IEEE P802.15
Wireless Personal Area Networks

Project	IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)	
Title	**Security and Efficiency Enhancements Overview**	
Date	December 14, 2009	
Source	René Struik Certicom Corp. 5520 Explorer Drive, 4th Floor Mississauga, ON L4W 5L1	E-mail: rstruik@certicom.com Phone: +1 (905) 501-6083 Fax: +1 (905) 507-4230
Re:	Security and Efficiency Enhancements for IEEE 802.15.4e	
Abstract	This document provides an overview of security and efficiency enhancements for 802.15.4e, based on the streamlined version of Clauses 7.5.8 and 7.6 of IEEE 802.15.4-2006 (for details, cf. document: 08/0849r0).	
Purpose	Security and efficiency enhancements of IEEE 802.15.4-2006	
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.	

1.1 Overview of Provided Functionality

Frame security with IEEE 802.15.4e is based on the frame security provisions in the 802.15.4-2006 specification with the following provisions:

Same as with 802.15.4-2006:

Security provisions:

- Confidentiality, data authenticity, replay protection (with old specification, not always replay protection or data authenticity)
- Protection of broadcast and multicast frames possible (with old specification, this mechanism was broken)
- Easier set-up of protection parameters possible (with old specification, one had to pre-install these parameters via 'out-of-scope' mechanism)
- Possibility to vary protection per frame, using a single key (with old specification, protection was fixed and key was married to protection level)
- Consideration of system lifecycle issues, e.g., allowing unsecured communications until higher layer sets up key (with old specification, this was 'out-of-scope')
- Optimization of storage of keying material (with old specification, frame counter was function of device and key; with new specification, this is function of device only [thus, saving cost, e.g., when working with two versions of network key])
- Security policy checks per frame possible (with old specification, protection level fixed irrespective of frame type)
- Key usage policy checks possible (with old specification, any key could be used with any frame)

Further enhancements to 802.15.4-2006:

Security provisions:

- Strong replay protection rather than weak replay protection (since clock available)
- More refined security policy check (also prevents some DoS attacks)
- Protection of acknowledgement frames possible

System lifecycle support:

- Facility for smooth key updates network-wide keys
- Refinement to facility for unsecured initial device enrolment (device-dependent rather than just frame type dependent)

Implementation cost:

- Reorganization of tables, to facilitate low-cost implementations
- Additional status messages
- Reduced storage cost of keying material (frame counters, device addresses, keys)

NOTE: Implementation of enhancement does *not* jeopardize 802.15.4-2006 compliance

1.2 How to Implement Enhancements to 802.15.4-2006 Security Functionality for 802.15.4e
Enhancements to 802.15.4-2006 Security Functionality may be implemented by using the streamlined version of the 802.15.4-2006 security specification, with the following provisions:

1.2.1 Transmission (§7.5.6.1):
- p. 188, l. 16: Add language to the effect that the current time *macCurrentTime* will be stored.

1.2.2 Reception and rejection (§7.5.6.2):
- p. 190, l. 24: Add language to the effect that the current time *macCurrentTime* will be stored.

1.2.3 Outgoing frame security procedure (§7.5.8.2.1):
- p. 202, l. 29-31: Add FrameCounterMode parameter; add *macCurrentTime* parameter. Adapt MAC sublayer service primitives (§7.1) accordingly.
- p. 202, Step d), ii). l. 47-48: Extend definition of AuxLen parameter, to take into account FrameCounterMode as well.
- p. 203, Step f): Obtain *macFrameCounter* attribute from *macCurrentTime* parameter and locally maintained info (so-called frame counter conversion), such that value never decreases.
- p. 203, Step i), iii): Set frame counter to representation of *macFrameCounter* compliant with FrameCounterMode parameter.
- p. 203, Step m, l. 35: Mute frame header fields in the protected frame compliant with representation mode parameter settings.

1.2.4 Incoming frame security procedure (§7.5.8.2.3):
- p. 204, l. 37-41: Add FrameCounterMode parameter; add *macCurrentTime* parameter. Adapt MAC sublayer service primitives (§7.1) accordingly.
- p. 205, Step i), l. 36-39: Reconstruct frame counter from representation hereof in auxiliary security header, taken into account the frame counter mode and locally maintained info as to the current time (so-called frame counter conversion).
- p. 205, Step j), l. 40-43: Correlate the frame counter and the current time *macCurrentTime*; reject frame if these differ by more than a set amount (presumably, because the frame was stale).
- p. 205, Step k), l. 44-47: Reconstruct muted frame header fields from information in the received frame and locally maintained status information.

Remarks (RS):
- p. 205, Step g), l. 26-29: What if device not there? If one does not do source address filtering, one might still wish to accept incoming frame (e.g., to allow forwarding of frames secured using network-wide key). We may wish to implement a source address filtering mechanism anyway, also for unsecured incoming traffic.
- Changes to facilitate secured acknowledgements:
  - §7.5.8.2.1: Add language on how to compress auxiliary security header and other header fields.
  - §7.5.8.2.3: Add language on how to reconstruct full auxiliary security header and other header fields.
  - §7.5.6.1, p. 189, l. 24-29: Rewrite this paragraph, so as to include outgoing frame processing on acknowledgement messages. Adapt §7.5.6.4 accordingly, to take into account changes to acceptable latency (e.g., parameter *aTurnAroundTime*) and resends.

– §7.5.6.2, pp. 189-190: Expand description to cover handling of incoming secured acknowledgment frames as well.

1.2.5 PIB security material (§7.6.1):

- p. 203, Table 93: represent frame counter as 6-octet integers, rather than 4-octet integers. Adapt overflow checks with security processing of outgoing frames (§7.5.8.2.1) and of incoming frames (§7.5.8.2.3) accordingly (i.e., replace 0xffffffff by 0xffffffffffff).

1.3 A Note on Higher-Layer Security Functionality

Higher-layer functionality may be implemented almost the same as MAC Layer Security Functionality (cf. §1.2 above), with the following caveats:

1.3.1 Common information elements across layers

- Addresses: cryptographic processing and retrieval of keying information assumes that the IEEE extended address EUI-64 is available. If necessary, address conversion needs to take place.
- Timing information: cryptographic processing assumes that timing information related to time of actual receipt of frame is available. This information needs to be propagated 'up the stack' (hence, mentioning hereof as I/O parameter in §1.2.3 and §1.2.4 above).

1.3.2 Different information elements across layers

- Timeliness criteria: correlation of the frame counter and the current time may yield rejection of the frame if these differ by more than a set amount, presumably because the frame was stale (cf. §1.2.4 above). The conditions under which this test leads to rejection of the incoming frame may depend on the layer in question, e.g., to take into account that multi-hop traffic has longer latency than single-hop traffic.
- Security policy information: the security policy under which incoming frames are rejected may depend on the frame type/stack layer in question. Note RS: In fact, the timeliness test above is another example of such a security policy check, but now not with respect to the protection purportedly applied to the frame or key used to implement this security transformation, but with respect to the time the frame was purportedly sent by the purported originating device.

1.4 How to Use Parameter Settings

The security services offered via frame security, both at the MAC level (§1.2) and at higher levels (as alluded to in §1.3), is guided by appropriate settings of security related parameters. A short discussion, in the context of MAC and higher-layer communications, follows.

Security services offered

The cryptographic mechanism provides particular combinations of the following security services:

– *Data confidentiality*. Assurance that transmitted information is only disclosed to parties for which it is intended.
– *Data authenticity*. Assurance of the source of transmitted information (and, hereby, that information was not modified in transit).
– *Replay protection*. Assurance that duplicate information is detected.
– *Timeliness (delay protection)*. Assurance that transmitted information was received in a timely manner.

The actual frame protection provided can be adapted on a frame-by-frame basis and allows for varying levels of data authenticity (to minimize security overhead in transmitted frames where required) and for optional data confidentiality. When nontrivial protection is required, replay protection is always provided.

The acceptable delay can be adapted on a frame-by-frame basis and allows for varying levels of latencies (to facilitate longer latencies in frames transmitted via a multi-hop communication path or, e.g., shorted latencies for acknowledgements).

Note: Replay protection is provided via the use of a non-repeating value (nonce) in the frame protection process and storage of some status information for each originating device on the receiving device, which allows detection of whether this particular nonce value was used previously by the originating device. In addition, so-called delay protection is provided via some loosely synchronized notion of time maintained across the network.

Key Usage

Cryptographic frame protection may use a symmetric key shared between two peer devices (link key) or a key shared among a group of devices (group key), thus allowing some flexibility and application-specific trade-offs between key storage and key maintenance costs versus the cryptographic protection provided. If a group key is used for peer-to-peer communication, protection is only provided against outsider devices and not against potential malicious devices in the key-sharing group.

The number of keys in the network depends on network topology and application-dependent requirements for infrastructure security and application security. As a minimum, each device uses one symmetric key for frame protection. In scenarios where keying material is not pre-installed or may be updated, each device will use a master key or public key (which does not necessarily need to be stored on the device itself).

A network-wide key may be used to protect frames against outsiders (i.e., devices that are not part of the network). The architecture allows the use of a network-wide key, but also allows a more fine-grained logical separation of information, both by using group keys (whereby one restricts access to information to group members only) and link keys (whereby one protects information communicated between two peer devices). Again, key usage depends on network topology and application-dependent requirements for infrastructure security and application security.

Number of keys

The architecture allows for the establishment of a different key for each node pair. Again, key usage depends on network topology and application-dependent requirements for infrastructure security and application security. While it is certainly possible to imagine high-security applications where having logical key separation between keys based on device pairs, in most deployment scenarios, this is not necessary. The number of keys and key usage depend on lifecycle trust management requirements imposed by a particular application at hand. As an example, if one has a centralized network set-up with one fixed security manager, one generally requires a peer-to-peer key between each node and the security manager, but not necessarily a peer-to-peer key between each node (different from the security manager).

The architecture allows re-use of keys across different layers of the stack, thus economizing on key storage cost and facilitating ease of trust management. Thus, keys are not logically tied to a layer of the protocol stack. It is to be expected that keys are used to provide infrastructure structure – which is

realized by single-hop security and may be implemented at the network layer or MAC layer – or to provide application security – which is realized by end-to-end security and may be implemented at the application/session layer.

Cryptographic building blocks across layers
The architecture uses cryptographic building blocks based on the symmetric-key block cipher AES and based on the public-key scheme ECC. Cryptographic protection of frames uses CCM*, a particular mode of operation of this block cipher; trust management uses a symmetric-key entity authentication scheme as well as particular symmetric-key and public-key based key agreement schemes based on this block-cipher and this public key scheme, respectively. Cryptographic device authentication is based on public-key based certificates.

Key establishment (higher-layer functionality)
Key establishment may use a master key shared between a security manager and a device or a certified public key issued by a certificate authority to the device, where public keys are mostly suited for flexible trust management and where symmetric keys may be used in a more static topology. The details on how initial keying material is generated depend on network topology and application-dependent requirements for infrastructure security and application security. It is to be expected that public keys are generated by the device itself and certified in a controlled environment prior to deployment (e.g., during manufacturing or personalization of the device) and that the root key of the certificate authority is installed on the device in an authentic manner at the same time. If one were to use (symmetric-key based) master keys, these can be expected to be generated during device manufacturing or personalization of the device and has to happen in a highly secured and environment (to prevent disclosure of symmetric keys). Key installation should be governed by proper policies for logging and auditing.

Key updates (higher-layer functionality)
The architecture facilitates key updates based on any event stipulated by the trust management policy. In particular, this allows key updates that are periodic or event-driven. The architecture allows semi-automatic lifecycle management and, thereby, semi-automatic key updates.

APPENDIX A – Detailed Textual Changes

This section outlines the detailed textual changes with respect to the IEEE 802.15.4-2006 specification and/or the current draft-4e (09/604r3). Unless stated otherwise, all references are with respect to 802.15.4-2006.

§7.2.1 General MAC frame format

Replace Fig. 41 by the following figure (i.e., adapt length of frame control field, resp. FCS field).

octets: 1/2	0/1	0/2	0/2/8	0/2	0/2/8	0/5/6/10/14	variable	0/2
Frame control	Sequence number	Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address	Auxiliary Secuity Header	Frame Payload	FCS
		Adddressing fields						
MHR							MAC payload	MFR

§7.2.1.1 Frame control field

Change the text as follows:

The frame control field is 1 or 2 octets in length and contains information defining the frame type, addressing fields, and other control flags. For ease of reference, the 1-octet frame control field shall be referred to as the short frame control field in this clause, whereas the 2-octet frame control field may be referred to as the full frame control field.

Add the following two subclauses:

§7.2.1.1.1 Full frame control field

The frame control field shall be formatted as illustrated in Figure 42a or Figure 42b, depending on the value of the frame type subfield.

(*Fig. 42a*)

bits: 0-1	2	3	4	5	6	7	8-9	10-11	12	13	14-15
Frame Class	sFCF=0	Security	Frame Pending	ACK request	PANId Compression	Frame version	Reserved	Dest. Addressing Mode	Reserved	Set to 1	Source Addressing Mode

(*Fig. 42b*)

bits: 0-1	2	3	4	5	6	7	8-9	10-11	12	13	14-15
Frame Class	sFCF=0	Security	Ignored	Ignored	Ignored	Frame version	Reserved	Ignored	Ignored	Set to 1	Ignored

§7.2.1.1.2 Short frame control field

The short frame control field shall be formatted as illustrated in **Error! Reference source not found.**a or Figure 43b, depending on the value of the frame type subfield.

(*Fig. 43a*)

bits: 0-1	2	3	4	5	6	7
Frame Class	sFCF=1	Security	Frame Pending	ACK request	Ext Frame Type	Frame version

(*Fig. 43b*)

bits: 0-1	2	3	4	5	6	7
Frame Class	sFCF=1	Security	Ignored	Ignored	Ext Frame Type	Frame version

§7.2.1.1.1 Frame type subfield

Change the clause title as follows: §7.2.1.1 Frame class subfield.

Change the text as follows:

The frame class subfield is 2 bits in length and shall be set to one of the values listed in Table 79.

The frame type identifier has variable length and is defined dependent upon whether the frame control field is a short or full frame control field.

Add the following two subclauses:

§7.2.1.1.1.1 Frame type identifier for full frame control field

The frame type identifier is 3 bits in length and shall be set to one of the nonreserved values listed in **Error! Reference source not found.**a.

Change Table 79 as follows (*to be cleaned up*):

(*Table 79a*)

Frame class b1b0	Ext frame type b6	Description
00	0	Beacon
	1	EGTS-Beacon
01	0	Data
		Reserved
10	0	ACK
		Reserved
11	0	Command
		Reserved

§7.2.1.1.1.1 Frame type identifier for short frame control field

The frame type subfield is 3-5 bits in length and shall be set to one of the nonreserved values listed in Table 79.

Change Table 79 as follows (*to be cleaned up*):

(*Table 79b*)

Frame class b1b0	Ext. frame type b6	Subframe type b5b4	Description
00	0	n.a.	LL-Beacon
	1	n.a.	EGTS-Beacon
01	0	n.a.	Data
	1	n.a.	Reserved
10	0	00	Acknowledgement
	0	01	ACK w/ source
	0	10	Reserved
	0	11	Reserved
10	1	00	Blink
	1	01	Blink w/ source
	1	10	CSL-frame
	1	11	Reserved
10	0	n.a.	Command
	1	n.a.	Reserved

Add the following clause:

§7.2.1.1.2x Short Frame Control Field Subfield

The Short Frame Control Field (sFCF) subfield is 1 bit in length and shall be set to one if the frame control field is a short frame control field and shall be set to zero otherwise.

§7.2.1.1.6 Destination address subfield

Change the text as follows:

If this subfield is equal to zero, and the Frame Type subfield does not specify that this frame is an acknowledgment or beacon, the Source Addressing Mode subfield shall be nonzero, implying that the frame is directed to the PAN coordinator with the PAN identifier as specified in the Source PAN identifier field.

§7.2.1.1.7 Frame version subfield

Change the text as follows:

The frame version subfield is 1 bit in length and specifies the version number corresponding to the frame.

This subfield shall be set to 0x00 to indicate a frame compatible with IEEE Std 802.15.4e. All other subfield values shall be reserved for future use. See **Error! Reference source not found.** for details on frame compatibility.

§7.2.1.2 Sequence number field

Change the text as follows:

The sequence number field is 1 octet in length and specifies the sequence identifier for the frame.

Add the following text at the end of this clause:

This field shall not be present if the frame type indicates an LL-frame type and the security enabled subfield is set to zero.

Editorial note RS:
- This allows removal of §7.2.5.1 of 09/604r3, since equivalent functionality.

Do not forget to add remarks on §7.2.5.2 of 09/604r3:

§7.2.1.9 FCS field

Change the text as follows:

The FCS field is 2 octets in length and contains a 16-bit ITU-T CRC. The FCS is calculated over the MHR and MAC payload parts of the frame. This field shall be present only if the security enabled subfield is set to zero or if frame protection does not result in data expansion of the frame payload field (see **Error! Reference source not found.**).

§7.2.2 Format of individual frame types

§7.2.2.1 Beacon frame format

Update Fig. 44 to align octet sizes of frame subfield with those in §7.2.1.

§7.2.2.1.1 Beacon frame MR fields

Change the following text:
The Frame Version subfield shall be set to the version corresponding to 802.15.4-2006 or TG4e only if the Security Enabled subfield is set to one.

Change the text as follows:
The Sequence Number field, if present, shall contain the current value of *macBSN*.

§7.2.2.1 Beacon frame format

Update Fig. 44 to align octet sizes of frame subfield with those in §7.2.1

Editorial note RS:
Make similar editorial changes for the data frame (§7.2.2.2 – Fig. 52) and command frame (§7.2.4 – Fig. 54).

§7.2.2.3 Acknowledgement frame format

Replace Fig.53 by the following figure (i.e., allow security, addressing, etc.).

<table>
<tr><td>octets: 1/2</td><td>0/1</td><td>0/2</td><td>0/2/8</td><td>0/2</td><td>1/2/2008</td><td>0/5/6/10/14</td><td>variable</td><td>0/2</td></tr>
<tr><td rowspan="2">Frame control</td><td rowspan="2">Sequence number</td><td>Destination PAN Identifier</td><td>Destination Address</td><td>Source PAN Identifier</td><td>Source Address</td><td rowspan="2">Auxiliary Secuity Header</td><td rowspan="2">Frame Payload</td><td rowspan="2">FCS</td></tr>
<tr><td colspan="4">Adddressing fields</td></tr>
<tr><td colspan="7">MHR</td><td>MAC payload</td><td>MFR</td></tr>
</table>

§7.2.2.3.1 Acknowledgement frame MHR fields

Editorial note RS:
The acknowledgement frames introduced with various proposals, such as TSCH, low-energy subgroup, and group acknowledgement, should be treated similarly as the various command frames and warrant a separate section. General format follows the following principles:

- legacy 802.15.4-2006 acknowledgement frame is supported as special case (no payload, no security, etc.);
- if frame is sent with cryptographic protection, corresponding acknowledgement is sent with the same key, frame counter, and security level as indicated in security policy. Using the same key and frame counter allows compressing the auxiliary security header field and associated frame overhead entirely.
- if acknowledgement is sent with much delay, security processing which depends on correlation of frame counter with on-device time notion will fail or cause unacceptable ambiguities. This can be remedied, but may require a slight change of the incoming and outgoing frame security procedure (which may not entirely be an extension of 802.15.4-2006).

Coordination between various proposers required.

Insert the following Clause:

§7.2.2.3.1 Acknowledgement frame MHR fields

The MHR for an acknowledgment frame shall contain the short Frame Control field, the Sequence Number field, and may contain addressing fields of the originator of the frame.

In the Short Frame Control field, the subfields identifying the frame type shall contain the value that indicates an acknowledgment frame, as shown in Table 79. If protection is used for the acknowledgement frame, the Security Enabled subfield shall be set to one. The (virtual) Source Addressing Mode subfield shall be set to the value that indicates an extended address if the Addressing Mode Subfield of the Short Frame Control Field is set to one and to the value indicating that a source address is not present

otherwise. The Frame Version subfield shall be set to 0x02 to indicate a TG4e frame, as shown in Table {xxx}.

The Sequence Number field shall contain the value of the sequence number received in the frame for which the acknowledgment is to be sent.

The addressing fields shall comprise only the source addressing fields. The Source Address field shall contain the address of the device originating the short acknowledgement frame according to the value of the virtual Source Addressing Mode subfield.

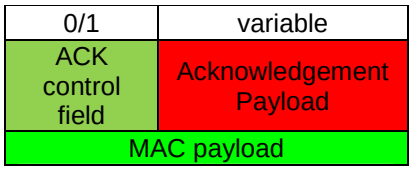
If protection is used for the acknowledgement frame, the Auxiliary Security Header field shall be set to the same value as the corresponding field of the frame that is being acknowledged and shall not be included in the acknowledgement frame to be sent.

§7.2.2.3.2 Acknowledgement frame payload fields

The acknowledgement frame payload field has a variable length and specifies information useful for synchronizing communications between sender and recipient, including loosely synchronizing timing information and capability information (*Editorial note RS:* the so-called “piggy-backing”).

NOTE - Inclusion of this field is determined via inspection of the Frame Length subfield of the PHY header field of the PPDU and the other frame fields.

The acknowledgement payload fields shall be formatted as illustrated in Fig. {xxx}:



§7.2.2.3.2.1 Acknowledgement control subfield

The acknowledgement control subfield, when present, is 1 octet in length and specifies which synchronization information, if any, is communicated back to the originator of the frame that is being acknowledged.

bits: 0-2	3	4	5	6	7
ACK Identifier	Frame pending	Reserved	Time sync	Time offset	Security sync

§7.2.2.3.2.1 ACK identifier subfield

Editorial note RS: include table with ACK types with LE, LL, PA.

§7.2.2.3.2.2 Frame pending subfield

Editorial note RS: the frame pending subfield is the same as used within 802.15.4-2006, but now grouped with other synchronization information.
The Frame Pending subfield is 1 bit in length and shall be set to one if the device sending the frame has more data for the recipient and shall be set to zero otherwise (see 7.5.6.3).

If the acknowledgment frame is being sent in response to a received data request command, the device sending the acknowledgment frame shall determine whether it has data pending for the recipient. If the device can determine this before sending the acknowledgment frame (see 7.5.6.4.2), it shall set the Frame Pending subfield according to whether there is pending data. Otherwise, the Frame Pending subfield shall be set to one. If the acknowledgment frame is being sent in response to either a data frame or another type of MAC command frame, the device shall set the Frame Pending subfield to zero.

§7.2.2.3.2.3 Time sync subfield

The Time sync subfield is 1 bit in length and shall be set to one if the acknowledgement contains time synchronization information.

§7.2.2.3.2.4 Time offset subfield

The Time sync subfield is 1 bit in length and shall be set to one if the acknowledgement is sent with time delay.

§7.2.2.3.2.5 Security sync subfield

The Time sync subfield is 1 bit in length and shall be set to one if the acknowledgement contains security synchronization information.

Editorial note RS: to be finalized after receipt of offline feedback from different subgroups.

§7.2.4 (of 09/604r3) PA-frame formats (*Editorial note RS: this refers to Secured ACK*)

Editorial note RS:
This entire clause §7.2.4 can be removed, since secured ACKs, both with and without payload fields, are handled elsewhere in the TG4e draft specification (see §7.2.2.3 as described in this document).

§7.2.5 (of 09/604r3) LL-frame formats (*Editorial note RS: this refers to LL-frame types*)

§7.2.5.1 (0f 09/604r3) General MAC frame format with MHR of 1 octet

Editorial note RS:
This entire clause §7.2.5.1 can be removed, since the functionality is provided by particular instantiations of the general frame format (see §7.2.1, as described in this document).

§7.2.5.2.1 (of 09/604r3) General (*Editorial note RS: this refers to LL-frame types*)

Add the following text at the end of this clause:

All frame formats in this clause shall use the short frame control field (see §7.2.1.1).

Editorial note RS:
This allows lots of editorial clean-up in §7.2.5.2 of 09/604r3, All editorial changes are aimed at replacing explicit cross-references to the to bit positions indicating low latency frame type to corresponding name for this frame type (this is similar to referring to, e.g., security subfield of the FCF, rather than to bit b3 of the FCF ["replacement of literal value by variable indicating this value"]).

We illustrate this for the LL-beacon frame below:
§7.2.5.2.2 (of 09/604r3) Beacon frame
§7.2.5.2.2.1:
l. 11: *Replace* "The Beacon frame with shortened frame control (1 octet MAC header)" *by* "The LL-Beacon frame".
l. 17-18: *Replace* "The beacon frame does have a very short MAC header (MHR) of one octet containing the frame type and sub frame type, followed by the beacon payload and the MAC footer (MFR)" *by* "The beacon frame consists of a short message header, followed by the beacon payload and the MAC footer (MFR)".
§7.2.5.2.2.2: *Replace this clause by the following text:*
"In the frame control field, the frame type subfield shall contain the value that indicates an LL- beacon frame.

Editorial note RS:
Text below on blink frame based on email received from Dalibor Pokrajac as of Monday November 30, 2009, 3:44pm EST.

§7.2.2.x Blink frame format {TG4f format}

Editorial note RS: descriptive text for blink frames, as suggested by Dalibor Pokrajac, Monday November 30, 2009, 3:44pm EST:

Suggested text for blink frame format:

§7.2.2.x.1 Blink frame MHR fields
In the frame control field, the frame type subfield shall contain the value that indicates a blink frame, as shown in Table {xxx}. The blink frame may use the short frame control field or the full frame control field. When the short frame control field is used, the addressing fields of the message header may either include the extended source address of the originator of the frame or no addressing information at all. The full frame control field should be used, if one wishes to have more flexibility in selectively suppressing addressing information in the message header of the frame and selectively suppress the PAN Identifier, Source Address, or the Destination Address.

§7.2.2.x.2 Blink frame payload field
The blink frame payload field is an optional sequence specified to be transmitted by the next higher layer. The set of octets contained in *macBlinkPayload* shall be copied into this field.

Editorial note RS:
The payload field, if present, is expected to encode and alternative identifier for the originating device. The details of this encoding are outside scope of this specification.

Annex M.x.y – blink frame {*Editorial note: informal description*}
The Blink Frame provides a mechanism for an 802.15.4 device to communicate its ID (i.e. the EUI-64 Source Address) and/or an alternate ID (in payload), and optionally additional payload data to other 802.15.4 devices without prior association and without an acknowledgement. The frame can be used by "transmit only" devices to co-exist within an 802.15.4 network, utilizing Aloha protocol. Any 802.15.4 devices that are not interested in this Blink Frame have an opportunity to reject the frame at early stage during frame processing and not burden the MAC or higher communication layers with this, potentially high volume, data traffic.

§7.3.10.2.1 (of 09/604r3) Join command

Editorial note RS:
I am not sure whether the join command technically fits in the MAC layer, since it concerns an end-to-end communication between a joining device and a device that arbitrages access to the network (PAN coordinator, security manager, network manager, and the-like). Since most of these entities are unknown to the MAC layer (PAN coordinator aside), it seems this functionality needs to be provided at a higher layer – and, thereby, are outside scope of this specification. As an example, with ISA SP100.11a, this is application layer traffic. This requires more explanation.

§7.3.10.2.6 (of 09/604r3) Join security information field

Editorial note RS:
See previous editorial remark (see §7.3.10.3.1).

§7.3.10.3.1 (of 09/604r3) Activate command

Editorial note RS:
I am not sure whether the activate command technically fits witin the MAC layer, since it concerns an end-to-end communication to a joining device from a device that arbitrages access to the network or its resources (PAN coordinator, security manager, network manager, and the-like). Since most of these entities are unknown to the MAC layer (PAN coordinator aside), it seems this functionality needs to be provided at a higher layer – and, thereby, are outside scope of this specification. As an example, with ISA SP100.11a, this is application layer traffic. As an aside, this command may include the distribution of keying material (e.g., network wide keys and the-like), so embedding this with the MAC layer implies that key distribution functionality, end-to-end traffic pur sang, would now be single hop traffic. Multi-hop behavior aside, this would also raise a number of other issues, including definition of structure of keying material, including key usage policy fields and, e.g., validity period of keys. This requires more explanation.

§7.3.10.3.7 (of 09/604r3) Activate security information field

Editorial note RS:
See previous editorial remark (see §7.3.10.3.1).

§7.3.11 (of 09/604r3) LL commands

Editorial note RS:
This clause misses details so as to allow secure operation (see §7.5.6.2, §7.5.8 and §7.6 for details on I/O parameters and other MAC parameters required to properly process outgoing frames and incoming frames – note that *all* incoming frames pass the incoming frame security processing procedure, no matter whether security is enabled or not).

§7.3.13 (of 09/604r3) SUN commands

§7.3.13.1.1 (of 09/604r3) SUN-enhanced beacon request command

Editorial note RS:
Incoming frame security processing requires the extended address of the device originating the frame. The language on p. 93, ll. 2-8, seems to be conflicting here. This requires more explanation.

§7.3.14 (of 09/604r3) LE commands

§7.3.14.1 (of 09/604r3) Wake-up frame

Replace this section by the following text:

The wake-up frame shall be formatted as illustrated in Figure {xxx}:

octets: 1	1	4	0/5/6/10/14	2	variable	0/2
sFCF	Sequence number	Addressing fields	Auxiliary Security Header	RZ time	Frame payload	FCS
MHR				MAC payload		MFR

The order of the fields of the wake-up frame shall conform to the order of the general MAC frame as illustrated in Figure 43.

§7.3.14.1.1 (of 09/604r3) Wake-up frame MHR fields

The MHR for a wake-up frame shall contain the Short Frame Control Field, the Sequence Number Field, the Destination PAN Id, and the Destination Address field.

In the Short Frame Control Field, the Frame Type shall contain the value that indicates a wake-up frame, as shown in Table {xxx}. The (virtual) Destination Addressing Mode subfield shall be set to the value that indicates a short address and the (virtual) Source Addressing Mode subfield shall be set to the value indicating that source addressing fields are not present, as shown in Table 80. If protection is used for the wake-up frame, the Security Enabled subfield shall be set to one. The Frame Version subfield shall be set to 0x02 to indicate a TG4e frame, as shown in Table {xxx}.

The Sequence Number field shall be set to the current value of *macDSN*.

The addressing fields shall comprise only the destination addressing fields. The Destination PAN Identifier and the Destination Address fields shall contain the PAN Identifier and address of the device receiving the wake-up frame.

§7.3.14.1.2 (of 09/604r3) Wake-up frame RZ time field

Editorial note RS:
Keep as is in 09/604r3.

§7.3.14.1.3 (of 09/604r3) Wake-up frame payload field

The wake-up frame payload field is an optional field specified to be transmitted in the wake-up frame.

NOTE - Inclusion of this field is determined via inspection of the Frame Length subfield of the PHY header field of the PPDU and the other frame fields.

§7.3.14.2 (of 09/604r3) New optional payload field

Editorial note RS:
Change "optional MHR payload" towards "optional payload field", so as to make this consistent with treatment of payload fields with secured ACK, etc.

For frames where the payload field has a fixed length without the presence of the CSL-piggy back field, the CSL-sync bit can be derived from the length of the frame (as contained in the PHY header) and the length of the other subfields of this frame. Hence, in those cases the CSL-synch bit is not necessary. For other frames, inclusion of this optional payload field needs to be indicated via a CSL-sync bit contained in the MHR.

§7.3.14.3 (of 09/604r3) Secure acknowledgement frame

Editorial note RS:
This frame should be aligned with the secured acknowledgement frame (see §7.2.3).

§7.5.6.2 Reception and rejection

Interchange the paragraphs Paragraph 1 and Paragraph 2 below:

(*Paragraph 1*)
For valid frames that are not broadcast, if the Frame Type subfield indicates a data or MAC command frame and the Acknowledgment Request subfield of the Frame Control field is set to one, the MAC sublayer shall send an acknowledgment frame. Prior to the transmission of the acknowledgment frame, the sequence number included in the received data or MAC command frame shall be copied into the Sequence Number field of the acknowledgment frame. This step will allow the transaction originator to know that it has received the appropriate acknowledgment frame.

If the PAN ID Compression subfield of the Frame Control field is set to one and both destination and source
addressing information is included in the frame, the MAC sublayer shall assume that the omitted Source PAN Identifier field is identical to the Destination PAN Identifier field.

(*Paragraph 2*)
The device shall process the frame using the incoming frame security procedure described in 7.5.8.2.3.If the status from the incoming frame security procedure is not SUCCESS, the MLME shall issue the corresponding confirm or MLME-COMM-STATUS.indication primitive with the status parameter set to the status from the incoming frame security procedure, indicating the error, and with the security-related parameters set to the corresponding parameters returned by the unsecuring process.

§7.5.6.4.2 Acknowledgement

Editorial note RS:
The so-called ACK delay was discussed during the IEEE 802 meeting, Atlanta, Georgia, November 10-15, 2009 (cf., e.g., 09/782r1). During that discussion, it was suggested to essentially keep the turn-around time the same (for 2.4 GHz PHY). Details to be looked up in the minutes of that meeting.

§7.4.2 MAC PIB Attributes

Editorial note RS:
Adapt the formula for the *macACKWaitDuration* parameter (Equation (13)), so as

- Same outcome with instantiation of unsecured 802.15.4-2006 style 5-octet ACK;
- Make formula independent of frame size variations of new ACK with payload (one way to realize this would be for the originating device to time the received frame by recognizing the incoming frame as acknowledgment frame, in anticipation of proper and successful remainder of incoming processing.

Again, details to be looked up in the minutes of that meeting.

§7.5.8 Frame security

Editorial note RS:
Replace this clause entirely by the corresponding clause of the draft text submitted to the Editing Team by August 15, 2009. This takes into account certain errors that are to be tackled with the Corrigendum to 802.15.4-2006, as also discussed during the IEEE 802 meeting, Atlanta, Georgia, November 10-15, 2009 (cf., e.g., 09/782r1). During that discussion, it was suggested that for TG4e editing purposes, one could anticipate the Corrigendum to include these updates. Details to be looked up in the minutes of that meeting.

§7.6 Security suite specifications

Editorial note RS:
Replace this clause entirely by the corresponding clause of the draft text submitted to the Editing Team by August 15, 2009. This takes into account certain errors that are to be tackled with the Corrigendum to 802.15.4-2006, as also discussed during the IEEE 802 meeting, Atlanta, Georgia, November 10-15, 2009 (cf., e.g., 09/782r1). During that discussion, it was suggested that for TG4e editing purposes, one could

anticipate the Corrigendum to include these updates. Details to be looked up in the minutes of that meeting.