# Supporting the IoT over Integrated Satellite-Terrestrial Networks using Information-Centric Networking

Vasilios A. Siris, Yiannis Thomas, and George C. Polyzos

Mobile Multimedia Laboratory
Department of Informatics, School of Information Sciences and Technology
Athens University of Economics and Business, Patission 76, 104 34 Athens, Greece
{vsiris, thomasi, polyzos}@aueb.gr

***Abstract*—We investigate the control and data message overhead when the IoT is supported over an integrated satellite-terrestrial network based on Information-Centric Networking (ICN). We consider a scenario where IoT sensor networks are connected via LEO satellites and present three optimization models: polling and data aggregation at a proxy, confidential data transfer using a single proxy, and individual proxy for each IoT node. The three models are implemented in an integrated ICN testbed that consists of a Publish-Subscribe Internet (PSI) prototype and the OpenSAND satellite emulation. The experimental results show that the optimization models, utilizing PSI's mechanisms, can significantly reduce the satellite traffic load while supporting different levels of security.**

***Index Terms* — Information-Centric Networks; Internet of Things; control and data overhead**

## I. Introduction

Inefficiencies of the current Internet architecture related to content delivery, traffic management, mobility, etc, have been highlighted along with the complexities of proposed work-arounds. The root of these inefficiencies is the current Internet's host-centric communication model that does not match its dominant usage, which involves information exchange and service access independent of the device where the information is located or that provides the service.

To address the above limitation, a number of research initiatives have proposed Information-Centric Networking (ICN) as the fundamental paradigm for the Future Internet [5]. ICN architectures decouple the data (service) from the actual devices storing (providing) it through location-independent naming. ICN's rendezvous (RV) service is responsible for locating the desired content, by matching information requests to publishers where the content is available.

The above decoupling facilitates data collection and data dissemination, thus allowing the seamless and efficient support for many/any-to-one, one-to-many/any, and many/any-to-many/any deliver modes. Such delivery modes are the basis for machine-to-machine communications and the Internet of Things (IoT). Satellite networks can augment these capabilities with their broadcasting support and wide-area coverage [1], allowing them to cover areas that are not (or not adequately) covered by terrestrial cellular systems.

The goal of this paper is to present and evaluate models for supporting IoT over integrated satellite-terrestrial networks using an Information-Centric Networking architecture. In such networks, aside the data traffic, the amount of control traffic transmitted over the satellite network is important [1][2]. In addition to the data and control overhead, the security and privacy properties of data transfer can be important. The optimization models we investigate consider trading data and control overhead for enhanced security.

The remainder of this paper is structured as follows. In Section II we discuss the IoT application scenario considered in this paper, which involves IoT sensor networks connected via LEO satellites. In Section III we present three models for supporting the IoT application scenario over integrated satellite-terrestrial networks using an ICN architecture. In Section IV we present experimental results from the implementation of the models in a testbed that includes the prototype implementation of the Publish-Subscribe Internet (PSI) ICN architecture [4], and satellite emulation using OpenSAND [6]. Finally, in Section V we conclude the paper.

## II. IoT Scenario

The application scenario considered in this paper involves collecting environmental data from massively deployed IoT sensors over a wide-area. The data typically consists of periodic or highly irregular message transmission, low message rates, and small message sizes. Message and control aggregators can be located on the ground or on board satellites, to enhance efficiency and scalability.

The logical entities and their corresponding functionality for this scenario are the following, Fig. 1.

- Data collector (Subscriber): Sends requests (subscriptions) for data updates from IoT sensor nodes.
- IoT sensor nodes (Publishers): Respond to update requests.
- Message aggregator (proxy): This entity can receive subscriptions from the data collector and forward data updates received from IoT nodes.

This work was supported in part by the European Space Agency (ESA) through the Satellite Network of Experts IV (SATNEX IV), Call-off Order 1, Work Item 5: Impact of future ICN traffic on multiple access schemes.

## III. ICN Optimizations Models for Supporting the IoT

Next we discuss three optimization models for the scenario discussed in the previous section, which involve different control and data message exchange between the entities.

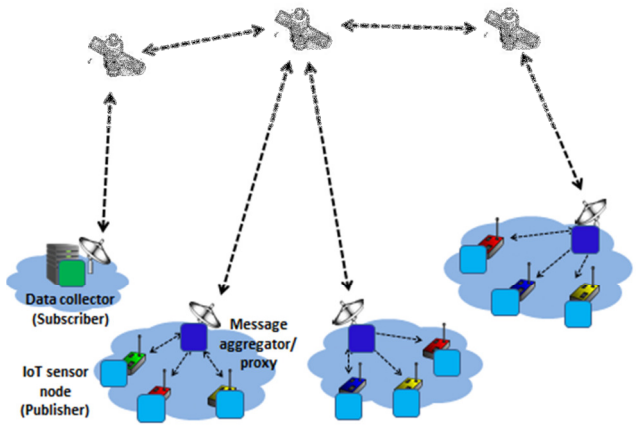


Fig. 1. Massively connected IoT sensor networks via LEO satellites.The proxy can handle requests on behalf of the data collector and forward data updates received from IoT nodes.

- Message aggregation at proxy: The proxy receives persistent subscriptions from the data collector and periodically polls the IoT nodes. In the other direction, the proxy aggregates data updates from the IoT nodes and sends aggregate updates to the data collector.
- Confidential data transfer with a single proxy: The proxy periodically polls the IoT nodes, as in the previous model. If an IoT node has an update, the proxy sends a notification the data collector, rather than sending the data update as in the first model.
- Individual proxy for each IoT node: In this model there is an individual proxy for each IoT node.

The models utilize PSI's communication and transfer mechanisms. Besides, native multicast and caching, PSI supports two types of content resolution mechanisms: slow and fast rendezvous. With slow rendezvous the network undertakes content discovery and connection establishment, whereas with fast rendezvous the end-hosts interact directly. Slow rendezvous can be used to establish both uni-direction and bi-directional communication [7]. Slow rendezvous with bi-directional communication is appropriate for light interactive services. Utilizing the different types of rendezvous mechanisms can improve the performance and deployment of IoT applications over integrated satellite-terrestrial. Next we describe in more detail each model, discussion the exchange of control and data message between the entities.

### A. *Message aggregation at proxy*

The first model reduces the control and data traffic over the satellite link by introducing an ICN-enabled proxy. The proxy, which resides at the satellite GW, periodically polls the IoT nodes and collects their responses, which are aggregated and transmitted over the satellite link to the data collector with a single response. Fig. 2 shows the control messages (pub/sub requests and responses from the Traffic Management, TM, module) and the data messages that are exchanged.

Messages 1-3 are part of a slow rendezvous that establishes a connection from the proxy to the data collector using the information item *proxy*. The proxy uses this connection to send the IoT data to the collector. A slow rendezvous follows (messages 4-8) to create a bi-directional connection between the proxy and the IoT nodes, using the information item *sensors*. The bi-directional FIDs calculated by the TM are used by the proxy to periodically probe for new updates (messages 11, 12) and by the IoT nodes to send new updates to the proxy (messages 13, 14). The IoT updates are aggregated and sent to the data collector using a group reply (message 15), reducing the data traffic over the satellite link.

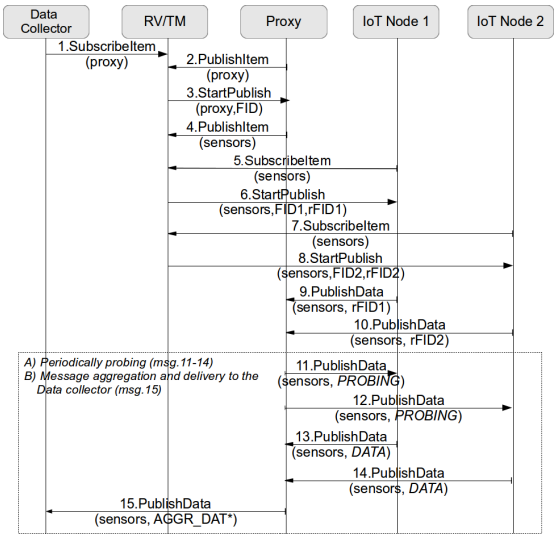


Fig. 2. Sequence diagram for the message aggregation model.

### B. *Confidential data transfer with a single proxy*

An alternative of the model described above is necessary when confidentiality is crucial and the proxy is not allowed to access the data from IoT nodes. One approach for achieving confidentiality is to use cryptographic methods for concealing the actual content. Another option that we consider below is to have the proxy only inform the data collector that an IoT node has an update, after which the data collector can obtain the updates directly from the IoT nodes. With this approach the control traffic over the satellite link is still reduced, because the proxy polls the IoT nodes on behalf of the data collector. However, the data updates from the IoT sensor nodes cannot be aggregated, hence the data traffic over the satellite link is higher than in the previous model.

Fig. 3 shows the control and data message exchange for this model. Initially, the data collector and the proxy use a slow rendezvous to establish a connection using the information item *proxy* (messages 1-3). Then, the proxy creates a bi-directional connection with each IoT node using the slow rendezvous mechanism (messages 4-8). The proxy periodically probes the IoT nodes for new data updates (message 10). Whenever one or more IoT nodes notify the proxy that new updates are available (message 11), the proxy

creates a random once-used information item called *nonce*, which is sent to the data collector and the IoT nodes (messages 12-13). Using this nonce, the data collector and the IoT nodes with new updates perform a slow rendezvous (messages 14-16), which creates a bi-directional link used for direct, hence private, data transmission from the IoT node to the collector (message 17), without involving the proxy. Notice, that these slow rendezvous subscriptions are transient and cannot be aggregated; each subscription is served by a unicast flow, unlike the persistent polling requests that support multicast transmissions. Consequently, in order to establish an end-to-end connection with each IoT sensor node the data collector transmits two control messages (message 14, 18) over the satellite link for each IoT update.

### C. *Individual proxy for each IoT sensor node*

The third model assumes that each IoT node utilizes an individual (personal) proxy which communicates directly with the data collector. The proxy can be collocated with the IoT sensor node. Rather than being probed by the data collector, the individual proxies push the IoT updates to the collector, e.g. periodically, thus avoiding the expensive signalling over the satellite link. In addition, the individual proxy for each IoT node supports enhanced data security, similar to the model of confidential data transfer with a single proxy; for example, the connection between the proxy and the data collector can be encrypted. Finally, similar to the first two models, the data collector runs on a satellite terminal node and the domain's RV and TM run at the satellite gateway.

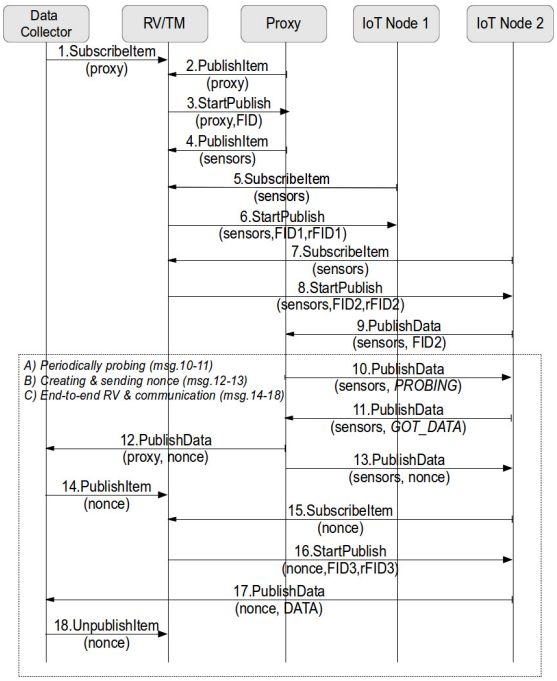


Fig. 3. Sequence diagram for the confidential data transfer model.

Fig. 4 shows the control message exchange for this model. Initially, the data collector and each proxy use the slow rendezvous mechanism (messages 1-3 & 4-5) to establish a bi-directional communication channel between the proxies and the collector. Notice that in the slow rendezvous the TM's notification is sent to the subscriber (proxy), therefore a single publication (message 1) satisfies multiple subscriptions (message 2,4), hence the signalling overhead on the satellite link is independent of the number of proxies. Next, each proxy sends a subscription to a unique per proxy/IoT node information primitive and establishes a connection with the corresponding IoT node (messages 6-8 & 9-11). Thereon, the IoT node simply publishes new data to its personal proxy, which forwards the data to the collector (messages 12-13 & 14-15). Indeed, the proxy can aggregate multiple messages from the corresponding IoT node, thus reducing the data traffic overhead over the satellite link. An alternative is for the proxy to periodically poll the IoT node for new data updates, which would avoid having the data collector send polling requests which traverse the satellite link; in this case the sequence diagram would be similar to Fig. 2, with the only difference that each proxy is connected to a single IoT node.

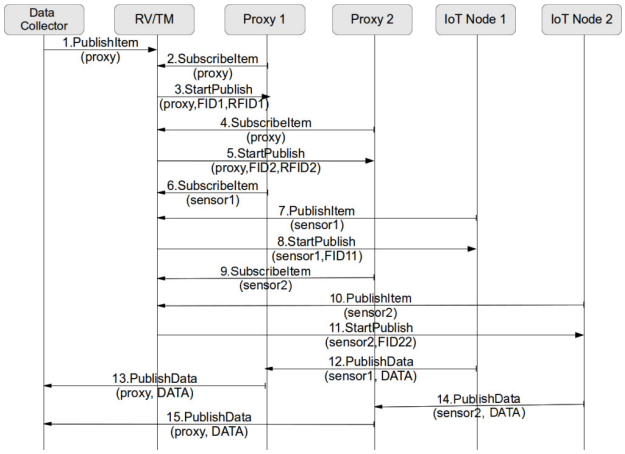


Fig. 4. Sequence diagram for the individual proxy per IoT node model.

## IV. Experimental Evaluation

In this section we quantify the signaling and data overhead of the three models presented in the previous section.

### A. *Testbed*

The testbed used for the evaluation consists of an open source implementation of the ICN PSI (Publish-Subscribe Internet) architecture Blackadder [4], which was developed in the FP7 EU project PURSUIT and the open source satellite emulator OpenSAND [6]. Blackadder is based on the Click modular router framework and implements the three core functions of the ICN/PSI architecture: Rendezvous, Topology Management, and Forwarding. Blackadder exposes a publish/subscribe API to facilitate application development, which in our case involves the implementation of proxies, the data collector, the software upgrade distributor, and the IoT sensor node modules.

Satellite links are emulated using OpenSAND, a tool which implements real satellite DVB encapsulation. OpenSAND supports three types of nodes: Satellite Terminal (ST), Satellite Emulator (SE), and Gateway (GW). STs transmit/receive traffic to/from the emulated satellite. The SE

emulates a transparent or regenerative satellite link including adding a preconfigured propagation delay. Finally, the GW acts as the central access point for STs and as the satellite NCC (Network Control Centre).

The testbed topology used for the experiments is shown in Fig. 5. The topology contains a satellite network, which is composed of three OpenSAND entities (Terminal, Emulator and Gateway), and Blackadder nodes (labelled "BA" in the figure) at the Terminal and Gateway networks. The MAC module at the satellite gateway emulates the delay over the satellite MAC. The Blackadder entity running at the satellite gateway hosts the Rendezvous node (RV), the Topology Manager (TM), and the message aggregator/proxy.

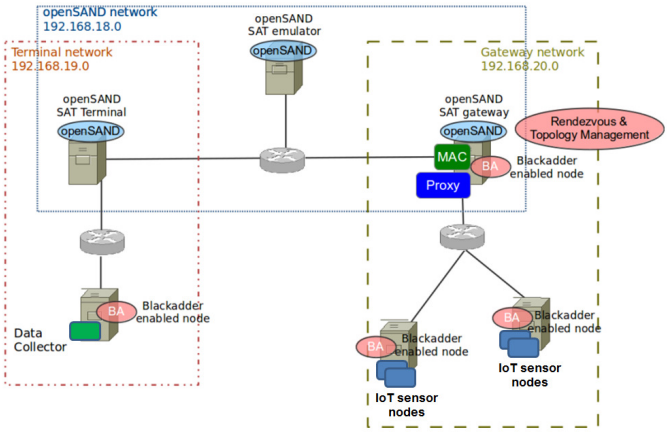


Fig. 5. Integrated satellite-terrestrial ICN testbed topology.

In the model with an individual proxy for each IoT node, rather than at the satellite gateway, the proxy runs on the IoT sensor node or on a node connected to the IoT sensor node.

### B. Results

The configuration of Blackadder, OpenSAND and other network parameters are shown in Table I. Unless stated otherwise, we deploy 10, 50 and 100 IoT sensor nodes that produce updates every 2, 5 and 10 seconds. We call these data generation periods, and assume that each node generates exactly one new measurement (data update) in each such period. We also introduce polling periods during which all IoT nodes are probed, while the updates are aggregated and sent to the data collector. The deployment of the IoT nodes is sequential with a random delay ranging from 0 to 3 seconds, which follows a uniform distribution. Each experiment has duration 120 seconds, which follows a warm up phase where IoT sensor nodes are initiated.

#### 1) Message aggregation at proxy

The proxy periodically polls the IoT nodes for new data updates (measurements) and aggregates the replies into a single message that is forwarded to the data collector. We assume that the size of an update is relatively small (4 bytes) to allow packing all new measurements into the payload of a single packet.

This scenario requires one control message for each proxy to be sent over the satellite link, independent of the number of IoT nodes. This unique message is the subscription of the data collector to the publication of each proxy. On the other hand, the number of control (polling) messages in one polling period sent by the proxy to the IoT nodes is equal to the number of IoT nodes.

TABLE I
EXPERIMENT PARAMETERS

| | Parameter | Value | | Parameter | Value |
|---|---|---|---|---|---|
| OpenSAND | Version | 3.0.0 | Blackadder | Version | 0.2 – ext. |
| | Forward link BW | 36 MHz | | ID length | 8 bytes |
| | Return link BW | 10MHz | | FID length | 32 bytes |
| | Propagation delay | 250, 20 ms | | Cache capacity | 0 (cache disabled) |
| | Payload type | Transparent | | Execution | User space |
| | Encapsulation (return link) | AAL5/ATM | | Overlay mode | IP |
| | Encapsulation (forward link) | ULE MPEG2-TS | Network | Link types | Ethernet 100Mbps |
| | Encapsulation (forward link) | ULE MPEG2-TS | | Link delays | <1ms |
| | GW->ST throughput[1] | 0.9 Mbps | | | |
| | ST->GW throughput[1] | 2.1 Mbps | | | |

The number of data messages sent over the satellite link depends on the operation of the IoT nodes. If the IoT nodes are synchronized, then the updates can be perfectly aggregated by the proxy, hence the updates sent over the satellite link are *1/n* of the updates received by the proxy, where *n* is the number of IoT nodes. If the IoT nodes operate randomly, e.g. with random delay from 0 to 3, then level of aggregation is lower. Fig. 6 shows the reduction of the data messages over the satellite link, which is given by $reduction = 1 - \frac{\text{Packets\_Sent\_By\_Proxy}}{\text{Packets\_Received\_By\_Proxy}}$. Each set of columns corresponds to a different polling_period-to-update_generation_period ratio (2:2, 2:5, 2:10), and each column within a set corresponds to a different number of IoT nodes (10, 50, 100).

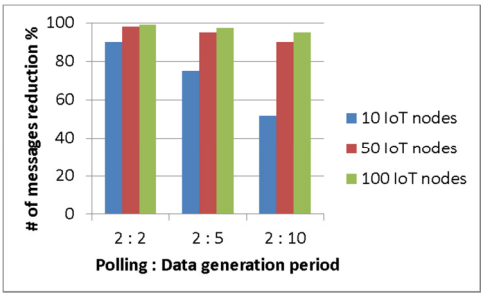


Fig. 6. Reduction of data messages over satellite link when the proxy performs aggregation of data from multiple IoT sensor nodes. Polling period=2 seconds.

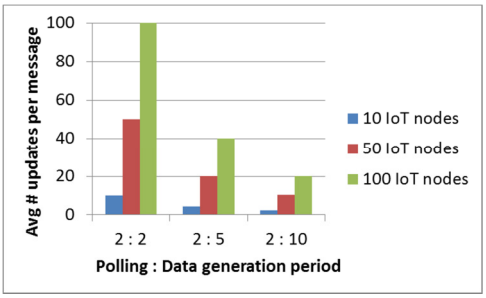


Fig. 7. Average number of updates in each message sent to the data collector. Polling period=2 seconds.

As expected, the reduction of messages is proportional to the number of IoT nodes and inversely proportional to the

period of data generation. Observe that for a larger number of IoT nodes, the number of measurements that are generated and consequently aggregated during a probing period is larger. Similarly, when IoT nodes generate data more frequently, then more data will be aggregated during a probing period, thus increasing the gains from aggregation. This argument is also verified by Fig. 7, which shows the aggregation efficiency of the model; that is the average number of data updates that are placed by the proxy in a single response message before it is sent to the data collector.

*2) Confidential data transfer with a single proxy*

In this model the data collector receives updates directly from the IoT nodes, which enhances privacy and confidentiality since data does not flow through the proxy, at the cost of increased signaling overhead as we will see below.

The control messages sent over the satellite link include the *nonce* message from the proxy to the data collector, in addition to the *publish* and *unpublish* messages from the data collector. The three messages are sent in each probing round, which has duration 2 seconds, hence in 120 seconds 180 control messages are transmitted.

This scenario does not offer data packet aggregation; for confidentiality, the IoT nodes send their updates directly to the data collector. Fig. 8 compares the number of data messages sent using this scheme against the model where the proxy performs data aggregation. When the proxy performs data aggregation, then the satellite load is independent of the data generation period. On the other hand, with the confidential data transfer scheme the number of data messages is proportional to the rate that IoT nodes generate updates.

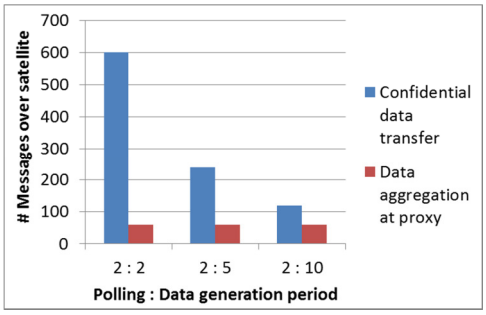


Fig. 8. Number of messages sent over satellite for confidential data transfer and data aggregation schemes.

*3) Individual proxy for each IoT sensor node*

Next we present results for the third model, where each IoT sensor node has a dedicated proxy, which operates as a personal relay that forwards data updates from the IoT node to the data collector.

Only one signalling message is transmitted over the satellite link - the initial publication of the data collector. As discussed in Sect.III.B, the control overhead is independent of the number of proxies because a single data collector's publication can serve multiple proxy subscriptions. Thereafter, the control overhead on the satellite link is minimal, but at the cost of a higher number of proxies.

Regarding the data overhead, in absence of aggregation, we do not foresee a noticeable load reduction. To quantify the overhead, we compare it with the data overhead in the first model where a single proxy performs data aggregation. Fig. 9 shows the ratio of the number of messages sent over the satellite with the individual proxy case, over the number of messages sent in the single proxy case. As expected, with individual proxies the number of messages is proportional to the number of IoT nodes and inversely proportional to the generation period. Indeed, the number of data messages is identical to the case of confidential data transfer with a single proxy. As in the previous scheme, data traffic reduction is exchanged for confidentiality. On the other hand, this model is superior to the other two in terms of control overhead, as it requires only one control message to be transmitted over the satellite link, while the second model requires three control messages per IoT update.

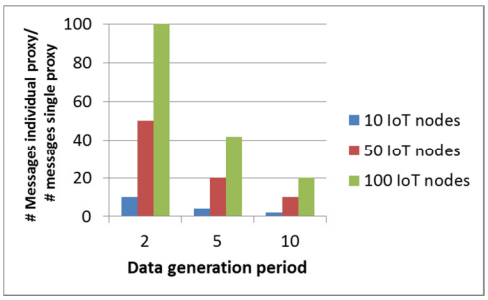


Fig. 9. Number of messages for individual proxy case over number of messages for single proxy case, for which polling period=2 seconds.

## V. Conclusions

We have presented and experimented with different models for supporting the IoT over integrated satellite-terrestrial networks using an ICN architecture. The models seek to reduce both the data and the control traffic transmitted over the satellite network, while supporting different levels of confidentiality. Our experiments consider scenarios with a different number of nodes, data generation periods, and proxy polling periods, illustrating the gains in terms of reduced control and data traffic for the different optimization models, which effectively utilize PSI's communication and transfer mechanisms.

## References

[1] E. Baccelli et al., "Information Centric Networking in the IoT: Experiments with NDN in the Wild," Proc. 1st ACM Conference on Information-Centric Networking (ICN 2014), Paris, France, Sept. 2014.

[2] S. Li, Y. Zhang, D. Raychaudhuri and R. Ravindran, "A comparative study of MobilityFirst and NDN based ICN-IoT architectures," Proc. QShine, Rhodes, Greece, August 2014.

[3] V.A. Siris, C.N. Ververidis, G.C. Polyzos, and K.P. Liolis, "Information-Centric Networking (ICN) Architectures for Integration of Satellites into the Future Internet," Proc. 1st Int'l IEEE-AESS Conference, October 2012.

[4] J D. Trossen and G. Parisis, "Designing and Realizing an Information-Centric Internet," *IEEE Commun. Mag.*, vol. 50, pp. 60–67, July 2004.

[5] G. Xylomenos et al., "A Survey of Information-Centric Networking Research," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 1024-1049, Second Quarter 2014.

[6] "OpenSAND." http://www.opensand.org/

[7] Y. Thomas et al., "Multisource and Multipath File Transfers through Publish-Subscribe Internetworking," Proc. 3rd ACM SIGCOMM workshop on Information-Centric Networking, Hong Kong, China, August 2013.