Issues and Scope of MMR

Document Number:

IEEE C802.16mmr-05/037

Date Submitted:

2005-11-11

Source:

Yousuf Saifullah, Yogesh Swami, Charlie Zhang, Haihong Zheng		Voice:	[972 894 5000]
Nokia	Fax:	[+1-972 894 5937]	
6000 Connection Drive	E-mail:	[yousuf.saifullah@nokia.com, yogesh.swami@nokia.com]	
Irving, TX 75039, USA		[charlie.zhang@nokia.com, haihong.zheng@nokia.com]	

Venue:

IEEE 802.16 Session #40, Vancouver, Canada.

Base Document:

None

Purpose:

This is a response to http://ieee802.org/16/sg/mmr/docs/80216mmr-05_021.pdf (call for contributions: IEEE 802.16's Mobile Multi-hop Relay Study Group) to present some discussion material.

Introduction

- Provides input on scope of the work in MMR SG

- Attempts to describe possible approach for solving RS problem

- Suggests to simplify RS problem space for cheaper RS

Security Issues
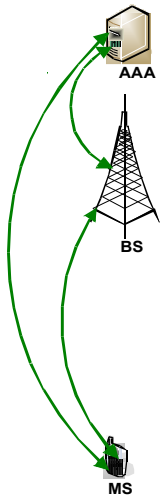
Current 3-party security model

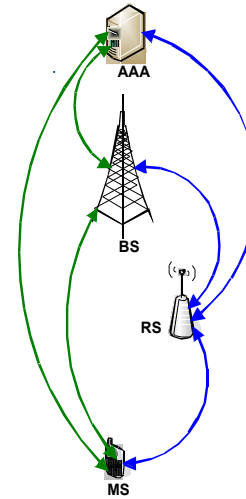With RS, it will become 4-party security model

Impact of RS on PKM

- From key management perspective, adding one RS, will convert the security problem into a 4 party model.
- In the 4 party model, the following security associations need to exist for ensuring trust and distributing session keys:
  - **AAA←→RS**: *New*
  - **AAA←→BS**: *Existing*
  - **AAA ←→MS**: *Existing*
  - **BS←→RS**: *Existing*
  - **RS←→MS**: *New*
  - **MS←→BS**: *Existing*
- Channel binding will be needed in the 4 party model
- Given the complexity of 4 party model, and the requirement that AAA server maintains a secure tunnel between each middle-party (be it BS or RS), it's better to minimize the RS involvement in the security mechanisms.
- Adding multiple RS will add more parties in the security model
- RS could be involved in traffic encryption and message authentication

Impact of RS on the Traffic Encryption

- We can keep traffic encryption/decryption in the BS and MS, the RS doesn't need to take part in the traffic encryption
- The advantage of this approach is that RS doesn't require key-exchange and any new security association between the AAA-server and RS, and doesn't suffer from the channel binding concerns of the "four-party" model.

Impact of RS on the Message Authentication

- Even with minimal functionality on RS, certain management messages (e.g. RNG-REQ/RSP) still need to be authenticated between the RS and MS
- Moreover, there would be some messaging between RS an BS
- This may require a mechanism at RS for message authentication.

Possible Approaches for Relaying

Same Frame Relay

BS->RS burst

RS relays the burst to MS in the same frame

| P | FCH | MAP | | | | P | FCH | MAP | | |

Frame

Different Frame Relay

BS->RS burst

RS relays the burst to MS in a later frame

| P | FCH | MAP | | |

Frame

| P | FCH | MAP | | |

Frame
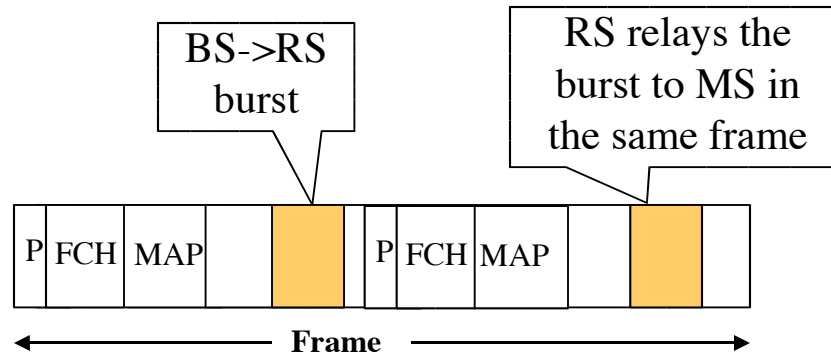
Same Frame Relay vs. Different Frame Relay

Same Frame Relay

+ Scheduling is centralized at the BS: BS schedules for BS<->RS, and also for RS<->MS
+ BS provides MAP for RS also, alleviates RS from managing MAP allocation
+ QoS setup between BS and MS is not impacted with the addition of RS.
+ BS and RS transfer frame within a frame boundary. In this way relaying doesn't increase delay beyond the frame size.
+ Fast feedback can be delivered within one frame

Different Frame Relay

– Scheduling is distributed: BS schedules for BS<-> RS, and RS schedules for RS<->MS
– BS provides MAP for BS<->RS, and RS needs to provide MAP for RS<->MS.
– Requires QoS setup on each hop.
– RS receives frame and then relays bursts in a later frame. Adds delay in frame transfer. Delay increases with the number of hops.
– Fast Feedback may have to go through multiple frames, could become slow

• A simpler RS can be achieved with the same frame relay

• Different frame relay adds more issues and consideration

Mobile RS
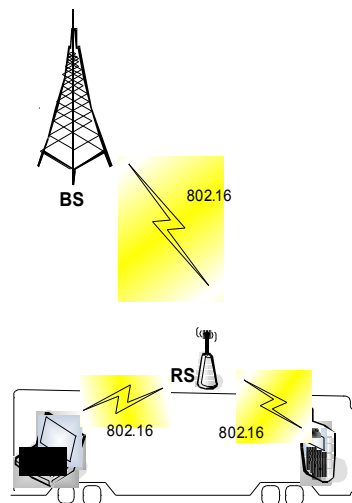
- Mobility of RS means that 802.16 air interface is also on the MS/SS side

- Mobile 802.16 RS may make sense, when an RS is moving with its associated MS/SS, e.g. on a bus or boat…. Continued

Do we need Mobile RS?

- However, in such use cases, an 802.16 MS with 802.11 (WLAN) interface towards the clients is more feasible

- 802.11 is suitable because it is designed for local area coverage.

- This is not an extending coverage case, 802.16 client could simply connect to the BS directly

- Therefore, suggestion is to consider only fixed RS in the scope of MMR

- Earlier contributions, in the MMR SG, also demonstrated a decrease in throughput if the RS is not positioned at an optimal location.
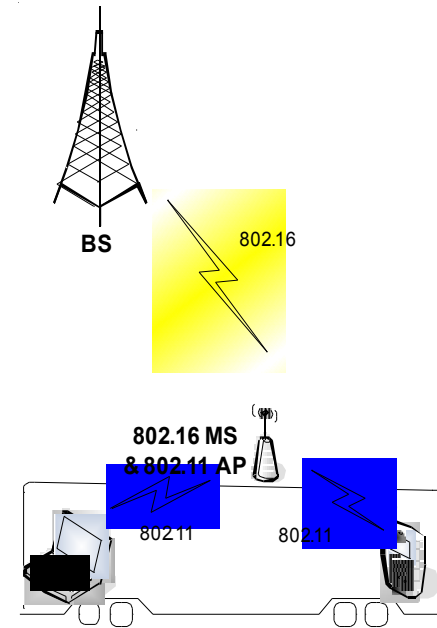
Summary

- We need to resolve security issues with the addition of RS

- Same Frame Relay simplifies functionalities in RS

- Fixed or Nomadic RS is appropriate for extending coverage and maximizing throughput