Delay-Tolerant Networking Working Group S. Burleigh
Internet Draft JPL, Calif. Inst. Of Technology
Intended status: Standards Track February 28, 2019
Expires: September 2019

Minimal TCP Convergence-Layer Protocol
draft-ietf-dtn-mtcpcl-00.txt

Status of this Memo

Copyright Notice

Abstract

This document describes a Minimal TCP (MTCP) "convergence-layer" protocol for the Delay-Tolerant Networking (DTN) Bundle Protocol (BP). MTCP uses Transmission Control Protocol (TCP) to transmit BP "bundles" from one BP node to another node to which it is topologically adjacent in the BP network. The services provided by the MTCP convergence-layer protocol adapter utilize a standard TCP connection for the purposes of bundle transmission.

Table of Contents

1. Introduction

This document describes the Minimal TCP (MTCP) protocol, a Delay-Tolerant Networking (DTN) Bundle Protocol (BP) [RFC5050] "convergence layer" protocol that uses a standard TCP connection to transmit bundles from one BP node to another node to which it is topologically adjacent in the BP network.

Conformance to the MTCP convergence-layer protocol specification is OPTIONAL for BP nodes.

Each BP node that conforms to the MTCP specification includes an MTCP convergence-layer adapter (MCLA). Every MCLA engages in communication via the Transmission Control Protocol [RFC0793].

Like any convergence-layer adapter, the MTCP CLA provides:

- A transmission service that sends an outbound bundle (from the bundle protocol agent) to a peer CLA via the MTCP convergence layer protocol.
- A reception service that delivers to the bundle protocol agent an inbound bundle that was sent by a peer CLA via the MTCP convergence layer protocol.

Transmission of bundles via MTCP is "reliable" to the extent that TCP itself is reliable. MTCP provides no supplementary error detection and recovery procedures. In particular, MTCP does not provide to the sender any interim reporting of reception progress.

2. Conventions used in this document

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].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying RFC-2119 significance.

3. MTCP Design Elements

3.1. MTCP Sessions

An MTCP "session" is formed when a TCP connection is established by the matching of an active TCP OPEN request issued by some MCLA, termed the session's "sender", with a passive TCP OPEN request issued by some MCLA, termed the session's "receiver". That portion of the state of a session that is exposed to the session's sender is termed the "transmission element" of the session. That portion of the state of a session that is exposed to the session's receiver is termed the "reception element" of the session.

The values of the parameters constraining MTCP's TCP connection establishment, including the establishment of Transport Layer Security (TLS; [RFC8446]) sessions within the connections, SHALL be provided by management, by means that are beyond the scope of this specification.

The use of TLS to secure MTCP sessions is optional but is strongly recommended. When it is determined, by management, that an MTCP session between a given sender and receiver is to be secured by TLS:

- Following establishment of the session's TCP connection, the sender and receiver SHALL undertake a TLS handshake in

accordance with [RFC8446] with the sender acting in the role of "client". The parameter settings governing each such handshake (again, determined by management) are an implementation matter, but the handshake SHOULD conform to all recommended best practices of [RFC7525] and its updates and successors.

. If the handshake does not result in successful establishment of a TLS session, then the session's TCP connection SHALL be terminated and the attempt to form an MTCP session shall be abandoned.

MTCP sessions are unidirectional; that is, bundles transmitted via an MTCP session are transmitted only from the session's sender to its receiver. When bidirectional exchange of bundles between MCLAs via MTCP is required, two MTCP sessions are formed, one in each direction.

Closure of either element of a session MAY occur either upon request of the bundle protocol agent or upon detection of any error. Closure of either element of an MTCP session SHALL cause the corresponding TCP connection to be terminated (unless termination of that connection was in fact the cause of the closure of that session element). Since termination of the associated TCP connection will result in errors at the other element of the session, termination of either element of the session will effectively terminate the session.

3.2. MTCP Protocol Data Units

An MTCP protocol data unit (MPDU) is simply a serialized bundle preceded by an integer indicating the length of that serialized bundle. An MPDU is constructed as follows.

Each MPDU SHALL be represented as a CBOR array. The number of items in the array SHALL be 2.

The first item of the MPDU array SHALL be the length of the serialized bundle that is encapsulated in the MPDU, represented as a CBOR unsigned integer.

The second item of the MPDU array SHALL be a single serialized BP bundle, termed the "encapsulated bundle", represented as a CBOR byte string of definite length (NOT an indefinite-length byte string).

4. MTCP Procedures

4.1. MPDU Transmission

When an MCLA is requested by the bundle protocol agent to send a bundle to a peer MCLA identified by some IP address and port number:

- If no MTCP session enabling transmission to that MCLA has been formed, the MCLA SHALL attempt to form that session. If this attempt is unsuccessful, the MCLA SHALL inform the bundle protocol agent that its data sending procedures with regard to this bundle have concluded and transmission of the bundle was unsuccessful; no further steps of this procedure will be attempted.
- The MCLA SHALL form an MPDU from the subject bundle.
- The MCLA SHALL attempt to send this MPDU to the peer MCLA by TCP via the transmission element of the session formed for this purpose.
    - If that transmission is completed without error, the MCLA SHALL inform the bundle protocol agent that its data sending procedures with regard to this bundle have concluded and transmission of the bundle was successful.
    - Otherwise:
        - The transmission element SHALL be closed.
        - The MCLA SHALL inform the bundle protocol agent that its data sending procedures with regard to this bundle have concluded and transmission of the bundle was unsuccessful.

4.2. Reception Session Formation

An MCLA that is required to receive (rather than only transmit) bundles SHALL issue a passive TCP OPEN. Whenever TCP matches that passive OPEN with an active TCP OPEN issued by some MCLA, an MTCP session is formed as noted earlier; MPDUs may be received via the reception element of such session.

4.3. MPDU Reception

From the moment at which an MTCP session reception element is first exposed to the moment at which it is closed, in a continuous cycle, the corresponding session's receiver SHALL:

- Attempt to receive, by TCP via the corresponding session, the length of the next bundle sent via this session. If this attempt fails for any reason, the reception element SHALL be

closed and no further steps of this procedure will be attempted.

- Attempt to receive, by TCP via the corresponding session, a serialized bundle of the indicated length. If this attempt fails for any reason, the reception element SHALL be closed and no further steps of this procedure will be attempted.
- Deliver the received serialized bundle to the bundle protocol agent.

5. Security Considerations

Because MTCP constitutes a nearly negligible extension of TCP, it introduces virtually no security considerations beyond the well-known TCP security considerations. To address these considerations, the use of TLS to secure MTCP sessions is strongly recommended.

Even when TLS is used to secure an MTCP session, the ciphersuite specified for the TLS session may be insecure. For example, TLS can be configured to support authentication without confidentiality. MCLA management MUST ensure that the ciphersuites employed to secure MTCP sessions meet transport security requirements. This constraint echoes constraints on STARTTLS in [RFC2595].

An adversary could mount a denial-of-service attack by repeatedly establishing and terminating MTCP sessions; well-understood DOS attack mitigations would apply.

Maliciously formed bundle lengths could disrupt the operation of MTCP session receivers, but MTCP implementations need to be robust against incorrect bundle lengths in any case.

Maliciously crafted serialized bundles could be received and delivered to the bundle protocol agent, but that is not an MTCP-specific security consideration: all bundles delivered to the BPA by all convergence-layer adapters need to be processed in awareness of this possibility.

6. IANA Considerations

No new IANA considerations apply.

7. References

7.1. Normative References

[RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525, May 2015.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, August 2018.

7.2. Informative References

[RFC2595] Newman, C., "Using TLS with IMAP, POP3 and ACAP", RFC 2595, August 2018.

[RFC5050] Scott, K. and S. Burleigh, "Bundle Protocol Specification", RFC 5050, November 2007.

8. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

Appendix A. For More Information

Please refer comments to dtn@ietf.org. The Delay Tolerant Networking Research Group (DTNRG) Web site is located at http://www.dtnrg.org.

Authors' Address

Scott Burleigh
Jet Propulsion Laboratory, California Institute of Technology
4800 Oak Grove Dr.
Pasadena, CA 91109-8099
US
Phone: +1 818 393 3353
Email: Scott.Burleigh@jpl.nasa.gov