Position paper

IETF IAB workshop on IoT Semantics, 2016

Document No.:	TAR13510
Version:	
Description:	Overview of the deployment experience gathered during the design and configuration of connected Z-Wave networks for home control, sensor data gathering, alarm systems, irrigation control, hotel rooms and more.
Written By:	Anders Brandt, Sigma Designs
Restrictions:	Public

Table of Contents

1 INTRODUCTION

Z-Wave technology has been deployed for more than a decade in home control and building automation installations. This paper provides an overview of the deployment experience gathered during the design and configuration of connected networks for home control, sensor data gathering, alarm systems, irrigation control, hotel rooms and more.

IoT interoperability is not just about aggregating data in the cloud. A complete solution has to include real-time event handling, coordinated control of multiple actuators and proxies for support of devices that are powered by constrained energy sources.

2 ACCESS TO DATA

It is often attractive to collect data in the cloud. However, battery powered sensors typically wake up, deliver a sensor report and return to sleep. The sensor report is lost if it is not delivered to the data sink.

Power may have been interrupted
Sensors may run on battery, but to continue uninterrupted, the gateway needs to employ a battery too.

Internet access may be broken
The gateway needs to employ a SIM card for access to a wireless backup connection.

The data sink in the cloud may be down for service
The gateway must be able to cache sensor data that cannot be delivered to the destination. When returning online, the data sink cannot pull data directly from sensors as the sensors are sleeping to save power. Thus, the gateway must provide caching for sensor data so that sensor data is not lost during connectivity glitches.

There are also cases where communication from the cloud cannot reach a PAN device immediately. One such example is when it is necessary to change configuration parameters for a battery powered sensor that sleeps.
The gateway therefore must act as a mailbox proxy for access to sleeping devices.

3 AWARENESS OF DELIVERY DELAYS

There is a broad range of battery powered devices in modern home control.

One category covers sensors which may sleep for hours between looking for new messages in a mailbox.
Another category that gives higher priority to response time than battery life includes LED lamps, door locks and window covering devices. Depending on the actual PAN technology, mechanisms such as “duty cycling” or “beacon” may be used. It may take up to 1 second before such a device is awake and ready to receive a message.

In both cases, a responsive user interface needs to know if it takes some time to deliver the message to its recipient. Therefore, the gateway needs to provide immediate feedback to indicate that the message has reached the gateway and that it may take another x seconds before the message will reach its final destination.

4 SENDER-MANAGED MULTICAST GROUPS

In home control applications, there is a need for controlling actuators in a synchronized fashion. For instance, this is needed in order to make three battery-powered window coverings wake up and start moving downwards at the same time.

Receiver group memberships are managed by the controlling application. The receivers do not know when to join or leave the group.
This is unlike classic IP Multicast where the individual receivers manage their memberships.

A mechanism is needed which allows a controlling application to manage receiver group memberships.

5 SERVICE DISCOVERY

Multicast message distribution is not trivial in multi-hop PANs. It is either slow or unreliable and most likely it puts significant load on the PAN. Even if the ideal PAN multicast solution existed it would not be really useful for service discovery:
Sensors may be permanently sleeping (e.g. window sensor powered by kinetic energy harvesting) or only waking up on rare occasions (temperature sensor powered by battery or ambient energy harvesting). Such devices will never respond to multicasted service discovery requests.

A service discovery proxy is needed in the PAN Border Router serve information such as supported services (for sensors: the actual sensor type), name and geographical location, next expected wake-up, etc. to PAN nodes as well as LAN hosts.

6 ACTUATOR STATUS MONITORING

Control applications often feature a GUI which reflects the actual state of the system components. A user may instruct a door lock to go to its locked state. The GUI will not show the door lock as locked before it has been actively confirmed that the device is locked.

Many first-generation control applications achieve this by repeatedly polling a device until it has reached its intended state. While this may be harmless in a classic cabled IP environment, this puts a significant load on a PAN.
At the same it causes the GUI to respond in a sluggish way; only updating seconds after the operation was completed.

Second-generation control applications feature a mechanism to instruct a controlled device to actively report state changes. In case of the above door lock, it may immediately advertise that it accepts the command, that the operation has started and that the operation is expected to take, say, 4 seconds. This allows a GUI to show a progress bar that reaches 100% after 4 seconds. The door lock may either complete as expected, or it may realize after 2 seconds that it has been jammed – in which case it immediately issues a “Door Lock Jammed” notification to the control application. The IETF CoAP Observe feature is an example of such a mechanism. Other technologies offer a more generic mechanism; only advertising the overall process status such as “Success”, “Working” (+ duration), “Fail”.

7 ONLY ONE UNIT IN SENSORS AND ACTUATORS

A temperature may be represented in many units on a display. Any of the units Fahrenheit, Celsius or Kelvin could be used. Exchanging multiple but similar units just increases the number of required conversions and thus increases the code size and the number of test cases that must be performed. Only one unit should be allowed for the exchange and storage of a given data type.

The general principle should be to stick to SI units, but for instance with temperature, there may be benefits of being pragmatic: Kelvin is only rarely used. By using Celsius, it is only necessary to convert to Fahrenheit in displays.

In the same way, there should only be one way to control a lighting device. The light level may be specified by a value in the range {0..100%} in a sufficiently high resolution.
In the same way, the color tone may be specified by 4 values (RGB+White) in the range {0..100%} in a sufficiently high resolution. Conversion to other popular color palettes may be done with a few simple arithmetic operations.

8 PREDICTABLE SENSOR MESSAGE PATTERNS

It must be possible to query and change the parameters for meters, sensors and detectors

For instance: How often does a meter or sensor send data reports?
For instance: How dark should it be before a motion sensor starts detecting motion?
For instance: When does a motion sensor indicate that there is no motion anymore?
For instance: How often should a window sensor report that the window is still open?

The parameter types need to be standardized so that M2M systems and installer can configure sensor parameters with expert assistance. SNMP and MIBs are one example of M2M readable parameter metadata.

9 METRIC FOR SECURITY LEVELS

IoT deployments may encompass a range of PAN technologies with varying security solutions in the coming decades. Some of these PANs may be upgraded to stronger security mechanisms while others may not be maintained at all, for instance if a gateway manufacturer is not providing updates or if PAN end devices do not have sufficient code space to be updated.

It may be critical if a door lock uses an outdated security mechanism while it may be acceptable that an outdoor temperature sensor is not using state-of-the-art security.

A standard scale should be established for characterising the protection level that a given device can provide.
If different security mechanisms are used at various link layers, a security tag should be added to the message for each link layer that is used from the PAN device to the destination. This will allow a cloud server to determine to which degree sensor data and door lock reports can be trusted.

10 GATEWAY BACKUP DATA CONTAINER

The PAN gateway may need to be replaced because it breaks down, is stolen or because the user wants to assign the PAN master role to another gateway provided by a new service provider.
Often, the gateway handles the assignment of PAN ID, Node IDs and the management of PAN routing protocol parameters.

A standardised PAN gateway backup format is needed in order to continue PAN operation with a new gateway without completely re-building the PAN.

An empty container format should be standardized which only advertises the PAN technology, the version of the PAN technology and a backup payload block. The backup payload format should be documented by relevant PAN technology alliances.