| | | |
|---|---|---|
| Project | **IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16> | |
| Title | **Message authentication in Distributed Security Architecture** | |
| Date Submitted | **2007-07-05** | |
| Source(s) | Masato Okuda<br>Fujitsu Laboratories LTD.<br>Kamikodanaka 4-1-1, Nakahara-ku<br>Kawasaki, Japan. 211-8588 | Voice: +81-44-754-2811<br>E-mail: okuda@jp.fujitsu.com |
| Re: | IEEE802.16j-07/19, "Call for Technical Comments Regarding IEEE Project 802.16j" | |
| Abstract | This contribution clarifies message authentication in distributed security architecture | |
| Purpose | To propose text to describe message authentication in distributed security architecture | |
| Notice | *This document does not represent the agreed views of the IEEE 802.16 Working Group or any of its subgroups*. It represents only the views of the participants listed in the "Source(s)" field above. It is offered as a basis for discussion. It is not binding on the contributor(s), who 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 | The contributor is familiar with the IEEE-SA Patent Policy and Procedures:<br><http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and<br><http://standards.ieee.org/guides/opman/sect6.html#6.3>.<br>Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and <http://standards.ieee.org/board/pat>. | |

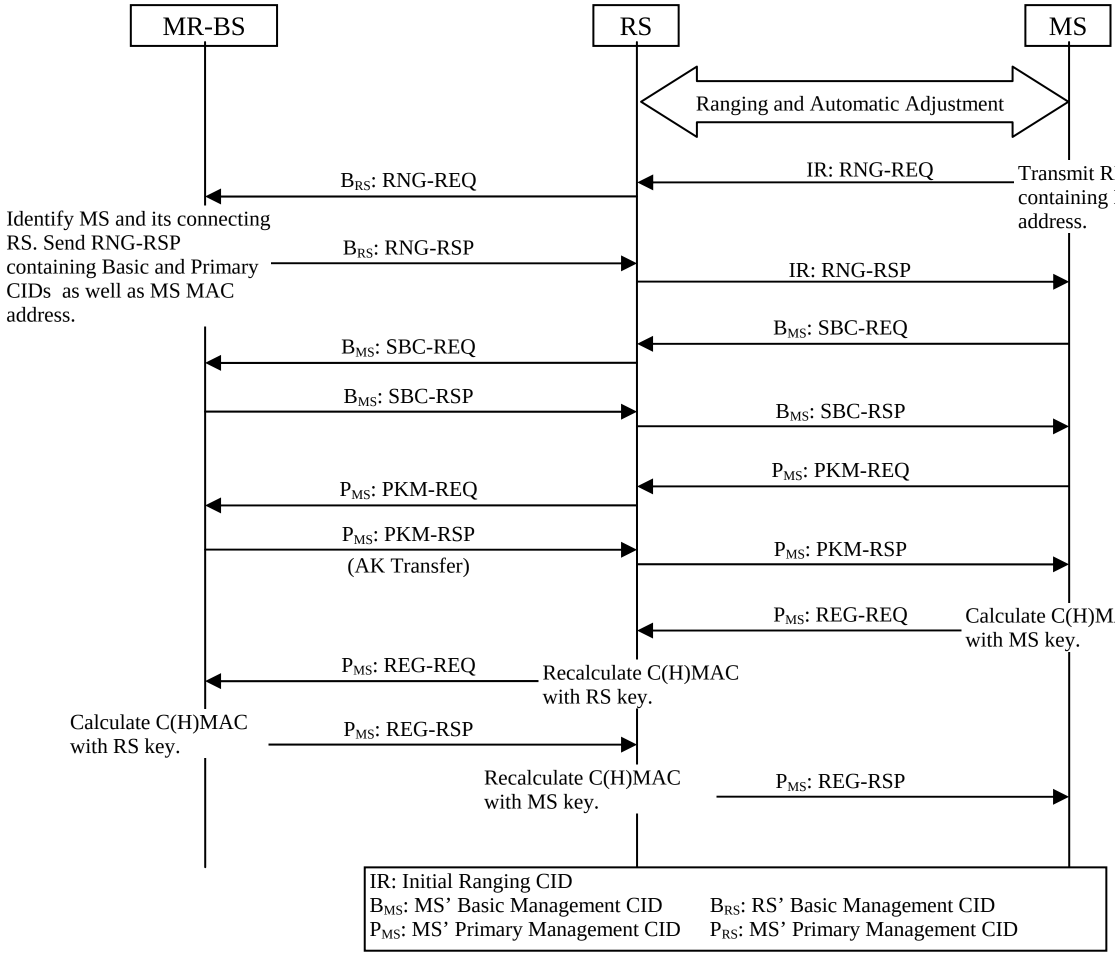
# Message Authentication in Distributed Security Architecture

*Masato Okuda*

## Introduction

The baseline Document [1] specifies distributed security model in the subclause 7.1. However, the baseline does not clearly specify how this security model works in network entry procedure, especially message authentication.

This contribution clarifies message authentication for distributed security model.


MR-BS
RS
MS
Ranging and Automatic Adjustment
$B_{RS}$: RNG-REQ
IR: RNG-REQ
Transmit RNG-REQ containing MS MAC address.
Identify MS and its connecting RS. Send RNG-RSP containing Basic and Primary CIDs as well as MS MAC address.
$B_{RS}$: RNG-RSP
IR: RNG-RSP
$B_{MS}$: SBC-REQ
$B_{MS}$: SBC-REQ
$B_{MS}$: SBC-RSP
$B_{MS}$: SBC-RSP
$P_{MS}$: PKM-REQ
$P_{MS}$: PKM-REQ
$P_{MS}$: PKM-RSP
(AK Transfer)
$P_{MS}$: PKM-RSP
$P_{MS}$: REG-REQ
Calculate C(H)MAC with MS key.
$P_{MS}$: REG-REQ
Recalculate C(H)MAC with RS key.
Calculate C(H)MAC with RS key.
$P_{MS}$: REG-RSP
Recalculate C(H)MAC with MS key.
$P_{MS}$: REG-RSP
IR: Initial Ranging CID
$B_{MS}$: MS' Basic Management CID
$B_{RS}$: RS' Basic Management CID
$P_{MS}$: MS' Primary Management CID
$P_{RS}$: MS' Primary Management CID

The Figure-1 shows an explanatory example of a message exchange sequence in distributed security model.

In the figure-1, MAC management messages are exchanged with MS basic or primary CID after RNG-RSP in the same way as centralized security model. However, scope of message authentication (CMAC/HMAC), which is attached to MAC management messages, is different between centralized and distributed security model because MS security context is shared between MS and the access RS in distributed security while it is shared between MS and the MR-BS in centralized one. After completing MS authentication and establishing security association between MS and the access RS (see detail in 7.1), MAC management messages on the access link shall contain CMAC/HAMC calculated by a key shared between MS and its access RS, while MAC management messages on relay link shall contain CMAC/HAMC calculated by a key shared between RS and the MR-BS. The access RS shall recalculate CMAC/HAMC accordingly when it relays MAC management messages.

Benefits of this scheme are;

- Same connection architecture with centralized security model.
- The access RS can verify SLP-RSP and SCN-RSP which are sent from MR-BS to MS, and get MS sleep and scan information without additional signaling messages, such as MR_SLP-INFO and MS_SCN-INF messages.

## Specific Text Changes

*Insert the new subclause at the end of the 6.3.9.16.2.2 (Non-transparent RS with Distributed Scheduling):*

6.3.9.16.2.2.1 Message authentication in distributed security model

In the distributed security model where MS security context is shared between the MS itself and its access RS, messages authentication is different from the centralized security model where MS security context is shared between the MS itself and the MR-BS.

Once management CIDs are assigned by the MR-BS during ranging process, MAC management messages are exchanged with MS's MAC management CIDs between MS and MR-BS via RSs as described in the previous subclause. However, scope of message authentication (CMAC/HMAC), which is attached to MAC management messages, is different between centralized and distributed security model because MS security context is shared between MS and the access RS in distributed security while it is shared between MS and the MR-BS in centralized one. After completing MS authentication and establishing security association between MS and the access RS (see detail in 7.1), MAC management messages on the access link shall contain CMAC/HAMC calculated by a key shared between MS and its access RS, while MAC management messages on relay link shall contain CMAC/HAMC calculated by a key shared between RS and the MR-BS. The access RS shall recalculate CMAC/HAMC accordingly when it relays MAC management messages.

## References

[1] IEEE 802.16j-07_026r4