IEEE P802 Privacy ECSG

|  |
| --- |
| Privacy in 802.16 |
| Date: October 8, 2014 |
| *Authors:* |
| *Name* | *Company* | *Address* | *Phone* | *Email* |
| Phillip Barber  | Broadband Mobile Technologies |  |  | pbarber@broadbandmobiletech.com  |
| *Notice:*This document does not represent the agreed viewof the IEEE 802 EC Privacy Recommendation SG. It represents only the views of the participants listed in the ‘Authors:’ field above. It is offered as a basis for discussion. It is not binding on the contributor, who reserves the right to add, amend or withdraw material contained herein. |
| *Copyright policy:*The contributor is familiar with the IEEE-SA Copyright Policy <<http://standards.ieee.org/IPR/copyrightpolicy.html>>. |
| *Patent policy:*The contributor is familiar with the IEEE-SA Patent Policy and Procedures:<<http://standards.ieee.org/guides/bylaws/sect6-7.html#6>> and <[http://standards.ieee.org/guides/opman/sect6.html#6.3](http://standards.ieee.org/guides/opman/sect6.html%236.3)>. |

# Abstract

This document provides details of Privacy methods in 802.16 standards.

# History

Privacy features introduced as part of IEEE 802.16m-2011 amendment, later re-published as the standalone standard IEEE 802.16.1-2012, the ‘WirelessMAN-Advanced Air Interface’ [1]. The Privacy features applied only to Advanced Mobile Stations and Advanced Base Stations; were not backwards compatible.

# Architecture Overview

Mobile metropolitan area wireless communications system of Advanced Mobile Station(s) (AMS) and Advanced Base Station(s) (ABS).



Figure 1-2—IEEE 802.16.1 Network reference model [1]

IEEE 802.16.1 Protocol layer model



Figure 1-1—IEEE 802.16.1 protocol layering, showing service access points (SAPs) [1]

# 802.16.1 MAC Convergence Sublayer Process

MAC data plane process to encapsulate higher layer protocol payloads with 802.1.1 MAC headers. 802.16.1 MAC header added at ingress at the CS\_SAP, stripped at egress of the communications peer CS\_SAP; exposing only higher layer protocol SDUs out of the top of the CS\_SAP.

For both data plane and management/control plane, station identifier to uniquely identify the AMS-ABS transmission source and destination. Identifier has relevance only within the 802.16.1 communications link AMS-ABS.



Figure 5-2—Classification and CID (or STID/FID) mapping (ABS to AMS) [1]



Figure 1 - Simplified representation of 802.16.1 MAC data plane SDU formation/de-formation

# System Overview

Some relevant IEEE 802.16.1 system characteristics:

* operating on licensed frequencies only
* ABS controlled/scheduled wireless transmission medium resource; ABS transmitted resource mapping including source and destination identities, with time and frequency granularity
* passive network detection method only; no active network detection
* well defined and understood network architecture, as defined by over 50 WiMAX Forum complementary networking specifications, governing all aspects of Access Network, and Core Network configuration and operation
* x.509 manufacturer certificate used by network to identify true device prior to service subscripton acquisition; x.509 subscription certificate on device, supplied by operator at time of subscription acquistion, used by network post- service subscription acquisition to identify true device; true MAC address bound in certificate; certificates used for both device identification during network entry, and for Lawful Intercept network prosecution

# Privacy Feature Overview

Privacy achieved through near total replacement of the use of MAC Address (MAC-48/EUI-48) as the AMS identifier in AMS-ABS communications, both data plane and management/control plane. Replaced with a transitory, 12-bit Station Identifier (STID) on the AMS; replaced with ABSID (24-bit 802.16 Operator ID + 24-bit operator set programmable number). STID assigned from a managed number pool by the ABS. [802.16 Operator ID](http://standards.ieee.org/develop/regauth/bopid/) a managed number space administered by the IEEE RAC.

# Privacy Feature Process Details: Management/Control Plane

All instances of use of MAC-48/EUI-48 as Station Identifier in MAC management/control plane message communications replaced with STID—with two exceptions.

AMS begins network entry process to ABS by first passively acquiring channel and ABS operating info (AMS DL Synchronization), then by AMS sending an active AAI-RNG-REQ unicast control message to the target ABS.

If the ABS has identified that Privacy is NOT ENABLED for AMS-ABS communications, the AMS sends its AMSID (MAC Address) as the station identifier in the first AAI-RNG-REQ message. If the ABS has identified that Privacy IS ENABLED for the AMS-ABS communications, the AMS sends AMSID\* as the station identifier where AMSID\* is:

AMSID\* = Dot16KDF(AMSID|80-bit zero padding, NONCE\_AMS, 48),

where

NONCE\_AMS is a random 64-bit value generated by the AMS [1; pages 329-330]

and where

Dot16KDF(key, astring, keylength)

{

result = null;

Kin = Truncate (key, 128);

for (i = 0; i <= int((keylength-1)/128); i++) {

result = result | CMAC(Kin, i | astring | keylength);

}

return Truncate (result, keylength);

} [2; page 557]

In either instance the ABS acquires the MAC Address of the AMS as part of the initial entry process. AMS MAC Address is transmitted only once more, in an encypted AAI-REG-REQ management/control message during network entry, and that is the last time MAC Address is transmitted in any management/control messages for that session.

During the steps of network entry, including authentication and key distribution, the AMS is first assigned a Temporary STID (TSTID; number from the STID number pool) which is subsequently used to protect the mapping between AMS MAC address and STID so that intruders cannot obtain the mapping information between the MAC address and STID.

The STID is assigned during the registration process after successful completion of the initial authentication/authorization process, and it is encrypted during transmission. The temporary STID is released after STID is securely assigned. The STID is thereafter used as the AMS method of station identification in all AMS-ABS communications, for the duration of the session, or until the STID is reassigned/changed by the ABS (possibly during a handover or re-entry from Idle Mode operation event).



Figure 6-26—Network entry procedure to support AMS location privacy [1]

Figure 6-27 shows the following three levels of protection over control messages:

* No protection: If the AMS and the ABS have no shared security contexts or protection is not required, then the control messages are neither encrypted nor authenticated. The control messages before the authorization phase also fall into this category.
* CMAC based integrity protection: CMAC Tuple is added in a MAC PDU either carrying an unfragmented CMAC protected MAC control message or the last fragment of a CMAC protected MAC control message. CMAC protects the integrity of entire control messages. An actual control message is plaintext.
* AES-CCM based authenticated encryption: ICV part of the encrypted MAC PDU is used for the integrity protection about the payload of control messages as well as AGMH. [1; pages 331-332]

All MAC state change messages are either integrity protected or encrypted.



Figure 6-27—Flow of AAI selective control message protection [1]

For more details on 802.16.1 privacy see 6.2.5.3 Privacy [1].

# Privacy Feature Process Details: Data Plane

The data plane process is much simpler. MAC Address never appears in the MAC header for data SDUs.

However, if the underlying higher layer SDUs are Ethernet, then MAC Address will certainly appear in the Ethernet header of the higher layer SDU, though encapsulated by the 802.16.1 Advanced Generic MAC Header (AGMH). Deep packet inspection will identify the MAC Address in this instance (see Figure 1).

802.16.1 provides two methods to assert privacy and address this threat: payload header suppression(PHS)/robust header compression(RoHC), and encryption of the MAC SDU.

Encryption of the MAC SDU provides the most obvious protection and is readily applied.

But even if encryption of the data is not elected 802.16.1 provides both PHS and RoHC. While the features PHS and RoHC are duplicative and cannot be combined, and RoHC is only defined for application on IP protocol, either of these methods may provide privacy support for higher layer SDUs encapsulated within the 802.16.1 MAC. PHS achieves this by supressing all or part of the higher layer protocol header through an index mapping mask scheme. Alternately RoHC compresses the IP header. Both solutions are applied in the 802.16.1 convergence sublayer and provide a significant measure of obfuscation of the identities of the communications parties of the higher layer protocol in the data plane.

# Summary

Overall it is the combination of management/control plane and data plane techniques that provide the method of 802.16.1 privacy protection. The use of transitory, randomly assigned temporary addresses, the suppression of identifiers embedded in the data stream, and ciphering and integrity protection provide a combination of methods to improve privacy protection in 802.16.1 systems.

**References**

**[1] IEEE 802.16.1TM-2012, IEEE Standard for WirelessMAN-Advanced Air Interface for Broadband Wireless Access Systems, September 2012**

**[2] IEEE Std 802.16™-2009, IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems, May 2009**