MOST

Media **O**riented **S**ystems **T**ransport

Multimedia and Control Networking Technology

Application Note DTCP Robustness
Rev 1.0
07/2008

MOSTCO CONFIDENTIAL

See page 3 for the terms of disclosure

Legal Notice

COPYRIGHT

LICENSE DISCLAIMER

Nothing on any MOST Cooperation Web Site, or in any MOST Cooperation document, shall be construed as conferring any license under any of the MOST Cooperation or its members or any third party's intellectual property rights, whether by estoppel, implication, or otherwise.

CONTENT AND LIABILITY DISCLAIMER

MOST Cooperation or its members shall not be responsible for any errors or omissions contained at any MOST Cooperation Web Site, or in any MOST Cooperation document, and reserves the right to make changes without notice. Accordingly, all MOST Cooperation and third party information is provided "AS IS". In addition, MOST Cooperation or its members are not responsible for the content of any other Web Site linked to any MOST Cooperation Web Site. Links are provided as Internet navigation tools only.

MOST COOPERATION AND ITS MEMBERS DISCLAIM ALL WARRANTIES WITH REGARD TO THE INFORMATION (INCLUDING ANY SOFTWARE) PROVIDED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

In no event shall MOST Cooperation or its members be liable for any damages whatsoever, and in particular MOST Cooperation or its members shall not be liable for special, indirect, consequential, or incidental damages, or damages for lost profits, loss of revenue, or loss of use, arising out of or related to any MOST Cooperation Web Site, any MOST Cooperation document, or the information contained in it, whether such damages arise in contract, negligence, tort, under statute, in equity, at law or otherwise.

FEEDBACK INFORMATION

Any information provided to MOST Cooperation in connection with any MOST Cooperation Web Site, or any MOST Cooperation document, shall be provided by the submitter and received by MOST Cooperation on a non-confidential basis. MOST Cooperation shall be free to use such information on an unrestricted basis.

TRADEMARKS

MOST Cooperation and its members prohibit the unauthorized use of any of their trademarks. MOST Cooperation specifically prohibits the use of the MOST Cooperation LOGO unless the use is approved by the Steering Committee of MOST Cooperation.

SUPPORT AND FURTHER INFORMATION

For more information on the MOST technology, please contact:

MOST Cooperation
Administration
D-76185 Karlsruhe
Germany

Tel: (+49) (0) 721 966 50 00
Fax: (+49) (0) 721 966 50 01
E-mail: contact@mostcooperation.com
Web: www.mostcooperation.com

Contents

1 INTRODUCTION 6

1.1 References 6
1.2 Purpose 6
1.3 Description 6

2 ROBUSTNESS MEASURES 7

3 APPENDIX A: INDEX OF FIGURES 10

4 APPENDIX B: INDEX OF TABLES 10

Document History

Change Ref.	Section	Changes
1V0_001	General	Initial Version.

1 Introduction

1.1 References

All documents, which are referenced by this MOST document, are listed here along with their versions.

Document		Revision
[1]	**MOST Specification**	2.5
[2]	**MOST Content Protection Scheme DTCP Implementation**	2.2
[3]	**MOST Specification for Stream Transmission**	1.3.1

Table 1-1: Document references

1.2 Purpose

This document describes the measures used to increase DTCP stream transmission robustness in a disturbed environment.

1.3 Description

Problems with DTCP stream transmission can arise from

- Errors in the DTCP packet structure
- Errors in the DTCP packet header
- Errors in the DTCP packet InfoBytes
- Errors in the DTCP packet payload

This document offers ways to remedy the effects of those errors. In particular, the DTCP Robustness application note aims at reducing or entirely eliminating fatal odd/even errors and helps to detect simple bit errors in the data area.

The diagram below is based on the example that is included in the Content Protection Scheme DTCP Implementation Specification [2]. The arrows indicate which areas are covered by the measures detailed in this application note.

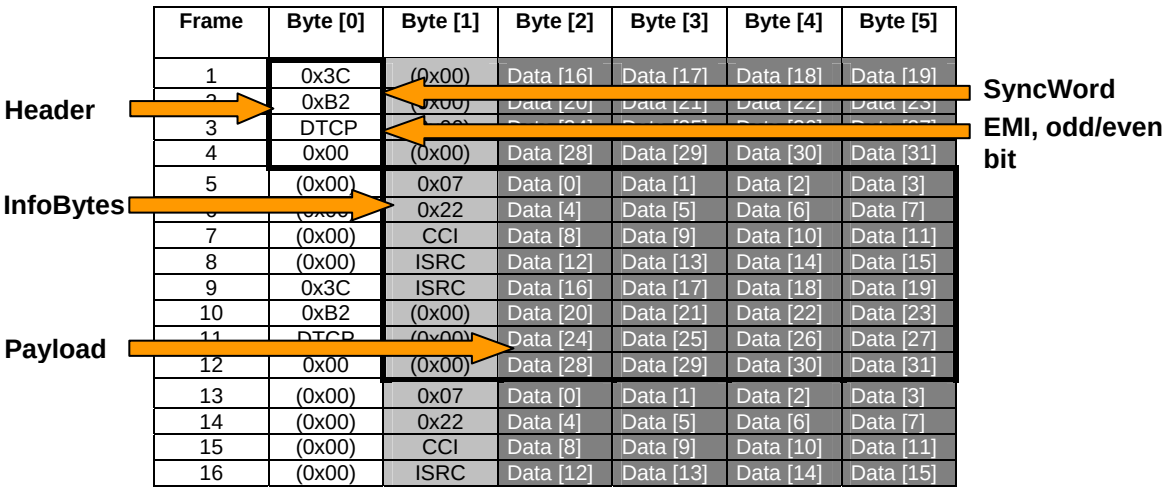

Figure 1-1: Robustness measures in DVD-Audio Stream Protected by MOST-DTCP

2 Robustness Measures

The diagram on page 8 presents the details of the preventive measures and the reaction on certain DTCP errors. The diagram gives evidence of the different error causes. It is not intended to describe error detection.

Packet structure errors
Packet structure errors usually manifest themselves as SyncWord corruption. Bit errors within the non encrypted area occur and no DTCP Block will be recognized.
The measure taken is to mute the data output.

Packet header errors - odd/even bit change
When packet header errors occur, the decipher engine may use the wrong (next) content key, which will, for example, lead to disturbed audio.
The measure taken is to not change the content key if the odd/even bit change time is shorter than 30 seconds.

Note: *Before every content key increment, the current content key is stored.*

Packet header errors - EMI errors
When Encryption Mode Indicator (EMI) errors occur, the decipher engine might be using the wrong content key.
The solution is to mute the data output.

Note: *If the EMI is corrupted, the associated frame will be damaged; however, the following frames will be valid again.*

Packet InfoBytes errors
This group of errors is characterized by inconsistent InfoBytes after decryption where the InfoBytes remain defective for several DTCP packets.
The measure taken is to mute the data output and retrieve the current *nonce* from the DTCP source. This is done through the use of DTCP_Control.StartResult (see the EstablishContentKeys MSC in the DTCP Content Protection Scheme Specification.)
If the InfoBytes still remain defective, a new AKE is triggered.

Packet payload errors
The severity of content corruption differs depending on the type of content. For example, in streaming PCM data, bit errors that occur at low rates are often hardly audible. On the other hand, when streaming compressed data, a bit error might lead to the corruption of the complete packet.
The solution is to mute the output if the data decoder recognizes errors in compressed data. Optionally, a detected error in an audio sample can be corrected by interpolation instead of muting.

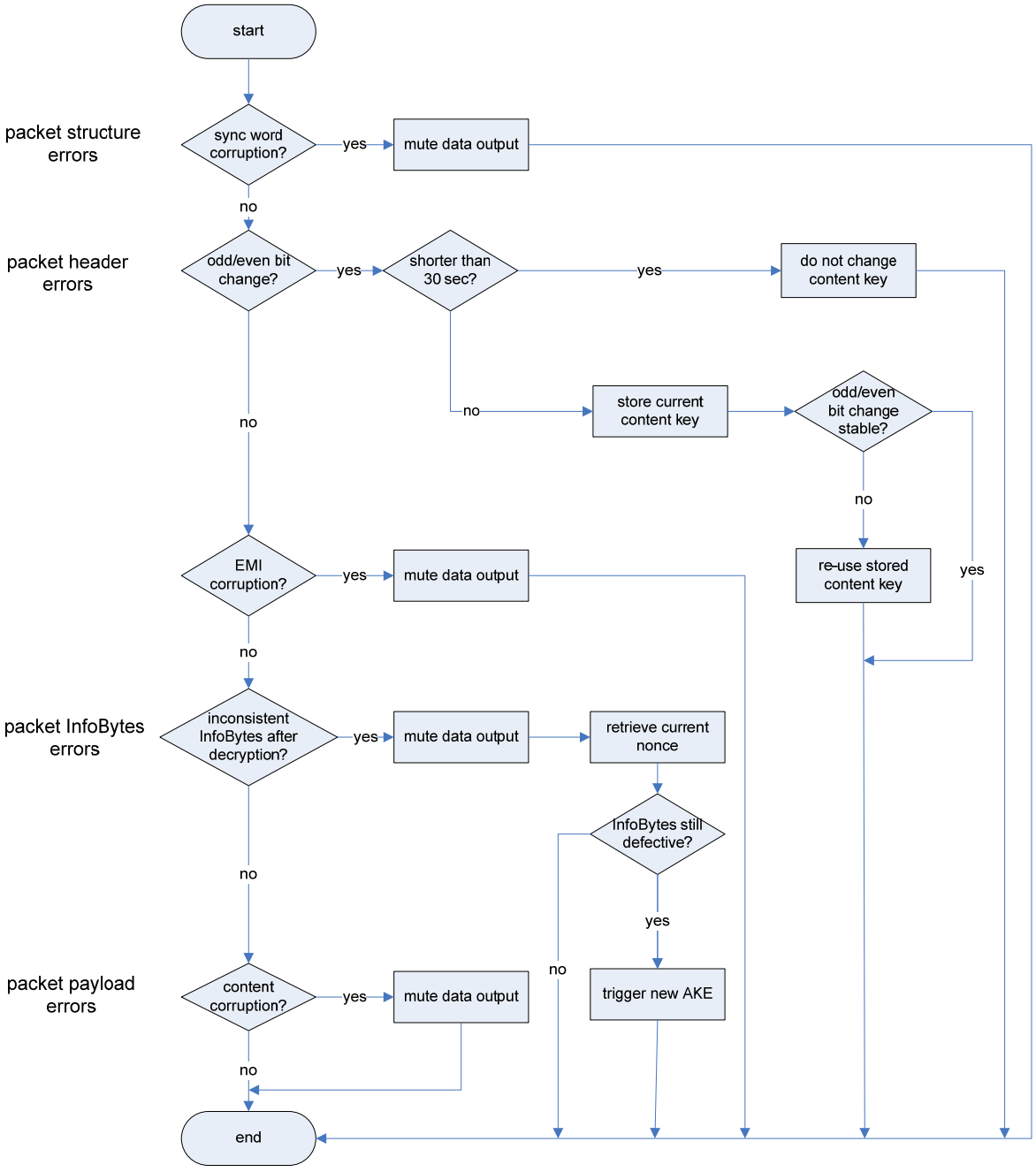

Figure 2-1: DTCP robustness flowchart

Notes:

3 Appendix A: Index of Figures

Figure 1-1: Robustness measures in DVD-Audio Stream Protected by MOST-DTCP.....6
Figure 2-1: DTCP robustness flowchart 8

4 Appendix B: Index of Tables

Table 1-1: Document references.....6