| | | |
|---|---|---|
| Project | **IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16> | |
| Title | **An asymmetric security mechanism used in security zone** | |
| Date Submitted | **2007-07-05** | |
| Source(s) | David Comstock, John Lee, Guohui Zou, Yan Peng, Bin Xia<br>Huawei Technologies<br>No.98, Lane91, Eshan Road, Shanghai, P.R.C | Voice: +1 858 735 9382<br>E-mail: {dcomstock, john_lee, ghzou, }@huawei.com<br><br>*<http://standards.ieee.org/faqs/affiliationFAQ.html> |
| Re: | IEEE 802.16j-07/019: "Call for Technical Comments Regarding IEEE Project 802.16j" | |
| Abstract | This contribution aims to introduce an asymmetric security mechanism into the security zone of 802.16j system to protect the integrity of the downlink transmission of the MAC management messages among a group of RSs and MR-BS. This mechanism can coexist with the SZK and protect the message against being modified by the middle RS. | |
| Purpose | This contribution is submitted for discussion and adoption in 802.16j. | |
| 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>. | |

# An asymmetric security mechanism used in security zone

*David Comstock, John Lee, Guohui Zou, Yan Peng, Bin Xia*
*Huawei Technologies Co. Ltd*

## Introduction

This contribution aims to introduce an asymmetric security mechanism into the security zone of 802.16j system to protect the integrity of the downlink transmission of the MAC management messages among a group of RSs and MR-BS. This mechanism can coexist with the SZK and protect the message against being modified by the middle RS.

## Problem Statements

In current 802.16j draft, the SZK mechanism is symmetrical in mature. That is, the same key is used to generate and anthenticate message. As a result, the RS in the middle could modify message, re-calculate the MAC and forword it. Yet the receiver can't determine whether this message is modified during transporting. Figure 1 shows this security threat.

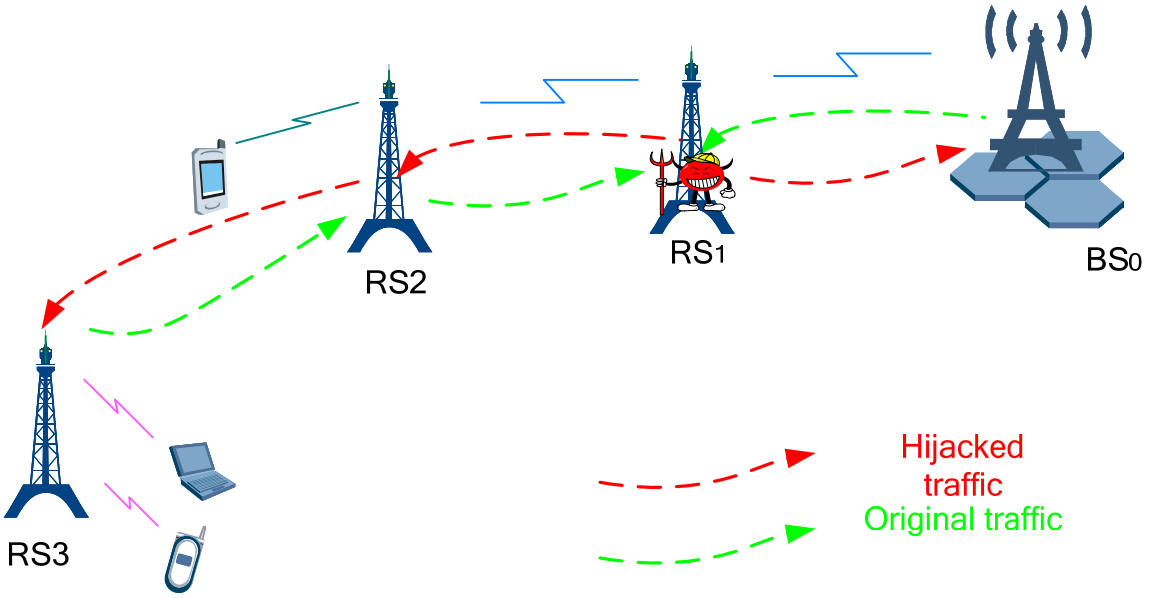


Figure. 1 security threat to SZK mechanism

In commercial networks, different RSs can be deployed. They may be owned by infrastructure provider or customer. They also may be owned by different operators. When the RS belongs to the same operator with the MR-BS, it can be trusted by MR-BS, so SZK can be used to protect relay link. On the contrary, as for the other RSs which belong to the customer or other operator, BS doesn't trust them very much. And then BS should not deliver SZK to them, or it will be a great threat to the system when the RS are malicious or they are cracked. In these cases SZPK, an asymmetrical key mechanism, is proposed to protect the Relay link.

When SZPK is induced, the messages in .16j can be classified into three types:
1) Messages sent by MR-BS or access RS and processed (intermediate RS may modify the messages) by intermediate RS. This applies to MAC management message for admission control. The SZK defined in baseline supports this.

2) Messages sent by MR-BS or access RS and processed (modification to these messages by intermediate RS is not allowed) by intermediate RS. This applies to MAC management message for Path management and admission control（the specific messages of this type are partly listed below . The SZPK we proposed supports this.
3) Messages sent by MR-BS or access RS and not processed by intermediate RS. This applies to all the cases of direct communication between MR-BS and access RS. The security association between MR-BS and access RS takes care of this scenario already. Even intermediate RS modifies the message, the final destination (i.e., MR-BS or access RS) can detect it by verifying the HMAC/CMAC.

Our proposal focuses on the second type. If the SZK is used in this message of this type, there will be a security threat to the system. As shown in Figure 1 of this proposal, the malicious middle relay station has chance to modify the message, and then re-calculate CMAC/HMAC by the SZK. In this case, the receiver can't detect this modification. Our proposal can just be used to protect the message from modifying by middle relay station because the malicious middle RS with SZPK can only authenticate the received message, but it is not able to re-calculate the MAC for the its modified message.

example of messages of type 2 in baseline IEEE 802.16j-06/026r4:
6.3.25.2.1 Path Establishment, Removal and Update
[snip]
page 128: line 32 to line 41.
The RNG_RSP message secured by Group Key is of this type. There is a security threat to the system if group key is used.

6.3.25.2.2 CID to Path Binding
[snip]
page 129: line 4 to line 9
the DSA-REQ message is of this type. There messages should be secured by SZPK.

## Key Management

The SZPK (Security Zone Public Key) is a group key shared by the MR-BS and a group of RS within the same security zone which is used to protect the integrity of the downlink transmission of the MAC management messages among the group. The membership of the security zone (i.e., which security zone(s) a RS should be belong to) is determined by the MR-BS. The Security Zone Public Key (SZPK) is the public key of an asymmetry key pair generated by MR-BS and is distributed by the MR-BS to RS after the RS gets authenticated during initial network entry.

## SZPK Exchange

In order to distribute the Security Zone Public Key (SZPK) to the RS safely within one particular security zone, MR-BS would use security handshake to protect the attacks, i.e. Replay attacks, interception attack. The TEK exchange 3-way handshake procedure specified in the PKMv2 could be used for such purpose.

## Advantages

On downlink, RS can verify the new MAC and trust that the message is unchanged since it is generated by MR-BS.

All RS on downlink can authenticate the message, but are not able to change it.

This proposal is able to coexist with SZK proposed by C802.16j-07/134;

## Specific Text change

++++++++++++ start text proposal ++++++++++++++++++++++++++++++++++
*[Insert the followings at the end of section 3]*

3.107: Security Zone Public Key (SZPK): A Public key shared by the MR-BS and a group of RS within the same security zone which is used to protect the integrity of the downlink transmission of the MAC management messages among the group.

*[Insert section 7.4.4 as following]*

7.4.4 Security Zone Public Key for Multi-hop Relay

The Security Zone Public Key (SZPK) is the public key of an asymmetry key pair generated by MR-BS and is distributed by the MR-BS to RS after the RS gets authenticated during initial network entry. The SZPK can be used to protect the integrity of downlink transmission of MAC management messages among a group. On the uplink, the messages can be protected by the SA between MR-BS and access RS only.

7.4.3.1 Security Zone Integrity Key Exchange

The TEK exchange 3-way handshake procedure specified in the PKMv2 is used for MR-BS to distribute the Security Zone Public Key (SZPK) to the RS within one security zone.

*[Insert the followings in section 7.2.2.2.9]*

SZPK can be generated by MR-BS by RSA algorithm.

*[Change section 7.5.4.4.1 as following]*

For authentication multicast message a SZPK and/or CMAC_KEY_GD shall be used (one for each group). If the SZPK is used only, the MR-BS should calculate hash of the message with a hash algorithm known by all RS on the downlink, and selects the first K bits as input to the RSA algorithm. And then the MR-BS calculate the MAC by the RSA algorithm . If CMAC_KEY_GD is used only, MAC management message can be protected by CMAC. The group authentication key is derived from GKEK, which is the same as SZK. If SZPK and CMAC_KEY_GD are both used, the MR-BS should calculate the CMAC first, and then input the CMAC to the RSA algorithm to calculate the MAC.

For an authentication unicast message transmitted between Relay Stations within the same security zone, a CMAC_KEY_GU or the SA between the Access RS and MR-BS should be used on uplink, and the message is protected by CMAC. SZPK and/or CMAC_KEY_GD shall be used on downlink. The calculation of the MAC on downlink is same as the calculation in multicast situation.

++++++++++++++++++++ *End of text proposal* ++++++++++++++++++++++

## References

[1] IEEE 802.16j-06/026r4