The checksum in DIASER/UDP/IP is a XOR without STX

draft-petrescu-ipwave-diaser-checksum-00

Abstract

This document defines the manner in which to calculate the checksum for the protocol DIASER. DIASER is a protocol for communication with traffic lights controllers used in France. DIASER is specified at AFNOR. The specification misses an instruction on how to compute the ‘BCC’ checksum (‘Byte Character Control’).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 28, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. DIASER Protocol and IETF Protocols

The DIASER protocol does this and that with a Traffic Lights controller - it is an Application Layer protocol. DIASER can be transported over UDP and over IP. The DIASER specification is available at a cost from AFNOR, on the World Wide Web. The DIASER specification does not describe the mechanism to compute the checksum ‘BCC’ (Byte Control Character). There exist several verbal (oral) versions of this mechanism: to cover or not to cover the STX (Start of Text), or the ETX (End of Text). Studying some implementations of a particular controller (Aximum) and packet dumps from independent sources, lead to a possibility to reverse engineer the specification of the checksum calculation of DIASER.

The DIASER protocol is an application layer protocol. Initially it was designed to run on serial lines like RS-232. Later on it was put on UDP (User Datagram Protocol). The UDP protocol is an IETF protocol. Running DIASER over UDP over IP is a great fact; contrary to RS-232, it allows to query a Traffic Lights Controller from a remote ‘Poste de Commande et Control’, and further from any other point in the Internet; second, it allows to query the controller over the future generation of Internet Protocol namely IPv6; thirdly, it allows to query the controller from nearby like an autonomous shuttle, with lower latency communications, thus supporting higher autonomous shuttle speeds; fourthly, it is easy to secure - rely on numerous security tools for software (IPsec, VPN) widely available and enjoy trust developped by Certificate Authorities and Let’s Encrypt.
IETF has its own way to specify a checksum. UDP, ICMP and other IETF protocols use a unique kind of checksum, which is specified in a particular RFC. It is clear that the RFC checksum is different from the DIASER checksum, at least because it involves also a notion of complement (not just XOR).

3. Checksum

The DIASER checksum is independent of the checksum field in the UDP header preceding the DIASER payload. In a DIASER/UDP packet there are two checksums: the DIASER checksum and the UDP checksum.

The DIASER checksum is an exclusive or operation (XOR) performed sequentially on the DIASER command; the bytes are read from left to right; the STX character is not read; the ETX character is read.

A python implementation of the DIASER checksum is the following. Note the use of the `^` operator for XOR and the 'for' iteration on each byte. Note that only ETX is covered by the checksum, not the STX.

```
#!/usr/bin/env python
# Mariama for CEA
packet="\x43\x6B\x30\x33\x47\x30\x30\x47\x30\x31\x47\x30\x32\x47\x30\x33\x47\x30\x34\x47\x30\x35\x47\x30\x36\x47\x30\x37\x47\x30\x38\x2A\x2A\x2A\x2A\x2A\x2A\x2A\x2A\x03"
# packet is 'Ck03G00G01G02G03G04G05G06G07G08*********|ETX'
checksum = 0
for el in packet:
    checksum ^= ord(el)
print hex(checksum)
```

Figure 1: Code snippet for DIASER Checksum

4. Security Considerations

Wrongly calculating a checksum may lead to security risks.

5. IANA Considerations

no request.
6. Contributors
   Listed.

7. Acknowledgements
   Listed

8. Normative References


Appendix A. ChangeLog

The changes are listed in reverse chronological order, most recent changes appearing at the top of the list.

Authors’ Addresses

Alexandre Petrescu
CEA, LIST
CEA Saclay
Gif-sur-Yvette, Ile-de-France 91190
France

Phone: +33169089223
Email: Alexandre.Petrescu@cea.fr

Mariama Sarr
CEA, LIST
CEA Saclay
Gif-sur-Yvette, Ile-de-France 91190
France

Phone: +phone
Email: Mariama.Sarr@cea.fr