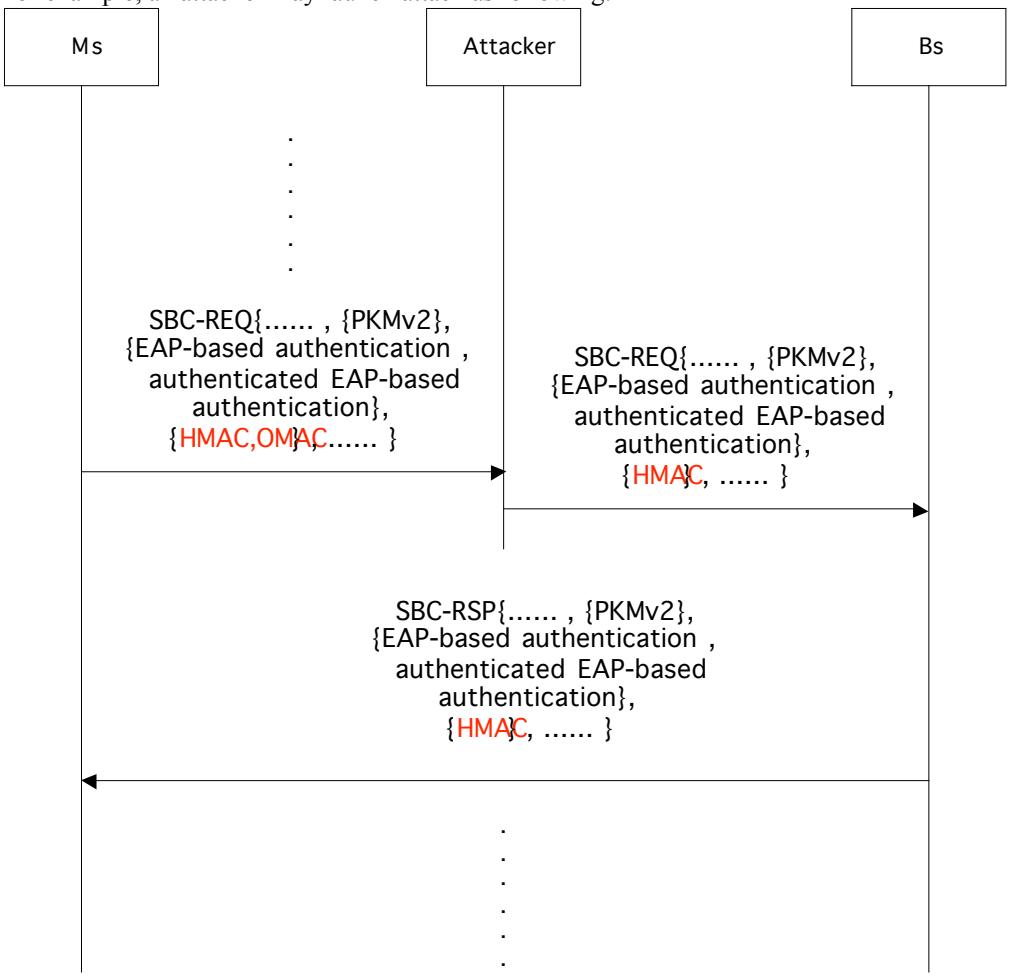
Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Protection Of Security Parameter Integrity**
Date Submitted	**2005-04-24**
Source(s)	Tian Feng, Li Rui Voice: [86-0755-26772016] Fax: [86-0755-26772004] [mailto:li.rui2@zte.com.cn] ZTE corporation ZTE Plaza , Keji Road South , Hi-tech Industrial Park , Nanshan District , Shenzhen , P.R.China , 518057
Re:	Response to Sponsor Ballot on IEEE802.16e/D7 document
Abstract	This contribution describes the enhancement of AK lifetime.
Purpose	To incorporate the text changes proposed in this contribution into the 802.16e/D8 draft.
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>.

Protection Of Security Parameter Integrity

Tian Feng, Li Rui
ZTE corporation

1. Problem Statement

Security parameters(such as PKM version support , authorization policy support , MAC mode , PN window size) are negotiated in basic capability negotiation process . But because SBC-REQ/RSP message doesn't be integrity protected , attacker may juggle those security parameters , and reduce the security capability between MS and BS .
For example, an attacker may launch attack as following:



MS sends SBC-REQ message to BS . The MS support OMAC and HMAC two type MAC mode .
attacker captures the SBC-REQ message , and juggles the MAC mode from "OMAC and HMAC" to "HMAC" , then sends the juggled SBC-REQ message to BS
BS receives the juggled SBC-REQ message , and choice the basic capability , then sends SBC_RSP message to MS . In the SBC-RSP message , the MAC mode is HMAC .
Now the MS and BS will use HMAC to protect message integrity, but HMAC can't resist reply attack , so the attacker can launch reply attack on MS .
The contribution proposes to protect the security parameter of basic capability negotiation message. After authorization, MS sends REG-REQ message protected by OMAC or HMAC to BS. The REG-REQ message includes the security parameters which are identical to those in SBC-REQ message. When BS receives REG-REQ message, it should compare the security parameters between REG-REQ message and SBC-REQ message. If the security parameters are identical, BS can judge that the security parameters of SBC-REQ message have not been juggled by attacker.

2. Proposed solutions

See Error! Reference source not found. for details.

3. Specific text changes

=== Start text changes ====

6.3.2.3.8 Registration response (REG-RSP) message

A REG-RSP shall be transmitted by the BS in response to received REG-REQ .

To provide for flexibility , the message parameters following the response field shall be encoded in a TLV format .

A BS shall generate RET-RSPs in the form shown in Table 22 , including both of the following parameters:

CID (in the generic MAC header)

The CID in the generic MAC header is the Primary Management CID for this SS .

Response

A 1 byte quantity with one of the ~~two~~following values :

0 = OK

1 = Message authentication failure

2 = the Security parameters of REG-REQ are not identical with that of SBC-REQ message

11.7.8.7 ~~Authorization Policy Support~~ Security Negotiation Parameters

~~This field indicates authorization policy that both SS and BS need to negotiate and synchronize . A bit value of 0 indicates " not supported " while 1 indicates "supported" . If this field is omitted , then both SS and BS shall use the IEEE 802.16 security , consistuting X.509 digital certificates and the RSA public key encryption algorithm , as authorization policy .~~

Type	Length	Value	Scope
~~16~~	~~1~~	~~Bit #0 : IEEE 802.16 privacy supported~~ ~~Bits #1-7 : Reserved ,shall be set to zero~~	~~REG-REQ~~ ~~REG-RSP~~

As defined in 11.8.4

The security parameters of REG-REQ message should be identical with those of SBC-REQ message . When BS receives REG-REQ , it should compare the security parameters between SBC-REQ message and REG-REQ message . If they are not identical , BS should judge that the security parameters of SBC-RSP message have been juggled , and response with a REG-RSP message indicating that register failure .
The security parameters of REG-RSP message should be identical with those of SBC-RSP message . When MS receives REG-RSP , it should compare the security parameters between SBC-RSP message and REG-RSP message , if they are not identical , MS may judge that the security parameters of SBC-RSP message have been juggled .

[modify the following as show]

11.8.4 Security Negotiation Parameters

This field is a compound attribute indicating security capabilities to negotiate before performing the initial authorization procedure and the reauthorization procedure.

Type	Length	Value	Scope
25	Variable	The compound field contains the subattributes as defined in Table xxx .	SBC-REQ SBC-RSP REG-REQ REG-RSP

.

=== End text changes ====

4. References

[1] IEEE Standard 802.16e/D7-2004
[2] IEEE Standard 802.16-2004