CINTERION
WIRELESS MODULES

Application Note 45

Jamming Detection - Radio Link Stability Monitor

Version: 02
DocId: WM_AN45_JammingDetectionRLS_v02

Application Note 45:

Jamming Detection - Radio Link Stability Monitor

Version: **02**

Date: **2008-08-20**

DocId: **WM_AN45_JammingDetectionRLS_v02**

Status **Confidential / Released**

Contents

0 Document History

Preceding document: Application Note 45 "Jamming Detection", v01
New document: Application Note 45 "Jamming Detection", v02

Chapter	What is new
Throughout document	Added further supported products.

1 Introduction

The purpose of this document[1] is to describe how modules monitor their radio link stability and how the monitoring data may be used by software programs to detect jamming of the module's radio downlink by an evenly strong RF transmitter. Such a program can become part of an external application and may as such be employed to detect deliberate GPRS/GSM network interferences posing possible security risks.

The document starts of by describing the monitoring data provided by the module. It goes on to explain how this information can be used to analyze radio link stability.

1.1 Supported Products

This application note applies to the following GPRS/GSM modules and terminals:
- TC65 Module (as of Release 3)
- TC65 Terminal (as of Release 3)
- TC63 Module (as of Release 3)
- XT65 Module
- XT75 Module
- MC75i Module
- TC65i Module
- TC63i Module
- EGS3 Module
- EGS5 Module
- EES3 Module

1.2 Related Documents

[1] AT command set related to your Cinterion Wireless Modules product

To visit the Cinterion Wireless Modules website you can use the following link:

http://www.cinterion.com

1.3 Abbreviations

Abbreviation	Description
ARFCN	Absolute radio frequency channel number
BCCH	Base Control Channel
BS	Base Station
Edv	Error downcounter value
Rssi	Received Signal Strength Indication
URC	Unsolicited result code

1. The document is effective only if listed in the appropriate Release Notes as part of the technical documentation delivered with your Cinterion Wireless Modules product.

2 Monitoring Radio Link Stability

Using the AT command AT^SIND an indicator ("lsta") can be specified that configures the module to monitor the stability of its radio downlink.

Once configured the module will issue URCs providing information on the radio link stability. There are two types of URC provided:

- The first type of URC indicates radio link errors. This type of URC is issued for consecutive radio link errors. A so-called error downcounter value (Edv) is decremented by 1 for every consecutive error. Depending on network settings the Edv count down begins at different values between 1 and 10 (on successful signal decoding the Edv is incremented again). The URC is issued as long as Edv has not reached 0, and is smaller than a given <lstaLevel>. The <lstaLevel> is configured with the AT command AT^SIND and can be set to a value between 0 and 10.
  The first type of "lsta"-URC has 0 as indicator value (<indValue>) and provides the current Edv (<lstaEdv>) and received signal strength (<lstaRssi>) of the radio link:

  +CIEV: "lsta", <indValue>, <lstaEdv>, <lstaRssi>

- The second type of URC indicates loss of network coverage. If Edv has reached 0 the module has lost its radio link and will start the cell re-selection process. The module scans its neighboring cells and issues an URC with information on the scanned radio frequencies. In case the neighboring cell scan is not successful, the module continues with a full band scan, i.e., registering a maximum of 40 ARFCNs for which the signal strength is at least above the minimum received power level. The URC is issued for a second time with the results of the full band scan.
  The second type of "lsta"-URC has 1 as indicator value (<indValue>) and provides the number of scanned frequency channels (<lstaNo>), the maximum frequency value (<lstaMax>), the minimum frequency value (<lstaMin>), the mean of the scanned values (<lstaMean>) as well as the variance of the frequency values (<lstaVar>):

  +CIEV: "lsta", <indValue>, <lstaNo>, <lstaMax>, <lstaMin>, <lstaMean>, <lstaVar>

Note: The first type of URC is not available during active voice or data call connections. In this case only the second type of URC will be issued should the radio link be disturbed or lost. Both URCs are not available in Airplane mode.

For more information on the AT command AT^SIND and the link stability URCs see also [1].

The following Figure 1 illustrates the sequence of URCs during IDLE mode in case the module's radio downlink is interfered with by a jammer.

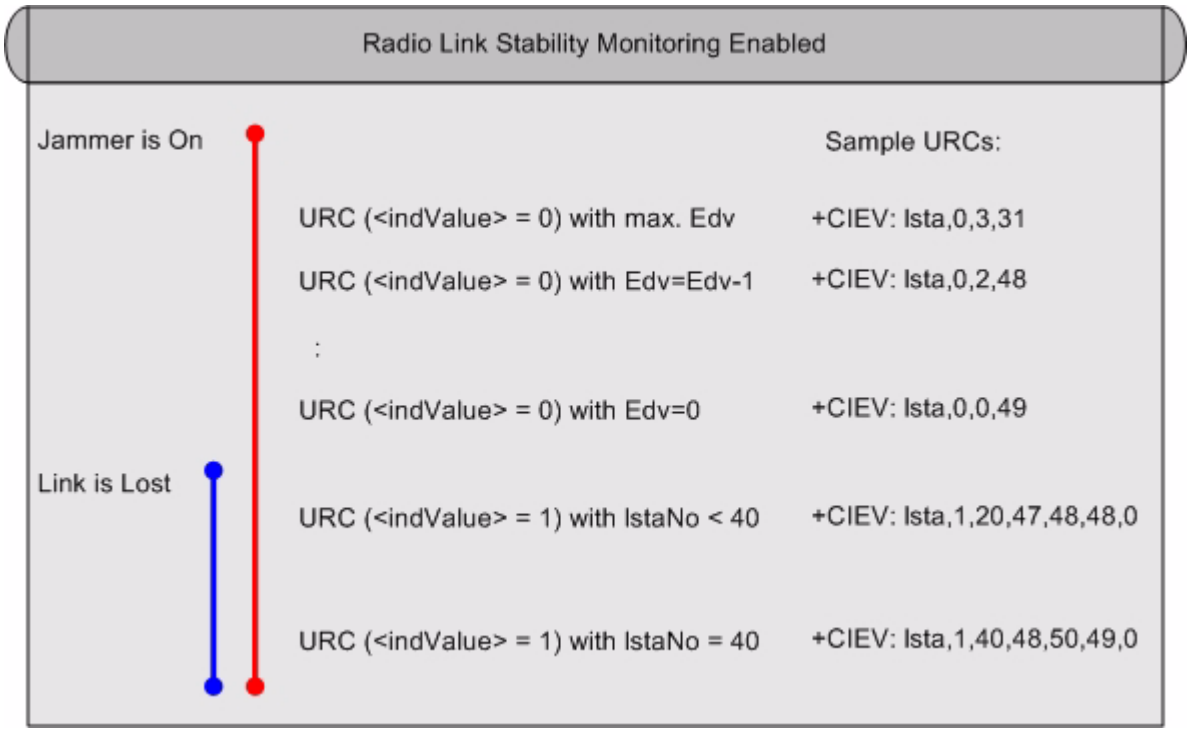

Figure 1: Radio link stability monitoring

3 Analyzing Radio Link Stability

Employing the "lsta" URCs described in Chapter 2 it is possible to analyze the stability of the radio link in order to detect possible jamming by an RF transmitter emitting a strong jamming signal evenly distributed accross the GSM bands. This jamming leads to the module loosing its radio link even though the number of channels as well as the mean of the received signal strength across frequencies are high.

The first type of "lsta"-URC (<indValue>=0) indicates the stability of the radio link. If <lstaEdv>=0, the radio link has been lost. In combination with a rising received signal strength (<lstaRssi>) this could be a first indication for a jammer. However, this type of URC is issued as a warning only during IDLE or SLEEP mode.

The second type of "lsta"-URC (<indValue>=1) indicates a loss of radio link. It may confirm the first jamming indication and allows assumptions about the reasons for the network loss. This URC is also issued during a voice or data call connection.

The following assumptions can be made based on a full band scan and its appropriate URC:

- If <lstaNo>, i.e., the number of registered ARFNCs, is less than 40, the module may be out of network coverage.
- If <lstaVar>, i.e., the signal strength variance across frequencies, is high (~>10), there could be industrial interferences of the radio link. Industrial (non-jamming) interference signifies unintentional radio link disturbances by strong industrial radio sources.
- If the <lstaVar> is low and the <lstaMean> is high (~>40), this could be an indication for jamming. Depending on the distance of the jammer, the <lstaMean> could also be medium.

The terms "high", "medium" and "low" are used in the above assumptions for <lstaMean> and <lstaVar> since it is not possible to state exact value ranges for these parameters that could indicate a jammer. The parameter values are "high" or "low" if compared to the values in a normal transmission situation.

The following Figure 2 illustrates how the issued URCs might be analyzed to determine whether a radio link is corrupted by a jammer or not.

Section 3.1 lists URC examples for radio link monitoring and jamming indications.

Please note that in order to monitor the module's network registration status and to note whether a possible jammer might be on or off again while the module is registered the +CREG URC as well as the +CIEV URCs ("service", "rssi" and "lsta" indicators) should be enabled and checked. For details on how to enable these URCs please see [1].

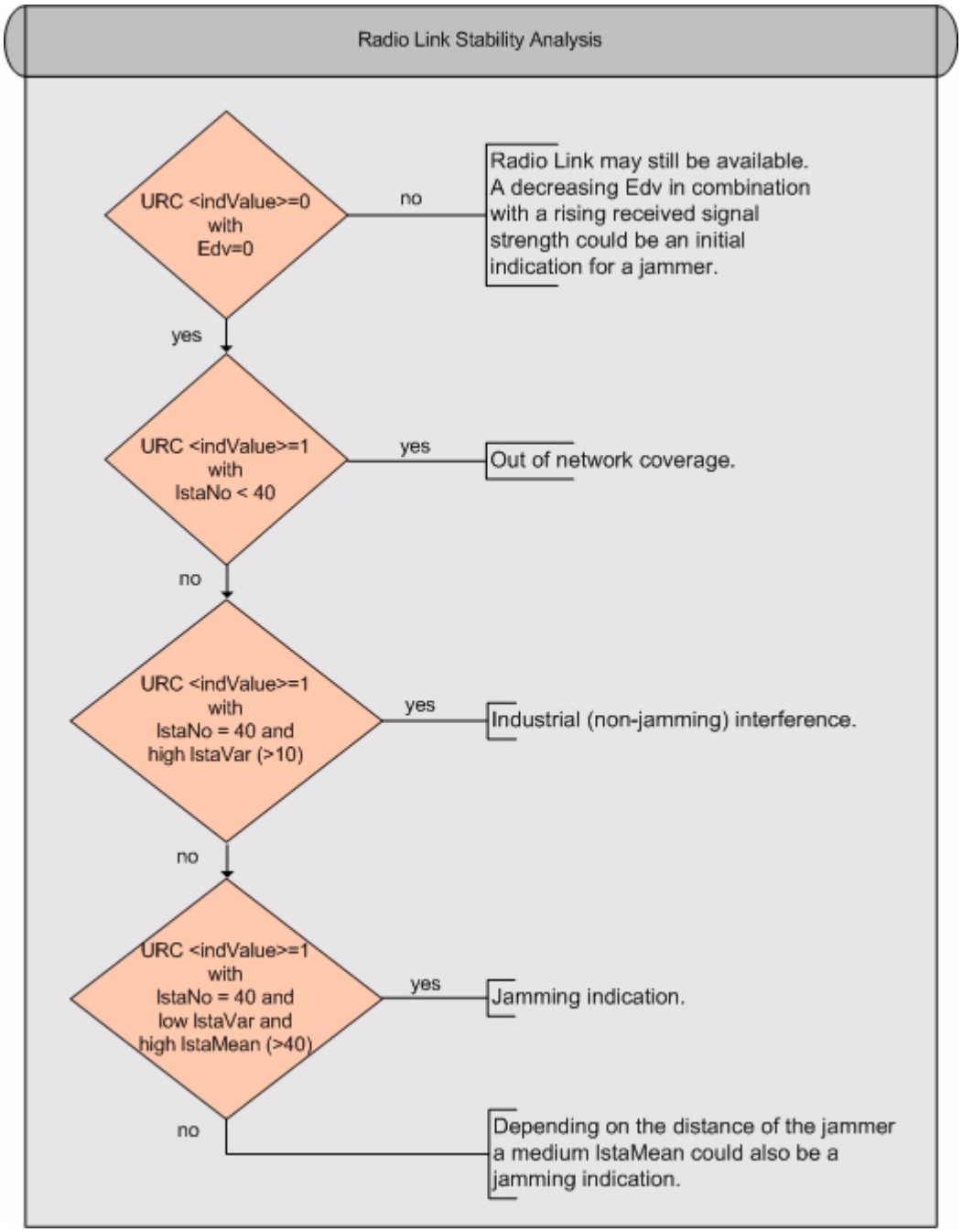

Figure 2: Radio link stability analysis

3.1 Sample Monitoring URCs

This section lists URC sequences for typical monitoring situations. The according "lsta" URCs are marked red and set in italics.

Example 1: No jamming but loss of network coverage, i.e., lstaNo < 40.

```
at^moni
Serving Cell                                    I Dedicated channel
chann rs  dBm MCC MNC  LAC cell NCC BCC PWR RXLev  C1 I chann TS timAdv PWR  dBm Q
ChMod
   65 47  -63 262  02 013A 0516   7   3  33  -107  43 I    No connection

OK

+CREG: 1,"013C","06CD"

+CIEV: rssi,3
+CIEV: rssi,1
+CREG: 1,"013C","06CE"
+CIEV: lsta,0,2,7
+CIEV: lsta,0,1,0
+CIEV: lsta,0,0,0
+CIEV: lsta,1,0,0,0,0,0
+CIEV: lsta,1,5,1,12,8,27
+CIEV: service,0
+CREG: 2
```

Example 2: Jamming while registered and in SLEEP mode, i.e., lstaNo = 40, low lstaVar, high lstaMean. The below sample could also occur if not registered or while searching, and with or without SIM inserted.

```
+CIEV: lsta,0,2,52
+CIEV: lsta,0,1,61
+CIEV: lsta,0,0,60
+CIEV: lsta,1,9,58,60,59,0
+CIEV: lsta,1,40,60,63,60,0
+CIEV: service,0
+CREG: 2
+CIEV: rssi,5
```

Example 3: Jamming during voice call, i.e., URC with <indValue> = 1 only, lstaNo = 40, low lstaVar, high lstaMean

```
atd00496131206930;
atd00496131206930;

OK

+CIEV: sounder,0
+CIEV: rssi,4
+CIEV: call,1
+CIEV: signal,0
+CIEV: call,0
NO CARRIER
+CIEV: lsta,1,8,59,60,59,0
+CIEV: lsta,1,40,60,63,60,0
```