Network Working Group
Internet-Draft
Intended status: Informational
Expires: March 10, 2022

T. Dreibholz
SimulaMet

September 06, 2021

Ideas for a Next Generation of the Stream Control Transmission Protocol (SCTP)

draft-dreibholz-tsvwg-sctp-nextgen-ideas-14

Abstract

This document collects some ideas for a next generation of the Stream Control Transmission Protocol (SCTP) for further discussion. It is a result of lessons learned from more than one decade of SCTP deployment.

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 March 10, 2022.

Copyright Notice

Copyright (c) 2021 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.

Table of Contents

1. Introduction 2
1.1. Abbreviations 2
1.2. Stream Control Transmission Protocol 2
1.3. Scope 2
2. What to Change in the Next Generation of SCTP? 2
2.1. Security Considerations 3
2.2. IANA Considerations 3
3. Experimental Implementations 3
4. Testbed Platform 4
5. Acknowledgments 4
6. References 4
6.1. Normative References 4
6.2. Informative References 6
Author's Address 8

1. Introduction

1.1. Abbreviations

- SCTP: Stream Control Transmission Protocol

1.2. Stream Control Transmission Protocol

The Stream Control Transmission Protocol (SCTP) has been defined as RFCs in [1], [2], [3], [4], [5], [6], [7], [8], [10], [11], [12], [13], [14], [15]. There is also a detailed introduction provided by [22] as well as lots of further information material on [19]. SCTP is therefore not introduced in more detail here.

1.3. Scope

The scope of this document is to collect some ideas of what to update/change for a next generation of the SCTP protocol. It is a result of lessons learned from more than one decade of SCTP deployment (see also [22]) as well as ongoing discussions on applying SCTP for WebRTC Data Channels (as introduced in more detail in [18]).

2. What to Change in the Next Generation of SCTP?

- Make useful extensions part of the next generation core protocol itself (that is, make their implementation a MUST):

  * Partial Reliablility ([4])

  * Chunk Authentication ([6])

  * Partial Reliablility ([8])

  * Stream Reconfiguration ([13])

  * SACK Immediately ([15])

- o Consider additional features as part of the next generation core protocol:

  * Non-Renegable Selective Acknowledgments (NR-SACK) ([24])

  * Concurrent Multi-Path Transfer for SCTP (CMT-SCTP) ([16])

- o Chunk Authentication provides integrity but not confidentiality. There could be a feature for encryption as well, for example like [17]. Having encryption directly included inside the core transport protocol may make it easier to use (less error-prone work for application developers).

- o SCTP assigns a fixed TSN per DATA chunk. The TSN cannot be changed any more. That is, it is not possible for a middlebox to split chunks into smaller pieces (for example, for hardware offloading). For further discussion: may it be useful to consider a different behavior?

- o Definition of path: For SCTP, a path is defined by a remote destination address. [20], [21] shows that CMT-SCTP performance also depends on the local endpoint's outgoing links. Considering each pair of local outgoing and remote incoming address as different path may lead to improved performance in many Internet scenarios.

2.1. Security Considerations

Security considerations for SCTP can be found in [9].

2.2. IANA Considerations

This document introduces no additional considerations for IANA.

3. Experimental Implementations

An Open Source simulation model for SCTP is available for OMNeT++ within the INET Framework. See [23] for the Git repository. For documentation on the model, see [25] and [22]. This model can be used to evaluate future ideas for SCTP.

4. Testbed Platform

NorNet is a large-scale and realistic Internet testbed platform with support for multi-homing. A description of and introduction to NorNet is provided in [26], [27], [28], [29]. Further information can be found on the project website [30] at https://www.nntb.no.

5. Acknowledgments

The author would like to thank Martin Becke for discussions and support.

6. References

6.1. Normative References

[1] Tuexen, M., Xie, Q., Stewart, R., Shore, M., Ong, L., Loughney, J., and M. Stillman, "Requirements for Reliable Server Pooling", RFC 3237, DOI 10.17487/RFC3237, January 2002, <https://www.rfc-editor.org/info/rfc3237>.

[2] Jungmaier, A., Rescorla, E., and M. Tuexen, "Transport Layer Security over Stream Control Transmission Protocol", RFC 3436, DOI 10.17487/RFC3436, December 2002, <https://www.rfc-editor.org/info/rfc3436>.

[3] Bellovin, S., Ioannidis, J., Keromytis, A., and R. Stewart, "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec", RFC 3554, DOI 10.17487/RFC3554, July 2003, <https://www.rfc-editor.org/info/rfc3554>.

[4] Stewart, R., Ramalho, M., Xie, Q., Tuexen, M., and P. Conrad, "Stream Control Transmission Protocol (SCTP) Partial Reliability Extension", RFC 3758, DOI 10.17487/RFC3758, May 2004, <https://www.rfc-editor.org/info/rfc3758>.

[5] Tuexen, M., Stewart, R., and P. Lei, "Padding Chunk and Parameter for the Stream Control Transmission Protocol (SCTP)", RFC 4820, DOI 10.17487/RFC4820, March 2007, <https://www.rfc-editor.org/info/rfc4820>.

[6] Tuexen, M., Stewart, R., Lei, P., and E. Rescorla, "Authenticated Chunks for the Stream Control Transmission Protocol (SCTP)", RFC 4895, DOI 10.17487/RFC4895, August 2007, <https://www.rfc-editor.org/info/rfc4895>.

[7] Stewart, R., Ed., "Stream Control Transmission Protocol", RFC 4960, DOI 10.17487/RFC4960, September 2007, <https://www.rfc-editor.org/info/rfc4960>.

[8] Stewart, R., Xie, Q., Tuexen, M., Maruyama, S., and M. Kozuka, "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration", RFC 5061, DOI 10.17487/RFC5061, September 2007, <https://www.rfc-editor.org/info/rfc5061>.

[9] Stillman, M., Ed., Gopal, R., Guttman, E., Sengodan, S., and M. Holdrege, "Threats Introduced by Reliable Server Pooling (RSerPool) and Requirements for Security in Response to Threats", RFC 5355, DOI 10.17487/RFC5355, September 2008, <https://www.rfc-editor.org/info/rfc5355>.

[10] Tuexen, M., Seggelmann, R., and E. Rescorla, "Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)", RFC 6083, DOI 10.17487/RFC6083, January 2011, <https://www.rfc-editor.org/info/rfc6083>.

[11] Tuexen, M. and R. Stewart, "Stream Control Transmission Protocol (SCTP) Chunk Flags Registration", RFC 6096, DOI 10.17487/RFC6096, January 2011, <https://www.rfc-editor.org/info/rfc6096>.

[12] Stewart, R., Tuexen, M., Poon, K., Lei, P., and V. Yasevich, "Sockets API Extensions for the Stream Control Transmission Protocol (SCTP)", RFC 6458, DOI 10.17487/RFC6458, December 2011, <https://www.rfc-editor.org/info/rfc6458>.

[13] Stewart, R., Tuexen, M., and P. Lei, "Stream Control Transmission Protocol (SCTP) Stream Reconfiguration", RFC 6525, DOI 10.17487/RFC6525, February 2012, <https://www.rfc-editor.org/info/rfc6525>.

[14] Tuexen, M. and R. Stewart, "UDP Encapsulation of Stream Control Transmission Protocol (SCTP) Packets for End-Host to End-Host Communication", RFC 6951, DOI 10.17487/RFC6951, May 2013, <https://www.rfc-editor.org/info/rfc6951>.

[15] Tuexen, M., Ruengeler, I., and R. Stewart, "SACK-IMMEDIATELY Extension for the Stream Control Transmission Protocol", RFC 7053, DOI 10.17487/RFC7053, November 2013, <https://www.rfc-editor.org/info/rfc7053>.

[16] Amer, P. D., Becke, M., Dreibholz, T., Ekiz, N., Iyengar, J., Natarajan, P., Stewart, R. R., and M. Tuexen, "Load Sharing for the Stream Control Transmission Protocol (SCTP)", draft-tuexen-tsvwg-sctp-multipath-22 (work in progress), August 2021.

[17] Hohendorf, C., Unurkhaan, E., and T. Dreibholz, "Secure SCTP", draft-hohendorf-secure-sctp-31 (work in progress), March 2021.

[18] Jesup, R., Loreto, S., and M. Tuexen, "WebRTC Data Channels", draft-ietf-rtcweb-data-channel-13 (work in progress), January 2015.

6.2. Informative References

[19] Dreibholz, T., "Thomas Dreibholz's SCTP Page", Online: https://www.uni-due.de/~be0001/sctp/, 2019, <https://www.uni-due.de/~be0001/sctp/>.

[20] Becke, M., Adhari, H., Rathgeb, E., Fu, F., Yang, X., and X. Zhou, "Comparison of Multipath TCP and CMT-SCTP based on Intercontinental Measurements", Proceedings of the IEEE Global Communications Conference (GLOBECOM), December 2013, <https://www.wiwi.uni-due.de/fileadmin/fileupload/I-TDR/Forschung/GLOBECOM2013.pdf>.

[21] Adhari, H., "Practical Experiences with an Inter-Continental Testbed for Multi-Path Transport", Proceedings of the 1st International NorNet Users Workshop (NNUW-1), September 2013, <https://web.archive.org/web/20141127063815/https://simula.no/publications/Simula.simula.2144/simula_pdf_file>.

[22] Dreibholz, T., "Evaluation and Optimisation of Multi-Path Transport using the Stream Control Transmission Protocol", Habilitation Treatise, March 2012, <https://duepublico.uni-duisburg-essen.de/servlets/DerivateServlet/Derivate-29737/Dre2012_final.pdf>.

[23] Varga, A., "INET Framework for OMNeT++", 2014, <http://inet.omnetpp.org/>.

[24] Natarajan, P., Ekiz, N., Yilmaz, E., Amer, P., and J. Iyengar, "Non-Renegable Selective Acknowledgments (NR-SACKs) for SCTP", Proceedings of the 16th IEEE International Conference on Network Protocols (ICNP) Pages 187-196, ISBN 978-1-4244-2506-8, DOI 10.1109/ICNP.2008.4697037, October 2008, <http://www.eecis.udel.edu/~amer/PEL/poc/pdf/ICNP2008-natarajanNonRenegableSacks.pdf>.

[25] Ruengeler, I., "SCTP - Evaluating, Improving and Extending the Protocol for Broader Deployment", December 2009, <http://duepublico.uni-duisburg-essen.de/servlets/DerivateServlet/Derivate-23465/Diss.pdf>.

[26] Gran, E., Dreibholz, T., and A. Kvalbein, "NorNet Core - A Multi-Homed Research Testbed", Computer Networks, Special Issue on Future Internet Testbeds Volume 61, Pages 75-87, ISSN 1389-1286, DOI 10.1016/j.bjp.2013.12.035, March 2014, <https://www.simula.no/file/simulasimula2236pdf/download>.

[27] Dreibholz, T. and E. Gran, "Design and Implementation of the NorNet Core Research Testbed for Multi-Homed Systems", Proceedings of the 3nd International Workshop on Protocols and Applications with Multi-Homing Support (PAMS) Pages 1094-1100, ISBN 978-0-7695-4952-1, DOI 10.1109/WAINA.2013.71, March 2013, <https://www.simula.no/file/threferedinproceedingsreference2012-12-207643198512pdf/download>.

[28] Dreibholz, T., "The NorNet Core Testbed - Introduction and Status", Proceedings of the 1st International NorNet Users Workshop (NNUW-1), September 2013, <https://www.simula.no/file/simulasimula2124pdf/download>.

[29] Dreibholz, T., "The NorNet Core Testbed - An Experiment Tutorial", Proceedings of the 1st International NorNet Users Workshop (NNUW-1), September 2013, <https://www.simula.no/file/simulasimula2130pdf/download>.

[30] Dreibholz, T., "NorNet - A Real-World, Large-Scale Multi-Homing Testbed", Online: https://www.nntb.no/, 2019, <https://www.nntb.no/>.

Author's Address

Thomas Dreibholz
Simula Metropolitan Centre for Digital Engineering
Pilestredet 52
0167 Oslo, Oslo
Norway

Phone: +47-6782-8200
Fax: +47-6782-8201
Email: dreibh@simula.no
URI: https://www.simula.no/people/dreibh