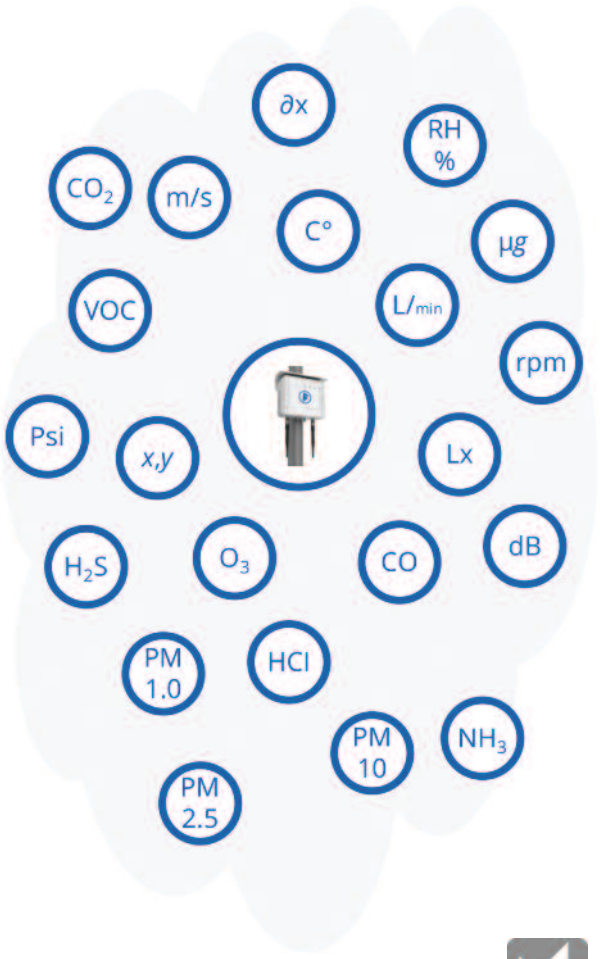
FRAP

Free2move Radio Air Protocol and Application Interface



Product Overview

FRAP is a leightweight protocol specifically designed for situations when a large number of battery-driven and processing-limited end-point devices, such as sensors and actors, need to simultaneously yet reliably exchange information with a much smaller number of gateways. Extreme such situations may involve several thousands of end-point devices exchanging data with a single gateway – not uncommon in IoT and RFID applications. They represent demands where common open air protocol standards such as Bluetooth and ZigBee are less ideal.

Product Features

- Very high anti-collision performance.
- Strongly minimised air traffic through size minimal 8-bit commands, indication payload paging, sequencing and low level error handling via request-response pairing.
- Supports both Beacon mode and Ondemand (Wake-up) mode.
- Implements a comprehensive pre-set state diagram based operating framework for the most common sensor and actor tasks, including Sensing, Logging, Triggers, Alarms and Autonomous Controls. States are controlled via single 8-bit device state flag (DSF).
- Support for network-wide seclusion/stealth via seclusion codes.
- Support for multi-level access codes.
- Shares the same radio hardware and processor with Bluetooth Smart.

Ordering Information

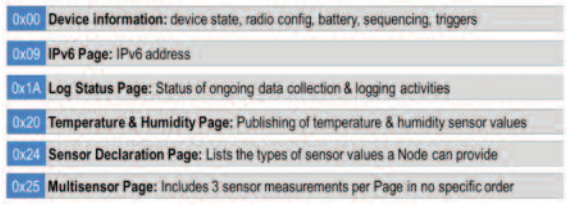
Product Code	Definition
F2MSSC-001	FRAP seclusion code assignment (1 code)
F2MSSC-010	FRAP seclusion code assignment (10 codes)

FREE2MOVE

FRAP overview

FRAP comprises of two main parts: (1) the radio air protocol for traffic between end-point devices and gateways and (2) the application programming interface which offers FRAP services to other applications. The latter is also called FRAPI. In most cases, both the air protocol and the FRAPI are invisible to the users.

The air protocol regulates the exchange of information between the gateways and the endpoint devices. Information may be sent from sensors to gateways on time regulated intervals, typically after completion of each sensor reading. It may also be sent on demand from the gateway, or by a sensor alert, such as exceeding of a pre-set sensor threshold, or by other type of event. In FRAP, all information sent from end-point device to gateway follows a page structure. This is to ensure that only necessary information is sent. A unique page code also ensures that the gateway knows what type of information it is receiving. Some common pages are listed below preceded by their page codes.



Electromagnetic interference

Electromagnetic interference is principally hardware related. As industrial noise is present in the HF and lower VHF bands (kHz and lower MHz) using FRAP with 2.4 GHz GFSK will prevent industrial noise from affecting data communication. Furthermore, FRAP makes use of channel selection, instant retransmission and other Quality of Service (QoS) techniques to further improve resilinence.

Security

FRAP offers several security methods.

Multilayered passwords

The purpose of the multi-layered password feature is to prevent unauthorised access or control of individual gateways which may cause privacy issues or malfunction of asset protection systems. By using the multilayered password system, the user can protect individual parts of the gateway, so that if one password is exposed through normal course of operation, other parts will not be exposed. However, it is important to point out that a total approach to the complete network security must also be in place.

Seclusion

FRAP's seclusion feature is in some ways similar to Bluetooth's pairing, with the difference that it is network-wide and not merely limited to two paired devices. FRAP's seclusion allows wireless networks, regardless of how many devices are involved, to be invisible to other networks. For instance if two industries, Factory A and Factory B, are neighbours their gateways and devices will likely be overlapping in terms of range. If Factory A sets a Seclusion Code for all his devices, they will be invisible to Factory B at all times. The Seclusion Code also prevents an unauthorised gateway, even if the gateway is produced by Free2move, to view or influence secluded devices. The assignment and configuration of a Seclusion Code is performed at production and is a service provided by Free2move.

Encryption

FRAP supports AES encryption of sensor and command information. The encryption standard used is the same as for Bluetooth v4.2 and above. The penalty for enabling encryption is always a small reduction in network speed and battery life.

FREE2MOVE

Free2move AB, Upplandsgatan 7, 112 23 Stockholm, Sweden. Tel: +46 8 642 25 55. Url: www.free2move.se