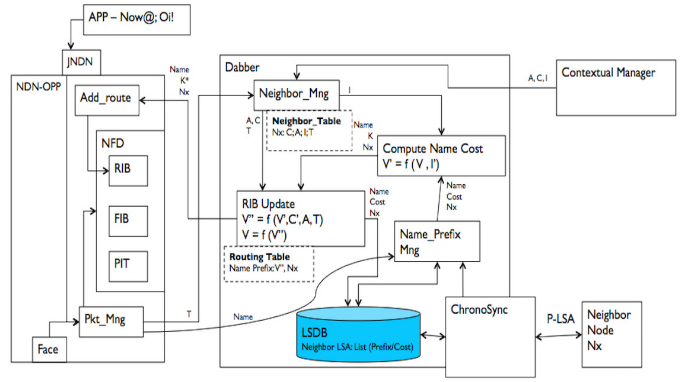

Figure 1: DABBER Architecture.

When DABBER is notified that a neighbor as posted/updated a new Name Prefix LSA, it computes a new cost for each name prefix in such LSA, based upon the cost announced by the neighbor, and the data reachability metrics towards that neighbor (c.f. section 2.1). Once costs are updated, DABBER interacts with the RIB of NFD based on the Downward Path Criterion. The FIB is then updated from the RIB, following the regular NDN operation (a multicast forwarding strategy is used). Periodically, DABBER recomputes the cost of each Name Prefix in its internal routing table, adapting to changes of the data reachability metrics. This operation is followed by the update of the RIB, and the update of its own Name Prefix LSA in the Link State Data Base (LSDB) used by ChronoSync.

ACKNOWLEDGMENTS

This research received funding from the European Union (EU) Horizon 2020 program under grant agreement No 645124 (UMOBILE: Universal, mobile-centric and opportunistic communications architecture).

REFERENCES

[1] Bernard Aboba and Dave Thaler. 2008. *What Makes for a Successful Protocol?* Technical Report. IETF RFC5218.

[2] Seweryn Dynerowicz and Paulo Mendes. 2017. Named-Data Networking in Opportunistic Networks. In *Proc. of ACM ICN*. Berlin, Germany.

[3] Vince Lehman, A Mahmudul Hoque, Yingdi Yu, Lan Wang, Beichuan Zhang, and Lixia Zhang. 2016. *A Secure Link State Routing Protocol for NDN.* Technical Report. NDN Technical Report NDN-0037.

[4] Luis Amaral Lopes, Rute C. Sofia, Paulo Mendes, and Waldir Moreira. 2016. Oi! - Opportunistic Data Transmission based on Wi-Fi Direct. In *IEEE Infocom 2016 (Demo)*. San Francisco, USA.

[5] P. Mendes, R. Sofia, V. Tsaoussidis, S. Diamantopoulos, and C. Sarros. 2018. *Information-centric Routing for Opportunistic Wireless Networks.* Technical Report. IETF Internet Draft (draft-mendes-icnrg-dabber-00).

[6] Rute C. Sofia. 2018. *The UMOBILE Contextual Manager Service.* Technical Report. Technical Report Senception 001.

[7] Miguel Tavares, Omar Aponte, and Paulo Mendes. 2018. Named-data Emergency Network Services. In *in Proc. of ACM MOBISYS (poster)*. Munich, Germany.

[8] Zhenkai Zhu and Alexander Afanasyev. 2013. Let's ChronoSync: Decentralized dataset state synchronization in named data networking. *in Proc. of International Conference on Network Protocols* (2013).