Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	Generating Fresh Keys	
Date Submitted	**2005-04-27**	
Source(s)	**Narayanan Venkitaraman,** **Madjid Nakhjiri** **Mark Cudak** **Motorola Inc.**	Narayanan.Venkitaraman@motorola.com Madjid.Nakhjiri@motorola.com Mark.Cudak@motorola.com
Re:	IEEE P802.16e/D6	
Abstract	This contribution describes a method for generating fresh keys between MSS and BS when a MSS does a handoff from one BS to another. It provides the option of sending the BS nonce to MSS prior to handover and sending MSS nonce in RNG-REQ. It also provides the option a timestamp may be used to provide freshness. Furthermore it also provides the BS with the option of using the existing approach where the key is deterministically generated and re-authentication is done based on context tracking.	
Purpose	Generation of fresh keys (HMAC, OMAC, KEK) is essential for protecting against replay attacks and protecting longer term keys (such as PMK). The ability to create such keys freshly without requiring full re-authentication is essential for protecting long term keys and every time can also expedite handoffs.	
Notice	This document has been prepared to assist IEEE 802.16. 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 grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.	
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.	

Generating Fresh Keys

Narayanan Venkitaraman and Madjid Nakhjiri

Motivation

According to the current specification, the keys used for protecting the over-the-air messaging (keys below the AK in the key hierarchy such as HMAC or OMAC key) are not freshly derived. Since the AK is generated from the PMK deterministically for each MSS-BS pair, all the derived keys are also deterministic. For example when using EAP-only authentication AK is derived as follows:

AK = Dot16KDF(PMK, SSID | BSID | "AK", 160).

HMAC_KEY_U | HMAC_KEY_D | KEK <= Dot16KDF(AK, SSID | BSID | "HMAC_KEYS+KEK", 448)

OMAC_KEY_U | OMAC_KEY_D | KEK <= Dot16KDF(AK, SSID | BSID | "OMAC_KEYS+KEK", 384)

Therefore upon reentry of a MSS at a BS on Handover, using same PMK would result in the same HMAC/ OMAC keys and render the channel vulnerable to spoofing or replay attacks. Additionally, due to the frequency of use of HMAC and OMAC keys (for traffic packets), and the deterministic relation between these keys and AK, the AK will be exposed to the various cryptographic attacks made to break these keys.

With reference to RFC 4017, so called Housely criteria used by IETF EAP working group as a method to gauge the appropriateness of use of EAP in authentication and key management methods, domino effect is an important concern, specifically "*compromise of a single authenticator cannot compromise any other part of the system, including session keys and long-term secrets*". Creation of HMAC/ OMAC/ KE keys from the PMK and AK in a deterministic way may cause such a domino effect. Session key freshness is another concern: "*Session keys must be demonstrated to be strong and fresh in all circumstances, while at the same time retaining algorithm independence*." Again creation of HMAC/ OMAC keys from the same PMK and AK upon mobile's re-entry to the same base station does not provide freshness.

Proposed Solution

Freshness of keys could be achieved using unrepeated numbers (referred to as Freshness Values, FV), such as timestamps. The proposal is to provide the option for the MSS and BS to add a freshness parameter so that they can generate fresh keys and also protect against replay attacks. Specifically the proposal is to include the FV in generation of ALL child keys from AK. For instance the current specification provides the following:

HMAC_KEY_U | HMAC_KEY_D | KEK <= Dot16KDF(AK, SSID | BSID | "HMAC_KEYS+KEK", 448)

OMAC_KEY_U | OMAC_KEY_D | KEK <= Dot16KDF(AK, SSID | BSID | "OMAC_KEYS+KEK", 384)

The proposal is to modify it as follows

HMAC_KEY_U | HMAC_KEY_D | KEK <= Dot16KDF(AK, SSID | BSID | MSFV | BSFV | "HMAC_KEYS+KEK", 448)

OMAC_KEY_U | OMAC_KEY_D | KEK <= Dot16KDF(AK, SSID | BSID | MSFV | BSFV | "OMAC_KEYS+KEK", 384).

The BSFV is a fresh value provided to the MSS by the old serving BS as part of the RNG-RSP. The MSFV is a fresh value provided to the current serving BS by the MSS during the re-entry in the RNG-REQ. Using the MSFV, BSFV and the AK, derives HMAC/ OMAC keys and uses these keys as described in the specification. The MS includes the BSFV inside a BSFV TLV and the MSFV inside the MSFV TLV (newly introduced in this contribution). The method by which, the old and current serving BSs share the BSFV (specific backbone messages such as HO-CONFIRM) is out of scope of this document.

A time stamp or a nonce received from the old serving BS can act as BSFV. MSS can either include a local time stamp or generate a random MSNONCE as the MSFV. Using a nonce would be preferable due to the added entropy it provides. By exchanging fresh values as part of existing ranging messaging, the proposed approach will not cause any increase in handover latency, while at the same time providing several cryptographic benefits.

Changes Summary

In section 7.2.2.2, in the newly added last paragraph (before 7.2.2.2.1) changes are:

As detailed in [3], the AAA-key is the shared "master key" that is derived by the two sides in the course of executing the EAP inner method. To ensure that neither the master key nor the EAP long-term credentials get compromised and to provide replay protection, all keys derived from the shared "master key" that are used to secure (authenticate or encrypt) transmissions between the MSS and BS shall be freshly derived. The authentication part of the authorization flow (and the involvement of the generic EAP layer) is now complete.

In section 7.2.2.2.9 Message authentication keys (OMAC/HMAC) and KEK derivation the following changes are made:

MAC (message authentication code) keys are used to sign management messages in order to validate the authenticity of these messages. The MAC to be used is negotiated at SS Basic Capabilities negotiation. There is a different key for UL and DL messages and also a OMAC key for each multicast group (this is DL direction only). As mentioned in section 7.2.2.2, all keys derived from the master key must be freshly derived to ensure protect against domino effect and replay attacks. So a BS Freshness Value (BSFV) and an MSS Freshness Value (MSFV) shall be used when deriving any key from the AK. Timestamps or freshly generated random numbers may be used as freshness value. An MSS shall retain the most recent BS freshness value provided to it in the RNG-RSP or BS-HO-REQ/RSP message from the serving BS. This shall be sent by the MSS during network entry or reentry as the BSFV TLV. In addition the MSS shall create a MSS freshness value and include it as a MSFV TLV in its RNG-REQ message. The BS and the MSS shall use these values to derive keys from the AK as described below. During initial network entry, BSFV value may be skipped and a value of 0 shall be used as the BSFV to compute the keys. A BS may use the freshness values in the RNG-REQ from MSS to protect against replay attacks. The BSFV can be shared between the current serving BS and old serving BS via backbone messages.

The keys used for OMAC calculation and for KEK are as follows:
OMAC_KEY_U | OMAC_KEY_D | KEK <= Dot16KDF(AK, SSID | BSID | MSFV | BSFV | "OMAC_KEYS+KEK", 384)
OMAC_KEY_GD <= Dot16KDF(GKEK, "GROUP OMAC KEY",128) (Used for group management messages MAC)
The keys used for HMAC calculation and for KEK are as follows:
HMAC_KEY_U | HMAC_KEY_D | KEK <= Dot16KDF(AK, SSID | BSID | MSFV | BSFV | "HMAC_KEYS+KEK", 448)
HMAC_KEY_GD <= Dot16KDF(GKEK, "GROUP HMAC KEY", 160) (Used for group management messages MAC)

Figure 134, add the modified formula for HMAC and OMAC

In section 7.2.2.4.1 AK Context, at the end of paragraph "In HO scenario, if the MS was previously connected to the TBS, the derived AK will be identical to the last one, as long as the PMK stays the same. In order to maintain security in this scenario: the context of the AK must be cached by both sides and to be used from the point it stopped if context lost by one side, re-authentication is needed to establish new PMK and new AK context." insert:

A BS may skip re-authentication if the MSS includes a valid MSFV and BSFV TLV in the RNG-REQ. If re-authentication is skipped, fresh keys shall be computed by the MSS and BS as described in section 7.2.2.2.9 and the RNG-REQ and RNG-RSP shall be authenticated using the freshly derived HMAC or OMAC keys.

In section 6.3.2.3.5 Ranging request message, at end of section before the paragraph on HMAC tuple, insert:

The following parameter shall be included in the RNG-REQ message when the MS is attempting to perform network entry

MSFV (see 11.16.2)
BSFV (see 11.16.3)

In section 6.3.2.3.6 Ranging response message, at the end of the section insert:

The following TLV parameter shall be included by the BS in response to RNG_REQ from MSS during network initial entry or reentry.

BSFV (see 11.16.3)
MSFV (see 11.16.2)

In section 11.16 Handover management encodings, after 11.16.1 insert the following:

11.16.2 MSFV

This value may be a freshly generated random number or the lowest (8-32) bits in the current timestamp value maintained by the MSS. It shall be included in the RNG-REQ from MSS during network entry or reentry. A BS may include this in its RNG-RSP as a copy of the value it received from the MSS in the corresponding RNG-REQ

Type	Length	Value	Scope
2	TBD (8-32 bits)	Fresh random number or current time stamp	RNG-REQ, RNG-RSP, MOB_HO-IND

11.16.3 BSFV

When a BS includes this in its RNG-RSP, this value may be a freshly generated random number or the lowest (8-32) bits in the timestamp value. When the MSS includes this in its RNG-REQ, this is the most recent BSFV received from the BS. During initial entry this value may be skipped. If included, it shall be set to 0 and on a handover this value would have been provided by previous serving BS.

Type	Length	Value	Scope
3	TBD (8-32 bits)	Fresh random number or time stamp	RNG-RSP, RNG-REQ, BS_HO-REQ, BS_HO-RSP

In Section 6.3.2.3.51 BS_HO-REQ message, end of section after".. MOB_BSHO-REQ may contain the following TLVs : Resource Retain Time (see 11.16.1"), insert:

BS Freshness Value (BSFV) (see 11.16.3)

In Section 6.3.2.3.53 BS_HO-RSP message, *of section after".. MOB_BSHO-RSP may contain the following TLVs : Resource Retain Time (see 11.16.1"), insert:*

BS Freshness Value (BSFV) (see 11.16.2)

In Section 6.3.2.3.54 HO Indication at the end of the section insert: MOB_HO-IND may contain the following TLVs:

MS Freshness Value (MSFV) (see 11.16.3)
BS Freshness Value (BSFV) (see 11.16.2)