IEEE P802.15
Wireless Personal Area Networks

Project	IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)
Title	**IEEE P802-15_TG4 NTRU Security Architecture Proposal**
Date Submitted	[May 10, 2002]
Source	[Daniel V. Bailey, Ari Singer] [NTRU] [5 Burlington Woods Burlington, MA 01803 USA] Voice: [+1 781 418-2522] Fax: [+1 781 418-2532] E-mail: [dbailey@ntru.com]
Re:	Draft P802.15.4/D14, April-2002
Abstract	[This document provides proposed security text to complete the security section and related text in other sections of the 802.15.4 draft standard. This text provides a complete specification of the proposed security architecture and a clear framework within which security suite specific requirements may be specified. This proposal focuses on limiting the requirements placed on the MAC while providing the flexibility to accommodate strong security implementations.]
Purpose	[This document is intended as a security text submission to the 802.15 TG4 for inclusion in the 802.15.4 draft standard. It is intended that this submission will enable TG4 to define a simple security specification to be implemented by the MAC, while providing an interface to allow additional security services to be provided at higher layers. The text from this submission may be incorporated directly into the draft standard.]
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. Introduction

The 802.15.4 draft D14 does not specify a complete or cohesive security architecture for providing security at the MAC layer. In an e-mail request from Jose Gutierrez, a number of requirements were put forth for any security solution for 802.15.4. The primary areas of interest are the following.

1) The security architecture must be algorithm agile to allow different implementations to utilize different algorithms with different security and efficiency properties.
2) There must be at least a baseline for interoperability for all devices.
3) The design must lend itself to reduced computational effort, and limited software and hardware complexity.
4) The required bandwidth overhead must be kept to a minimum
5) The cost of adding security must be kept to a minimum
6) The requirements must fit both kinds of 802.15.4 topology and be scalable and easy to maintain

In this proposal, we present a security architecture that focuses on the implementation of symmetric

1.1 Scope

This document covers all text related to the security architecture for the 802.15.4 draft standard. In particular, this includes descriptions of the security model, security architecture and security services to be provided by 802.15.4 devices and it includes formats for security related messages. Additional informative text and security considerations supporting the security architecture are included as well.

1.2 Purpose

This document is intended to provide a complete security architecture for the 802.15.4 draft standard that more fully satisfies the requirements of the highly constrained and highly cost sensitive 802.15.4 devices. It is intended that this document be used to replace currently existing text in the 802.15.4 draft standard.

1.3 Notes to the Reader

Throughout the document, the author has included notes to the reader that are not part of the proposed text or submission. These notes are supplied to aid in the review process of this document and to indicate directions to the editor for portions of the standard to add or remove. These notes are not intended to be a part of the standard itself.

Author's note: Notes are prefixed by the words "Author's note:" and written in this font to indicate that they are not part of the intended draft text.

2. References

Author's note: The references to be listed in this section are normative references for the security implementations defined in this document. At this time, the security algorithms that will be included as normative references have not been decided upon.

3. Clause 3 Text (Definitions)

Author's note: The following security related definitions are included to aid in the reading of this document as well as to provide additional definition text for the draft standard.

Access control list: A table used by a device to determine which devices are authorized to perform what functions.

Authentic data: Data that has its integrity cryptographically protected.

Confidentiality: Assurance that communicated data remains private to the parties for whom the data is intended.

Data integrity: Assurance that the data has not been modified from its original form.

Integrity code: A data string generated using a symmetric key that is typically appended to data in order to provide data integrity and source authentication.

Author's note: This is usually called a message authentication code (MAC) but that term will not be used here because of the confusion it may cause with the medium access control (MAC).

Key establishment: A public-key process by which two entities securely establish a symmetric key that is known only by the participating entities.

Key management: Methods for controlling keying material throughout its life cycle including creation, distribution and destruction

Key transport: A process by which an entity sends a key to another entity.

Payload data: The contents of a data message that is being transmitted.

Payload protection: The generic term for providing security services on payload data, including confidentiality, integrity and authentication.

Pseudo-random number generation: The process of generating a deterministic sequence of bits from a given seed that has the statistical properties of a random sequence of bits when the seed is not known.

Random number generator: A device that provides a sequence of bits that is unpredictable.

Security suite: A group of security operations designed to provide security services on MAC frames.

Symmetric key: A secret key that is shared between two or more parties that may be used for encryption/decryption or integrity protection/integrity verification depending on its intended use.

4. Clause 4 Text (Acronyms)

Author's note: The following security related acronyms are included to aid in the reading of this document as well as to provide modified text for the draft standard.

ACL	access control list
DEK	data encryption key
DIK	data integrity key
PRNG	pseudo-random number generator
RNG	random number generator

SEC security

5. Clause 5 Text (General Description)

5.1 Functional overview

Author's note: Replace clause 5.4.2 with the following text.

5.1.1 Security Considerations

Although the diverse range of applications to which this standard is targeted imposes significant constraints on requiring a baseline security implementation in the MAC, some required security functionality is needed in order to provide basic security services and interoperability among all devices implementing this standard. This baseline includes the ability to maintain an access control list and use symmetric cryptography to protect transmitted frames. The ability to perform this security functionality does not imply, however, that security must be used at any given time by any given device. The higher layers determine when security is to be used at the MAC layer and provide all keying material necessary to provide the security services. Key management, device authentication and freshness protection may be provided by the higher layers, but are out of scope for this document.

Author's note: The beacon payload, data payload and command payload will be modified in clause 7 when security is in use. In order to minimize overhead and allow simple implementation of the acknowledgement frame, security will always be turned off in acknowledgement frames. This implies that there is no mechanism provided for a cryptographically assured acknowledgement of receipt. If this is desired, it must be implemented at a higher layer using data frames.

6. Clause 6 Text (PHY layer specification)

Author's note: The security mechanisms in this document deal exclusively with the MAC. No changes are required to the PHY specification.

7. Clause 7 Text (MAC sublayer specification)

7.1 MAC sublayer service specification

Author's note:Due to the increased complexity and cost of specifying key management operations at the MAC layer, we elected to recommend removal of all key management operation from the specification, including authentication. The protocols implemented by the commands that relate to key management and authentication may be implemented at a higher layer. The related commands and references to these commands should be removed from the draft.

Author's note: From the MAC's perspective, key management consists solely of the higher layers writing information into the MAC PIB. The symmetric keys and security relationship information will be written into the MAC PIB using the MLME-SET.request.

7.1.1 MAC data service

7.1.1.1 MCPS-DATA.request

7.1.1.1.1 Semantics of the service primitive

Author's note: Replace the table entry for TxOptions with the following entry:

Table 1—MCPS-DATA.request parameters

Name	Type	Valid Range	Description
TxOptions	Bitmap	0000-xxxx (Where x can be 0 or 1)	The transmission options for this MSDU. These shall be a bitwise OR of one or more of the following: 0x01 = immediate acknowledgment required. 0x02 = transmit in the current GTS. 0x04 = frame to follow 0x08 = security enabled

Author's note: Add the following text at the end of clause 7.1.1.1.3

If the TxOptions parameter specified that the frame does not have security enabled, the MAC sublayer shall set the SEC bit to zero and perform no security operations on the frame. If the TxOptions parameter specified that the frame has security enabled, the MAC sublayer shall set the SEC bit in the frame control field to 1, and obtain from the MAC PIB the appropriate key(s) and security suite (giving precedence to the entry in the ACL over the default) corresponding to the device address in the DstAddr field and perform the operations on the frame as indicated by the security suite using the selected key(s). If there is an error in the secur processing of the frame, the MLME shall return an MLME-SECURITY-ERROR.indication to the SSCS with the appropriate ReasonCode to indicate that the frame could not be protected.

7.1.1.2 MCPS-DATA.indication

7.1.1.2.1 Semantics of the service primitive

Author's note: Replace the MLME primitive in clause 7.1.1.3.1 with the following:

```
MCPS-DATA.indication        (
                            SrcPANId,
                            SrcAddr,
                            DstPANId,
                            DstAddr,
                            msduLength,
                            msdu,
                            mpduLinkQuality,
                            TxOptions
                            )
```

Author's note: Add the following entry to Table 30 on page 53.

Table 2—MCPS-DATA.indication parameters

Name	Type	Valid Range	Description
Security-Use	Integer	0 or 1	This indicates to the higher layer whether the received data frame was protected by security or not.

7.1.2 MAC management service

Author's note: Remove the entries for MLME-AUTHENTICATE, MLME-CHALLENGE, MLME-DE-AUTHENTICATE, MLME-DISTRIBUTE-KEY and MLME-REQUEST-KEY from Table 31 on page 55.

Author's note: Add the following entry to table 31 on page 55.

Table 3—Summary of the primitives accessed through the MLME-SAP

Name	Request	Indication	Response	Confirm
MLME-SECURITY-ERROR		**7.x.x.x**		

7.1.3 Association primitives

7.1.3.1 MLME-ASSOCIATE.request

7.1.3.1.1 Semantics of the service primitive

Author's note: Replace the interface for MLME-ASSOCIATE.request with the following interface:

```
MLME-ASSOCIATE.request          (
                                PID,
                                AssociationAddress,
                                CapabilityInformation,
                                AssocTimeoutPeriod,
                                TxOptions
                                )
```

Author's note: Insert the following entry into Table 32 on page 56:

Table 4—MLME-ASSOCIATE.request parameters

Name	Type	Valid Range	Description
TxOptions	Bitmap	0000-x000 (Where x can be 0 or 1)	The transmission options for this command. These shall be a bitwise OR of one or more of the following: 0x08 = security enabled

7.1.3.1.2 Effect on receipt

Author's note: Add the following text after the first paragraph in clause 7.1.3.1.3:

If the TxOptions parameter specified that the frame does not have security enabled, the MAC sublayer shall set the SEC bit to zero and perform no security operations on the frame. If the TxOptions parameter specified that the frame has security enabled, the MAC sublayer shall set the SEC bit in the frame control field to 1, and obtain from the MAC PIB the appropriate key(s) and security suite (giving precedence to the entry in the ACL over the default) corresponding to the device address in the AssociationAddress field and perform the operations on the frame as indicated by the security suite using the selected key(s). If there is an error in the secur processing of the frame, the MLME shall return an MLME-SECURITY-ERROR.indication to the higher layers with the appropriate ReasonCode to indicate that the frame could not be protected.

7.1.3.2 MLME-ASSOCIATE.indication

7.1.3.2.1 Semantics of the service primitive

Author's note: Replace the interface for MLME-ASSOCIATE.indication with the following interface:

```
MLME-ASSOCIATE.indication       (
                                DeviceAddress,
                                CapabilityInformation,
                                AssocTimeoutPeriod,
                                SecurityUse
                                )
```

Author's note: Add the following entry to table 33 on page 57.

Table 5—MLME-ASSOCIATE.indication parameters

Name	Type	Valid Range	Description
SecurityUse	Integer	0 or 1	This indicates to the higher layer whether the received command frame was protected by security or not.

7.1.3.3 MLME-ASSOCIATE.response

7.1.3.3.1 Semantics of the service primitive

Author's note: Replace the interface for MLME-ASSOCIATE.response with the following interface:

```
MLME-ASSOCIATE.response     (
                            DeviceAddress,
                            AssocDeviceAddress,
                            status,
                            TxOptions
                            )
```

Author's note: Insert the following entry into Table 34 on page 57:

Table 6—MLME-ASSOCIATE.reponse parameters

Name	Type	Valid Range	Description
TxOptions	Bitmap	0000-x000 (Where x can be 0 or 1)	The transmission options for this command. These shall be a bitwise OR of one or more of the following: 0x08 = security enabled

7.1.3.3.2 Effect on receipt

Author's note: Add the following text after the first paragraph in clause 7.1.3.3.3:

If the TxOptions parameter specified that the frame does not have security enabled, the MAC sublayer shall set the SEC bit to zero and perform no security operations on the frame. If the TxOptions parameter specified that the frame has security enabled, the MAC sublayer shall set the SEC bit in the frame control field to 1, and obtain from the MAC PIB the appropriate key(s) and security suite (giving precedence to the entry in the ACL over the default) corresponding to the device address in the AssocDeviceAddress field and perform the operations on the frame as indicated by the security suite using the selected key(s). If there is an error in the secur processing of the frame, the MLME shall return an MLME-SECURITY-ERROR.indication to the higher layers with the appropriate ReasonCode to indicate that the frame could not be protected.

7.1.4 Disassociation primitives

7.1.4.1 MLME-DISASSOCIATE.request

7.1.4.1.1 Semantics of the service primitive

Author's note: Replace the interface for MLME-DISASSOCIATE.request with the following interface:

```
MLME-DISASSOCIATE.request    (
                             DeviceAddress,
                             DisassociationReason,
                             TxOptions
                             )
```

Author's note: Insert the following entry into Table 36 on page 60:

Table 7—MLME-DISASSOCIATE.request parameters

Name	Type	Valid Range	Description
TxOptions	Bitmap	0000-x000 (Where x can be 0 or 1)	The transmission options for this command. These shall be a bitwise OR of one or more of the following: 0x08 = security enabled

7.1.4.1.2 Effect on receipt

Author's note: Add the following text after the first paragraph in clause 7.1.4.1.3:

If the TxOptions parameter specified that the frame does not have security enabled, the MAC sublayer shall set the SEC bit to zero and perform no security operations on the frame. If the TxOptions parameter specified that the frame has security enabled, the MAC sublayer shall set the SEC bit in the frame control field to 1, and obtain from the MAC PIB the appropriate key(s) and security suite (giving precedence to the entry in the ACL over the default) corresponding to the device address in the DeviceAddress field and perform the operations on the frame as indicated by the security suite using the selected key(s). If there is an error in the secur processing of the frame, the MLME shall return an MLME-SECURITY-ERROR.indication to the higher layers with the appropriate ReasonCode to indicate that the frame could not be protected.

7.1.4.2 MLME-DISASSOCIATE.indication

7.1.4.2.1 Semantics of the service primitive

Author's note: Replace the interface for MLME-DISASSOCIATE.indication with the following interface:

```
MLME-DISASSOCIATE.indication    (
                                DeviceAddress,
                                DisassociationReason,
                                SecurityUse
                                )
```

Author's note: Add the following entry to table 37 on page 60.

Table 8—MLME-DISASSOCIATE.indication parameters

Name	Type	Valid Range	Description
Security-Use	Integer	0 or 1	This indicates to the higher layer whether the received command frame was protected by security or not.

7.1.5 Authentication and challenge

Author's note: Remove sub-clause 7.1.5 in its entirety.

7.1.6 Request key

Author's note: Remove sub-clause 7.1.6 in its entirety.

7.1.7 Distribute key

Author's note: Remove sub-clause 7.1.7 in its entirety.

7.1.8 De-authentication

Author's note: Remove sub-clause 7.1.8 in its entirety.

Author's note: Add the following sub-clause to clause 7.1.

7.1.9 Beacon notification primitive

7.1.9.1 MLME-BEACON-NOTIFY.indication

7.1.9.1.1 Semantics of the service primitive

Author's note: Replace the interface for MLME-BEACON-NOTIFY.indication with the following interface:

```
MLME-BEACON-NOTIFY.indication (
                              PANid,
                              SrcAddr,
                              SuperframeSpec,
                              PendAddrSpec,
                              AddrList,
                              sduLength,
                              sdu,
                              LinkQuality,
                              TimeStamp,
                              SecurityUse
                              )
```

Author's note: Add the following entry to table 57 on page 82.

Table 9—MLME-BEACON-NOTIFY.indication parameters

Name	Type	Valid Range	Description
Security-Use	Integer	0 or 1	This indicates to the higher layer whether the received beacon frame was protected by security or not.

7.1.10 Primitives for reading MAC PIB attributes

7.1.10.1 MLME-GET.request

7.1.10.1.1 Semantics of the service primitive

Author's note: Since a new table was added for the MAC PIB ACL, this should be referenced in this sub-clause. Add a reference to Table 18 from this document under the Valid Range for PIBAttribute in Table 59 on page 84.

7.1.10.2 MLME-GET.confirm

7.1.10.2.1 Semantics of the service primitive

Author's note: Since a new table was added for the MAC PIB ACL, this should be referenced in this sub-clause. Add a reference to Table 18 from this document under the Valid Range for PIBAttribute and PIBAttributeValue inTable 60 on page 85.

7.1.11 GTS management primitives

7.1.11.1 MLME-GTS.request

7.1.11.1.1 Semantics of the service primitive

Author's note: Replace the interface for MLME-GTS.request with the following interface:

```
MLME-GTS.request        (
                        GTSId,
                        GTSCharacteristics,
                        TxOptions
                        )
```

Author's note: Insert the following entry into Table 61 on page 86:

Table 10—MLME-GTS.request parameters

Name	Type	Valid Range	Description
TxOptions	Bitmap	0000-x000 (Where x can be 0 or 1)	The transmission options for this command. These shall be a bitwise OR of one or more of the following: 0x08 = security enabled

7.1.11.1.2 Effect on receipt

Author's note: Add the following text after the first paragraph in clause 7.1.4.1.3:

If the TxOptions parameter specified that the frame does not have security enabled, the MAC sublayer shall set the SEC bit to zero and perform no security operations on the frame. If the TxOptions parameter specified that the frame has security enabled, the MAC sublayer shall set the SEC bit in the frame control field to 1, and obtain from the MAC PIB the appropriate key(s) and security suite (giving precedence to the entry in the ACL over the default) corresponding to the device address of thePAN coordinator and perform the operations on the frame as indicated by the security suite using the selected key(s). If there is an error in the secur processing of the frame, the MLME shall return an MLME-SECURITY-ERROR.indication to the higher layers with the appropriate ReasonCode to indicate that the frame could not be protected.

7.1.11.2 MLME-GTS.indication

7.1.11.2.1 Semantics of the service primitive

Author's note: Replace the interface for MLME-GTS.indication with the following interface:

```
MLME-GTS.indication     (
                        GTSId,
                        SecurityUse
                        )
```

Author's note: Add the following entry to table 63 on page 88.

Table 11—MLME-GTS.indication parameters

Name	Type	Valid Range	Description
Security-Use	Integer	0 or 1	This indicates to the higher layer whether the received command frame was protected by security or not.

7.1.12 Primitives for orphan notification

7.1.12.1 MLME-ORPHAN.indication

7.1.12.1.1 Semantics of the service primitive

Author's note: Replace the interface for MLME-ORPHAN.indication with the following interface:

```
MLME-ORPHAN.indication  (
                        OrphanAddress,
                        SecurityUse
                        )
```

Author's note: Add the following entry to table 64 on page 90.

Table 12—MLME-ORPHAN.indication parameters

Name	Type	Valid Range	Description
Security-Use	Integer	0 or 1	This indicates to the higher layer whether the received command frame was protected by security or not.

7.1.12.2 MLME-ORPHAN.response

7.1.12.2.1 Semantics of the service primitive

Author's note: Replace the interface for MLME-ORPHAN.response with the following interface:

```
MLME-ORPHAN.response        (
                            ExtendedAddress,
                            AllocatedAddress,
                            PANMember,
                            TxOptions
                            )
```

Author's note: Insert the following entry into Table 65 on page 91:

Table 13—MLME-ORPHAN.reponse parameters

Name	Type	Valid Range	Description
TxOptions	Bitmap	0000-x000 (Where x can be 0 or 1)	The transmission options for this command. These shall be a bitwise OR of one or more of the following: 0x08 = security enabled

7.1.12.2.2 Effect on receipt

Author's note: Add the following text after the first paragraph in clause 7.1.13.2.3:

If the TxOptions parameter specified that the frame does not have security enabled, the MAC sublayer shall set the SEC bit to zero and perform no security operations on the frame. If the TxOptions parameter specified that the frame has security enabled, the MAC sublayer shall set the SEC bit in the frame control field to 1, and obtain from the MAC PIB the appropriate key(s) and security suite (giving precedence to the entry in the ACL over the default) corresponding to the device address of the orphaned device and perform the operations on the frame as indicated by the security suite using the selected key(s). If there is an error in the secur processing of the frame, the MLME shall return an MLME-SECURITY-ERROR.indication to the higher layers with the appropriate ReasonCode to indicate that the frame could not be protected.

7.1.13 Primitives for writing MAC PIB attributes

7.1.13.1 MLME-SET.request

7.1.13.1.1 Semantics of the service primitive

Author's note: Since a new table was added for the MAC PIB ACL, this should be referenced in this sub-clause. Add a reference to Table 18 from this document under the Valid Range for PIBAttribute and PIBAttributeValue inTable 70 on page 96.

7.1.13.2 MLME-SET.confirm

7.1.13.2.1 Semantics of the service primitive

Author's note: Since a new table was added for the MAC PIB ACL, this should be referenced in this sub-clause. Add a reference to Table 18 from this document under the Valid Range for PIBAttribute in Table 71 on page 97.

7.1.14 Primitives for starting beacon transmissions

7.1.14.1 MLME-START.request

7.1.14.1.1 Semantics of the service primitive

Author's note: Replace the interface for MLME-START.request with the following interface:

```
MLME-START.request      (
                        BPID,
                        LogicalChannel,
                        SuperframeOrder,
                        PANCoordinator,
                        GTSCapability,
                        TxOptions
                        )
```

Author's note: Insert the following entry into Table 72 on page 99:

Table 14—MLME-START.request parameters

Name	Type	Valid Range	Description
TxOptions	Bitmap	0000-x000 (Where x can be 0 or 1)	The transmission options for this command. These shall be a bitwise OR of one or more of the following: 0x08 = security enabled

7.1.14.1.2 Effect on receipt

Author's note: Add the following text after the first paragraph in clause 7.1.17.1.3:

If the TxOptions parameter specified that the beacon frame does not have security enabled, the MAC sublayer shall set the SEC bit to zero and perform no security operations on the beacon frame. If the TxOptions parameter specified that the frame has security enabled, the MAC sublayer shall set the SEC bit in the frame control field to 1, and obtain from the MAC PIB the appropriate key(s) and security suite (giving precedence to the entry in the ACL over the default) corresponding to the broadcast address and perform the operations on the frame as indicated by the security suite using the selected key(s). If there is an error in the secur processing of the frame, the MLME shall return an MLME-SECURITY-ERROR.indication to the higher layers with the appropriate ReasonCode to indicate that the frame could not be protected.

Author's note: Add the following sub-clause to clause 7.1.

7.1.15 Security management primitives

These primitives define how the MLME communicates security related events to the SSCS.

7.1.15.1 MLME-SECURITY-ERROR.indication

This primitive allows the MLME to indicate a failed security processing operation.

7.1.15.1.1 Semantics of the service primitive

This primitive shall provide the following interface:

```
MLME-SECURITY-ERROR.indication (
                                SrcAddress
                                DestAddress
                                ReasonCode
                                )
```

Table 15 specified the parameters for the MLME-SECURITY-ERROR.indication primitive.

Table 15—MLME-SECURITY-ERROR.indication parameters

Name	Type	Valid Range	Description
SrcAddress	Device Address	A short 8-bit allocated address or an extended 64-bit IEEE address.	The individual device address of the entity from which the frame causing the error originated.
DestAddress	Device Address	A short 8-bit allocated address or an extended 64-bit IEEE address.	The individual device address of the device that the frame was intended for.
ReasonCode	Enumeration	UNAVAILABLE-KEY, FAILED-SECURITY-CHECK	The reason for the security error.

7.1.15.1.2 When generated

This primitive is issued by the MLME when it receives an MLME message from a higher layer that requires security, but it is unable to find an appropriate key in the ACL, when it receives a validly formatted frame from another device that induces a failed security check according to the security suite, or when it receives an unprotected frame (SEC bit set to 0) when it is expecting to receive a protected frame (SEC bit set to 1).

7.1.15.1.3 Effect on receipt

On receipt of this primitive, the next higher layer of the initiating device is notified of a security error and the reason for the security error.

Author's note: The four errors that are being caught here are the case when the higher layer tells the MAC to protect a frame that it is unable to protect (e.g. the ACL is missing a key to be used for that device), the case when the MAC is unable to apply the security to the outgoing frame, the case when it receives a frame that has the SEC bit set to 1, but it is unable to process the security (e.g. the ACL is missing a key to be used for that device), and the case when it receives a frame that has the SEC bit set to 1 and the security fails a check (e.g. a faulty integrity code).

7.2 MAC frame formats

7.2.1 General MAC frame format

7.2.1.1 Frame control field

Author's note: Replace table 78 with the following table:

Table 16—Format of the frame control field

Bits: 0-2	3	4	5	6	7-8	9	10-11	12	13	14-15
Frame type	Dest. fields present	Dest. addressing mode	Source fields present	Source addressing mode	Reserved	SEC	Frame fragment specifier	Frame sequence bit	Frame following	Ack. policy

Author's note: Add the following sub-clause to clause 7.2.1.1:

7.2.1.1.1 SEC field

The SEC field is one bit in length. When the SEC bit is set to 0, the frame is not cryptographically protected by the MAC. When the SEC bit is set to 1, the frame is protected using the keys stored in the MAC PIB for that security relationship. The cryptographic operations used to protect the frame are defined by the security suite selected for that security relationship. If no security suite is defined for that relationship, the SEC bit shall be set to 0.

7.2.1.2 Payload field

Author's note: Replace clause 7.2.1.7 with the following text:

The payload field has a variable length and contains information specific to individual frame types. If the SEC bit is set to 1 in the frame control field, the payload is protected as defined by the security suite selected for that relationship.

7.2.2 Format of individual frame types

7.2.2.1 Beacon frame format

7.2.2.1.1 Beacon frame MAC header field

Author's note: Replace the second paragraph in clause 7.2.2.1.1 with the following text:

In the frame control field, the frame type field shall contain the value which indicates a beacon frame, as shown in Table 79, the source fields present field shall be set to one and the source addressing mode field shall be set as appropriate for the address of the beacon. If security is used for the beacon, the SEC bit shall be set to one. All other fields shall be set to zero and ignored on reception.

7.2.2.1.2 Beacon frame payload field

Author's note: Append the following sentence to the end of the paragraph in clause 7.2.2.1.5

If the SEC field is set to 1 in the frame control field, the device shall process the frame according to the selected security suite.

7.2.2.2 Data frame format

7.2.2.2.1 Data payload field

Author's note: Replace the text in clause 7.2.2.2.2 with the following text:

If the SEC bit in the frame control field is set to 0, the payload of a data frame shall contain the sequence of bytes which the next higher layer has requested the MAC sublayer to transmit. If the SEC bit is set to 1, the device shall process the frame according to the selected security suite before passing the data to the higher layer.

7.2.2.3 MAC command frame format

7.2.2.3.1 Command payload field

Author's note: Replace the text in clause 7.2.2.4.3 with the following text:

If the SEC bit in the frame control field is set to 0, the command payload field contains the MAC command itself. If the SEC bit in the frame control field is set to 1, the device shall process the frame according to the selected security suite before processing the command. The formats of the individual commands are described in clause 7.3.

7.3 MAC command frames

7.3.1 Association and disassociation

Author's note: Remove the entries for Authentication request, Authentication response, Challenge request, Challenge response, Request key request, Request key response, Distribute key request, Distribute key response and De-Authenticate request.

7.3.1.1 Association request command

Author's note: Add the following text to clause 7.3.1.1 after the third paragraph:

If security is used for the association request command, the SEC bit shall be set to 1 and the frame shall be protected by the method defined by the selected security suite. Otherwise, the SEC bit shall be set to 0.

7.3.1.1.1 Capability information field

Author's note: Replace table 90 with the following table.

Table 17—Capability information field format

bits: b0	b1	b2	b3-b4	b5	b6	b7
Alternative coordinator	GTS Capability	Power Source	Reserved	Security capability	Allocate address	Withhold address

Author's note: Add the following text after the third paragraph after table 90 in clause 7.3.1.1.1:

The security capability subfield is one bit in length and shall be set to 1 if the device is capable of sending and receiving secure MAC frames. Otherwise the security capability subfield shall be set to 0.

7.3.1.2 Association response command

Author's note: Add the following text after the third paragraph in clause 7.3.1.2

If security is used for the association response command, the SEC bit shall be set to 1 and the frame shall be protected by the method defined by the selected security suite. Otherwise, the SEC bit shall be set to 0.

7.3.1.3 Disassociation notification command

Author's note: Add the following text after the second paragraph in clause 7.3.1.2

If security is used for the disassociation notification response command, the SEC bit shall be set to 1 and the frame shall be protected by the method defined by the selected security suite. Otherwise, the SEC bit shall be set to 0.

7.3.2 Authentication and challenge

Author's note: Remove sub-clause 7.3.2 in its entirety.

7.3.3 Request key

Author's note: Remove sub-clause 7.3.3 in its entirety

7.3.4 Distribute key

Author's note: Remove sub-clause 7.3.4 in its entirety

7.3.5 De-authenticate

Author's note: Remove sub-clause 7.3.5 in its entirety

7.3.6 GTS allocation and deallocation

7.3.6.1 GTS request command

Author's note: Add the following text after the second paragraph in clause 7.3.6.1

If security is used for the GTS request command, the SEC bit shall be set to 1 and the frame shall be protected by the method defined by the selected security suite. Otherwise, the SEC bit shall be set to 0.

7.3.6.2 GTS allocation command

Author's note: Add the following text after the second paragraph in clause 7.3.6.2

If security is used for the GTS allocation command, the SEC bit shall be set to 1 and the frame shall be protected by the method defined by the selected security suite. Otherwise, the SEC bit shall be set to 0.

7.3.7 Coordinator interaction

7.3.7.1 Coordinator interaction command

Author's note: Add the following text after the first paragraph after table 108 in clause 7.3.7.1

If security is used for the coordinator interaction command, the SEC bit shall be set to 1 and the frame shall be protected by the method defined by the selected security suite. Otherwise, the SEC bit shall be set to 0.

7.3.7.2 Coordinator realignment command

Author's note: Add the following text after the second paragraph in clause 7.3.7.2

If security is used for the coordinator realignment command, the SEC bit shall be set to 1 and the frame shall be protected by the method defined by the selected security suite. Otherwise, the SEC bit shall be set to 0.

7.4 MAC functional description

Author's note: The following table should be included along with Table 114 to indicate the MAC PIB Security Attributes.

Table 18—MAC PIB ACL Entries

Attribute	Identifier	Type	Range	Description	Default
macDefaultSecurity	mDS	Boolean	TRUE or FALSE	This indicates whether the device is able to accept or transmit secure frames to devices that are not in the ACL or not.	FALSE
macDefaultSecuritySuite	mDSS	Integer	0x00 - 0xff	The unique identifier of the security suite to be used to protect communications between the MAC and devices not in the ACL.	0
macDefaultSecurityKeys	mDSK	Byte string	Variable	The specific symmetric keys that will be used to protect frames between the MAC and devices not in the ACL.	Empty string
macACLAddress	mACLA	DevAddress	Any valid device address	The 64-bit extended IEEE address or the 8-bit allocated address of the device in this ACL entry.	Device specific
macACLSecuritySuite	mACLSS	Integer	0x00 - 0xff	The unique identifier of the security suite to be used to protect communications between the MAC and the device indicated by the associated macACLAddress.	0
macACLSecurityKeys	mACLSK	Byte string	Variable	The specific symmetric keys that will be used to protect frames between the MAC and the device indicated by the associated macACLAddress.	Empty string

Author's note: Add the following text to the end of clause 7.5:

When the next higher layer requests that security be implemented on a particular frame, the MAC protects the frame using the mechanism defined in sub-clause {xref - 7.5.10}.

Author's note: Add the following sub-clauses to the end of clause 7.5 (after clause 7.5.9):

7.4.1 Frame Security

The MAC is responsible for providing cryptographic security on specified frames when requested to do so by the higher layers. The information for how to provide the security is found in the MAC PIB ACL. Each ACL entry contains an indication of the device(s) that it supposedly shares a key with, an indication of the cryptographic operations it is to perform on sent and received frames from the device(s), and a key or keys that will be used to perform the cryptographic operations.

The cryptographic operations performed on the frames are defined by the security suites. Each device has a number of security suites that it is able to implement. For each entry in the MAC PIB ACL, a security suite is assigned for that entry.

The keys used for these cryptographic operations are inserted into the MAC PIB ACL by the higher layers. For each entry in the MAC PIB ACL, keying material is assigned for that entry. This keying material is then used to provide protection on the frames.

7.4.1.1 MAC PIB ACL

The MAC PIB ACL contains a single default ACL entry and a number of additional ACL entries.

The default ACL entry consists of the macDefaultSecurity field, which indicates whether security is in use for devices not in the ACL, the macDefaultSecuritySuite field, which indicates the default security suite to use for frames to and from devices not in the ACL and the macDefaultSecurityKeys field, which indicates the keying material to use in secure communications to and from devices not in the ACL. If the macDefaultSecurity field is set to FALSE, the macDefaultSecuritySuite field and the macDefaultSecurityKeys fields will not be used.

The additional ACL entries consist of an address of a peer device (may be the 1 byte or 8 byte address) stored in a macACLAddress field, an associated security suite, stored in a macACLSecuritySuite field and some keying material that is stored in a macACLSecurityKeys field.

7.4.1.2 Using the ACL for outgoing frames

If the MLME receives a message from a higher layer to prepare a secure frame for transmission, the MLME shall scan the entries in the MAC PIB ACL for the correct entry to use. The MLME shall first search through the list of macACLAddress entries to find an entry that matches the destination address of the frame to be created. If a match is found, the MLME shall perform operations on the frame according to the security suite from the associated macACLSecuritySuite field and utilize the keying material from the associated macACLSecurityKeys field.

If the MLME is unable to locate a macACLAddress that matches the destination address of the frame to be created, the MLME shall examine the macDefaultSecurity field. If the macDefaultSecurity field is set to TRUE, the MLME shall perform operations on the frame according to the security suite from the macDefaultSecuritySuite field and utilize the keying material from the macDefaultSecurityKeys field.

If the MLME is unable to locate a macACLAddress that matches the destination address of the frame to be created and the macDefaultSecurity field is set to FALSE, the MLME shall return an MLME-SECURITY-ERROR.indication to the higher layer with the ReasonCode set to UNAVAILABLE-KEY.

7.4.1.3 Using the ACL for incoming frames

Author's note: The decision was made for the MAC to accept both secured (SEC = 1) and unsecured (SEC = 0) frames whenever it receives them and to simply indicate to the higher layers whether it was secured or unsecured. The decision to accept or reject the frame based on security considerations is left to the higher layers. This implies that the MAC should not perform any action based on a received frame aside from processing it and sending the appropriate indication to the higher layers. It might be possible instead to add information to the ACL indicating when the MAC should accept or reject unsecured commands if the group desires that feature.

Any incoming frame may be protected by security. If the MLME receives a frame from another device, the MLME shall check the SEC bit in the frame control field to determine if the ACL needs to be consulted.

If the SEC bit in the frame control field is set to 0, the device shall not consult the ACL and shall process the frame as usual.

If the SEC bit in the frame control field is set to 1 the MLME shall scan the entries in the MAC PIB ACL for the correct entry to use. The MLME shall first search through the list of macACLAddress entries to find an entry that matches the source address of the frame received. If a match is found, the MLME shall perform operations on the frame according to the security suite from the associated macACLSecuritySuite field and utilize the keying material from the associated macACLSecurityKeys field.

If the MLME is unable to locate a macACLAddress that matches the source address of the received frame, the MLME shall examine the macDefaultSecurity field. If the macDefaultSecurity field is set to TRUE, the MLME shall perform operations on the frame according to the security suite from the macDefaultSecuritySuite field and utilize the keying material from the macDefaultSecurityKeys field.

If the MLME is unable to locate a macACLAddress that matches the source address of the received frame and the macDefaultSecurity field is set to FALSE, the MLME shall return an MLME-SECURITY-ERROR.indication to the higher layer with the ReasonCode set to UNAVAILABLE-KEY.

7.4.1.4 Applying security to frames

After the MLME receives a request to transmit a secure frame and obtains the appropriate security suite and key(s) from the ACL, the MAC shall apply the operations defined by the security suite using the key(s) to the frame.

Author's note: Since we define encryption and integrity fields to only be included in payload fields of MAC frames, ACK frames are not affected by the security suite and the SEC bit in the frame control field should be set to 0 for all ACK frames.

If the security suite defines encryption, the encryption operation shall be applied to data in the payload field of the frame only. The remaining fields shall be left unencrypted. The result of the encryption operation shall be inserted into the payload field of the frame in the place of the data that was encrypted.

If the security suite defines an integrity code, the integrity code shall be applied to all fields except for the FCS. The result of the integrity code computation shall be placed in the payload field of the frame in addition to any other data in the payload field.

The ordering of the encryption and integrity operations and the placement within the payload field of the outputs of those operations is defined by the security suite.

If any of the security operations fail, the MLME shall return an MLME-SECURITY-ERROR.indication to the higher layers with the ReasonCode set to FAILED-SECURITY-CHECK and shall not transmit the requested frame.

If the security operations have been successfully performed and the payload field has been modified appropriately, the device shall then compute the FCS over the modified frame.

7.4.1.5 Removing security from frames

After the MLME receives a frame that has the SEC bit set to 1and obtains the appropriate security suite and key(s) from the ACL, the MAC shall apply the operations defined by the security suite using the key(s) to the frame.

Before the security operations have been performed and the payload field has been modified, the MLME shall check the FCS (if applicable).

If the security suite defines encryption, the decryption operation shall be applied to data in the payload field of the frame only. The result of the decryption operation shall be inserted into the payload field of the frame in the place of the encrypted data.

If the security suite defines an integrity code, the integrity code shall be checked with the input of all fields except for the FCS and the integrity code itself. If the integrity code succeeds, the integrity code shall be removed from the payload field.

The ordering of the encryption and integrity operations and the location of the security data within the payload field is defined by the security suite.

If any of the security operations fail, the MLME shall return an MLME-SECURITY-ERROR.indication to the higher layers with the ReasonCode set to FAILED-SECURITY-CHECK and shall not perform any additional operations on the received frame.

If the security operations have been successfully performed and the payload field has been modified appropriately, the device may then continue to process the frame.