IETF MANET Working Group
Internet-Draft
Intended status: Experimental
Expires: August 2010

T. Ramrekha
E. Panaousis
G. Millar
C. Politis
WMN Research Group
Kingston University London
FEB 24, 2010

ChaMeLeon (CML): A hybrid and adaptive routing protocol for Emergency Situations.
draft-ramrekha-manet-cml-00.txt

Status of this Memo

This Internet-Draft will expire on August 24, 2010.

Abstract

This document describes the ChaMeLeon (CML) routing protocol designed for Mobile Ad hoc NETworks (MANETs) supporting emergency communications. CML is a hybrid and adaptive routing protocol operating within a defined disaster area denoted as the Critical Area (CA). The main concept behind CML is the adaptability of its routing mechanisms towards changes in the physical and logical state of a MANET. For autonomous emergency communications, there is a likelihood that the network size will vary whenever more rescuers join or leave the network. In addition, battery exhaustion of lightweight mobile communication devices used by rescuers could stipulate another reason for changes in the network size. Hence, this version of CML adapts its routing behavior according to changes in the network size within a pre-defined CA. For small networks, CML routes data proactively using the Optimized Link State Routing (OLSR) protocol whereas for larger networks it utilizes the reactive Ad hoc On-Demand Distance Vector (AODV) Routing protocol so that overall routing performance is improved. These transitions occur via the CML oscillation phase. This document focuses on the description of the processes involved in the CML Adaptive module, CML Oscillation phase and transition between phases.

Table of Contents

1. Introduction

This protocol is an adaptive and hybrid routing protocol for MANETs designed to be used by rescuers within the realm of extreme emergency communications. It consists of 3 phases of operation namely Proactive, Oscillation and Reactive. The Proactive (p-) and Reactive (r-) phases operate in the same way as the core functions of [3] and [5] respectively and are discrete from each other. The Oscillation phase (o-phase), therefore, acts as an intermediate between p- and r-phases and decides on whether a shift from p-phase to r-phase is appropriate based on criteria defined in section 4.2. The main purpose of the o-phase is to avoid the oscillation problem as described in section 5.3. In addition, ChaMeLeon (CML) introduces an Adaptive module which runs in parallel to and is accessible by all phases of operation. The module is designed to monitor relevant MANET characteristics, detect a certain quantitative threshold

exhibited by specific monitored characteristics and in such an event, transfer the control to the o-phase.

This version of CML monitors the number of nodes in MANETs within a defined Critical Area (CA) where extreme emergency rescue operations take place. In such a situation, rescuers tend to join or leave the network according to the severity of the situation. CML aims to adapt its routing mechanism to the size of such MANETs, thus enhancing overall efficiency and effectiveness (both terms defined in [4]) as compared to [3] and [5]. CML uses [5], [3], [8], [10] and, optionally, [1]. 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. CML Terminology

This section defines terminology associated with CML that is not already defined in or that differs from the meaning of the terminology in [8], [5] and [3].

- Node - A MANET router that implements the CML protocol as specified in this document.
- CML interface - A network device that participates in a MANET that runs CML. A node may have several CML interfaces. Each interface SHOULD be assigned a unique IP address. Each interface SHOULD have a unique IP address.
- Non CML interface - A network device that does not participate in a MANET that runs CML. A node MAY have several non CML interfaces.
- Single CML interface node - A node in a MANET that has only one CML interface.
- Multiple CML interface node - A node in a MANET that has more than one CML interface.

- Link - A pair of CML interfaces, from two different nodes, within the same radio range that can communicate directly with each other. A node has a link to another node when at least one of its interfaces has a link to one of the interfaces of the other node.

- Symmetric link - A verified bi-directional link between two CML interfaces.

- Asymmetric link - A verified link between two CML interfaces in one direction only.

- Main address - The main address of a node, to be used in CML packet as the "originator address" for all control messages generated by the node. It MUST be the address of one of the CML node interfaces.

- Neighbor node - A node X is a neighbor node of node Y if node Y can hear node X.

- MANET Context – A set of characteristics describing the MANET and its environment as defined in [4]. This includes node mobility levels, small and large node groups as well as technological and environmental constraints such as limited battery life of devices and bandwidth limitations of wireless links.

- Source - A node that initiates data communication in the network or a node which generates control packets.

- Sink - A node that is the intended recipient of data sent by source nodes.

- Router - A node that implements the CML protocol. All collaborating nodes are potential routers. Router nodes are intermediate nodes located on routes between source and destination nodes. They are responsible for forwarding packets according to the CML routing algorithm.

- Source address - An address that is unique (within the MANET) to each individual source node. A node MUST select an originator address; it MAY choose one of its interface addresses as its originator address.

- Destination address - An address that is unique (within the MANET) to each individual sink node.

- Stable phases - The set of CML routing phases that operates efficiently for a given MANET context. In this CML version, r-phase and p-phase are the only stable phases.

- R-phase - A routing phase where the protocol adopts routing mechanisms from [3].

- P-phase - A routing phase where the protocol adopts routing mechanisms from [5].

- CML Oscillation phase - A routing phase where the protocol continues to operate in the current stable phase. It also checks whether the network size or hop threshold has been genuinely exceeded or whether node oscillation has taken place. It also alerts neighbors whenever it decides that the network has to shift phases. This phase is initiated by the CML Adaptive module.

- Phase-shift - A shift from r-phase routing to p-phase routing via the o-phase.

- Oscillation - An event where at least one node regularly joins and leaves a MANET so that the CML Network Size Threshold is each time exceeded by such activity.

- CML Adaptive module - A module which encompasses the Monitor and Adapt functions. This module runs in parallel to and is accessible by all phases. It is used to determine the number of nodes in the network and checks whether this number has breached Network Size Limits. It also changes the node phase to o-phase if the threshold is exceeded.

- CML Network Size Threshold (NST) - A threshold for the number of nodes in the network. Below the NST point, p-phase routing is more efficient and effective (both terms defined in [4]) than the r-phase routing. Beyond the NST point, r-phase routing outperforms p-phase. The NST varies according to the context of the MANET such as transmission range of the devices and node density (for a given critical area). NST is exceeded in the r-phase when the number of nodes is less than NST. In the p-phase, this occurs when the number of nodes is greater than NST.

- CML Network Size Limit (NSL) - The NSL is a couple of values which deviate by an equal amount greater/less than the NST. The Upper value of NST is denoted by (U-NST) and the Lower value by (L-NST). The deviation value from Network Size Threshold is selected based on node oscillation properties.

- CML Change Phase (CP) packet - A control packet unique to CML that is sent during the o-phase to alert other nodes in the network that a phase-shift has occurred locally. In p-phase mode, CML CP packets are only forwarded by MPR nodes whereas in r-phase mode, the CP packets are flooded by all nodes in an RREQ flooding fashion.

- CML Change Phase (CP) Table - The CP Table is used to make sure that the originator sequence number and originator IP information of processed CML control packets are available for a given timeout period. This will help in ensuring loop free communication.

- Network Hop Threshold (NHT) - A hop count value which indicates that the NST has been reached. The relationship between NHT and NST is defined in section 9.1.

- CML Hop Count Request (HCReq) Packet - A CML control packet sent to probe whether the Network Hop Threshold (NHT) has been exceeded.

- CML Hop Count Reply (HCRep) Packet - A CML control packet sent as a unicast reply to a HCReq packet. When it is received by the originator node, it indicates that the Network Hop Threshold (NHT) has not been exceeded.

3. Applicability

This protocol has been designed with Ad hoc Communications in extreme emergency scenarios in mind, where rescuers are equipped with lightweight communication devices. The autonomous nature of MANETs is very suitable for extreme emergency communications within the CA because communication infrastructures in such disaster sites are usually incapacitated. Also, in such a context, the number of MANET nodes varies depending on the severity of the rescue operations. CML has the ability to adapt its routing behavior to changes in MANET size. Hence, it is a more suitable routing alternative than pure routing approaches for small, large as well as variable sized MANETs operating in a defined CA. A MANET including but not limited to such unique contextual considerations is defined as an emergency MANET (eMANET) in [6]. Future versions of CML will include functions in the Adaptive module to adapt to some of the other eMANET contexts such as mobility and those described in [4]. In this document, it is assumed that nodes are uniformly distributed in the CA so that rescuers can cover the maximum CA.

In addition, CML MAY also be used for general purpose MANETs.

4. Protocol Overview

This protocol is designed to work as a hybrid and adaptive routing protocol for eMANETs. The normal mode of operation is under one of the stable phases. The default stable operating phase is the p-phase. This section describes the various processes and structures introduced by CML. Thus, it focuses on the interaction between the Adaptive Module and the o-phase as well as the operation of the o-phase. The routing behaviors of the r-phase and p-phase have been described in [3] and [5] respectively.

4.1. Adaptive Module

4.1.1. Monitor function

When a control message is received at a CML interface, the node MUST call the monitor function of the Adaptive module after regular control message processing by the stable phase, as described in [3] and [5]. The current mode of operation is indicated by passing a phase specific flag to the function, i.e. a “Pphase” flag for p-phase operation and “Rphase” flag for R-phase operation. The monitor function, when called, MUST check the number of nodes in the network. This is accomplished differently depending on the current stable phase of operation.

In the p-phase, this task consists of calculating the number of reachable hosts from the routing table that is defined in [5]. This calculation is done by counting the number of rows in the 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, the monitor function must call the Adapt function with the phase flag set as “Pphase” and the context flag set as “Nsize” (for Network Size). The last argument passed is the call flag and denotes the source of the call. In this case the call flag is set as “Monitor”.

In the r-phase, 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

NHT, 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 NHT, it decides that the NST is not exceeded.

2. If HC in RRep is less than the NHT, the data packets are transmitted through the established route. After data transmission, the CML Hop Count Request (HCReq) packet described in section 6.3. will 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 4*NET_TRAVERSAL_TIME, no HCRep has been received. If the HC is less than the NHT, the monitor function decides that the r-phase NST (calculated using the relationship in section 9.1.), has been exceeded and calls the Adapt function with the phase flag set as “Rphase”, the context flag set as “Nsize” and the call flag set as “Monitor”.

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 CML CP Packet described in section 6.2. , it MUST flood the packet in the network after decreasing its TTL count. Then, the node MUST call the adapt function from its Adaptive module with the current phase flag, the context flag set as “Nsize” and the call flag set as “CML_CM”.

4.1.2. Adapt function

The Adapt function, when called by the monitor function makes sure one of the following is valid:

1. The phase flag is set to “Pphase”, the context flag is set to “Nsize” and the call flag set as “Monitor”.

2. The phase flag is set to “Rphase”, the context flag is set to “Nsize” and the call flag set as “Monitor”.

3. The phase flag is set as either “Pphase” or “Rphase”, the context flag is set as “Nsize” and the call flag is set as “CML_CM”.

If any one of the above cases is true, the Adapt function changes operation to o-phase by maintaining the current values of the phase flag, context flag and call flag which will be accessed by o-phase processes.

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

4.2. O-phase

In the o-phase, 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 call for o-phase is ignored and the stable phase of routing denoted by the phase flag is resumed. If the timer has expired, the o-phase checks the flag values:

1. If the phase flag is set to “Pphase”, the context flag is set to “Nsize” and the call flag set as “Monitor”:

   The routing mechanism of p-phase 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 [5]). If the number of nodes is then found to be greater than NST at least once, the o-phase switches to r-phase and resets the oscillation timer. It also generates and floods a CML CP Packet. The CP packet includes its address as originator address and its incremented sequence number. The CP field value of the CML packet is set as “Rphase”.

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

2. If the phase flag is set to “Rphase”, the context flag is set to “Nsize” and the call flag is set as “Monitor”:

The routing mechanism of r-phase will continue to operate. At the same time, the node will check the HC of the network using two more HCReq packets, as described in section 6.3. , waiting for 4*NET_TRAVERSAL_TIME (NET_TRAVERSAL_TIME is explained in [3]) each time. If in at least one occurrence, no HCRep is obtained for the HCReq with TTL=NHT, it is implied that the network size is smaller than the NST. In this case, the o-phase switches to p-phase and resets the oscillation timer. It also generates and floods a 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 "Rphase".

Otherwise, stable r-phase routing is resumed.

3. If the phase flag is set as either "Pphase" or "Rphase", the context flag is set as "Nsize" and the call flag is set as "CML_CP":

The node 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 n 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 the phase flag.

For non-discarded packets, the node MUST check the CP field value in the CP packets and compare it with the phase flag:

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

2. If they are not equal, the o-phase changes the operation phase 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 CML MUST follow in the p-phase, r-phase and o-phase.

5.1. P-phase

In the p-phase, the node receives packets with all message types but only processes packets with message types 1-4 and routes data packets as described in [5]. It also processes packets with message types 9-11 as described in this document. In addition, it calls the Adaptive module each time a TC routing packet is received.

In this phase, NST is equal to U-NST to cater for group oscillation which is described in section 5.3.1.

5.2. R-phase

In the r-phase, the node 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 calls the Adaptive module each time it receives a RRep routing packet as a source node.

In this phase, NST is equal to L-NST to cater for group oscillation.

5.3. 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 eMANETs that use CML. The o-phase can only be initiated by the Adaptive module as described in section 4.1. The basic operations of the current stable phase still apply in the o-phase. However, there are added processes to check for oscillation instances.

5.3.1. The Oscillation Problem

Oscillation occurs when nodes join and leave the network repeatedly so that the total number of nodes fluctuates exceeding and returning below the NST on a sequential basis. This causes performance degradation in CML due to frequent phase shifts. The level of oscillation is characterized by the number of nodes that oscillates and the frequency of oscillation.

5.3.2. Operation

The solution to the oscillation problem is twofold. 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, a node checks 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 actually exceeded, the o-phase 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 then shifts to the relevant stable phase of operation.

Furthermore, the o-phase is also responsible for phase shifting if a valid CP packet is received from a neighboring node. In such a case, it floods back the CP packet in the network. Figure 1 illustrates the different modules and phases of the CML protocol along with the interactions among them.

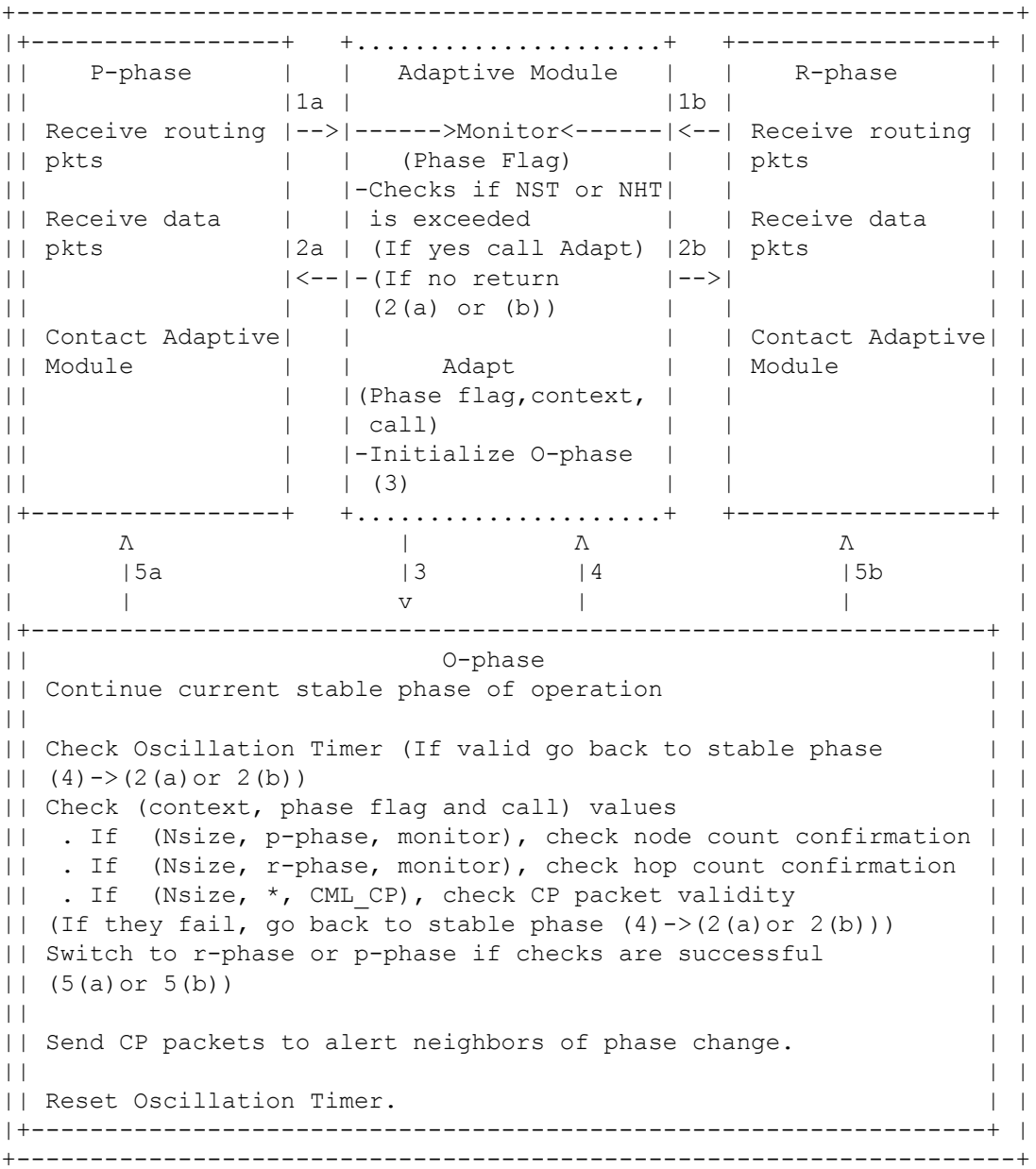
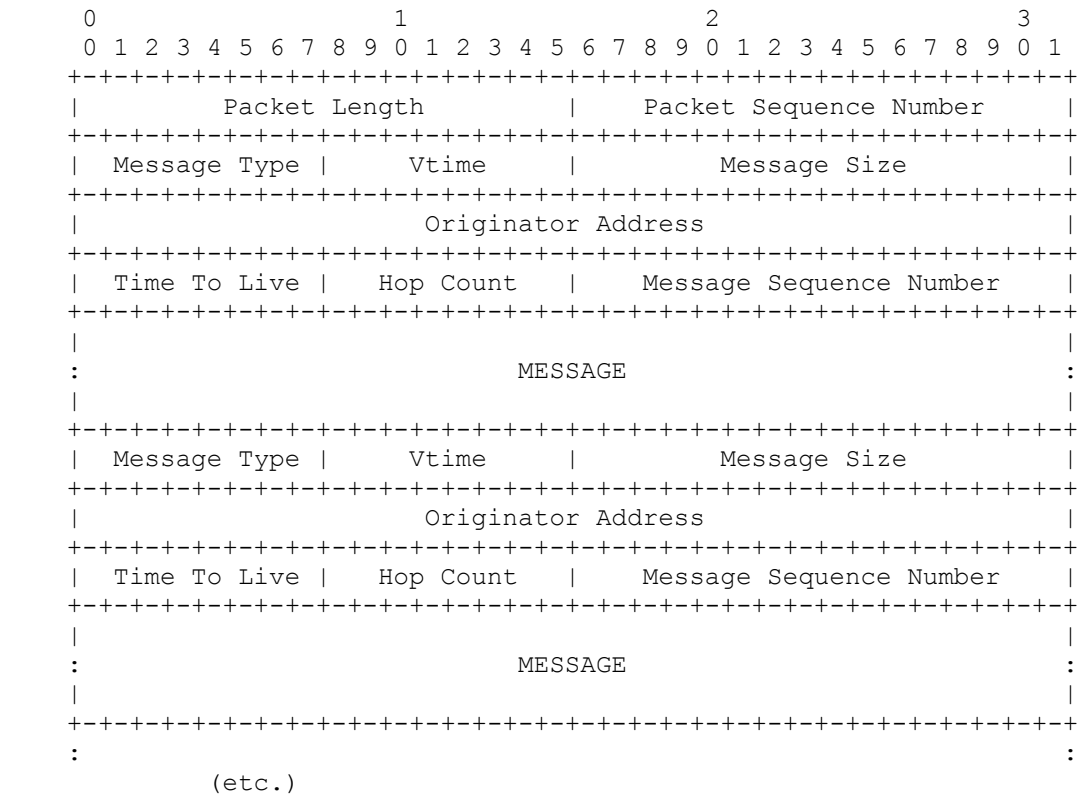


Figure 1 CML Protocol Overview.

6. CML Packet and Message Formats

6.1. Packet Format

The basic layout of a CML packet is as follows (IP and UDP headers are omitted):

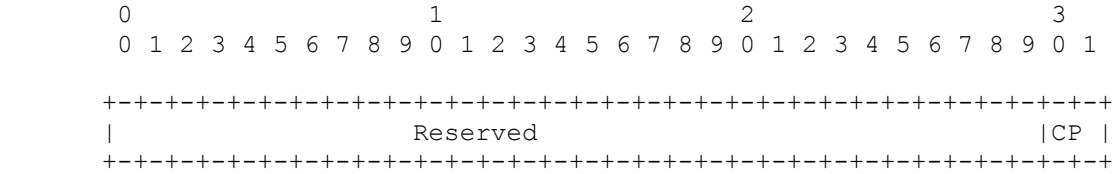


- Packet Length - The length of the CML packet in bytes.
- Packet Sequence Number - The Packet Sequence Number MUST be incremented by one each time a new CML packet is transmitted.
- Message Type - This field indicates the type of message found in the "MESSAGE" section. This could be a CML message or messages from [5] or [3].

The rest of the packet fields are defined in [5].

6.2. Change Phase (CP) Message

The Change Phase message format is shown below:



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

  01-"Rphase"

  10-"Pphase"

- Reserved - This field is filled with 0 and ignored at reception.

6.3. Hop Count Request (HCReq) Message

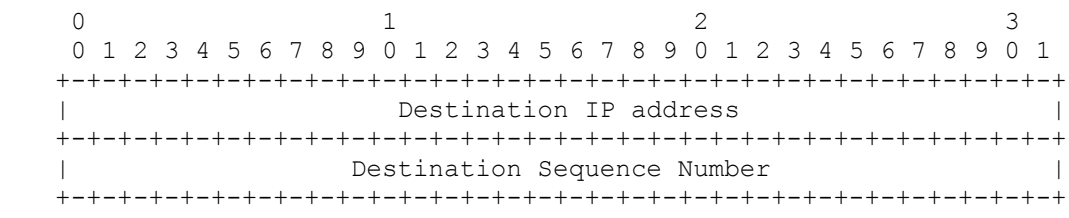
The HCReq message has an empty message body. It can be identified as a CML packet with:

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

- TTL – The TTL value is set to NHT.

6.4. Hop Count Request (HCRep) Message

The message format for the HCRep message is:



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

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

7. CML tables

7.1. CML Change Phase table

The CML CP Table fields are listed below:

- Originator IP Address - The IP address of the node which generated the packet.
- 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.
- Message Type - The message type value of the message through which the table row was populated.

8. 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 CML are described below:

- 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 and efficient compared to a reactive routing approach. Below the NST point, proactive routing approaches outperform reactive routing approaches.
- 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”.

- 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”.

- 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. Parameter Values

Parameter values used by the CML protocol and also defined in [3] and [5] are:

Parameter Name	Value
NET_DIAMETER	35
NET_TRAVERSAL_TIME	2 * NODE_TRAVERSAL_TIME * NET_DIAMETER
NODE_TRAVERSAL_TIME	40 milliseconds
PATH_DISCOVERY_TIME	2 * NET_TRAVERSAL_TIME

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 CML packets and messages need to be replaced by IPv6 addresses. The packet and message sizes will also increase accordingly.

12. Security Considerations

CML does not specify any special security countermeasures. Although, different secure versions of AODV and OLSR have been proposed in the literature [11], CML introduces new vulnerabilities. Firstly, any malicious node can generate a change phase packet to call the o-phase of CML and the routing behaviors will accordingly change. In this way, CML will not operate in the proper routing mode and the MANET's performance will not be optimal considering the real number of nodes in the network. Apart from that, legitimate nodes will flood the network with the CML CP packet generating traffic overhead within the MANET. Furthermore, a set of malicious nodes that coordinate their actions against the CML may periodically come into and depart from the network. In this way, CML recognizes that the number of nodes in the MANET has changed and oscillates from the proactive phase to the reactive or vice-versa. The continuous oscillation of CML can result in draining the battery level of the emergency devices rapidly. Another version of the above attack is launched when malicious nodes change the "hop value" in the CML HCReq Packet. In this case, legitimate nodes believe that the size of the network has changed and CML oscillates unreasonably. On the other hand, if a phase shift should take place (due to a real change of the number of nodes) but malicious nodes succeed to drop some or all of the Change Phase packets the performance of MANET will not be optimized. Therefore, security intelligent approaches have to be integrated into CML to avoid the aforementioned attacks and to provide eMANET nodes with basic security requirements such as confidentiality, authentication, integrity and availability.

13. IANA Considerations

The IANA consideration section is required as recommended by [7] and [9]. The following values for the corresponding message types would be required:

Message Type	Value
HELLO_MESSAGE	= 1
TC_MESSAGE	= 2
MID_MESSAGE	= 3
HNA_MESSAGE	= 4
ROUTE REQUEST (RREQ)	= 5
ROUTE REPLY (RREP)	= 6
ROUTE ERROR (RERR)	= 7
ROUTE-REPLY ACK (RREP-ACK)	= 8
HOP COUNT REQUEST (HCREQ)	= 9
HOP COUNT REPLY (HCREP)	= 10
CHANGE PHASE (CP)	= 11

14. Conclusions

This I-D introduced the CML routing protocol. In extreme emergency situations, rescuers tend to join and/or leave the network frequently, thus changing network size. CML is a hybrid protocol which combines the functionalities of OLSR and AODV protocols in an adaptive manner. The motivation behind CML is the enhancement of the overall routing performance for varying size networks. The main features of CML include the Adaptive Module, which monitors and adapts to the changing network state, and the o-phase which

considers the case of node oscillation. Future CML versions will augment the Adaptive module and make CML adaptive to additional MANET contexts.

Furthermore, more security aspects of CML will be discussed towards the provision of security against adversaries that try to launch different types of network layer attacks.

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, February 2008.

[3] Perkins, C., Belding-Royer, E., and Das S., "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, July 2003.

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

[5] Clausen, T. and P. Jacquet, "The Optimized Link State Routing Protocol", RFC 3626, October 2003.

15.2. Informative References

[6] PEACE team, "First draft of the emergency framework" PEACE, ICT-SEC-2007.1.7, Deliverable 2.2 (Public), June 2009.

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

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

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

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

[11] Anjum, F. and Mouchtaris, P. "Security for Wireless Ad Hoc Networks", ISBN: 978-0-471-75688-0, John Wiley & Sons, March 2007.

16. Acknowledgments

The authors wish to acknowledge the support of the ICT European 7th Framework Program and all the partners in PEACE (IP-based Emergency Applications and services for next generation networks) project with contract number 225654.

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:

Tipu Arvind Ramrekha
Researcher, WMN Research Group
Kingston University London
UK KT1 2EE

Phone: (+44) 02084177025
Email: a.ramrekha@kingston.ac.uk

Emmanouil A. Panaousis
Researcher, WMN Research Group
Kingston University London
UK KT1 2EE

Phone: (+44) 02084177025
Email: e.panaousis@kingston.ac.uk

Grant P. Millar
Researcher, WMN Research Group
Kingston University London
UK KT1 2EE

Phone: (+44) 02084177025
Email: g.millar@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