libosmo-sccp + libosmo-sigtran - Bug #1995

Segfault when callin osmo_sccp_tx_unitdata() without being connected

04/07/2017 08:44 AM - dexter

Status:	Closed	**Start date:**	04/07/2017
Priority:	Normal	**Due date:**	
Assignee:	laforge	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

The problem occurs when a peer (server role) tries to send unitdata to a remote peer (client) that is not connected.

The attached code contains the source code snippets I used for experimentation.

Good case:
fist start dummy_msc (client), then dummy_bsc (server). The client will connect and when the timer at the server expires unitdata is sent from the server to the client.

Bad case:
start dummy_bsc, when the timer expires, the segfault occurs.

Note: The scheme is a bit odd and not covered by the examples, since there, the server never actively sends data without being stimulated through an existing connection. It is questionable if a server should send unsolicited data at all. In this test, the server role has been chosen for one side because of the lack of an STP.

History

#1 - 04/07/2017 05:22 PM - laforge

- File 0001-osmo_ss7-Fix-segfault-when-routing-MTP-TRANSFER.req-.patch added

- Status changed from New to In Progress

- % Done changed from 0 to 80

please see attached patch, it fixes the issue.

#2 - 04/10/2017 11:55 AM - laforge

- Status changed from In Progress to Resolved

- % Done changed from 80 to 100

has been merged to master.

#3 - 04/25/2017 01:57 PM - laforge

- Status changed from Resolved to Closed

Files

good_case_dummy_msc.log	8.12 KB	04/07/2017	dexter
good_case_dummy_bsc.log	7.53 KB	04/07/2017	dexter
bad_case_dummy_bsc.log	2 KB	04/07/2017	dexter
dummy_msc.tar	50 KB	04/07/2017	dexter
dummy_bsc.tar	60 KB	04/07/2017	dexter
0001-osmo_ss7-Fix-segfault-when-routing-MTP-TRANSFER.req-.patch	1.16 KB	04/07/2017	laforge