Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 3, 2019

B. Cheng
D. Wiggins
MIT Lincoln Laboratory
L. Berger
LabN Consulting, L.L.C.
S. Ratliff
VT iDirect

August 2, 2018

DLEP Credit-Based Flow Control Messages and Data Items
draft-ietf-manet-dlep-credit-flow-control-03

Abstract

This document defines new DLEP protocol Data Items that are used to support credit-based flow control. Credit window control is used to regulate when data may be sent to an associated virtual or physical queue. The Data Items are defined in an extensible and reusable fashion. Their use will be mandated in other documents defining specific DLEP extensions.

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 February 3, 2019.

Table of Contents

1. Introduction

The Dynamic Link Exchange Protocol (DLEP) is defined in [RFC8175]. It provides the exchange of link related control information between DLEP peers. DLEP peers are comprised of a modem and a router. DLEP defines a base set of mechanisms as well as support for possible extensions. DLEP defines Data Items which are sets of information that can be reused in DLEP messaging. The base DLEP specification does not include any flow identification beyond DLEP endpoints or flow control capability. There are various flow control techniques theoretically possible with DLEP. For example, a credit-window scheme for destination-specific flow control which provides aggregate flow control for both modem and routers has been proposed in [I-D.ietf-manet-credit-window], and a control plane pause based mechanism is defined in [I-D.ietf-manet-dlep-pause-extension].

This document defines DLEP Data Items and Messages which provide a flow control mechanism for traffic sent from a router to a modem. Flow control is provided using one or more logical "Credit Windows", each of which will typically be supported by an associated virtual or physical queue. Traffic sent by a router will use traffic flow classification information provided by the modem as defined in [I-D.ietf-manet-dlep-traffic-classification]. to identify which traffic is associated with each credit window. In this case, a flow is identified based on information found in a data plane header and one or more matches are associated with a single flow. (For general background on traffic classification see [RFC2475] Section 2.3.) Credit windows may be shared or dedicated on a per flow basis. The Data Items are structured to allow for reuse of the defined credit window based flow control with different traffic classification techniques.

Note that this document defines common Messages, Data Items and mechanisms that are reusable. They are expected to be required by DLEP extensions defined in other documents such as found in [I-D.ietf-manet-dlep-da-credit-extension].

This document supports credit window control by introducing two new DLEP messages in Section 2.2, and five new DLEP Data Items in Section 2.3.

1.1. Key Words

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Credit Window Control

This section defines additions to DLEP used in credit based flow control. Two new messages and five Data Items are defined to support credit window control. The use of credit window control impacts the data plane.

The credit window control mechanisms defined in this document support credit based flow control of traffic sent from a router to a modem. The mapping of specific flows of traffic to a particular credit window is based on the Traffic Classification Data Item defined in [I-D.ietf-manet-dlep-traffic-classification]. Both types of DLEP endpoints, i.e., a router and a modem, negotiate the use of extension during session initialization, e.g., see [I-D.ietf-manet-dlep-da-credit-extension]. When using credit

windows, data traffic is only allowed to be sent by the router to the modem when there are credits available.

Credits are managed on a per logical "Credit Windows" basis. Each credit window can be thought of as corresponding to a queue within a modem. Credit windows may be shared across, or dedicated to, destinations and data plane identifiers, e.g., DSCPs, at a granularity that is appropriate for a modem's implementation and its attached transmission technology. As defined below, there is a direct one-for-one mapping of credit windows to flows as identified by FIDs carried within the Traffic Classification Data Item. Modems pass to the router information on their credit windows and FIDs prior to a router being able to send data when an extension requiring the use of credit window control is used. In addition to the traffic classification information associated with an FID, routers provide an initial credit window size, as well as the maximum size of the logical queue associated with each credit window. The maximum size is included for informative and potential future uses.

Modems provide an initial credit window size at the time of "Credit Window Initialization". Such initialization can take place during session initiation or any point thereafter. It can also take place when rate information changes. Additional "Credit Grants", i.e., increments to Credit Window size, are provided using a Destination Up or the new "Credit Control" Message. A router provides its view of the Credit Window, which is known as "Status", in Destination Up Response and the new "Credit Control Response" Messages. Routers can also request credits using the new "Credit Control" Message.

When modems provide credits to a router, they will need to take into account any overhead of their attached transmission technology and map it into the credit semantics defined in this document. In particular, the credit window is defined below to include per frame (packet) MAC headers, and this may not match the actual overhead of the modem attached transmission technology. In that case a direct mapping, or an approximation will need to be made by the modem to provide appropriate credit values.

Actual flows of traffic are mapped to credit windows based on flow identification information provided by modems in the Traffic Classification Data item defined in [I-D.ietf-manet-dlep-traffic-classification]. This data item supports traffic classification on a per destination or more fine grain level. Routers use the combination of the DLEP identified destination and flow information associated with a credit window in order to match traffic they send to specific credit windows.

When a destination becomes reachable, a modem "Associates" (identifies) the appropriate traffic classification information via the TID to be used for traffic sent by the router to that destination. As defined, each credit window has a corresponding FID. This means that the use of FIDs, TIDs and the association of a TID to a DLEP destination enables a modem to share or dedicate resources as needed to match the specifics of its implementation and its attached transmission technology.

The defined credit window control has similar objectives as the control found in [I-D.ietf-manet-credit-window]. One notable difference from that credit control is that in this document, credits are never provided by the router to the modem.

2.1. Data Plane Considerations

When credit windowing is used, a router MUST NOT send data traffic to a modem for forwarding when there are no credits available in the associated Credit Window. This document defines credit windows in octets. A credit window value MUST be larger than the number of octets contained in a packet, including any MAC headers used between the router and the modem, in order for the router to send the packet to a modem for forwarding. The credit window is decremented by the number of sent octets.

A router MUST identify the credit window associated with traffic sent to a modem based on the traffic classification information provided in the Data Items defined in this document. Note that routers will typically view a DLEP destination as the next hop MAC address.

2.2. Credit Window Messages

Two new messages are defined in support for credit window control: the Credit Control and the Credit Control Response Message. Sending and receiving both message types is REQUIRED to support the credit window control defined in this document.

2.2.1. Credit Control Message

Credit Control Messages are sent by modems and routers. Each sender is only permitted to have one message outstanding at one time. That is, a sender (i.e., modem or router) MUST NOT send a second or any subsequent Credit Control Message until a Credit Control Response Message is received from its peer (i.e., router or modem).

Credit Control Messages are sent by modems to provide credit window increases. Modems send credit increases when there is transmission or local queue availability that exceeds the credit window value

previous provided to the router. Modems will need to balance the load generated by sending and processing frequent credit window increases against a router having data traffic available to send, but no credits available.

Credit Control Messages MAY be sent by routers to request credits and provide window status. Routers will need to balance the load generated by sending and processing frequent credit window requests against a having data traffic available to send, but no credits available.

The Message Type value in the DLEP Message Header is set to TBA2.

A message sent by a modem, MUST contain one or more Credit Window Grant Data Items as defined below in Section 2.3.3. A router receiving this message MUST respond with a Credit Control Response Message.

A message sent by a router, MUST contain one or more Credit Window Request Data Items defined below in Section 2.3.5 and SHOULD contain a Credit Window Status Data Item, defined in Section 2.3.4, corresponding to each credit window request. A modem receiving this message MUST respond with a Credit Control Response Message based on the received message and Data Item and the processing defined below, which will typically result in credit window increments being provided.

Specific processing associated with each Credit Data Item is provided below.

2.2.2. Credit Control Response Message

Credit Control Response Messages are sent by routers to report the current Credit Window for a destination. A message sent by a router, MUST contain one or more Credit Window Status Data Items as defined below in Section 2.3.4. Specific receive processing associated with the Credit Window Status Data Item is provided below.

Credit Control Response Messages sent by modems MUST contain one or more Credit Window Grant Data Items. A Data Item for every Credit Window Request Data Item contained in the corresponding Credit Control Response Message received by the modem MUST be included. Each Credit Grant Data Item MAY provide zero or more additional credits based on the modem's transmission or local queue availability. Specific receive processing associated with each Grant Data Item is provided below.

The Message Type value in the DLEP Message Header is set to TBA3.

2.3. Credit Window Control Data Items

Five new Data Items are defined to support credit window control. The Credit Window Initialization Data Item is used by a modem to identify a credit window and set its size. The Credit Window Association Data Item is used by a modem to identify which traffic classification identifiers (flows) should be used when sending traffic to a particular DLEP identified destination. The Credit Window Grant is used by a modem to provide additional credits to a router. The Credit Request is used by a router to request additional credits. The Credit Window Status is used to advertise the sender's view of number of available credits for state synchronization purposes.

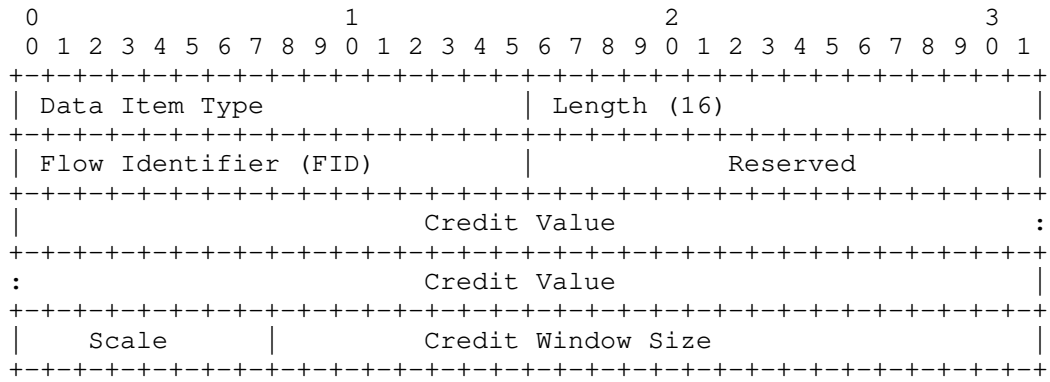
Any errors or inconsistencies encountered in parsing Data Items are handled in the same fashion as any other data item parsing error encountered in DLEP, see [RFC8175]. In particular, the node parsing the Data Item MUST terminate the session with a Status Data Item indicating Invalid Data.

2.3.1. Credit Window Initialization

The Credit Window Initialization Data Item is used by a modem to identify a credit window and set its size. This Data Item SHOULD be included in any Session Initialization Response Message that also indicates support for an extension that requires support for the credit window control mechanisms defined in this document, e.g., see [I-D.ietf-manet-dlep-da-credit-extension]. Updates to previously identified credit windows or new credit windows MAY be sent by a modem by including the Data Item in Session Update Messages. More than one data item MAY be included in a message to provide information on multiple credit windows.

The Credit Window Initialization Data Item identifies a credit window using a Flow Identifier, or FID. It also provides the size of the identified credit window. Finally, a queue size (in bytes) is provided for informational purposes. Note that to be used, a FID must be defined within a Traffic Classification Data Item and the associated TID must be provided via a Credit Window Association Data Item.

The format of the Credit Window Initialization Data Item is:



Data Item Type: TBA4

Length: 16

Per [RFC8175] Length is the number of octets in the Data Item. It MUST be equal to sixteen (16).

Flow Identifier (FID):

A flow identifier as defined by the Traffic Classification Data Item. The FID also uniquely identifies a credit window.

Reserved:

MUST be set to zero by the sender (a modem) and ignored by the receiver (a router).

Credit Value:

A 64-bit unsigned integer representing the credits, in octets, to be applied to the Credit Window. This value includes MAC headers as seen on the link between the modem and router.

Scale:

An 8-bit unsigned integer indicating the scale used in the Credit Window Size fields. The valid values are:

Value	Scale
0	B - Bytes (Octets)
1	KB - Kilobytes (B/1024)
2	MB - Megabytes (KB/1024)
3	GB - Gigabytes (MB/1024)

Credit Window Size:

A 24-bit unsigned integer representing the maximum size, in the octet scale indicated by the Scale field, of the associated credit window.

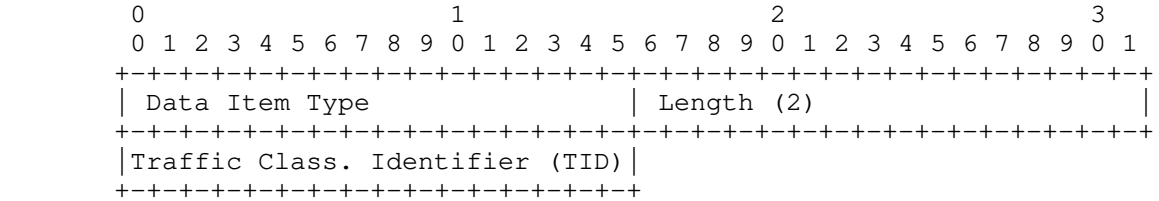
A router that receives a Credit Window Initialization Data Item MUST ensure that the FID field value has been provided by the modem in a Traffic Classification Data Item carried in either the current or previous message. If the FID cannot be found the router SHOULD report or log this information. Note that no traffic will be associated with the credit window in this case. After FID validation, the router MUST locate the credit window that is associated with the FID indicated in each received Data Item. If no associated credit window is found, the router MUST initialize a new credit window using the values carried in the Data Item. When an associated credit window is found, the router MUST update the credit window and associated data plane state using the values carried in the Data Item. It is worth noting, that such updates can result in a credit window size being reduced, for example, due to a transmission rate change on the modem.

2.3.2. Credit Window Associate

The Credit Window Associate Data Item is used by a modem to associate traffic classification information with a destination. The traffic classification information is identified using a TID value that has previously been sent by the modem or is listed in a Traffic Classification Data Item carried in the same message as the Data Item.

A single Credit Window Associate Data Item MUST be included in all Destination Up and Destination Update Messages sent by a modem when the credit window control defined in this document is used. Note that a TID will not be used unless it is listed in a Credit Window Associate Data Item.

The format of the Credit Window Associate Data Item is:



Data Item Type: TBA5

Length: 2

Per [RFC8175] Length is the number of octets in the Data Item. It MUST be equal to two (2).

Traffic Classification Identifier (TID):

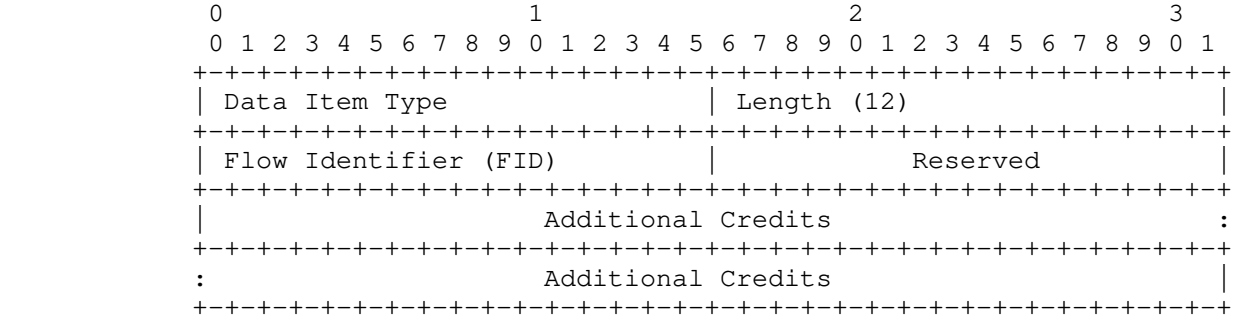
A 16-bit unsigned integer identifying a traffic classification set that has been identified in a Traffic Classification Data Item, see [I-D.ietf-manet-dlep-traffic-classification].

A router that receives the Credit Window Associate Data Item MUST locate the traffic classification information indicated by the received TID. If no corresponding information can be located, the Data Item MUST be treated as an error as described above. Once the traffic classification information is located, it MUST be associated with the destination and the router MUST ensure that any data plane state, see Section 2.1, that is associated with the TID and its corresponding FIDs is updated as needed.

2.3.3. Credit Window Grant

The Credit Window Grant Data Item is used by a modem to provide credits to a router. One or more Credit Window Grant Data Items MAY be carried in the DLEP Destination Up, Destination Announce Response, Destination Update, Credit Control Messages, and Credit Control Response Messages. Multiple Credit Window Grant Data Items in a single message are used to indicate different credit values for different credit windows. In all message types, this Data Item provides an additional number of octets to be added to the indicated credit window. Credit windows are identified using FID values that have been previously been sent by the modem or are listed in a Credit Window Initialization Data Item carried in the same messages as the Data Item.

The format of the Credit Window Grant Data Item is:



Data Item Type: TBA6

Length: 12

Per [RFC8175], Length is the number of octets in the Data Item. It MUST be equal to twelve (12).

Flow Identifier (FID):

A flow identifier as defined by the Traffic Classification Data Item. The FID also uniquely identifies a credit window.

Additional Credit:

A 64-bit unsigned integer representing the credits, in octets, to be added to the Credit Window. This value includes MAC headers as seen on the link between the modem and router. A value of zero indicates that no additional credits are being provided.

When receiving this Data Item, a router MUST identify the credit window indicated by the FID. If the FID is not known to the router, it SHOULD report or log this information and discard the Data Item. It is important to note that while this Data Item can be received in a destination specific message, credit windows are managed independently from the destination identified in the message carrying this Data Item, and the indicated FID MAY even be disjoint from the identified destination.

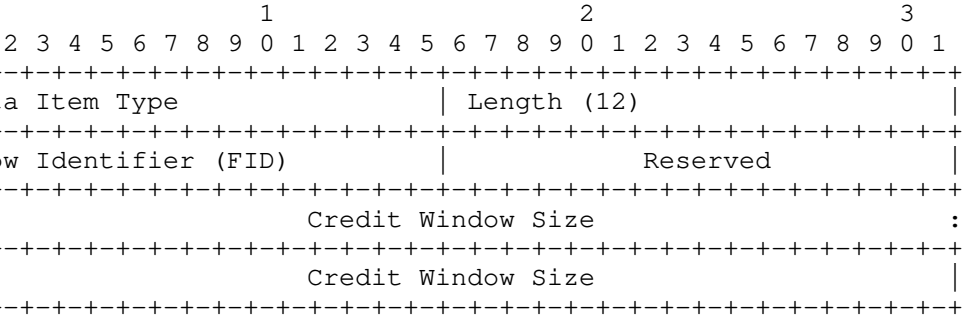
Once the credit window is identified, the credit window size MUST be increased by the value contained in the Additional Credits field. If the increase results in a window overflow, i.e., the size of the credit window after the increase is smaller than the original credit window size, the Credit Window must be set to its maximum (0xFFFFFFFFFFFFFFFF).

No response is sent by the router to a modem after processing a Credit Window Grant Data Item received in a Credit Control Response Message. In other cases, the receiving router MUST send a Credit Window Status Data Item or items reflecting the resulting Credit Window value of the updated credit window. When the Credit Grant Data Item is received in a Destination Up Message, the Credit Window Status Data Item(s) MUST be sent in the corresponding Destination Up Response Message. Otherwise, a Credit Control Message MUST be sent.

2.3.4. Credit Window Status

The Credit Window Status Data Item is used by a router to report the current credit window size to its peer modem. One or more Credit Window Status Data Items MAY be carried in a Destination Up Response Message or a Credit Control Response Message. As discussed above, the Destination Up Response Message is used when the Data Item is sent in response to a Destination Up Message, and the Credit Control Response Message is sent in response to a Credit Control Message. Multiple Credit Window Status Data Items in a single message are used to indicate different sizes of different credit windows. Similar to the Credit Window Grant, credit windows are identified using FID values that have been previously been sent by the modem.

The format of the Credit Window Status Data Item is:



Data Item Type: TBA7

Length: 12

Per [RFC8175] Length is the number of octets in the Data Item. It MUST be equal to twelve (12).

Flow Identifier (FID):

A flow identifier as defined by the Traffic Classification Data Item. The FID also uniquely identifies a credit window.

Credit Window Size:

A 64-bit unsigned integer, indicating the current number of credits, in octets, available for the router to send to the modem. This is referred to as the Modem Receive Window in [I-D.ietf-manet-credit-window].

When receiving this Data Item, a modem MUST identify the credit window indicated by the FID. If the FID is not known to the modem, it SHOULD report or log this information and discard the Data Item. As with the Credit Window Grant Data Item, the FID MAY be unrelated to the Destination indicated in the message carrying the Data Item.

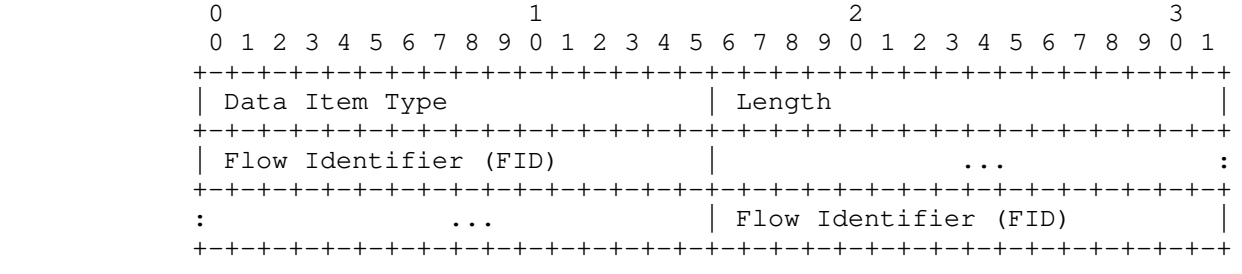
Once the credit window is identified, the modem SHOULD check the received Credit Window Size field value against the outstanding credit window's available credits at the time the most Credit Window Initialization or Grant Data Item associated with the indicated FID was sent. If the values significantly differ, i.e., greater than can be accounted for based on observed data frames, then the modem SHOULD send a Credit Window Initialization Data Item to reset the associated credit window size to the modem's current view of the available credits. As defined above, Credit Window Initialization Data Items are sent in Session Update Messages. When multiple Data Items need to be sent, they SHOULD be combined into a single message when possible. Alternatively, and also in cases where there are small differences, the modem MAY adjust the values sent in Credit Window Grant Data Items to account for the reported Credit Window.

2.3.5. Credit Window Request

The Credit Window Request Data Item is used by a router to request additional credits for particular credit windows. Credit Window Request Data Items are carried in Credit Control Messages, and one or more Credit Window Request Data Items MAY be present in a message.

Credit windows identified using a FID as defined above in Section 2.3.1. Multiple FIDs MAY be present to allow for the case where the router identifies that credits are needed in multiple credit windows. A special FID value, as defined below, is used to indicate that a credit request is being made across all queues.

The format of the Credit Window Request Data Item is:



Data Item Type: TBA8

Length: Variable

Per [RFC8175] Length is the number of octets in the Data Item, excluding the Type and Length fields. It will equal the number of FID fields carried in the Data Item times 2 and MUST be at least 2.

Flow Identifier (FID):

A flow identifier as defined by the Traffic Classification Data Item. The FID also uniquely identifies a credit window. The special value of 0xFFFF indicates that the request applies to all FIDs.

A modem receiving this Data Item MUST provide a Credit Increment for the indicated credit windows via Credit Window Grant Data Items carried in a new Credit Control Message. Multiple values and queue indexes SHOULD be combined into a single Credit Control Message when possible. Unknown FID values SHOULD be reported or logged and then ignored by the modem.

2.4. Management Considerations

This section provides several network management guidelines to implementations supporting the credit window mechanisms defined in this document.

Modems MAY support the configuration of the number of credit windows (queues) to advertise to a router.

Routers may have limits on the number of queues that they can support and, perhaps, even limits in supported credit window combinations, e.g., if per destination queues can even be supported at all. When modem-provided credit window information exceeds the capabilities of a router, the router MAY use a subset of the provided credit windows. Alternatively, a router MAY reset the session and indicate that the extension is not supported. In either case, the mismatch of capabilities SHOULD be reported to the user via normal network management mechanisms, e.g., user interface or error logging.

3. Compatibility

The data items defined in this document will only be used when extensions require their use.

4. Security Considerations

This document introduces credit window control and flow mechanisms to DLEP. These mechanisms do not inherently introduce any additional threats above those documented in [RFC8175]. The approach taken to Security in that document applies equally to the mechanism defined in this document.

5. IANA Considerations

This document requests the assignment of several values by IANA. All assignments are to registries defined by [RFC8175].

5.1. Message Values

This document requests 2 new assignments to the DLEP Message Registry named "Message Values" in the range with the "Specification Required" policy. The requested values are as follows:

Type Code	Description
TBA2	Credit Control
TBA3	Credit Control Response

Table 1: Requested Message Values

5.2. Data Item Values

This document requests the following new assignments to the DLEP Data Item Registry named "Data Item Type Values" in the range with the "Specification Required" policy. The requested values are as follows:

Type Code	Description
TBA4	Credit Window Initialization
TBA5	Credit Window Association
TBA6	Credit Window Grant
TBA7	Credit Window Status
TBA8	Credit Window Request

Table 2: Requested Data Item Values

6. References

6.1. Normative References

[I-D.ietf-manet-dlep-traffic-classification]
Cheng, B., Wiggins, D., and L. Berger, "DLEP Traffic Classification Data Item", August 2018.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8175] Ratliff, S., Jury, S., Satterwhite, D., Taylor, R., and B. Berry, "Dynamic Link Exchange Protocol (DLEP)", RFC 8175, DOI 10.17487/RFC8175, June 2017, <https://www.rfc-editor.org/info/rfc8175>.

6.2. Informative References

[I-D.ietf-manet-credit-window]
Ratliff, S., "Credit Windowing extension for DLEP", draft-ietf-manet-credit-window-07 (work in progress), November 2016.

[I-D.ietf-manet-dlep-da-credit-extension]
Cheng, B., Wiggins, D., and L. Berger, "DLEP DiffServ Aware Credit Window Extension", draft-ietf-manet-dlep-da-credit-extension-05 (work in progress), May 2018.

[I-D.ietf-manet-dlep-pause-extension]
Cheng, B., Wiggins, D., and L. Berger, "DLEP Control Plane Based Pause Extension", draft-ietf-manet-dlep-pause-extension-04 (work in progress), June 2018.

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, DOI 10.17487/RFC2475, December 1998, <https://www.rfc-editor.org/info/rfc2475>.

Appendix A. Acknowledgments

Many useful comments were received from contributors to the MANET working group, notably Rick Taylor. This document was derived from [I-D.ietf-manet-dlep-da-credit-extension] as a result of discussions at IETF101.

Authors' Addresses

Bow-Nan Cheng
MIT Lincoln Laboratory
Massachusetts Institute of Technology
244 Wood Street
Lexington, MA 02421-6426

Email: bcheng@ll.mit.edu

David Wiggins
MIT Lincoln Laboratory
Massachusetts Institute of Technology
244 Wood Street
Lexington, MA 02421-6426

Email: David.Wiggins@ll.mit.edu

Lou Berger
LabN Consulting, L.L.C.

Email: lberger@labn.net

Stan Ratliff
VT iDirect
13861 Sunrise Valley Drive, Suite 300
Herndon, VA 20171
USA

Email: sratliff@idirect.net

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 3, 2019

B. Cheng
D. Wiggins
MIT Lincoln Laboratory
L. Berger
LabN Consulting, L.L.C.
August 2, 2018

DLEP DiffServ Aware Credit Window Extension
draft-ietf-manet-dlep-da-credit-extension-06

Abstract

This document defines an extension to the DLEP protocol that enables a DiffServ aware credit-window scheme for destination-specific and shared flow 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 February 3, 2019.

Copyright Notice

Table of Contents

1. Introduction

The Dynamic Link Exchange Protocol (DLEP) is defined in [RFC8175]. It provides the exchange of link related control information between DLEP peers. DLEP peers are comprised of a modem and a router. DLEP defines a base set of mechanisms as well as support for possible extensions. This document defines one such extension.

The base DLEP specification does not include any flow control capability. There are various flow control techniques theoretically possible with DLEP. This document defines a DLEP extension which provides a DiffServ-based flow control mechanism for traffic sent from a router to a modem. Flow control is provided using one or more logical "Credit Windows", each of which will typically be supported by an associated virtual or physical queue. Traffic sent by a router will use traffic flow classification information provided by the modem to identify which traffic is associated with each credit window. Credit windows may be shared or dedicated on a per flow basis. See [I-D.berger-manet-dlep-ether-credit-extension] for an Ethernet-based version of credit window flow control.

This document uses the traffic classification and credit window control mechanisms defined in [I-D.ietf-manet-dlep-traffic-classification] and [I-D.ietf-manet-dlep-credit-flow-control] to provided credit window based flow control based on on DLEP destination and DiffServ [RFC2475] DSCPs (differentiated services codepoints). The defined mechanism allows for credit windows to be shared across traffic sent to multiple DLEP destinations and DSCPs, or used exclusively for traffic sent to a particular destination and/or DSCP. The extension also supports the "wildcard" matching of any DSCP.

The extension defined in this document is referred to as "DiffServ Aware Credit Window" or, more simply, the "DA Credit" extension. The reader should be familiar with both the traffic classification and credit window control mechanisms defined in [I-D.ietf-manet-dlep-traffic-classification] and [I-D.ietf-manet-dlep-credit-flow-control].

This document defines a new DLEP Extension Type Value in Section 2 which is used to indicate support for the extension.

1.1. Key Words

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Extension Usage and Identification

The extension defined in this document is composed of the mechanisms and processing defined in [I-D.ietf-manet-dlep-traffic-classification] and [I-D.ietf-manet-dlep-credit-flow-control]. To indicate that the DiffServ Aware Credit Window Extension is to be used, an implementation MUST include the DiffServ Aware Credit Window Type Value in the Extensions Supported Data Item. The Extensions Supported Data Item is sent and processed according to [RFC8175]. Any implementation that indicates use of the DiffServ Aware Credit Window Extension MUST support all Messages, Data Items, the DiffServ Traffic Classification Sub Data Item, and all related processing defined in [I-D.ietf-manet-dlep-traffic-classification] and [I-D.ietf-manet-dlep-credit-flow-control].

The DiffServ Aware Credit Window Extension Type Value is TBA1, see Section 5.

3. Management Considerations

This section provides several network management guidelines to implementations supporting the DiffServ Aware Credit Window Extension.

The use of the extension defined in this document SHOULD be configurable on both modems and routers.

Modems SHOULD support the configuration of DSCP to credit window (queue) mapping.

Modems MAY support the configuration of the number of credit windows (queues) to advertise to a router.

Routers may have limits on the number of queues that they can support and, perhaps, even limits in supported credit window combinations, e.g., if per destination queues can even be supported at all. When modem-provided credit window information exceeds the capabilities of a router, the router MAY use a subset of the provided credit windows. Alternatively, a router MAY reset the session and indicate that the extension is not supported. In either case, the mismatch of capabilities SHOULD be reported to the user via normal network management mechanisms, e.g., user interface or error logging.

4. Security Considerations

This document defines a DLEP extension that uses base DLEP mechanisms and the credit window control and flow mechanisms defined in [I-D.ietf-manet-dlep-traffic-classification] and [I-D.ietf-manet-dlep-credit-flow-control]. The use of those mechanisms, and the introduction of a new extension, do not inherently introduce any additional threats above those documented in [RFC8175]. The approach taken to Security in that document applies equally to the mechanism defined in this document.

5. IANA Considerations

This document requests one assignment by IANA. All assignments are to registries defined by [RFC8175].

5.1. Extension Type Value

This document requests 1 new assignment to the DLEP Extensions Registry named "Extension Type Values" in the range with the "Specification Required" policy. The requested value is as follows:

Code	Description
TBA1	DiffServ Aware Credit Window

Table 1: Requested Extension Type Value

6. References

6.1. Normative References

[I-D.ietf-manet-dlep-credit-flow-control]
Cheng, B., Wiggins, D., and L. Berger, "DLEP Credit-Based Flow Control Messages and Data Items", draft-ietf-manet-dlep-credit-flow-control-02 (work in progress), June 2018.

[I-D.ietf-manet-dlep-traffic-classification]
Cheng, B., Wiggins, D., and L. Berger, "DLEP Traffic Classification Data Item", August 2018.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8175] Ratliff, S., Jury, S., Satterwhite, D., Taylor, R., and B. Berry, "Dynamic Link Exchange Protocol (DLEP)", RFC 8175, DOI 10.17487/RFC8175, June 2017, <https://www.rfc-editor.org/info/rfc8175>.

6.2. Informative References

[I-D.berger-manet-dlep-ether-credit-extension]
Wiggins, D. and L. Berger, "DLEP IEEE 802.1Q Aware Credit Window Extension", draft-berger-manet-dlep-ether-credit-extension-00 (work in progress), May 2018.

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, DOI 10.17487/RFC2475, December 1998, <https://www.rfc-editor.org/info/rfc2475>.

Appendix A. Acknowledgments

The sub data item format was inspired by Rick Taylor’s "Data Item Containers". He also proposed the separation of credit windows from traffic classification at IETF98. Many useful comments were received from contributors to the MANET working group.

Authors’ Addresses

Bow-Nan Cheng
MIT Lincoln Laboratory
Massachusetts Institute of Technology
244 Wood Street
Lexington, MA 02421-6426

Email: bcheng@ll.mit.edu

David Wiggins
MIT Lincoln Laboratory
Massachusetts Institute of Technology
244 Wood Street
Lexington, MA 02421-6426

Email: David.Wiggins@ll.mit.edu

Lou Berger
LabN Consulting, L.L.C.

Email: lberger@labn.net

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 3, 2019

B. Cheng
D. Wiggins
MIT Lincoln Laboratory
L. Berger
LabN Consulting, L.L.C.
August 2, 2018

DLEP Traffic Classification Data Item
draft-ietf-manet-dlep-traffic-classification-00

Abstract

This document defines a new DLEP protocol Data Item that is used to support traffic classification. Traffic classification information is used to identify traffic flows based on frame/packet content such as destination address. The Data Item is defined in an extensible and reusable fashion. It's use will be mandated in other documents defining specific DLEP extensions. This document aloas introduces DLEP sub data items, and sub data items are defined to support DiffServ and Ethernet traffic classification.

Table of Contents

1. Introduction

The Dynamic Link Exchange Protocol (DLEP) is defined in [RFC8175]. It provides the exchange of link related control information between DLEP peers. DLEP peers are comprised of a modem and a router. DLEP defines a base set of mechanisms as well as support for possible extensions. DLEP defines Data Items which are sets of information that can be reused in DLEP messaging. The base DLEP specification does not include any flow identification beyond DLEP endpoints. This document defines DLEP Data Item formats which provide flow identification on a more granular basis. Specifically it enables traffic sent by a router to use traffic flow classification information provided by the modem to identify which traffic flows. In this case, a flow is identified based on information found in a data plane header and one or more matches are associated with a single flow. (For general background on traffic classification see [RFC2475] Section 2.3.) Credit windows may be shared or dedicated on a per flow basis. The Data Item is structured to allow for reuse of the defined traffic classification information with applications such

as credit window control, such as found in [I-D.ietf-manet-dlep-da-credit-extension]

This document defines traffic classification based on a DLEP destination and flows identified by either DiffServ [RFC2475] DSCPs (differentiated services codepoints) or IEEE 802.1Q [IEEE.802.1Q_2014] Ethernet Priority Code Points (PCP). The defined mechanism allows for flows to be described in a flexible fashion and when combined with applications such as credit window control, allows credit windows to be shared across traffic sent to multiple DLEP destinations and flows, or used exclusively for traffic sent to a particular destination and/or flow. The extension also supports the "wildcard" matching of any flow (DSCP or PCP). Traffic classification information is provided such that it can be readily extended to support other traffic classification techniques, or be used by non-credit window related extensions, such as [I-D.ietf-manet-dlep-pause-extension] or even 5-tuple IP flows.

This document defines support for traffic classification using a single new Data Item in Section 2.1 for general support and two new sub Data Items are defined to support identification of flows based on DSCPs and PCPs.

1.1. Key Words

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Traffic Classification

The Traffic Classification Data Item is used to represent a list of flows that may be used at the same time for traffic sent from a router to a modem. The data plane information used to identify each flow is represented in a separate sub Data Item. The Data Item and Sub Data Item structure is intended to be independent of any specific usage of the flow identification, e.g., flow control. The Sub Data Item structure is also intended to allow for future traffic classification types, e.g., 5-tuple flows. While the structure of the Data Items is extensible, actual flow information is expected to be used in an extension dependent manner. Support for DSCP and PCP-based flows are defined via individual sub Data Items below. Other types of flow identification, e.g., based on IP protocol and ports, may be defined in the future via new sub Data Items.

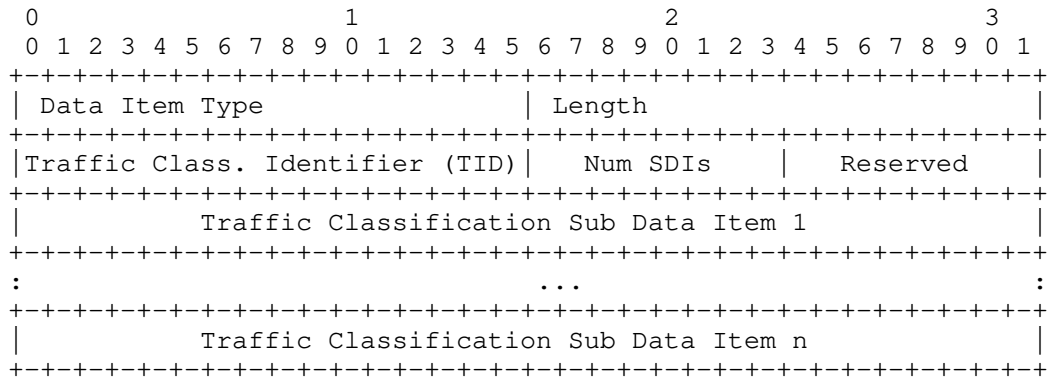
The list of flows contained in the Data Item can be used per sender or shared across multiple senders. Each list of flows is identified using a "Traffic Classification Identifier" or "TID" and is expected to represent a valid combination of data plane identifiers that may be used at the same time. Each flow is identified via a "Flow Identifier" or "FID". Each FID is defined in a sub Data Item which carries the data plane identifier or identifiers used to associate traffic with the flow. A DLEP destination address is also needed to complete traffic classification information used in extensions such as flow control. This information is expected to be provided in an extension specific manner. For example, this address can be provided by a modem when it identifies the traffic classification set in a Destination Up Message using the Credit Window Associate Data Item defined in [I-D.ietf-manet-dlep-credit-flow-control]. The scope of TID and FID values is a modem.

2.1. Traffic Classification Data Item

This sections defines the Traffic Classification Data Item. This Data Item is used by a modem to provide a router with traffic classification information. When an extension requires use of this Data Item the Traffic Classification Data Item SHOULD be included by a modem in any Session Initialization Response Message, e.g., see [I-D.ietf-manet-dlep-da-credit-extension]. Updates to previously provided traffic classifications or new traffic classifications MAY be sent by a modem by including the Data Item in Session Update Messages. More than one Data Item MAY be included in a message to provide information on multiple traffic classifiers.

The set of traffic classification information provided in the data item is identified using a Traffic Classification Identifier, or TID. The actual data plane related information used in traffic classification is provided in a variable list of Traffic Classification Sub Data Items.

The format of the Traffic Classification Data Item is:



Data Item Type: TBA1

Length: Variable

Per [RFC8175] Length is the number of octets in the Data Item, excluding the Type and Length fields.

Traffic Classification Identifier (TID):

A 16-bit unsigned integer identifying a traffic classification set. There is no restriction on values used by a modem, and there is no requirement for sequential or ordered values.

Num SDIs:

An 8-bit unsigned integer indicating the number of Traffic Classification Sub Data Items included in the Data Item. A value of zero (0) is allowed and indicates that no traffic should be matched against this TID.

Reserved:

MUST be set to zero by the sender (a modem) and ignored by the receiver (a router).

Traffic Classification Sub Data Item:

Zero or more Traffic Classification Sub Data Items of the format defined below MAY be included. The number MUST match the value carried in the Num SDIs field.

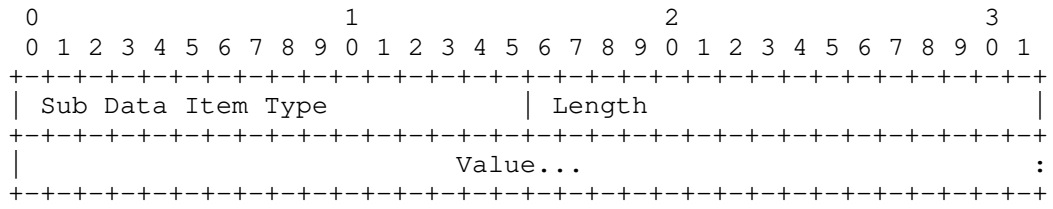
A router receiving the Traffic Classification Data Item MUST locate the traffic classification information that is associated with the TID indicated in each received Data Item. If no associated traffic

classification information is found, the router MUST initialize a new information set using the values carried in the Data Item. When associated traffic classification information is found, the router MUST update the information using the values carried in the Data Item. In both cases, a router MUST also ensure that any data plane state, e.g., [I-D.ietf-manet-dlep-credit-flow-control], that is associated with the TID is updated as needed.

2.1.1. Traffic Classification Sub Data Item

All Traffic Classification Sub Data Items share a common format that is patterned after the standard DLEP Data Item format, see [RFC8175] Section 11.3. There is no requirement on, or meaning to sub Data Item ordering. Any errors or inconsistencies encountered in parsing sub Data Items are handled in the same fashion as any other Data Item parsing error encountered in DLEP.

The format of the Traffic Classification Sub Data Item is:



Sub Data Item Type:

A 16-bit unsigned integer that indicates the type and corresponding format of the Sub Data Item's Value field. Sub Data Item Types are scoped within the Data Item in which they are carried, i.e., the Sub Data Item Type field MUST be used together with the Data Item Type to identify the format of the Sub Data Item. Traffic Classification Sub Data Item Types are managed according to the IANA registry described in Section 5.2.

Length: Variable

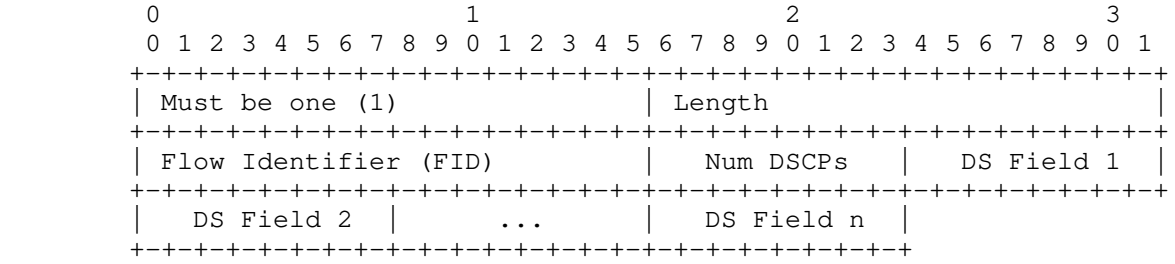
Copying [RFC8175], Length is a 16-bit unsigned integer that is the number of octets in the sub Data Item, excluding the Type and Length fields.

2.2. DiffServ Traffic Classification Sub Data Item

The DiffServ Traffic Classification Sub Data Item is used to identify the set of DSCPs that should be treated as a single flow, i.e., receive the same traffic treatment. DSCPs are identified in a list

of DiffServ fields. An implementation that does not support DSCPs and wants the same traffic treatment for all traffic to a destination or destinations would indicate 0 DSCPs.

The format of the DiffServ Traffic Classification Sub Data Item is:



Length: Variable

Length is defined above. For this Sub Data Item, it is equal to three (3) plus the value of the Num DSCPs field.

Flow Identifier (FID):

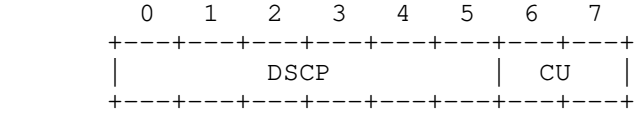
A 16-bit unsigned integer representing the data plane information carried in the sub Data Item that is to be used in identifying a flow. The value of 0xFFFF is reserved and MUST NOT be used in this field.

Num DSCPs:

An 8-bit unsigned integer indicating the number of DSCPs carried in the sub Data Item. A zero (0) indicates a (wildcard) match against any DSCP value.

DS Field:

Each DS Field is an 8-bit whose definition is the same as [RFC2474].



DSCP: differentiated services codepoint
CU: currently unused, MUST be zero

2.2.1. Router Receive Processing

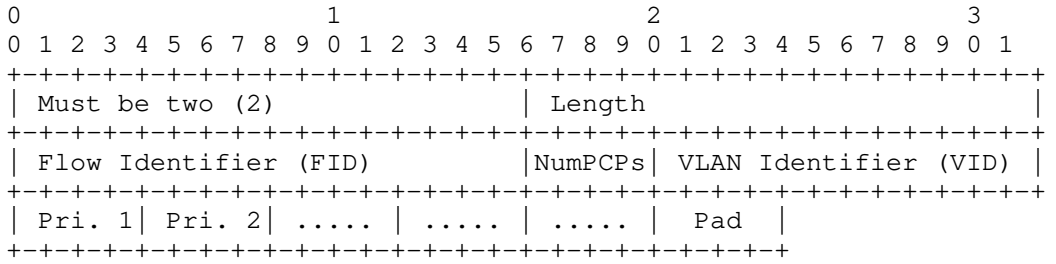
A router receiving the Traffic Classification Sub Data Item MUST validate the information on receipt, prior to using the carried information, including potentially updating the data behavior as determined by the extension requiring the use of the Sub Data Item. Validation failures MUST be treated as an error as described above.

Once validated, the receiver MUST ensure that each DS Field value is listed only once across the whole Traffic Classification Data Item. Note, this check is across the Data Item and not the individual sub Data Item. If the same DS Field value is listed more than once within the same Traffic Classification Data Item, the Data Item MUST be treated as an error as described above.

2.3. Ethernet Traffic Classification Sub Data Item

The Ethernet Traffic Classification Sub Data Item is used to identify the VLAN and PCPs that should be treated as a single flow, i.e., receive the same traffic treatment. Ethernet Priority Code Point support is defined as part of the IEEE 802.1Q [IEEE.802.1Q_2014] tag format and includes a 3 bit "PCP" field. The tag format also includes a 12 bit VLAN identifier (VID) field. PCPs are identified in a list of priority fields. An implementation that does not support PCPs and wants the same traffic treatment for all traffic to a destination or destinations would indicate 0 PCPs. Such an implementation could identify a VLAN to use per destination.

The format of the Ethernet Traffic Classification Sub Data Item is:



Length: Variable

Length is defined above. For this Sub Data Item, it is equal to four (4) plus the number of octets needed to carry the carried Priority fields is indicated by the NumPCPs field. Note that as length is in octets and each Priority field is 4 bits, the additional length is the value carried in the NumPCPs field divided by two and rounded up to the next higher integer quantity.

Flow Identifier (FID):

A 16-bit unsigned integer representing the data plane information carried in the sub Data Item that is to be used in identifying a flow. The value of 0xFFFF is reserved and MUST NOT be used in this field.

Num PCPs:

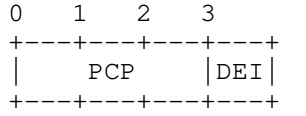
A 4-bit unsigned integer indicating the number of Priority fields carried in the sub Data Item. A zero (0) indicates a (wildcard) match against any PCP value.

VLAN identifier (VID):

A 12-bit unsigned integer field indicating the VLAN to be used in traffic classification. A value of zero (0) indicates that the VID is to be ignored and any VID is to be accepted during traffic classification.

Priority:

Each Priority Field is 4-bits long and indicates a PCP field defined in [IEEE.802.1Q_2014]. Note that zero (0) is a valid value for either PCP or DEI.



PCP: Priority code point
DEI: currently unused, MUST be zero

Pad:

A 4-bit long field included when NumPCPs is an odd number. This field MUST be set to zero when added, and MIST be ignored on receipt.

2.3.1. Router Receive Processing

A router receiving the Traffic Classification Sub Data Item MUST validate the information on receipt, prior to the using the carried information, including potentially updating the data behavior as determined by the extension requiring the use of the Sub Data Item. Validation failures MUST be treated as an error as described above.

Once validated, the receiver MUST ensure that each Priority Field value is listed only once across the whole Traffic Classification Data Item. Note, this check is across the Data Item and not the individual sub Data Item. If the same Priority Field value is listed more than once within the same Traffic Classification Data Item, the Data Item MUST be treated as an error as described above.

3. Compatibility

The formats defined in this document will only be used when extensions require their use.

4. Security Considerations

This document introduces finer grain flow identification mechanisms to DLEP. These mechanisms do not inherently introduce any additional threats above those documented in [RFC8175]. The approach taken to Security in that document applies equally to the mechanism defined in this document.

5. IANA Considerations

This document requests the assignment of several values by IANA. All assignments are to registries defined by [RFC8175].

5.1. Data Item Values

This document requests the following new assignments to the DLEP Data Item Registry named "Data Item Type Values" in the range with the "Specification Required" policy. The requested values are as follows:

Type Code	Description
TBA1	Traffic Classification

Table 1: Requested Data Item Values

5.2. DLEP Traffic Classification Sub Data Item Registry

Upon approval of this document, IANA is requested to create a new DLEP registry, named "Traffic Classification Sub Data Item Type Values". The registry shall identify the type code value, the Data Item which may use the value, and a description of the value. While the same value may be reused in different Data Items, this is not recommended at this time.

The following table provides initial registry values and the [RFC8126] defined policies that should apply to the registry:

Type Code	Description
0	Reserved
1	DiffServ Traffic Classification
2	Ethernet Traffic Classification
3-65407	Specification Required
65408-65534	Private Use
65535	Reserved

Table 2: Initial Registry Values

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8175] Ratliff, S., Jury, S., Satterwhite, D., Taylor, R., and B. Berry, "Dynamic Link Exchange Protocol (DLEP)", RFC 8175, DOI 10.17487/RFC8175, June 2017, <https://www.rfc-editor.org/info/rfc8175>.

6.2. Informative References

[I-D.ietf-manet-dlep-credit-flow-control] Cheng, B., Wiggins, D., and L. Berger, "DLEP Credit-Based Flow Control Messages and Data Items", draft-ietf-manet-dlep-credit-flow-control-02 (work in progress), June 2018.

[I-D.ietf-manet-dlep-da-credit-extension]
Cheng, B., Wiggins, D., and L. Berger, "DLEP DiffServ Aware Credit Window Extension", draft-ietf-manet-dlep-da-credit-extension-05 (work in progress), May 2018.

[I-D.ietf-manet-dlep-pause-extension]
Cheng, B., Wiggins, D., and L. Berger, "DLEP Control Plane Based Pause Extension", draft-ietf-manet-dlep-pause-extension-04 (work in progress), June 2018.

[IEEE.802.1Q_2014]
IEEE, "IEEE Standard for Local and metropolitan area networks--Bridges and Bridged Networks", IEEE 802.1Q-2014, DOI 10.1109/ieeestd.2014.6991462, December 2014, <http://ieeexplore.ieee.org/servlet/opac?punumber=6991460>.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, DOI 10.17487/RFC2474, December 1998, <https://www.rfc-editor.org/info/rfc2474>.

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, DOI 10.17487/RFC2475, December 1998, <https://www.rfc-editor.org/info/rfc2475>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

Appendix A. Acknowledgments

The sub Data Item format was inspired by Rick Taylor's "Data Item Containers". He also proposed the separation of credit windows from traffic classification at IETF98. Many useful comments were received from contributors to the MANET working group. This document was derived from [I-D.ietf-manet-dlep-da-credit-extension] as a result of discussions at IETF101.

Authors' Addresses

Bow-Nan Cheng
MIT Lincoln Laboratory
Massachusetts Institute of Technology
244 Wood Street
Lexington, MA 02421-6426

Email: bcheng@ll.mit.edu

David Wiggins
MIT Lincoln Laboratory
Massachusetts Institute of Technology
244 Wood Street
Lexington, MA 02421-6426

Email: David.Wiggins@ll.mit.edu

Lou Berger
LabN Consulting, L.L.C.

Email: lberger@labn.net

Network Working Group
Internet Draft
Intended status: Experimental
Expires: April 21,2019

A. Ladas
D. G C
N. Weerasinghe
C. Politis
WMN Research Group
Kingston University London, UK

October 22, 2018

Multipath ChaMeLeon (M-CML): A multipath hybrid routing protocol for MANETs

draft-ladas-manet-m-cml-01.txt

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on April 21,2019.

Copyright Notice

Abstract

This document describes the multipath ChaMeLeon (M-CML) routing protocol designed for Mobile Ad hoc Networks (MANETs). M-CML is a multi-path, hybrid routing protocol operating within a defined area denoted as the Critical Area (CA) in which the MANET is temporarily deployed during the post-disaster phase. The main concept behind M-CML is the adaptability of its routing mechanisms towards changes in the physical and logical state of a MANET. For autonomous communications in MANET, it is likely that the network size varies whenever additional devices join or subset of them leave the network. In addition, battery depletion of lightweight mobile communication devices will stipulate another reason for changes in the network size. As a result, the M-CML approach adapts its routing mechanism according to changes in the network scenario within a predefined CA. For small networks, M-CML routes data proactively using the Optimized Link State Routing version v2 (OLSRv2) protocol whereas for larger networks it utilizes the reactive Ad hoc On-Demand Distance Vector Version 2 (AODVv2) Routing protocol. The oscillation phase is the intermediate phase in which the transition of routing protocol occurs. M-CML creates multi-path routes for nodes with disjoint paths which increases the network reliability.

Table of Contents

1. Introduction

The protocol discussed in this document is a multipath hybrid routing protocol for MANETs. It consists of four phases of operation, which are considered to be Monitoring, Proactive, Oscillation and Reactive phases. The Proactive Phase, i.e., p-phase and Reactive Phase, i.e., the r-phase operates in the same way as the core functions of [3] and [6], respectively, and are discrete from each other. This draft focuses on the optimization of the p-phase by proposing a new route computation approach compared with [4] for multipath operation. By applying this multipath approach, our main aim is to ensure load balancing, improve QoS and delay, provide reliable communication among the nodes and maximize network life. In this draft, the r-phase of M-CML is not multipath, it is simply an on-demand route computation. M-CML makes no assumptions about the underlying link layer.

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 [1].

2.1. M-CML terminology used in this document

This section defines terminology associated with M-CML that is not already defined in or that differs from the meaning of the terminology in [3],[6],[8] and [12].

- The p-phase is based on MP-OLSRv2 Routing Protocols. The routing process is based on the specification [4],[6].

- The m-phase is the monitoring state of the routing node in which it monitors various network parameters, for example, network density, traffic pattern, energy consumption etc., based on which next routing phase is determined.

- Proactive Route Computation Terminology - The route computation process that is going to be used in M-CML is based on an Advanced Relay Routing (ARR) approach.

- The r-phase remains the same as defined in AODVv2 [3].

3. Applicability

The design of M-CML has been constructed to provide robust and efficient communication for wireless networks, by exploiting the multi-path information transfer and optimal combination of the two routing approaches. The autonomous nature of MANETs is very suitable for a variety of scenarios, especially when multiple disjoint paths exist within the CA . Also, in such a context, the number of MANET nodes varies depending on different parameters.

- Battery power constraint of mobile nodes is a very important consideration. Node failure as a consequence of battery depletion MAY result in network segmentation.

- Nodes MAY join or leave the network at anytime and at any random location.

- A certain quality of service (QoS) level has to be maintained to allow for multimedia communication. Mainly, certain delay bounds have to be established while also maintaining effective routing by minimizing battery consumption.

M-CML has the ability to adapt its routing behavior on-the-fly according to the changes in MANET size. Therefore, it is a more suitable routing alternative than individual routing approaches for small, large as well as variable sized MANETs operating in a defined CA. Moreover, the M-CML also adapts within the high level of node mobility, which makes it applicable in the very dynamic network topology.

4. Protocol Overview

This protocol is designed to work as a multi-path, hybrid and adaptive routing protocol for MANETs. The normal mode of operation is under one of the stable phases. The default operating phase is the p-phase. This section describes the various processes and structures introduced by M-CML.

4.1. Proactive Routing

As soon as the MANET is implemented in the CA, a default routing mode in M-CML is the p-phase, irrespective of the network scenario.

4.2. Monitoring and Analysis

The monitoring phase (m-phase) is triggered soon after the p-phase starts in section 4.1., i.e., it runs simultaneously with the p-phase. The m-phase is initiated when a control message is received by the monitoring module in the routing node [9]. However, m-phase is triggered in regular intervals even when M-CML runs either in p-phase or r-phase (but it is disabled in o-phase). The node MUST perform the following tasks.

1. Send a copy of the packet to the monitor part of the module. The monitoring component has a network size part that MUST check the number of nodes in the network. This is accomplished differently depending on the current stable phase of operation (as described later).

2. Send the packet to the regular control message processing by the stable phase, as described in [3] or section 5.2, which is the current active routing part.

In the m-phase, the network size is estimated as follows. The m-phase and the p-phase (where the OLSRv2 routing algorithm is active) run concurrently, this task consists of calculating the number of reachable hosts from the routing table as defined in [6]. This calculation is done by counting the number of rows in the proactive routing table. Each row includes fields of possible destination nodes, the next hop to reach the destination as specified in the possible destination field and its distance from the current source node. These field values are computed using periodical Topology Control (TC) and HELLO message broadcasts by each node in the network. If the number of nodes is found to exceed the NST, this monitor part must contact the L-NST part of the Adaptive Component.

In the r-phase (where the AODVv2 routing algorithm is active), the number of nodes in the network is estimated using the maximum value of the hop count from a source node to a destination. As defined in [3], a source finds a route to a destination 'on-demand' by flooding a Route Request (RReq) packet throughout the network using an expanding ring approach until a RRep is received from the destination.

The monitor function in the source node must use this RRep message to obtain the value of Hop Count (HC) towards the destination node. It then compares this with the U-NST, which is calculated according to the relationship defined in section 9.1. The monitor function MUST act as follows:

1. If HC in RRep is greater or equal to U-NST, it decides that the NST is not exceeded.

2. If HC in RRep is less than the U-NST, the data packets are transmitted through the established route. After data

transmission, the CMLv2 Hop Count Request (HCReq) packet described in section 6.3. MUST be generated and flooded in the network to probe for the network HC (as opposed to destination HC). The HC is said to be less than the NHT, if after RREQ_WAIT_TIME*DISCOVERY_ATTEMPTS_MAX, no HCRep has been received. If the HC is less than the U-NST, the monitor function decides that the r-phase NST (calculated using the relationship in section 9.1.), has been exceeded and calls the U-NST part of the Adaptive component.

If a node receives HCReq, it must first make sure that the sequence number of the packet is greater than that stored in the Change Phase (CP) table for the same originator address. Then, it checks if the TTL = 0. If the latter is true, it MUST store HCReq originator IP and packet sequence number information in the CP table and send back an HCRep to the originator, as described in section 6.4. Otherwise, it decreases the TTL value and floods back the HCReq packet in the network. It then generates and floods its own HCReq to probe for the HC with TTL value set to NHT. The value of the originator address of the original HCReq packet (triggering the probing locally) is stored in the CP table along with the sequence number.

The message type field is set equal to the value of message type "HCReq" as which is equal to ’9’ as mentioned in section 13. If for that particular HCReq, an HCRep is received, the node must send an additional HCRep to that HCReq originator address.

If a node receives a M-CML CP Packet described in section 6.2, it MUST flood the packet in the network after decreasing its TTL count. Then, the active routing algorithm part of the node MUST call the relevant Adaptive part from its Adaptive component.

4.3. Adaptive Component

The Adaptive component, when activated by the m-phase (i.e., a CP packet is received), the component MUST make sure the following:

1. The Adaptive part ID used in the calling message is valid.

2. The Adaptive part ID corresponds to the appropriate part with respect to the active routing component if contacted from the monitor part as described in the above section.

3. In the case where the CP packet requires that an inappropriate(see point 2 above) Adaptive part be contacted, this action is ignored and the CP is flooded back in the network.

Any of the activated Adaptive part, subsequent to the above steps, MUST change operation to o-phase as it is explained in section 4.4.

In any other situation, the Adapt function terminates and the appropriate stable phase operation is resumed.

4.4. Oscillation Phase

In the o-phase, the Adaptive component checks the o-phase validity time, "Osc_Interval" of the oscillation timer described in section 8.1, is first checked. If the timer is still valid, the o-phase variable in the core is cleared and consequently the stable phase of operation is maintained. If the timer has expired, the o-phase variable is set and:

1. If the routing algorithm ID (RID) is set to OLSRv2:

   The OLSRv2 mechanism will continue to operate. At the same time, the node will check the number of nodes in the network as described in section 4. for 2 * TC_Intervals (TC_Interval is described in [6]). If the number of nodes is then found to be greater than L-NST at least once, the o-phase switches to r-phase and resets the oscillation timer. It also generates and floods a CMLv2 CP Packet. The CP packet includes its address as originator address and its incremented sequence number. The CP field value of the M-CML packet is set as "AODVv2 RID".

   Otherwise, the node returns to operating in the p-phase.

2. If the routing algorithm ID (RID) is set to AODVv2:

   The routing mechanism of AODVv2 will continue to operate. At the same time, the Monitor and Adaptive component will check the HC of the network using two more HCReq packets, as described in section 6.3., waiting for RREQ_WAIT_TIME * DISCOVERY_ATTEMPTS_MAX (RREQ_WAIT_TIME and DISCOVERY_ATTEMPTS_MAX are explained in [3]) each time. If in at least one occurrence, no HCRep is obtained for the HCReq with TTL=U-NHT, it is implied that the network size is smaller than the NST. In this case, the o-phase switches to p-phase by clearing the o-phase variable and setting the RID to the OLSRv2 RID. The oscillation timer is also reset. It also generates and floods a M-CML CP packet. The CP packet includes its address as originator address and its incremented sequence number. The value of the CP field in the packet is set to "OLSRv2 RID".

   Otherwise, stable r-phase routing is resumed.

3. If this phase shift is initiated using a M-CML CP packet:

   The node core MUST check the value of the sequence number in the packet and compare it to any stored sequence number having the same originator address in the CP table. If no match is found in the CP table, a new entry is created with the aforementioned values obtained from the CP packet before further processing. Otherwise, if a match is found and the packet sequence number is

less than the sequence number stored in the table, the message is silently discarded and the node returns to the stable phase specified by its core RID variable.

For non-discarded packets, the node MUST check the CP field value in the CP packets and compare it with its own RID:

1. If they are equal, the CP packet is silently discarded and the node returns to the phase specified by its core RID.

2. If they are not equal, the o-phase changes the RID to the value specified in the CP field of the CP message and resets the oscillation timer.

In both cases, the CP packets are flooded back in the network.

5. Protocol Operation

This section describes the behavior M-CML MUST follow in the m-phase, p-phase, r-phase and o-phase.

5.1. M-Phase

In the m-phase, the node core receives packets with all message types but only processes packets with message types [1-2] and routes data packets as described in [8]. It also processes packets with message types 9-11 as described in this draft. In addition, it sends a copy of the packet to the Monitor component each time a TC routing packet is received. In this phase, NST is equal to U-NST to cater for group oscillation.

5.2. P-Phase

The proactive phase, i.e., p-phase, of M-CML is based on [4],[6] but the source to destination route is computed differently. According to [4], when a packet has to be forwarded from the source to the destination, the source node acquires a path from the Multi-path Routing Set, storing the path information in the datagram header as source routing header. Each of the intermediate nodes, is listed in the source routing header and it forwards the packet to the next hop as indicated in the source routing header.

In our approach, each node, upon receiving a packet, computes all the disjoint paths to the destination node. The next step is to check if it is on the best (or 2nd, or 3rd, and so on, best) path to the final destination. If this is valid, the packet is forwarded.

The routing decision for determining the best path will be taken by using the Expected Transmission Count ETX) [7] metric. If the number of paths is higher than 3, then the 3 best routes are selected according to the ETX metric. So, regarding this approach the

decision of which path(s) is going to be selected is taken according to the ETX metric instead of using the hop count metric.

5.3. R-Phase

In the r-phase, the node core receives packets with all message types but processes only packets with message types 5-8 and routes data packets as specified in [3]. It also processes packets with message types 9-11 as described in this document. In addition, it sends a copy of the packet to the Monitor component each time it receives RRep routing packets as a source node. In this phase, NST is equal to L-NST to cater for group oscillation.

5.4. O-Phase

In this subsection we describe the oscillation problem and the operation of the o-phase as a mechanism to counteract oscillation effects in MANETs that use the CMLv2 protocol. The basic operations of the current stable phase still apply in the o-phase. However, there are added phase dependent sampling processes to check for oscillation instances.

5.5. Algorithm for M-CML

M-CML is characterized by two major modifications compared to M-CML aiming to improve its operational efficiency. The first addition is the incorporation of optimal M-CML configurations in the new version and the second is the proposal of a new logic on the routing algorithm which calculates the multiple paths in a more efficient manner.

Multipath routing protocols can be employed to tackle challenges created by link instabilities caused by environmental conditions. However, it is obvious that implementing a routing protocol operating in a multipath manner has some significant drawbacks related to higher duplicate data packet generation, traffic congestion in the network and high energy consumption. On this note, we have modified the operation of our M-CML routing protocol in a way of taking advantage of the multiple routes only if it is absolutely necessary. Our main aim is to establish the way the multipath method is performed, reduce the generation of redundant duplicate packets, and apply the improved algorithm on top of the changes that we considered in the previous section. In order to further develop the operational efficiency of CMLv2, an extended version of CMLv2 is named as M-CML. Here, M-CML protocol exploits the attributes of CMLv2’s system model and aims to enhance its performance by applying the following changes:

Following up the analysis of M-ML in the p-phase, i.e., the default phase, M-CML selects the optimal configuration set, with the view of handling the generated routing load more effectively in the network.

M-CML employs the improved multipath algorithm for selectively calculating multiple paths in a more efficient way, acting as a single path or multipath routing protocol depending on the quality of the links. This way, we aim to reduce improvident emission of duplicate packets which impacts the network congestion and the nodes' energy consumption.

The proposed algorithm describes the technique to add a new entry M-CML's routing table. In particular, the set of next hop addresses are listed in an ascending order based on their ETX values. Upon transmitting data packets from source to destination, a gateway list is responsible for allocating the corresponding routing entry to the relevant destination, then parsing the ETX values which have been listed in ascending order and finally transmitting the information according to the two minimum ETX values.

Each time a node requests for a route towards the destination, it first calculates all next hops corresponding to that destination. In the case that there is not any available next hop, the packet is eventually dropped. Otherwise, node either transmits data using the two minimum values of ETX following the initial approach of M-CML, or dynamically decides to transmit data using a single path only if the ETX value is on its minimum value, i.e., ETX=1. This can reduce the unnecessary copies of the same packets which are distributed throughout the network due to the multipath attributes of the protocol and, at the same time, confine the energy consumption. Moreover, during the scenarios where the distance among source and destination is limited and the successful delivery of HELLO messages is high, we aim to eliminate the improvident emission of redundant information.

5.5.1. Protocol Operation

M-CML proposes a twofold solution to the oscillation problem. Appropriate NSL values (acting as NST) can restrain the effects of group oscillations whereas the right "Osc_Interval" value for the oscillation timer limits the impact of frequent oscillations.

In addition, during the o-phase, the monitor component samples more instances of the 'number of nodes' count or the network HC (depending on the current stable phase of operation) as described in section 4. In this way, it can confirm whether the NST or NHT has actually been exceeded. Otherwise, it determines that an oscillation has occurred and the stable phase of operation is resumed. If the NST is found to have been actually exceeded in the o-phase, the appropriate part of the Adaptive component (identified as explained above) resets the oscillation timer and generates CP packets. These CP packets are flooded into the network to alert neighboring nodes of such a phase shift. The o-phase is then terminated by the Adaptive Component part that then shifts routing operation to the relevant stable phase of operation.

Furthermore, during the o-phase, the core and active Adaptive component part are responsible for phase shifting if a valid CP packet is received from a neighboring node (as explained above). In such a case, it floods back the CP packet in the network.

Furthermore, during the o-phase, the core and active Adaptive component part are responsible for phase shifting if a valid CP packet is received from a neighboring node (as explained above). In such a case, it floods back the CP packet in the network. If the protocol phase changes from p-phase to r-phase, and a HELLO packet is received, the information about next hop is stored in the routing table. A TC packet information is used to either reset a timeout in the routing table or populate routing table information for potential data to be sent. In the case where the transition occurs from the r-phase to the p-phase, and RREQ are requested, if the destination is already in the routing table, a RREP is sent back with this information. Otherwise, the RREQ is stored until 2 *TC_INTERVAL before sending a RREP.

6. M-CML Packet and Message Formats

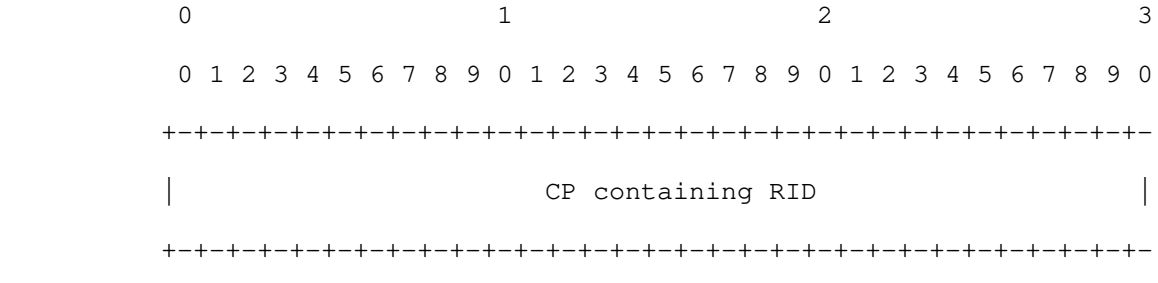
6.1. Packet Format

The basic layout of a M-CML packet is as recommended in [12]. The message type field indicates the type of message found in the "MESSAGE" section. This could be a M-CML message or messages from [6] or [3] or the CP message.

6.2. Change Phase (CP) Message

The Change Phase (CP) field contains the RID to which the originator node has shifted to and subsequently requests neighbor nodes to shift to.

The Change Phase message format is shown below:



6.3. Hop Count Request (HCReq) Message

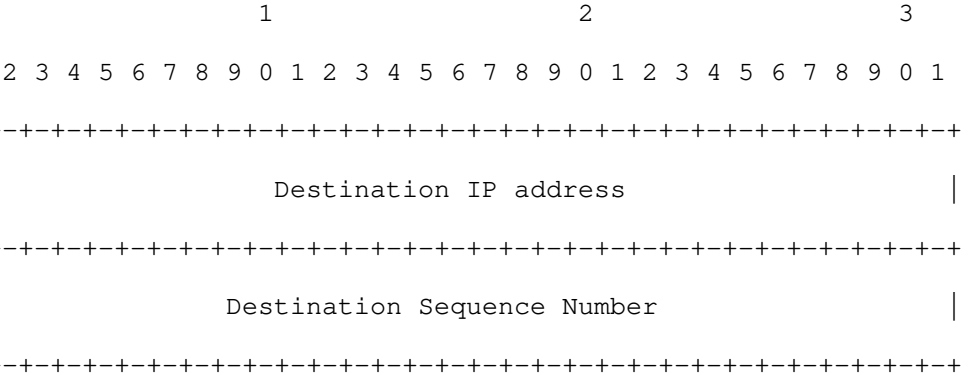
The HCReq message has an empty message body. It can be identified as a CML packet with:

o Message Type - The value of message type is set to 9.

o TTL - The TTL value is set to NHT.

6.4. Hop Count Request (HCRep) Message

The message format for the HCRep message is:



o Destination IP address - Originator IP address in corresponding HCReq packet.

o Destination Sequence Number - Originator Sequence Number of corresponding HCReq packet.

7. M-CML tables

7.1. M-CML Change Phase table

The M-CML CP Table fields are listed below:

o Originator IP Address - The IP address of the node which generated the packet.

o Originator Sequence Number - The Sequence number of the message that was sent by the node which generated the packet. This is incremented monolithically for each message generated by a node.

o Message Type - The message type value of the message through which the table row was populated.

8. M-CML Timers

8.1. Oscillation timer

The Oscillation timer is used in the o-phase to prevent phase shifts within the time period of "Osc_Interval". This timer prevents phase shift due to frequent oscillations.

9. Constants

9.1. Network Threshold Values

The Network threshold values for M-CML are described below:

o NST - The theoretical Network size threshold "Nt" of a network depends on the number of nodes N in the network, the critical area A of the network and the radio coverage area of each node. NST marks the point after which a reactive routing approach will be more effective (in terms of end to end packet delivery latency) and efficient (in terms of battery usage) compared to a reactive routing approach.

Below the NST point, proactive routing approaches outperform reactive routing approaches.

o U-NST - The Upper limit network size threshold "Nu" is given by:

Nu = Nt + Nosc

where "Nosc" is the number of nodes in the network which are expected to oscillate.

When operating in the p-phase the actual value of NST is equal to "Nu".

o L-NST - The Lower limit network size threshold "Nl" is given by:

Nl = Nt - Nosc

When operating in the r-phase the actual value of NST is equal to "Nl".

o NHT - The network hop threshold value "Nht" is directly proportional to the square root value of the NST:

Nht = Function (sqrt (Nt))

The optimal values for "Nt", "Nosc", "Nu", "Nl" and "Nht" as well as an accurate relationship between NST and NHT can be derived through experimentation and mathematical modeling for a given critical area, 'A' and node coverage radius 'R'.

9.2. Oscillation Interval (Osc_Interval)

The Osc_Interval is a time period for which no phase shift is allowed. While the U-NST and L-NST values cater for group oscillations, the Osc_Interval prevents unnecessary phase shift overheads due to regular oscillations. Thus, the Osc_Interval SHOULD be set according to the time period of node oscillations. The optimal value for Osc_Interval can be derived through

experimentation and mathematical modeling for a given critical area, 'A' and node coverage radius 'R'.

9.3. Parameters Value

Parameter values used by the M-CML protocol and also defined in [3] and [6] are:

Parameter Name	Value
RREQ_WAIT_TIME	2 seconds
DISCOVERY_ATTEMPTS_MAX	3 attempts
RREQ_HOLDDOWN_TIME	10 seconds
HELLO_INTERVAL	2 seconds
TC_INTERVAL	5 seconds

10. Message Emission and Jitter

Synchronization of control messages SHOULD be avoided as mentioned in [2].

11. IPv6 Considerations

All the operations and parameters described in this document can be used for both IP version 4 and IP version 6. For IPv6 networks, the IPv4 addresses in M-CML packets and messages need to be replaced by IPv6 addresses. The packet and message sizes will also increase accordingly.

12. Security Considerations

M-CML does not specify any security countermeasures. Security Threats for OLSRv2 are described in IETF draft, Security Threats for the Optimized Link State Routing Protocol Version 2 (OLSRv2) [10] and for the Ad-Hoc On-demand Distance Vector Version 2 (AODVv2)[3] which are applicable to MCML.

M-CML Packet/Message Format follow the Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format proposed in [12]. Hence the security mechanisms suggested in [12] and [15] can be directly applied to this protocol. The network performance can also be affected by artificial manipulation of metric values. More specific, if a link is, artificially, advertised with a higher value, the amount of incoming traffic may be reduced. A malicious node, might decrease or increase the value of the advertised links, in order to increase or decrease the data traffic. Thus, a malicious node can

potentially affect data throughput, by not sending data from good links and vice versa.

13. IANA Considerations

The IANA consideration section is required as recommended by [11] and [13]. The following values for the corresponding message types would be required:

Message Type	Value
HELLO_MESSAGE	= 1
TC_MESSAGE	= 2
ROUTE REQUEST (RREQ)	= 3
ROUTE REPLY (RREP)	= 4
ROUTE ERROR (RERR)	= 5
ROUTE-REPLY ACK (RREP-ACK)	= 6
HOP COUNT REQUEST (HCREQ)	= 7
HOP COUNT REPLY (HCREP)	= 8
CHANGE PHASE (CP)	= 9

14. Conclusions

This I-D introduced the M-CML routing protocol. Here, M-CML is a routing protocol which combines the functionalities of Multipath OLSRv2 and AODVv2 protocols in an adaptive and hybrid manner. The motivation behind M-CML is the enhancement and the increase of the reliability and robustness of the networks. The main features of MCML include the Adaptive Module, which monitors and adapts, within m-phase, to the changing network state, the p-phase which computes multiple routes according to the link quality metric (ETX), the r-phase which is computes multiple routes in an on-demand manner. In the next release, M-CML will be enhanced by removing the o-phase and will operate as a single protocol. Furthermore, M-CML will consider various route optimization to improve the mobility support.

15. References

15.1. Normative References

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

[2] Clausen, T., Dearlove, C., and B. Adamson, "Jitter considerations in MANETs", RFC 5148, March 2008.

[3] Perkins, et al., "Dynamic MANET On-demand (AODVv2) Routing", IETF Draft, December 2014.

[4] Yi,J. and Parrein,B., "Multi-path Extension for the Optimized Link State Routing Protocol version 2 (OLSRv2) ", IETF Draft, October 2014.

[5] Macker, J. and S. Corson, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", RFC 2501, January 1999.

[6] Clausen, T., Dearlove, C., Jacquet, P., Herberg, U., "The Optimized Link State Routing Protocol Version 2", RFC 7181, April 2014.

[7] Vasseur, JP., Kim, M., Pister, K., Dejean, N., Barthel, D., "Routing Metrics Used for Path Calculation in Low? Power and Lossy Networks", RFC 6551, March 2012.

[8] Ramrekha, A., Panaousis, E., Politis, C., "ChaMeLeon (CML): A hybrid and adaptive routing protocol for Emergency Situations", IETF Draft March 2011.

[9] Ladas, A., Deepak, G.C., Pavlatos, N. and Politis, C., 2018. "A selective multipath routing protocol for ubiquitous networks" Ad Hoc Networks, 77, pp.95-107, August 2018.

15.2. Informative References

[10] Clausen, T., Herberg, U., Yi, J., "Security Threats for the Optimized Link State Routing Protocol version 2 (OLSRv2) ", IETF Draft, August 2014.

[11] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226, BCP 26, May 2008.

[12] Clausen, T., Dean, J., Dearlove, C., and Adjih, C."Generalized MANET Packet/Message Format", RFC 5444, March 2009.

[13] Chakeres, I., "IANA Allocations for MANET Protocols", RFC 5498, March 2009.

[14] Clausen, T. and C. Dearlove, "Representing multi-value time in MANETs", RFC 5497, March 2009.

[15] Herberg, U., Dearlove, C., Clausen, T., "Integrity Protection for the Neighborhood Discovery Protocol (NHDP) and Optimized Link State Routing Protocol Version 2 (OLSRv2)", RFC 7183, April 2014.

16. Acknowledgments

The authors wish to acknowledge the support of the Engineering and Physical Science Research Council (EPSRC) Project DARE (Distributed Autonomous Resilient Emergency Management System) under the grant agreement number EP/P028764/1. Framework Program and all the partners in SALUS (Security And InteroperabiLity in Next Generation PPDR CommUnication InfrastructureS)project with contract number 313296 and also the support of the ICT European 7th Framework Program and all partners in PROACTIVE PRedictive reasOning and multi-source fusion empowering AntiCipation of attacks and Terrorist actions In Urban EnVironmEnts with contract number 285320.

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

Authors' Addresses

The following researchers who have contributed to this I-D are members of the Wireless Multimedia and Networking (WMN) Research Group at Kingston University London:

Alexandros Ladas

Researcher

Researcher, WMN Research Group

Kingston University London, UK, KT1 2EE

Phone: (+44) 02084177025

Email: k1242116@kingston.ac.uk

Deepak G C

Research Fellow, WMN Research Group

Kingston University London, UK, KT1 2EE

Phone: (+44)02084177025

Email: d.gc@kingston.ac.uk

Nuwan Weerasinghe

Researcher, WMN Research Group

Kingston University London, UK, KT1 2EE

Phone: (+44) 02084177025

Email: n.weerasinghe@kingston.ac.uk

Christos Politis

Head of WMN Research Group

Kingston University London, UK, KT1 2EE

Phone: (+44) 02084172653

Email: c.politis@kingston.ac.uk