Horizon 2020

Project title: Software-defined Intermittent Networking

Architecture Specification

Deliverable number: D1.2

Version 1.0/1.0

Funded by the European Union's Horizon 2020 research and innovation programme
under the Marie Sklodowska-Curie Grant Agreement No. 699924

Project Acronym: SINet
Project Full Title: Software-defined Intermittent Networking
Call: H2020-MSCA-IF-2015
Grant Number: 699924
Project URL: http://sinet.dpalma.eu

Editor:	David Palma, ITEM-NTNU
Deliverable nature:	Report (R)
Dissemination level:	Public (PU)
Contractual Delivery Date:	M06
Actual Delivery Date	M06
Number of Pages:	7
Keywords:	Architecture, Maritime Operations, Networking, Unmanned Vehicles, SmallSats
Authors:	David Palma ITEM, NTNU (main author) Artur Zolich IKT, NTNU Roger Birkeland IET, NTNU
Peer review:	Yuming Jiang ITEM, NTNU

Abstract

Maritime communications are strongly dependent on satellite links or even on proximity to target areas. As a consequence, several research expeditions are required to manually acquire and collect research data. This deliverable specifies a hierarchical architecture for interconnecting heterogeneous nodes in challenging maritime environments.

Contents

List of Figures

List of Acronyms

6LoWPAN IPv6 over Low power Wireless Personal Area Networks
AUV Autonomous Underwater Vehicles
C&C Command and Control
DTN Disruptive or Delay Tolerant Network
GW Gateway
IPv6 Internet Protocol version 6
LEO Low Earth Orbits
RA Route Advertisement
RPL IPv6 Routing Protocol for Low-Power and Lossy Networks
RSSI Received Signal Strength Indicator
SDN Software-Defined Networking
SINet Software-defined Intermittent Networking
SmallSat Small Satellite
SNR Signal to Noise Ratio
UAV Unmanned Aerial Vehicle
USV Unmanned Surface Vehicle
UV Unmanned Vehicle

1 Introduction

The **lack of infrastructures in maritime experiments** has a strong impact in many operations, such as the gathering of scientific data. Nowadays, communications typically resort to existing satellite links, which limit the amount of research data that can be transmitted. This results not only from the economic cost of these links, but also from their limited bitrate and availability. Consequently, **it is a common practice to periodically visit research sites to manually collect data** gathered for large amounts of time, from several months to years.

Manually collecting research data incurs on large costs and poses a threat to crews, in particular in harsh maritime environments. In order to overcome current communication limitations, **remote sensing using unmanned vehicles** has been proposed by several authors. These vehicles have the possibility to act as relay nodes, when in simultaneous communication-range of research sites and supporting infrastructures, or as data-mules being responsible for collecting and storing the data until physically near supporting systems.

Several vehicles and nodes regularly operate in the seas and oceans of the world, but they are commonly used for private needs only. This deliverable builds upon the scenario proposed in Deliverable 1.1 [1] and proposes the creation of **a networking architecture for challenging maritime environments**, where unmanned vehicles and heterogeneous communication technologies are used simultaneously. Its main objective will be to **address the communication challenges** of such a platform, capable of supporting different scenarios and experiments.

The proposed architecture is described in Chapter 2, defining the interfaces and technologies used for Unmanned Vehicles (UVs) coordinated with other vehicles and infrastructures. Realistic maritime operations in challenging and remote areas are considered and conclusions presented in Chapter 3.

2 An Architecture for the Internet of Maritime Things

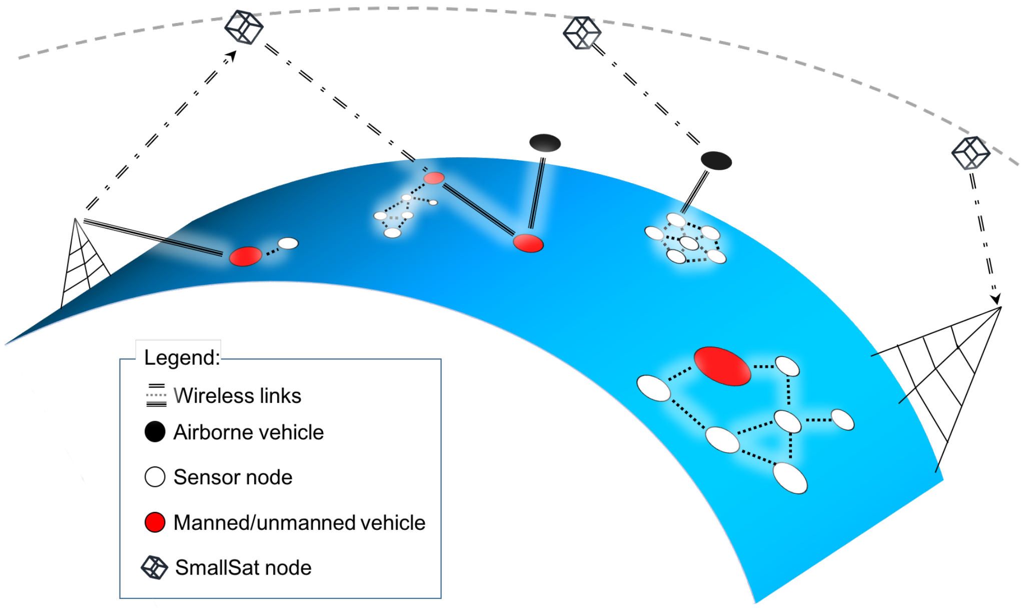


Figure 2.1: Co-existence of heterogeneous communications and vehicles

An overview of SINet's reference scenario is depicted in Figure 2.1, in which different nodes perform distinct operations. This scenario considers networking and communications for remote sensing in challenging maritime scenarios, where no infrastructures exist. Heterogeneous nodes and technologies are envisaged and their cooperation ensures appropriate coverage.

In order to enable the described scenario it is important to define a clear networking architecture. This architecture must include hierarchical roles for different nodes, ensuring a scalable and organised network, presented horizontally in Figure 2.2. Additionally, it must support dynamic changes in its structure due to the variability of conditions in maritime environments (e.g. intermittent links and mobility).

The proposed architecture exploits the hierarchical organisation in order to enforce the Software-Defined Networking (SDN) paradigm [2] in intermittent networks, which is the basis for Software-defined Intermittent Networking (SINet). This allows the control plane to be not only directly connected to ground stations, but also to be enforced by Gateway (GW) nodes, as proxies for created rules. Additionally, the proposed organisation further allows different protocols or mechanisms to locally run in parallel.

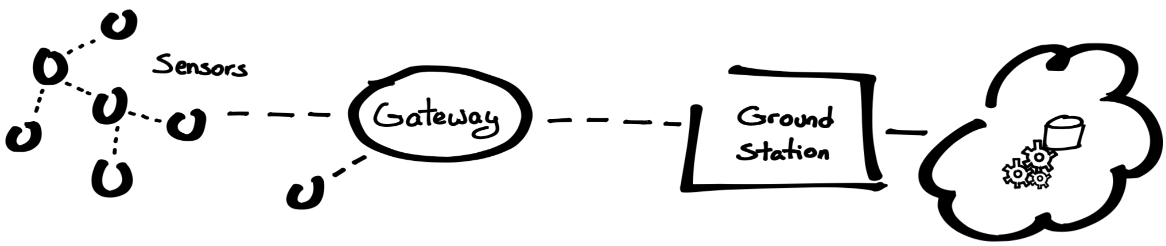


Figure 2.2: Top-level view of the network architecture

2.1 Hierarchy

The *root nodes* of the proposed hierarchical network correspond to those with access to a vast amount of resources, such as a large vessel, or more traditional nodes part of an infrastructure, such as a ground station or backbone vessel. Additionally, these nodes will be strongly connected to the Internet, which allows them to keep a synchronised perspective of the network, regardless of the distance between them. Root nodes should also include several communication interfaces, using different technologies, enabling higher levels of connectivity with different vehicles.

Manned and unmanned vehicles will be an integrant part of the proposed network architecture. These will serve as GWs between the root nodes and any other nodes in maritime deployments. The focus of this work will be on unmanned vehicles such as Unmanned Aerial Vehicles (UAVs), as on-demand GWs for reaching isolated nodes in a planned mission.

Gateway nodes are characterised for being able to carry or relay data from and to the Command and Control (C&C) centre. This should be enabled by at least two different communication technologies, one focused on improved bit-rates and another on achieving longer coverage ranges. Such heterogeneity will allow GWs to act as data-mules for delay-tolerant data, or to simply forward critical data between distant hops.

In addition to different communication technologies, heterogeneity also results from the use of different nodes. Small Satellites (SmallSats) also referred as CubeSats, operating in Low Earth Orbits (LEO), are another possible gateway capable of improving heterogeneity and coverage. By using dedicated SmallSat deployments (e.g. a small swarm of SmallSats), corridors of maritime regions can be covered by long-range communication links. These links can complement the coverage offered by other gateways, for low bitrate communications, optimising the use of vehicles such as UAVs whenever necessary.

Satellites can be an important resource for reaching more isolated sensor nodes, reducing the need for data collection by vehicles. LEO satellites are typically characterised for periodic coverage (around every 90 minutes), for short durations of time (around 10 minutes). However, this can be optimised by resorting to SmallSat constellations, where multiple SmallSats in the same orbit should be exploited together with two or more ground stations, as defined in Section 2.2.3. This will allow a satellite to download all the received data and requests to ground stations at the end of the monitored area, which in turn will forward requests to the another station at the beginning, so that it can intercept newly arriving satellites.

The GW nodes, satellites or vehicles, will not only collect data from the sensors but also deliver any data that may have been requested by the sensor nodes. Additionally, configuration messages from the C&C centre will also be sent throughout the network of nodes. This implies that not only GWs send these messages, but also the sensor nodes at the edge of the network, through multi-hop links between nearby sensor nodes.

At the bottom of the hierarchy, *leaf nodes* such as buoys and other monitoring devices, will be responsible for acquiring most of the data. Due to their limited resources, these nodes will strongly depend on GWs and the configuration sent by the C&C centre, but will also keep moderate levels of autonomic operation. These nodes will be able to perform multi-hop communications, based on the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) [3] protocol, and will dynamically apply SDN-flow rules according to the perceived conditions (e.g. adjust transmission power to measured Received Signal Strength Indicator (RSSI) or Signal to Noise Ratio (SNR) levels).

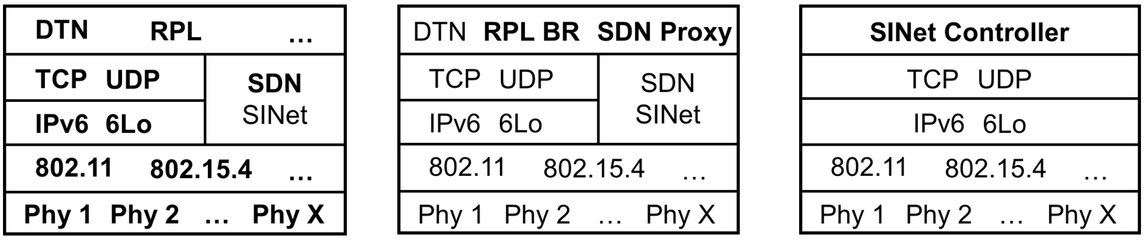
2.2 Roles and Capabilities

The defined hierarchy requires different nodes to assume specific roles at each hierarchical level. This leads to independent network stacks between nodes, with common interfaces for maintaining interoperability. Figure 2.3 depicts the necessary interfaces for the three distinct actors of the SINet architecture, further detailed in the following subsections.

2.2.1 Sensor Nodes

The vast majority of nodes will be sensor nodes, leaf nodes in the presented architecture, which can be deployed in different locations. The proximity between them may allow multi-hop routing so that data can be forwarded to nodes directly connected to a gateway. The forwarding paths will result either from routing messages sent by a GW acting as an RPL Border Router, or from SDN flows installed by the C&C.

Figure 2.3a illustrates the architecture of leaf nodes, which must use Internet Protocol version 6 (IPv6) [4] or IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) [5] in order to guarantee interoperability with other nodes. Physical layer options may vary according to the type of node, but all nodes must also take custody of received data



(a) Sensor network stack **(b)** Gateway network stack **(c)** Ground station network stack

Figure 2.3: Network stack for each hierarchical level

when it is forwarded through them to reach a GW node. For this purpose Disruptive or Delay Tolerant Network (DTN) primitives [6] must be included in these nodes, as well as support for RPL and SDN rules.

The need for Disruptive or Delay Tolerant Network (DTN) is due to the dynamic nature of maritime environments, as well as the dimensions of the areas to be monitored, where data relaying data using satellite or vehicles may not be possible. For this reason communications will have to be delay/disruption tolerant, storing data until it is possible to transmit it. Additionally, data pre-caching or aggregation will also be used, storing the data in nodes likely to be visited by vehicles or capable of reaching satellite links. These strategies should also be used to reduce channel interferences, regardless of the coverage provided by a vehicle/satellite, optimising channel utilisation (i.e. reducing the number of connected nodes per gateway).

2.2.2 Gateway Nodes

Gateway (GW) nodes, which can be several different vehicles (e.g. UAVs, Autonomous Underwater Vehicless (AUVs), Unmanned Surface Vehicles (USVs) or SmallSat), have a key role in the overall behaviour of the network. Each vehicle should complement each other, leveraging on their distinct hardware characteristics and specific behaviours or conditions. For example, periodically available satellite nodes will have different advantages and disadvantages when compared against an unmanned surface vehicle.

Even though GWs can be very heterogeneous, they all share the same functionalities. In particular, all GWs will use IPv6 and Route Advertisements (RAs) so that leaf nodes can forward the collected data. Moreover, despite having a networking stack similar to a leaf node, GWs will also support RPL as Border Routers, as highlighted by Figure 2.3b.

GWs have the role of acting as bridges between deployed nodes and existing infrastructures, requiring additional functionalities from their side. One of these functionalities is the possibility to serve the network as a relay node, forwarding all received packets directly to an infrastructure node. However, since a link to the infrastructure may be non-existent or limited in resources (e.g. a long-range low-bitrate link may not be able to relay all the collected data in real-time), GWs must also be able to act as data mules, collecting all possible data and delivering it later when closer to the infrastructure. Finally, GW nodes must be capable of acting as proxies of C&C centre (highlighted in Figure 2.3b), delivering SDN and other configuration to the nodes, even when not connected to it.

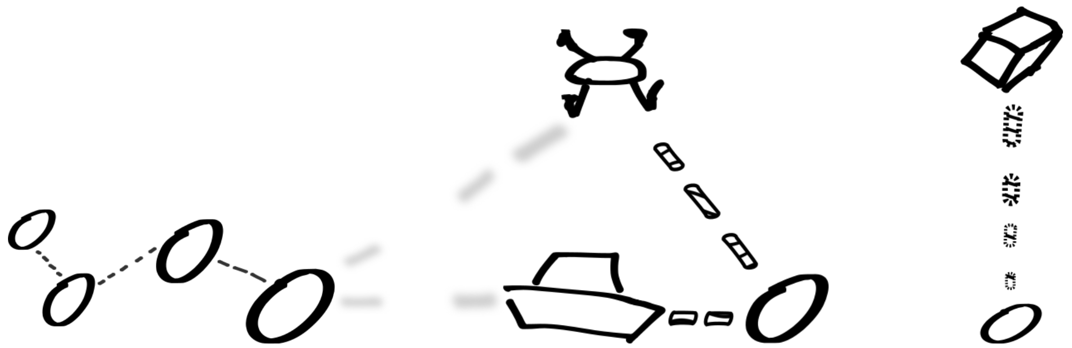
2.2.3 Ground Station Nodes

Dedicated nodes that are strongly connected to common Internet infrastructures, and amongst themselves, are considered as Ground Stations (Figure 2.3c). These will be the main interaction points for unmanned vehicles and satellite nodes, being responsible for interfacing with these GW nodes and providing connectivity to the Command and Control (C&C) centre. The C&C may be reached by other non-dedicated nodes that can communicate with GWs, however for security purposes communications may be restricted to ground stations only.

Special ground stations may also be responsible for hosting the C&C centre, however it may also operate elsewhere in the Cloud, provided that it has connectivity with relevant ground stations. The C&C must perform all the required planning and configuration decisions that will improve the system's performance and resource usage. Storage of the collected data must also be handled by the C&C, therefore ground stations will not only serve as a forwarding point for the C&C decisions, but also as a backhaul for all the gathered data.

The role of ground stations is crucial for the correct operation of the proposed scenario and architecture, connecting nodes and GW to the Internet. For this reason, the reference scenario will consider at least two ground stations, each at the edge of the area under observation. These will be aligned with vehicles and SmallSat trajectories, deployed to cover a given target area. The main assumption is that GW nodes with fixed routes will be able to synchronise their state with ground stations before and after visiting any existing sensor nodes. This will allow succeeding GWs to complement the communication from preceding ones, using the Internet link between ground stations to relay requests/responses between them and GWs at the other extreme of the area. However, if GW nodes are able to continuously and simultaneously reach one ground station and a sensor node, then data is to be relayed immediately.

2.2.4 Heterogeneity



(a) Sensor Multi-hop **(b)** Sensor to Vehicle **(c)** Sensor to Satellite

Figure 2.4: Interaction between multiple nodes

The different roles for each node in the network hierarchy and their characteristics create different communication opportunities. These distinct networking interactions are illustrated by Figure 2.4. Multi-hop networking between leaf nodes is shown in Figure 2.4a, where one node is used to cache information gathered by other nodes. This behaviour can be particularly relevant when only that node is able to reach a GW, either because it has different communication technologies or simply due to its location.

Some leaf nodes may be able to simultaneously communicate with different types of GWs, such as aerial and surface vehicles, as seen in Figure 2.4b. This option is particularly relevant when large amounts of data are to be transmitted, as larger bitrates are expected to be available when nearby GW vehicles exist. On the other hand, Small Satellite (SmallSat) may allow nodes in more isolated areas to periodically deliver their collected data, though at lower bitrates, regardless of the availability of GW vehicles (Figure 2.4c).

3 Conclusions

This deliverable presents the initial architecture for the SINet project. A hierarchical organisation for interconnecting different nodes according to their roles was defined, as well as a networking stack for each level of the hierarchy.

SDN for intermittent links is enforced by resorting to GW nodes as proxies for the control plane, using DTN as a basis for all communications. The goal of achieving an interoperable network is reached by combining IPv6 and 6LoWPAN in the nodes networking stack.

Bibliography

[1] SINet, “Deliverable D.1.1, Reference Scenario and Requirements Definition,” July 2016.

[2] S. Costanzo, L. Galluccio, G. Morabito, and S. Palazzo, “Software Defined Wireless Networks: Unbridling SDNs,” in *2012 European Workshop on Software Defined Networking (EWSDN)*, Oct. 2012, pp. 1–6.

[3] A. Brandt, J. Vasseur, J. Hui, K. Pister, P. Thubert, P. Levis, R. Struik, R. Kelsey, T. H. Clausen, and T. Winter, “RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks,” RFC 6550, Oct. 2015. [Online]. Available: https://rfc-editor.org/rfc/rfc6550.txt

[4] S. Deering and R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification,” RFC 2460, Dec. 1998. [Online]. Available: https://rfc-editor.org/rfc/rfc2460.txt

[5] G. Montenegro, J. Hui, D. Culler, and N. Kushalnagar, “Transmission of IPv6 Packets over IEEE 802.15.4 Networks,” RFC 4944, Oct. 2015. [Online]. Available: https://rfc-editor.org/rfc/rfc4944.txt

[6] L. Torgerson, S. C. Burleigh, H. Weiss, A. J. Hooke, K. Fall, D. V. G. Cerf, K. Scott, and R. C. Durst, “Delay-Tolerant Networking Architecture,” RFC 4838, Oct. 2015. [Online]. Available: https://rfc-editor.org/rfc/rfc4838.txt

The SINet project

October 31, 2016

SINet-D1.2-1.0/1.0

Horizon 2020