Project	**IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16>	
Title	**Acceleration of MS Ranging and Network Entrance Processes to Femtocell BS**	
Date Submitted	**2008-10-31**	
Source(s)	Wei-Peng Chen Fujitsu	E-mail:wei-peng.chen@us.fujitsu.com
Re:	IEEE 802.16m-08/040 Call for Comments and Contributions on Project 802.16m SDD TGm SDD: Femtocells	
Abstract	This contribution proposes Femtocell ranging process which enables Femtocell MSs to accelerate ranging and network entrance process via multiple secure ranging codes.	
Purpose	Discussion and approval by TGm.	
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: <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and <http://standards.ieee.org/guides/opman/sect6.html#6.3>. Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and <http://standards.ieee.org/board/pat>.	

Acceleration of MS Ranging and Network Entrance Processes to Femtocell BS

Wei-Peng Chen
Fujitsu

1. Introduction

In the legacy system, all the MSs have equal opportunity to access the BS during the ranging process. However, in Femtocell system, it is highly desirable to grant higher priority to the MSs belonging to the owner of the Femtocell BS (FBS), in particular to an FBS with open group of users. In this contribution, we propose a new Femtocell ranging and network entrance process such that the latency of the MSs accessing their FBS is shortened.

2. Femtocell Ranging Process

In this contribution we propose a new Femtocell ranging process dedicated to the Femtocell MSs (FMSs) when they access their own FBSs. In the common ranging region of the UL subframe, an FMS sends ***multiple*** ranging codes generated from a cryptographically secure pseudorandom number generator (CSPRNG) known only by the FBS and the FMS. The multiple ranging codes are transmitted over multiple ranging slots to increase the probability of successful ranging and thus reduce the ranging latency. Moreover, other MSs that do not know the secret between the FBS and the FMS cannot take advantage of Femtocell ranging process.

The secret used in the CSPRNG were provided by the FBS in an encrypted way when the FMS was connected to the FBS previously. The secret is an input to generate a seed which is used to generate random numbers. Only the FMS and FBS can derive the random numbers. Then the information of start ranging slot and a series of CDMA ranging codes can be extracted from the random number. Therefore, when an FBS transmits multiple ranging codes based on the CSPRNG in a frame, the FBS is able to recognize the sequence of ranging codes which is from a CSG-MS rather from several different MSs. Since the ranging codes are sent in plaintext over the air, there exists a possibility for a malicious attacker to figure out the femto ranging codes via eavesdropping. To prevent such an attack, it is advised that no single femto ranging code generated by a random number generator is used more than once. A reseed procedure is needed when the input to the CSPRNG appeared previously under the same seed.

To detect a sequence of Femtocell ranging codes, it is not necessary for the FBS to successfully decode all the ranging codes in the sequence. As long as a certain percentage of codes are detected, the FMS ranging codes can be identified. Moreover, since multiple raging codes transmitted by the same FMS across different ranging slots have approximately the same transmission time delay (TDD), the FBS can further verify whether an identified sequence of codes are from the same FMS by checking their TDDs. In summary, the proposed Femtocell ranging process can increases the probability of successful ranging and thus shorten the ranging latency.

3. Femtocell Network Entrance Process

After the FBS recognizes a sequence of Femtocell ranging codes with approximately the same TDD from an MS, it can assume the ranging codes are from the FMS. Then FMS is granted an UL allocation to send RNG-

REQ with CMAC TLV. Upon receipt of this RNG-REQ, the FBS can verify whether the message is from the identified FMS and send an RNG-RSP message with CMAC TLV back to the FMS. The FMS can verify the received RNG-RSP from the CMAC value as well and finish the mutual authentication process. After this step, the state at FMS becomes operational and the FMS finish the network entrance procedures.

Figure 1 shows the comparison between the regular network entrance procedures in the legacy system (blue path) and the proposed Femtocell network entrance procedures (red path). Several steps are skipped in the proposed Femtocell network entrance procedures while the security properties are still maintained. Therefore, the network entrance latency for FMSs is much shortened.

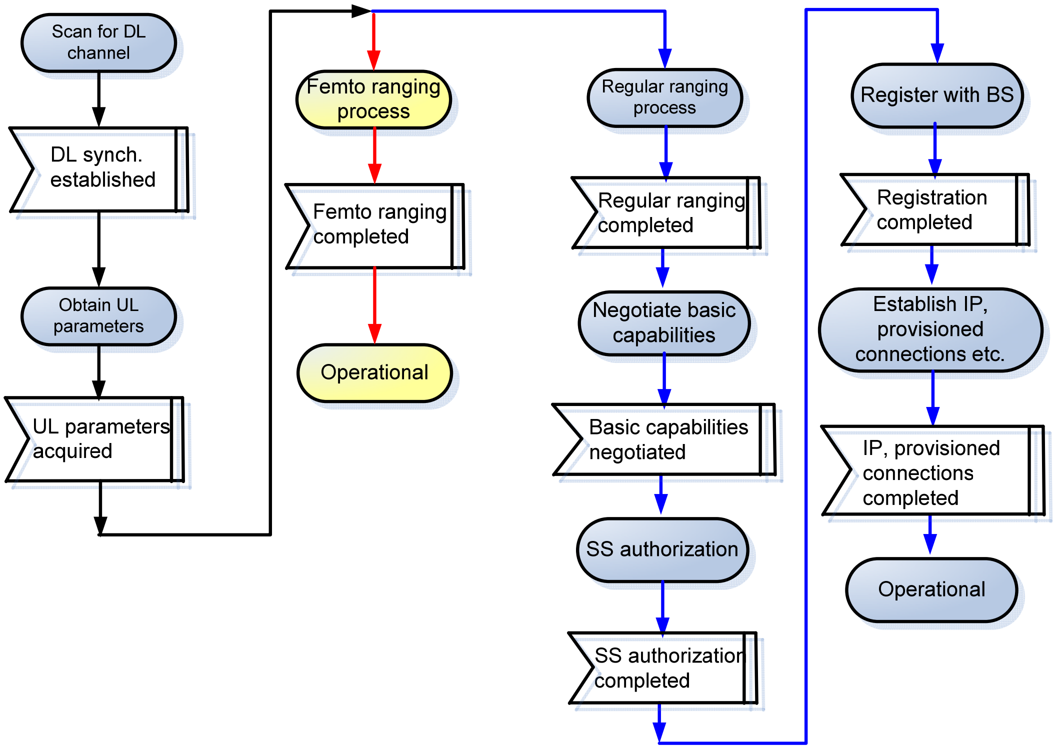

Figure 1 Comparison of the proposed femto network entrance procedures (red path) and regular network entrance procedures (blue path).

3. Proposed SDD Text

[Insert new subclause]

17 Support for Femtocells

17.X Femtocell Ranging Process

A Femtocell MS (FMS) can access its FBS via the Femtocell ranging process in which the FMS sends multiple ranging codes generated from a cryptographically secure pseudorandom number generator (CSPRNG) in the common ranging region of an UL subframe. The random number can be derived only by the FMS and the FBS based on a shared secret.

17.Y Femtocell Network Entrance Process

After an FBS recognizes a sequence of Femtocell ranging codes with approximately the same transmission time delay (TDD) from an FMS, it grants an UL allocation to the FMS to send an RNG-REQ message with the CMAC value. Upon receipt of the RNG-REQ, the FBS verifies whether the message is from the identified FMS and sends an RNG-RSP message with CMAC value back to the FMS. The FMS verifies the received RNG-RSP from the CMAC value as well and finishes the mutual authentication process. After this step, the network entrance state at FMS becomes operational.