Project	IEEE 802.16 Broadband Wireless Access Working Group <**http://IEEE 802.org/16**>	
Title	Hybrid authentication hierarchy in MMR Control Plane for the relay network	
Date Submitted	2007-01-08	
Source(s)	Sheng Sun; Guo-Qiang Wang; Hang Zhang; Peiying Zhu; Wen Tong; Mo-han Fong 3500 Carling Avenue Ottawa, Ontario K2H 8E9	Voice: 1-613-763-1315 [mailto:wentong@nortel.com] [mailto:pyzhu@nortel.com] [mailto:shengs@nortel.com]
	Jui-Tang Wang, Jen-Shun Yang, Tzu-Ming Lin, Wern-Ho Sheen, Fang-Ching Ren, Chie Ming Chou, , Ching-Tarng Hsieh, I-Kang Fu Industrial Technology Research Institute (ITRI)/ National Chiao Tung University (NCTU), Taiwan 195,Sec. 4, Chung Hsing Rd. Chutung, Hsinchu, Taiwan 310, R.O.C.	[mailto:jsyang@itri.org.tw] [mailto:rtwang@csie.nctu.edu.tw]
	Yuan-Ying Hsu Telcordia Applied Research Center Taiwan Co., Taipei, Taiwan	[mailto: yyhsu@tarc-tw.research.telcordia.com]
	D. J. Shyy MITRE, USA	[mailto: djshyy@mitre.org]
Re:	A response to a Call for Technical Proposal, http://wirelessman.org/relay/docs/80216j-07_007r1.pdf	
Abstract	Security elements and mechanisms for .16j MMR control plane	
Purpose	To incorporate the proposed text into the P802.16j Baseline Document (IEEE 802.16j-06/026r2)	
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://IEEE 802.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://IEEE 802.org/16/ipr/patents/notices>.

Hybrid authentication hierarchy in MMR Control Plane for the relay network

Sheng Sun; Guo-qiang Wang; Hang Zhang;
Peiying Zhu; Wen Tong; Mo-han Fong
Nortel

1 Introduction

This contribution aims to introduce security mechanisms into the.16j MMR control plane to protect the confidentiality and integrity of the transmission of the MMR control messages. The encryption key distribution and management model are laid on the security principles of PKMv2 required with respect to the IEEE 802.16-2004 and IEEE 802.16e-2005.

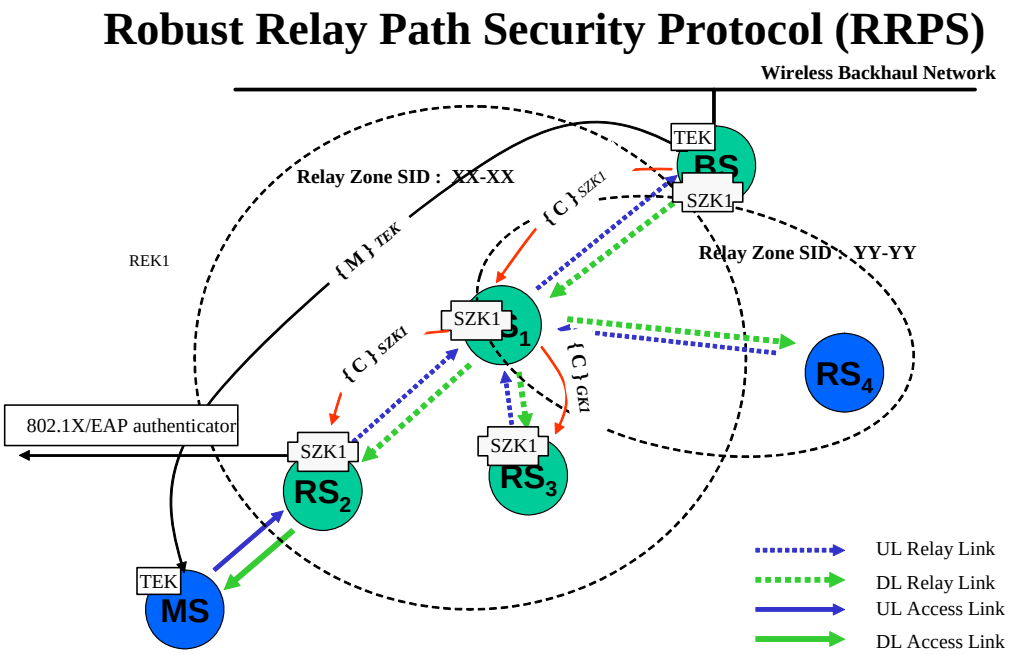

Figure 1 RRPS overview

1.1 RRPS (Robust Relay Path Security)

1.1.1 RRPS overview

Robust Relay Path Security (RRPS) service is used to permit efficient establishment of transmission between the Base Station (BS) and Relay Stations (RS) in a .16j MMR network.

Today's .16e network security services provide the minimum security protection to the control planes messages (Sec 7.1.1 of IEEE 802.16e-2005) in the Access link. The multi-hop based MMR relay network needs more complicated security model in order to satisfy both of the security objective and the performance

objective. In other words, the security mechanism in the .16j MMR network should impose very minimum overhead onto the control plane. Another metric of the security model required for .16j network is the fast link/path establishment and the fast re-association in the case of link failure or the handover operations, and the facilitation of relay grouping and multicast calls

.

RRPS is the security framework comprising the following security elements

Hybrid Association/Authentication Model

Encryption Keys and Keys distribution

The operation of RRPS relies on the BS which centralizes the authentication for the RSs within its Security Zone identified by the SZID (Security Zone ID). Each RS within the security zone becomes the Delegated Authenticator (DA) when it gets authenticated from its anchored authenticator as illustrated in the following diagram.

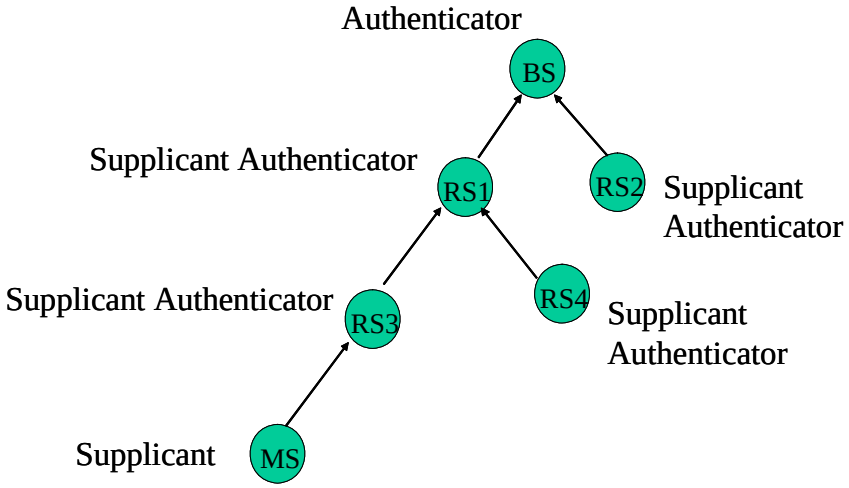

Figure 2 Authentication Hierarcy

This authentication hierarchy distributes the authenticator function to the perimeter of the security zone. Any RS assumes the authenticator role implements the full PKMv2 authentication function. The distributed authentication model virtually extends the BS's authentication function as closer to the .16e/d access link as possible, which brings the following characteristics:

- Basic uses IEEE 802.16e-2005 PKMv2
- Many relay operations are associated with paths, and these operations populate the same information to all RS along a given path
- MMR cell could be decomposed as security zones
- In each zone, the RSs share the same group key for path-oriented operations
- Group key is managed and distributed by BS

- Per Group SA associated HMAC/CMAC is used to authenticate the sender
- Group-cast signaling messages are defined to support path operations
- Greatly reduce the signaling overhead, especially in RS handover case

RRPS requires information to be exchanged during a RS's initial security association with a Authenticator, Subsequent security associations to other Authenticators within the same security zone may utilize the PKMv2 key hierarchy that is established during Initial RRPS Authentication.

Note: How to define security zone is out of scope of this contribution.

1.1.3 Link Establishment

The Initial RRPS Authentication mechanism permits an RS to enable the becoming of the Delegated Authenticator (DA) when establishing security for subsequent links. The DA here involves the process of authentication and key exchange to become the trustworthy authenticator within a specific security zone.

A MR-BS first announces its policy as the root of the security zone which is identified by the Security Zone ID (SZID), the SZID is randomly computed by the MR-BS involving the CID and MAC address of the MR-BS and other parameters. A RS1 bootstraps itself by 802.16 UL/DL sync association with the BS. Then RS1 requests the EAP authentication or be requested by the MR-BS depending on the EAP mode they negotiate. The MSK is distributed by the backend AAA (Radius) server as per PKMv2 as illustrated in Figure

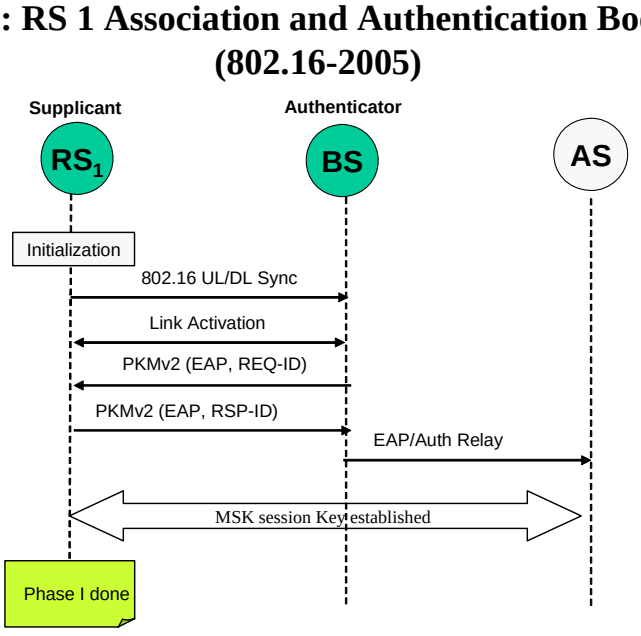

Figure 3 RRPS Security Link Establishment Phase I

Then the MR-BS generates the SZK and distributes it to the RS1 through the SZ Key exchange method. Up to this point, the RS1 becomes the Delegated Authenticator (DA) with the full set of authentication function. The SZ key exchange method could reuse the TEK exchange method specified in PKMv2

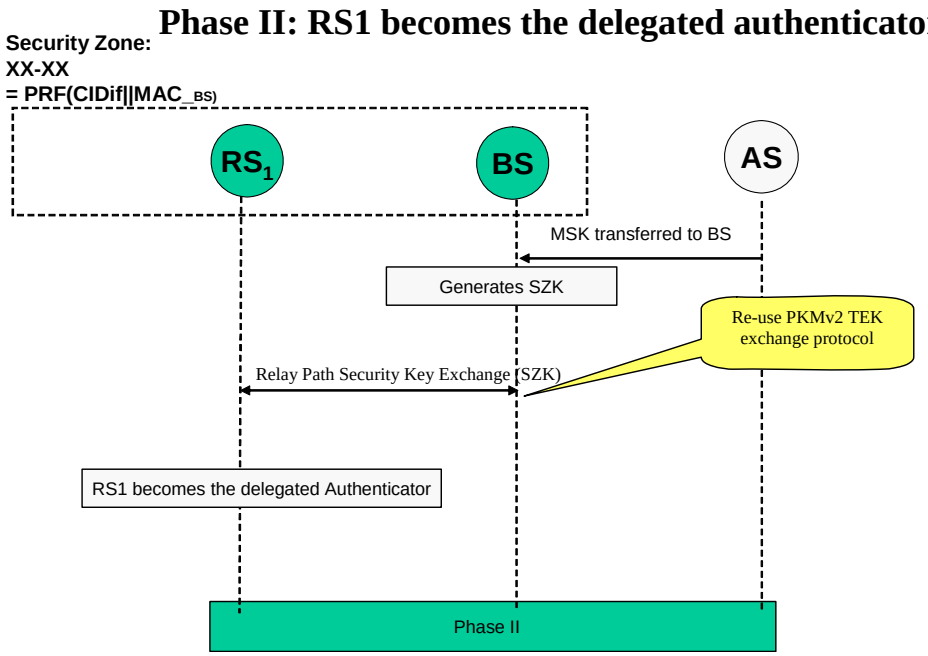

Figure 4 RRPS Security Link Establishment Phase II

Another RS goes through the same handshake and EAP authentication process to become the DA within the security zone. However, RS2 handshakes with the RS1's DA instead of the MR-BS.

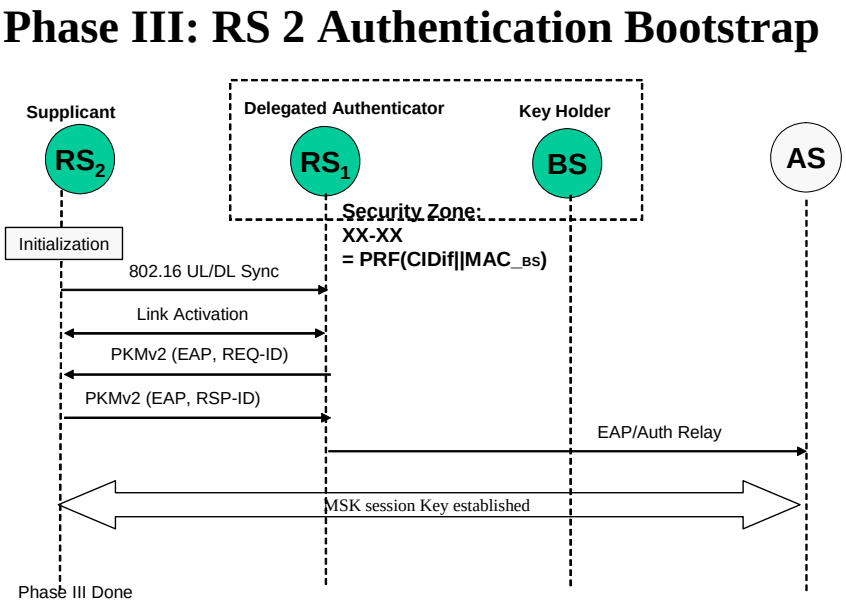

Figure 5 RRPS Security Link Establishment Phase III

Then BS sends the SZK (Security Zone Key) to the RS2 and RS2 inherently becomes the DA.

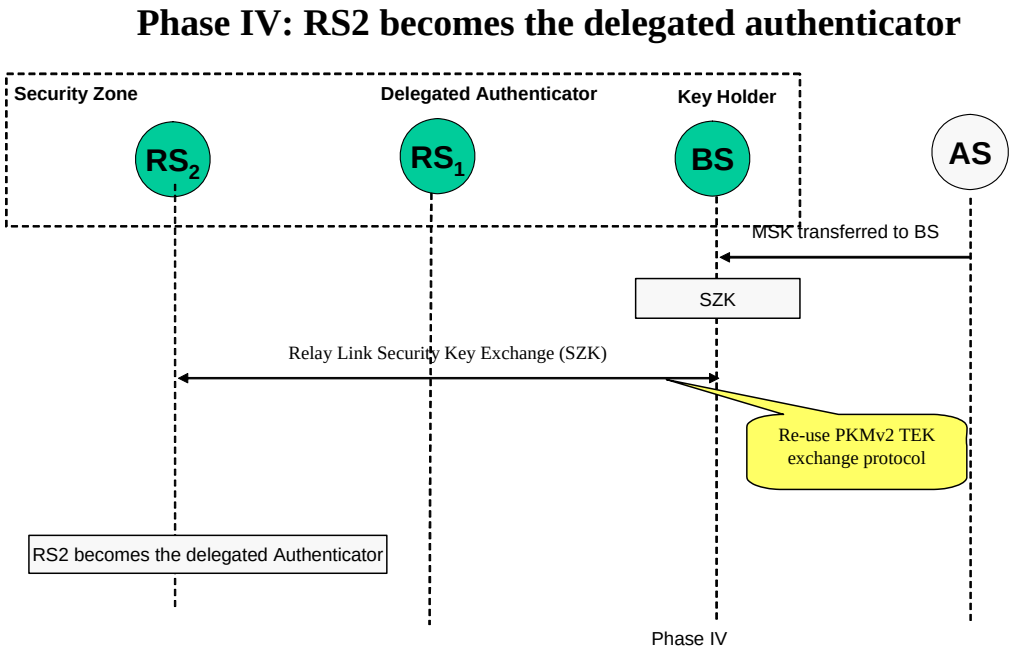

Figure 6 RRPS Security Link Establishment Phase IV

2. Aggregation of Authentication Relay Protocol

According to the specifications in NWG [], the end-to-end authentication structure is depicted as that the authentication protocols between Supplicant (i.e., MS) and Auth. Relay (AR, i.e., BS) is Extended Authentication Protocol/Privacy Key Management version 2 (EAP/PKMv2) protocol, between BS and ASN-GW is the EAP/Auth.Relay protocol, and between ASN-GW and Authentication Server (AS) is EAP/AAA protocol. By inheriting from legacy end-to-end authentication structure, access RS shall be acted like an AR. In other words, access RS shall perform the transformation between EAP/PKMv2 and EAP/Auth.Relay protocols, whereas the BS need not do the transformation again.

transmitting authentication message flow for each RS or MS will consume bandwidth resource and even block the MR network due to precious radio resource for relaying. Therefore, in this contribution, we propose to aggregate authentication messages for several MSs or RSs. As shown in Fig. 7, the access RS (RS_1) acts as an aggregator, whereas the ASN-GW acts like a deaggregator and vice versa. The access RS can collect some PKMv2 messages from several different MSs or RSs within a given period T and aggregate them for forwarding to ASN-GW. Here the period T shall be less than the re-authentication interval defined for each MS or RS. The aggregations are done as following ways.

EAP/PKMv2 (MS <-> AR)	Aggregation	Aggregated EAP/Auth. Relay (AR <-> ASN-GW)

PKMv2 EAP Start	---------->	Aggregated Authentication Relay EAP Start
PKMv2 EAP Transfer	---------->	Aggregated Authentication Relay EAP Transfer
PKMv2 Authenticated EAP Start	---------->	Aggregated Authentication Relay Authenticated EAP Start
PKMv2 Authenticated EAP Transfer	---------->	Aggregated Authentication Relay Authenticated EAP Transfer

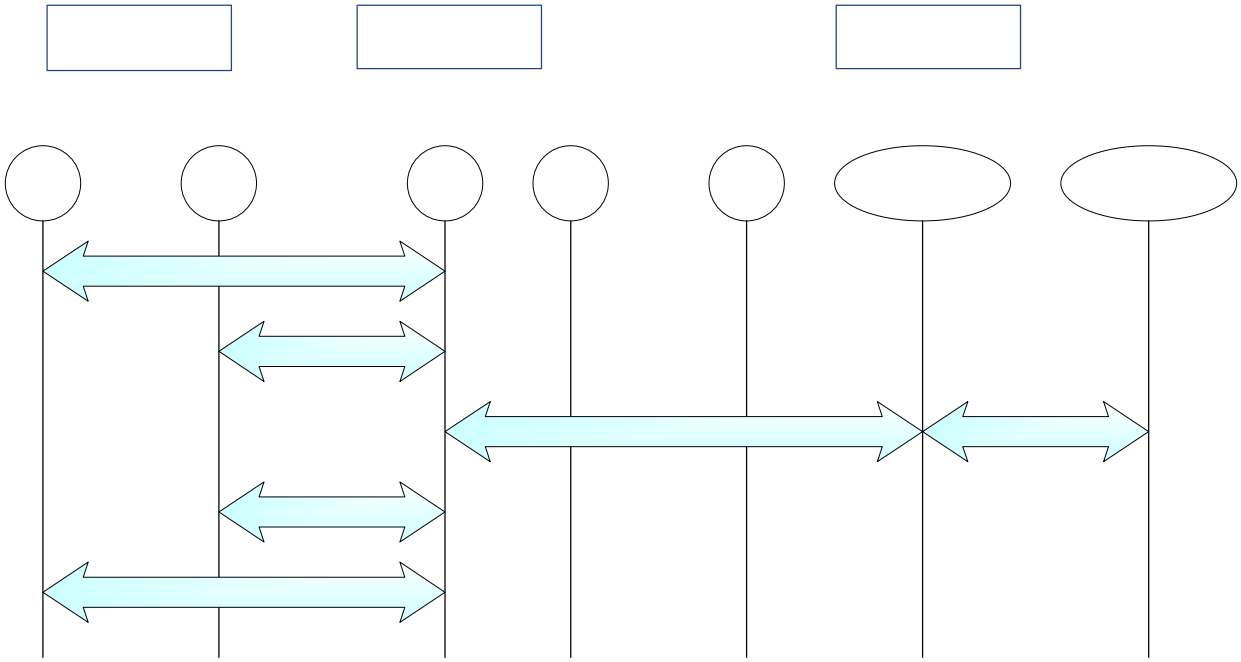

Fig 7. Authentication Message flow with Aggregated EAP/Auth. Relay

2.2 The Aggregation Message Formats

According to the messages defined in EAP/Auth.Relay protocol, we extend the TLV from single TLV to multiple TLVs and add "# of TLVs" filed to indicate the number of TLVs follows. Below messages are the formats for aggregations.

Function Type	Message Type	# of TLVs	TLVs				
TBD	TBD	1..N	1st TLV Name	2nd TLV Name	...	Nst TLV Name	M/O
			MS_1 Info	MS_2 Info	...	MS_n Info	M

Fig. 8 Aggregated Authentication Relay EAP Start

Function Type	Message Type	# of TLVs	TLVs				
TBD	TBD	1..N	1st TLV Name	2nd TLV Name	...	Nst TLV Name	M/O
			MS_1 Info	MS_2 Info	...	MS_n Info	M
			EAP Payload	EAP Payload	...	EAP Payload	M

Fig. 9 Aggregated Authentication Relay EAP Transfer

Function Type	Message Type	# of TLVs	TLVs				
TBD	TBD	1..N	1st TLV Name	2nd TLV Name	...	Nst TLV Name	M/O
			MS_1 Info	MS_2 Info	...	MS_n Info	M

Fig. 10 Aggregated Authentication Relay Authenticated EAP Start

Function Type	Message Type	# of TLVs	TLVs				
TBD	TBD	1..N	1st TLV Name	2nd TLV Name	...	Nst TLV Name	M/O
			MS_1 Info	MS_2 Info	...	MS_n Info	M
			EAP Payload	EAP Payload	...	EAP Payload	M

Fig. 11 Aggregated Authentication Relay Authenticated EAP Transfer

2. Proposed text changes

++++++++++++ start text proposal ++++++++++++++++++++++++++++++++++
[Insert the followings after the end of section 7.1]

The Security Architecture for .16j relay network consists of two concepts:

i) The hierarchal authentication protocol: The protocol has the foundation of the EAP/PKMv2 protocol as the vehicle to grant or deny the MS and RS's authentication. Delegated Authenticator(DA) RS is extending the authentication capability set to RS.

ii) Security Zone: The concept of Security Zone is used to uniquely identify a group comprising of a MR-BS and numerous RS that shares the common security zone key for a period of time. The security zone is constructed and decomposed on a dynamic basis.

The encryption/signature key derivation structure. So as to secure the control message transmitted over the open air, the security protocol defines the security zone key which is shared by all the Relay Stations (RS) for the delivery of the control messages.

The encryption key distribution and management model are laid on the security principles of PKMv2 required with respect to the IEEE 802.16-2004 and IEEE 802.16e-2005.

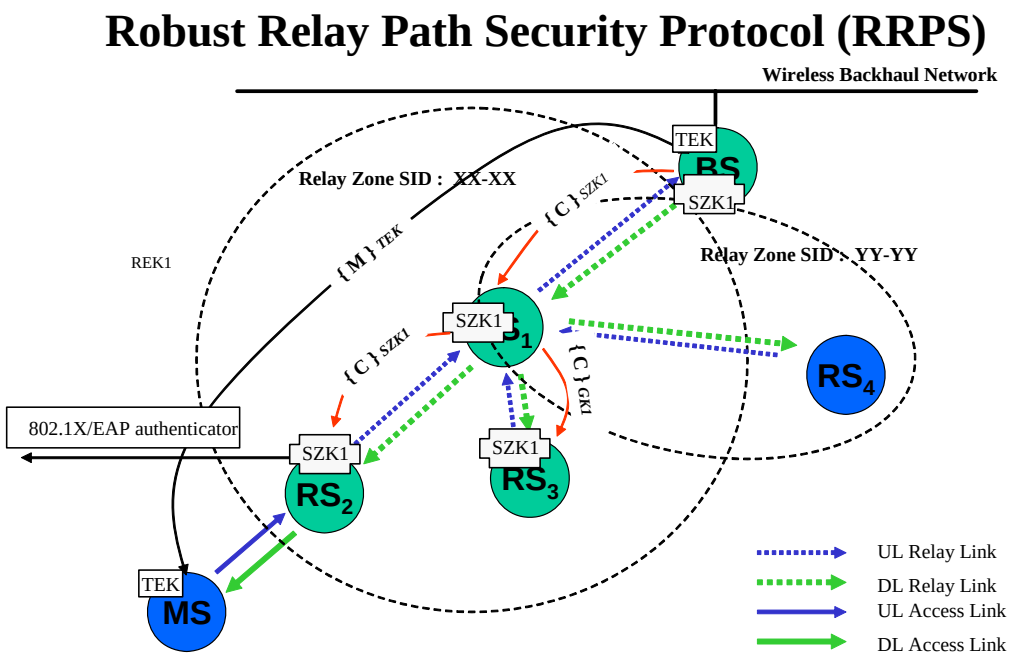

Figure X RRPS overview

Robust Relay Path Security (RRPS) service is used to permit efficient establishment of transmission between the Base Station (BS) and Relay Stations (RS) in a .16j MMR network.

Today's .16e network security services provide the minimum security protection to the control planes messages (Sec 7.1.1 of IEEE 802.16e-2005) in the Access link. The multi-hop based MMR relay network needs more complicated security model in order to satisfy both of the security objective and the performance objective. In other words, the security mechanism in the .16j MMR network should impose very minimum overhead onto the control plane. Another metric of the security model required for .16j network is the fast link/path establishment and the fast re-association in the case of link failure or the handover operations.

RRPS is the security framework comprising the following security elements

Hybrid Association/Authentication Model

Encryption Keys and Keys distribution

The operation of RRPS relies on the BS which centralizes the authentication for the RSs within its Security Zone identified by the SZID (Security Zone ID). Each RS within the security zone becomes the Delegated Authenticator (DA) when it gets authenticated from its anchored authenticator as illustrated in the following diagram.

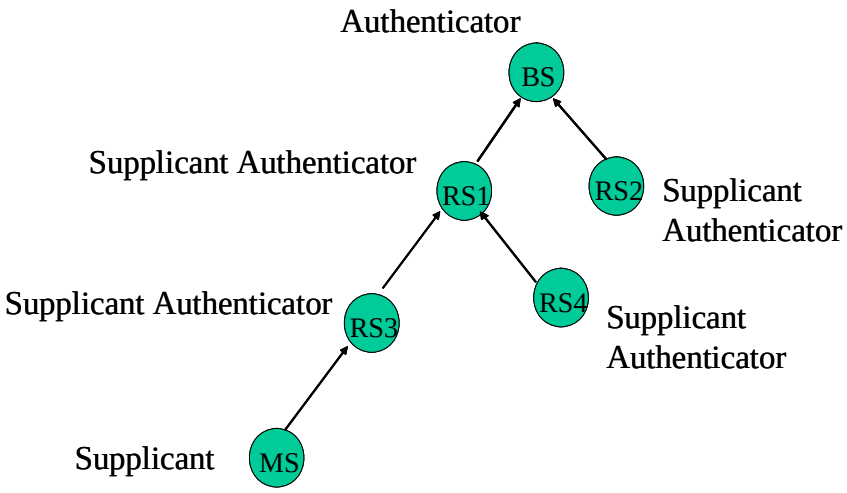

Figure Y Authentication Hierarcy

This authentication hierarchy distributes the authenticator function to the perimeter of the security zone. Any RS assumes the authenticator role implements the full PKMv2 authentication function. The distributed authentication model virtually extends the BS's authentication function as closer to the .16e/d access link as possible, which brings the following characteristics:

- Basic uses IEEE 802.16e-2005 PKMv2
- Many relay operations are associated with paths, and these operations populate the same information to all RS along a given path
- MMR cell could be decomposed as security zones
- In each zone, the RSs share the same group key for path-oriented operations
- Group key is managed and distributed by BS
- Per Group SA associated HMAC/CMAC is used to authenticate the sender
- Group-cast signaling messages are defined to support path operations
- Greatly reduce the signaling overhead, especially in RS handover case

RRPS requires information to be exchanged during a RS's initial security association with a Authenticator, Subsequent security associations to other Authenticators within the same security zone may utilize the PKMv2 key hierarchy that is established during Initial RRPS Authentication.

Note: How to define security zone is out of scope of this contribution.

[Insert the followings after the end of section 7.2]

The Initial RRPS Authentication mechanism permits an RS to enable the becoming of the Delegated Authenticator (DA) when establishing security for subsequent links. The DA here involves the process of authentication and key exchange to become the trustworthy authenticator within a specific security zone.

A MR-BS first announces its policy as the root of the security zone which is identified by the Security Zone ID (SZID), the SZID is randomly computed by the MR-BS involving the CID and MAC address of the

MR-BS and other parameters. A RS1 bootstraps itself by 802.16 UL/DL sync association with the BS. Then RS1

requests the EAP authentication or be requested by the MR-BS depending on the EAP mode they negotiate. The MSK is distributed by the backend AAA (Radius) server as per PKMv2 as illustrated in Figure

Phase I: RS 1 Association and Authentication Bootstrap (802.16-2005)

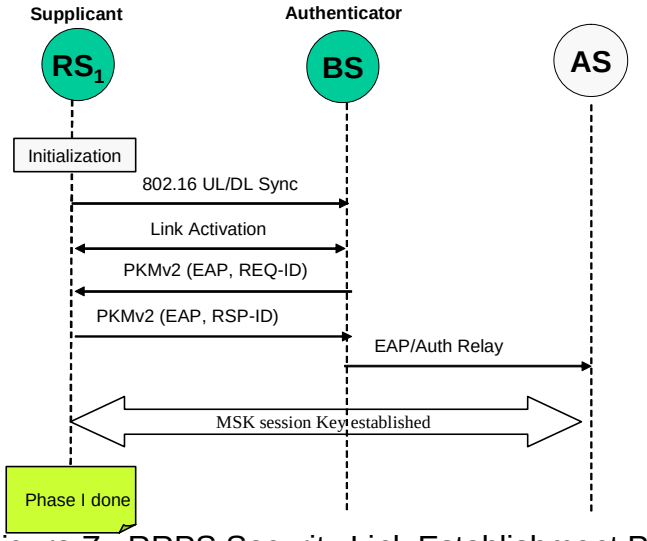

Figure Z RRPS Security Link Establishment Phase I

Then the MR-BS generates the SZK and distributes it to the RS1 through the SZ Key exchange method. Up to this point, the RS1 becomes the Delegated Authenticator (DA) with the full set of authentication function. The SZ key exchange method could reuse the TEK exchange method specified in PKMv2

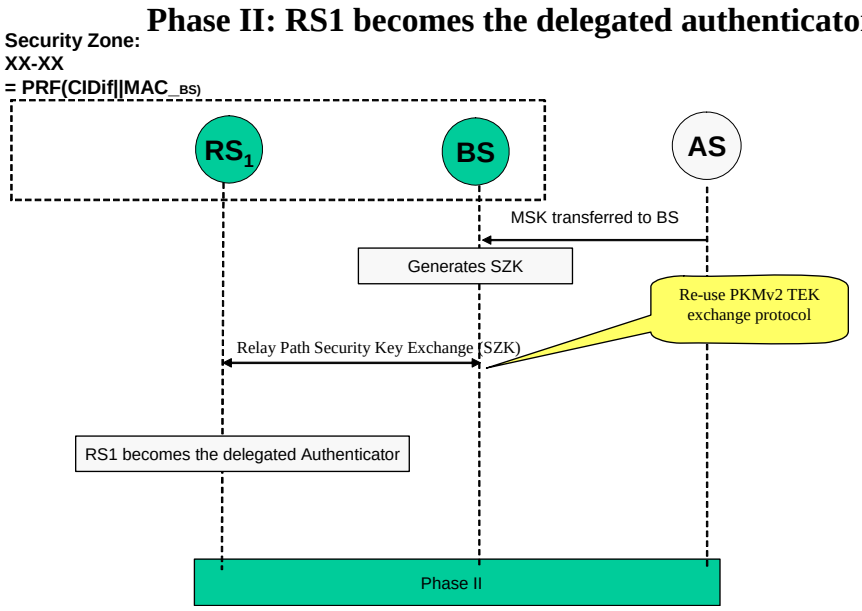

Figure U RRPS Security Link Establishment Phase II

Another RS goes through the same handshake and EAP authentication process to become the DA within the security zone. However, RS2 handshakes with the RS1's DA instead of the MR-BS.

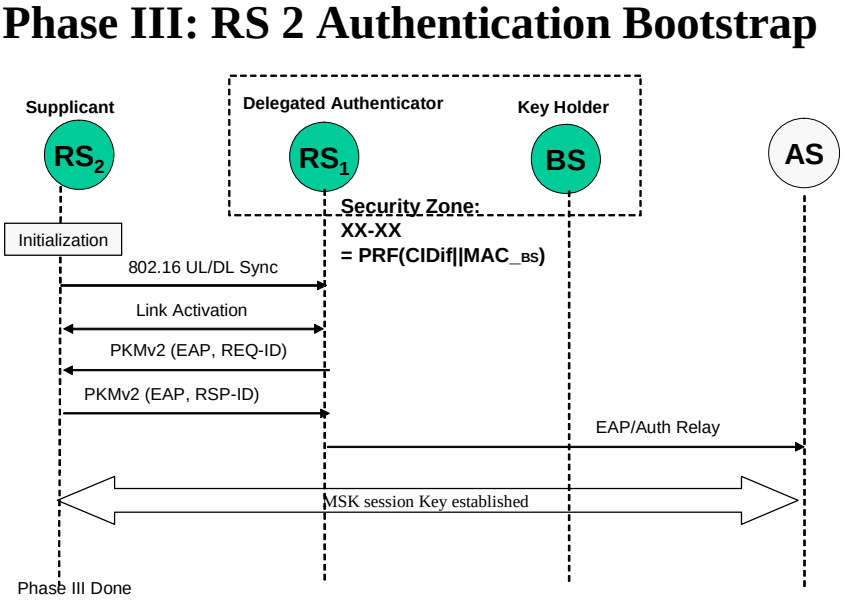

Figure V RRPS Security Link Establishment Phase III

Then BS sends the SZK (Security Zone Key) to the RS2 and RS2 inherently becomes the DA.

Phase IV: RS2 becomes the delegated authenticator

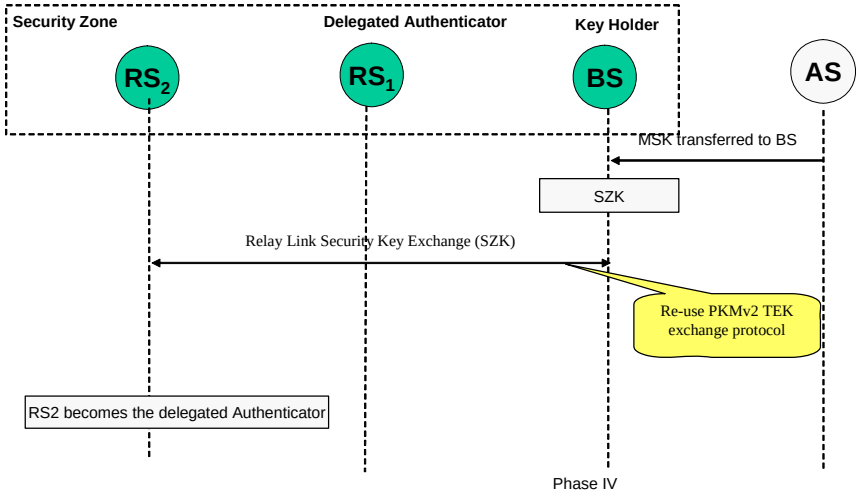

Figure W RRPS Security Link Establishment Phase IV

As shown in Fig. Z, the access RS acts as an aggregator, whereas the ASN-GW acts like a deaggregator and vice versa. The access RS can collect some PKMv2 messages from several different MSs or RSs within a given period T and aggregate them for forwarding to ASN-GW. Here the period T shall be less than the re-authentication interval defined for each MS or RS. By inheriting from legacy end-to-end authentication defined in [], access RS shall perform the transformation between EAP/PKMv2 and EAP/Auth.Relay protocols, whereas the BS need not do the transformation again.

The aggregations are done as following ways.

EAP/PKMv2 (MS <-> AR)	Aggregation	Aggregated EAP/Auth. Relay (AR <-> ASN-GW)
PKMv2 EAP Start	---------->	Aggregated Authentication Relay EAP Start
PKMv2 EAP Transfer	---------->	Aggregated Authentication Relay EAP Transfer
PKMv2 Authenticated EAP Start	---------->	Aggregated Authentication Relay Authenticated EAP Start
PKMv2 Authenticated EAP Transfer	---------->	Aggregated Authentication Relay Authenticated EAP Transfer

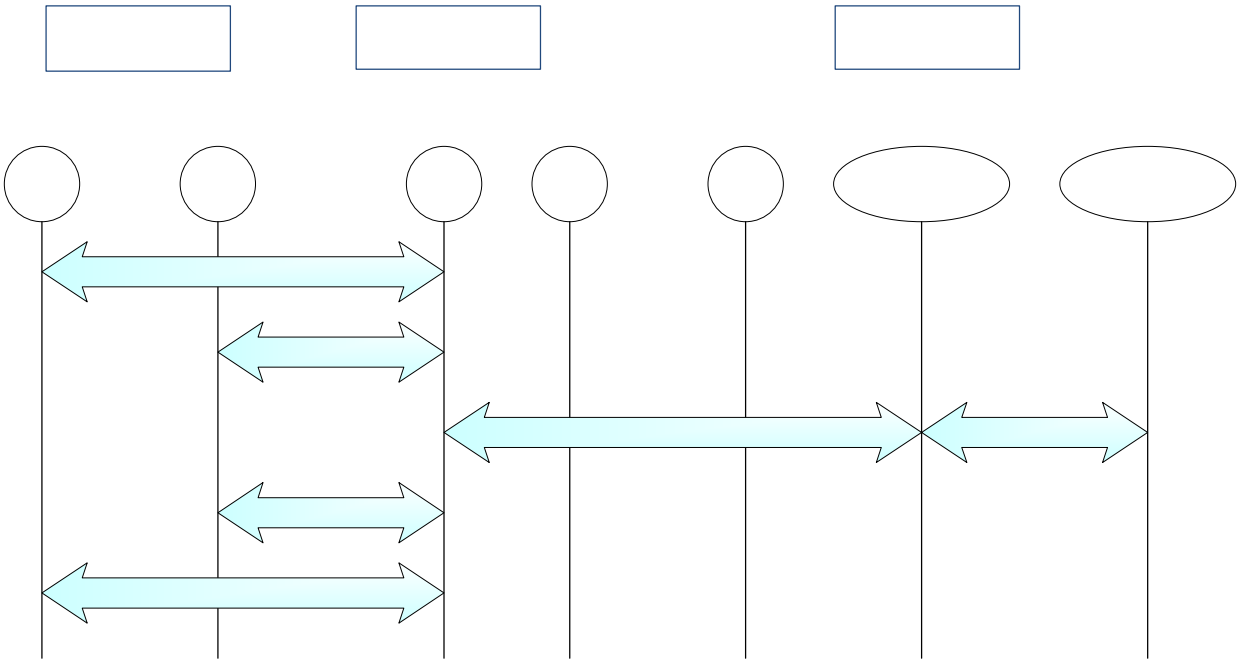

Fig X. Authentication Message flow with Aggregated EAP/Auth. Relay

Supplicants

- The Aggregation Message Formats

According to the messages defined in EAP/Auth.Relay protocol, we extend the TLV from single TLV to multiple TLVs and add "# of TLVs" filed to indicate the number of TLVs follows. Below messages are the formats for aggregations.

Function Type	Message Type	# of TLVs	TLVs				
TBD	TBD	1..N	1st TLV Name	2nd TLV Name	...	Nst TLV Name	M/O
			MS_1 Info	MS_2 Info	...	MS_n Info	M

Fig. Y Aggregated Authentication Relay EAP Start

EAP/PKMv2

EAP/PKMv

Function Type	Message Type	# of TLVs	TLVs				
TBD	TBD	1..N	1st TLV Name	2nd TLV Name	...	Nst TLV Name	M/O
			MS_1 Info	MS_2 Info	...	MS_n Info	M
			EAP Payload	EAP Payload	...	EAP Payload	M

Fig. Z Aggregated Authentication Relay EAP Transfer

Function Type	Message Type	# of TLVs	TLVs				
TBD	TBD	1..N	1st TLV Name	2nd TLV Name	...	Nst TLV Name	M/O
			MS_1 Info	MS_2 Info	...	MS_n Info	M

Fig. ZA Aggregated Authentication Relay Authenticated EAP Start

Function Type	Message Type	# of TLVs	TLVs				
TBD	TBD	1..N	1st TLV Name	2nd TLV Name	...	Nst TLV Name	M/O
			MS_1 Info	MS_2 Info	...	MS_n Info	M
			EAP Payload	EAP Payload	...	EAP Payload	M

Fig. ZB Aggregated Authentication Relay Authenticated EAP Transfer

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