**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **/ Technical Guidance Document subsections 2, 3, 5** |
| Date Submitted | [10 February, 2014] |
| Source | [Paul Chilton][NXP Semiconductors][Furnival Street, Sheffield UK S1 4QT] | Voice: [+44 114-281-2655]Fax: []E-mail: [paul.chilton@nxp.com] |
| Re: | [TG10 TGD] |
| Abstract | [Subsections 2 3 &5 of the TGD - Working document] |
| Purpose | [Sub-document of TGD] |
| Notice | This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. |

# Overview

# Definitions

## Conformance Levels and Requirements Language

The conformance level definitions used in this document follow those in clause 11.2.2 of the IEEE Style Manual.

SHALL: A key word indicating mandatory requirements to be strictly followed in order to conform to the standard; deviations from shall are prohibited (shall equals *is required to*).

SHOULD: A key word indicating that, among several possibilities, one is recommended as being particularly suitable, without mentioning or excluding others; that a certain course of action is preferred but not necessarily required; or, that (in the negative form) a certain course of action is deprecated but not prohibited (should equals *is recommended that*).

MAY: A key word indicating a course of action permissible within the limits of the standard (may equals *is permitted to*).

# Abbreviation and acronyms

# General requirements

## Summary of PAR

### Scope

### Purpose

## High level requirements

## Application requirements matrix

## Defined Behaviors Should Support the Following in 802.15.4

# Functional requirements

## Mesh Topology Discovery

The proposal shall enable automatic topology learning, including the status and quality of links between devices.

## Mesh Routing Protocol

MAC address-based protocol and algorithm shall be defined for dynamic auto-configuration of MAC-layer data delivery paths between devices in L2R network. Which path between devices should be established is up to network topology.

## Extensible Mesh Routing Architecture

The proposal shall define a protocol architecture that allows alternative path selection metrics and/or routing algorithms to be used, based on application requirements. In the case that multiple path selection metrics or routings algorithms are available, each device shall detect or be informed of which alternatives may be used or which alternative is currently being used by other devices.

*[ If there are multiple path selection metrics available:*

*a. Should it be possible to mix path selection metrics on different links within the same network?*

*b. Should it be possible to change the path selection metric in use while the network is operating?*

*c. Should it be possible to apply multiple metrics when determining a route?]*

## Mesh Broadcast Data Delivery

The proposal shall enable MAC-layer broadcast or multicast data delivery across the L2R network.

## Mesh Unicast Data Delivery

The proposal shall enable MAC-layer unicast data delivery across the L2R network.

Route discovery

## Mesh Network Size

The proposal shall support 1000-10000 devices in the L2R network. [*really a performance parameter may be better in section 6]*

Should be possible to operate without internet connection / gateway? (standalone)

Standalone network should offer similar level of security to connected operation

Should be possible to merge subnet into larger network – when independent networks have been built separately (security, route info)

Should allow the use of sleeping devices

## Mesh Security

### Security modes

The proposal shall allow the network to operate both secured and unsecured but not at the same time.

The security modes shall consist of “secured with MIC” or “secured with MIC and encryption”. The use of encryption without a MIC is prohibited.

The security shall be applied to the link layer.

The proposal shall specify a means to authenticate the identity of a node as part of the network joining process.

The proposal should specify a mechanism whereby security material can be delivered securely to an authenticated node

The proposal should specify a mechanism whereby the security material in a node or group of nodes can be changed or withdrawn. The mechanism should allow the update of security material to be selectively applied, in order to remove previously authenticated but now untrusted devices from the network.

The proposal should specify a method to ensure sleepy devices can maintain communications even when security material has been changed while they have been asleep

## Routing Metrics

The decision on which link to use to route a packet shall be based upon at least one routing metric. The routing decision may be a result of applying a combination of metrics

### Radio-Aware

* At least one radio-aware routing metric shall be defined for use by the routing protocol(s).
* Multi PHY interfaces
* Parameters which may be utilized include data rate, packet size, signal strength, link quality

### Device-Aware

* Energy constraints - remaining energy in battery, duty cycling
* Memory constraints – buffer space availability

### Network-Aware

* Optional upper layer information

### Bridge-Aware

* To networks using other standards (802.11, 802.1…)

## Discovery and Association with a L2R network

The proposal shall support the discovery of, and association with, a L2R network by devices.

Identification of a network

Joining

## Frequency Agility

The proposal shall support a method whereby the network can change frequencies either as a result of detecting interference or as a result of the underlying MAC configuration.

## Transmit Power control

The proposal may support a method to vary the transmit power of a node based on the proximity of other devices in a network in order to reduce the chance of packet collisions in a busy, dense network

## Network Acknowledgement

The proposal should provide a means for the sender of a multi-hop transmission to ensure that the message reached its intended recipient. In the case of multiple recipients, there may be no indication of the success or otherwise of the transfer. The notification mechanism, if present, shall be enabled on a per-transfer basis.

## Changes to the MAC and PHY

The proposal shall not require modifications to the 802.15.4 PHY or MAC layers with the exception of additional Information Elements to facilitate the exchange of PHY and MAC information.

## Multiple Entry and Exit points

The proposal should support the use of multiple ingress and egress points for data within the network if required by the application(s). Devices shall implement a method to select the most appropriate entry/exit point for their communications with entities outside the network. If a device becomes unable to communicate with an entity outside the network at the required quality of service using its preferred entry/exit point, it shall be possible for the device to find an alternative entry/exit point (if one exists) and begin to use that. It shall be possible for devices to use different entry/exit points to communicate with different external entities.

# Performance requirements

## Required memory resource

## Calculation cost

## Energy consumption

## Control traffic overhead

## Route acquisition time

## Recovery time of link failure

## Scalability to network size

## End to End packet loss rate

## End to End data throughput and delay

## Life time of battery operated network

# Regulatory Considerations/Aspects

# Evaluation methodology