IETF MANET Working Group
Internet-Draft
Expires: Jan 3, 2013
Intended status: Information

A. Baryun
UoG

July 2, 2012

# Terminology in Mobile Ad hoc Networks
draft-baryun-manet-terminology-00.txt

Abstract

This document defines Mobile Ad hoc NETwork (MANET) terminology for discussing routing requirements, solutions, and protocols of networking referred to as mobile, multihop, wireless networking.

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 http://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 January 3, 2013.

## 1. Introduction

This document presents definitions for many ad hoc networks terms to be used during discussions of various algorithms for enabling ad hoc networks of mobile computers, particularly over wireless media. Having the Internet community agree on definitions, it will be expected that protocol users and designers will be able to discuss more clearly protocols' applicability, advantages and disadvantages. Mobile Ad hoc NETworks (MANETs) are infrastructure-less networks that may use with many technologies. The MANET characteristics, applicability and use cases are described in [RFC2501].

## 2. The Terminology

**The purpose of this document is to define MANET terms and to** distinguish differences in definitions by routing protocols terms used. Security routing terminology related to MANET will be defined in a separate section.

### 2.1 Requirement Level Language

This document uses capitalized words defined in [RFC2119] to signify requirements. In this document these words are printed in small if not related to requirement level language. The document uses some defined terms from other RFCs which will be noted with each used term.

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 the RFC 2119.

### 2.2 Abbreviations Used in This Document

AH Authentication Header
ATM Asynchronous Transfer Mode
DAD Duplicate Address Detection
DPD Duplicate Packet Detection
DoS Denial of Service
ESP Encapsulating Security Payload
IP IPv4 or IPv6
ICMP Internet Control Message Protocol
IIB Interface Information Base
ETX Estimated Expected number of Transmission

FIB  Forwarding Information Base

LQI Link Quality Indicator
L2 Data Link Layer (i.e. 2nd layer in ISO model)
L3 Internet Layer (i.e. 3rd layer in ISO model)
LLN Low power and Lossy Network
MAC Medium Access Control
MIB Management Information Base
MTU Maximum Transmission Unit
NBMA Non-Broadcast Multi-Access link
NHDP Neighborhood Discovery Protocol
ND IP Neighbor Discovery
OSPF Open Shortest Path First
RIB Routing Information Base
SMF Simplified Multicast Forwarding
TCP Transmission Control Protocol
UDP User Datagram Protocol

## 2.3 Definitions for MANET Terms

### 2.3.1 Terms Definition of MANET Communication:

Communications' Technology or Facility:
The means employed by two or more devices/subsystems to transfer and/or receive information between them in one way or two way communication. MANET communications often uses the wireless transmission medium(s) and MAY use some wired mediums (e.g. free space, air, water, antenna, coaxial cables, etc.)

Communication Medium:
The transceiver system (e.g. such as L2 systems, IEEE802.11 systems, satellite system, etc.) that the routing device uses to communicates through the transmission medium(s), by providing connectionless and/or connection services that MAY be established. The system medium includes MAC layer and MAY include the physical Layer.

Communication Channel:
A subdivision of the physical communication medium (i.e. radio carrier signal bandwidth, or the system bandwidth) allowing possibly shared independent uses of the medium. Channels may be made available by subdividing the medium into; distinct time slots, distinct spectral bands, or coding sequence, etc.

MANET Protocol:
The communication system/subsystem that operates and maintains the ad hoc communication technology or facility within MANET. MANET routing Protocols often apply distributed algorithms/techniques to disseminate or forward routing messages within a MANET routing domain.

Topology:
An abstract representation of a network (physical or logical), as a graph (G) whose topology is defined by a set of routers/bridges (V) that communicate through set of links (E), where the G =(V, E).

Physical-level Topology:
A topology of the communication medium networks consists of routing devices and physical links. This topology information is updated by devices' technology in the L2 information Base.

Network-level Topology:
A topology of the communication system networks consists of routers and links. This topology information is updated by routers in its RIB.

Multihop MANET:
A MANET that its node(s) MAY need(s) more than one IP hop to reach the destination.

Reactive Routing:
An on-demand based routing protocol that operates route discover and maintenance the route(s), to reach the demanded destination(s).

Proactive Routing:
A topology RIB based routing protocol that operates routes and maintains the network topology, to reach its known destination(s). Each router maintains routes to all reachable destinations at all times, whether or not there is currently any demand to deliver packets to those destinations.

Upper Layer:
a protocol layer above IP layer (e.g. as TCP, UDP, OSPF).

MANET Domain: TBD

MANET Signaling:
Sending and exchanging some MANET messages/information.

### 2.3.2 Terms Definition of MANET Elements

Node:
A device/subsystem that MUST implement IP and SHOULD participate in MANET signaling. It either runs a MANET routing protocol or participate in MANET signaling.

Router:
A MANET node that MUST implement a MANET routing protocol and forwards IP packets not explicitly addressed to itself.

Host:
A node that is not a router. All destinations in MANET that receive delivered data are hosts.

Link:
A link between two node interfaces. This link may be Logical (i.e. virtual) link or physical link. Logical links are between two logical interfaces and physical links are between two physical interfaces. Links are either unidirectional or bidirectional (links may be on-link and off-link: see RFC4861).

Physical Link:
a communication facility or medium over which the nodes can communicate at the link layer, i.e., the layer immediately below IP. Physical interfaces are the nodes' attachment to physical links. Physical Link types are point-to-point, NBMA, multicast capable, and shared-media, etc (see link types in ND [RFC4861]).

Logical (virtual) Link:
a communication facility (at L3, or upper-layer) over which nodes can communicate. This logical link is between two MANET interfaces exists if either can be heard by the other.

Link MTU:
the maximum transmission unit (i.e. maximum unit size in octets), that can be conveyed in one transmission unit over the link.

Node Interface:
A node's point of attachment to a link. Each node MUST have at least one interface that SHOULD be assigned an IP address. If there is/are more than one interface(s) per node then the additional interface(s) MAY be assigned an IP address. If an interface is not assigned to an IP address it MUST be identified by the MANET routing protocol. An interface MAY be assigned one or more addresses.

MANET Interface:
A node interface that participate in; exchange MANET information used in MANET routing or exchange information in MANET neighbor node discovery (e.g as the term used in RFC6130). A MANET interface MUST be assigned to least one routable address to communicate. One router interface MUST be assigned to the router's main address.

### 2.3.3 Terms Definition of MANET Identifications:

An interface MAY be assigned one or more addresses. If the interface is a logical interface it MAY be assigned to only logical addresses, but if it is a physical interface MAY be assigned with physical address (e.g. MAC address) and/or logical address(es) (e.g. IP addresses, MANET addresses).

MANET Address
A MANET-subnet, node, or interface address. Node and interface addresses are either IP addresses or RFC5444 addresses. All subnet addresses are unicast IP addresses.

Address Block and TLV: as specified in RFC5444

Routable address:
A subnet address which can be a destination address. A router MUST be able to distinguish a routable address from a non-routable address. Broadcast, and multicast addresses, limited in scope to less than the entire MANET, MUST NOT be considered as routable addresses. Anycast addresses MAY be considered as routable addresses.

Main address:
A routable address (MANET address) that is assigned to one router's MANET interface.

Originator address:
A node address of the node that originated a MANET message (this message MUST include the originator address). It MAY be a routable or an unroutable address.

subnet prefix
A bit string that consists of some number of initial bits of an IP address.

Interface identifier
the remaining low-order bits in the node's IP address after the subnet prefix. A number used to identify a node's interface on a link.

### 2.3.4 Terms Definition of MANET exchange information formats:

Packet:
A MANET packet of a header plus payload. These packets are either IP packets or RFC5444 packets. RFC5444 packet MUST be encapsulated in IP packet. Packets are generated by nodes to be sent to destination(s) through MANET or through the Internet. RFC5444 packets information MAY not be used only by MANET routers.

Message:
A header and payload which is either a MANET data message or routing protocol message. Routing control messages are either MANET routing protocol messages or/and RFC5444 messages.

Type Length Value coding (TLV):
A generic way to represent MANET information (as in [RFC5444] and [RFC5497]).

Frame:
A L2 protocol TLV with a header and payload. In some technologies the L2 operates a MANET routing protocol as a local area networking system. Frames MAY encapsulate MANET packets to be tunneled through a telecommunication network.

Route Request Message (RREQ)
A message is used to discover a valid route to a particular destination address, called the RREQ Target Node. When a router processes a RREQ it learns routing information on how to Originator Node.

Route Reply Message (RREP)
A message is used to disseminate routing information about the RREP Target Node to the RREQ Originator Node and the intermediate routers.

Route Error Message (RERR)
A message is used to disseminate the information that a route is not available for one or more particular addresses. A RERR message is used to indicate that a router does not have a forwarding route to one or more particular addresses.

### 2.3.5 Terms Definition Related to MANET Protocol Operation:

Hop-by-hop Routing: (TBD)
A dynamic routing that routes to destination by routing table.

Source Routing: (TBD)
A dynamic routing that its route path is provided in the IP packet.

Route Discovery: TBD

Route Maintenance: TBD

Neighbor discovery: (TBD)
A node discovers neighbors only if the node receives from it's neighbors.

Multipoint relay (MPR): (TBD)
A router X1 is an MPR for a router Y1, if router Y1 has indicated its selection of router X1 as an MPR in a recent HELLO message. Router X1 may be a flooding MPR for Y1 if it is indicated to participate in the flooding process of messages received from router Y1, or it may be a routing MPR for Y1, if it is indicated to declare link-state information for the link from X1 to Y1. It may also be both at the same time.

MPR selector:
A router, Y, is a flooding/routing MPR selector of router X if router Y has selected router X as a flooding/routing MPR.

Router Parameters:
boolean or numerical values, specified for each router, and not specific to an interface. A router MAY change router parameter values at any time, subject to some MANET constraints.

MANET Routing Metric:
A MANET routing cost that is governed by specific rules and properties defined by the MANET routing protocol which captures specific link or node characteristics. Examples of basic metrics are hop-count, ETX, LQI, etc.

Distance Vector Metric
A metric class related to rules of the MANET interface and MANET path distance. The metric can be calculated by the distance vector routing algorithm class used by the MANET routing protocol. A metric of the distance a message or piece of information has traversed. The minimum value of distance is the number of IP hops traversed.

Link State Metric
A metric type related to the MANET network-topology status and logical links' states. This metric is calculated by the link state routing algorithm class used by the MANET routing protocol. A metric type maybe EXT, LQL, etc.

Link Metric: TBD

Neighbor Metric: TBD

Path accumulated:
The RREQ message accumulates intermediate routers that are in path to destination(s).

Protocol Sequence Number:
A Sequence Number related to a MANET protocol that maintained by each protocol subsystem process. This sequence number is used by other subsystems to identify the temporal order of protocol information

generated.

Router Sequence Number:
A router sequence number is maintained by each router process. The sequence number is used by other routers to identify the temporal order of routing information generated and ensure loop-free routes.

MANET Information Base:
A collection of information (in Table or Cache structure) maintained by MANET protocols and which is to be made available to MANET routing protocols. An Information Base may be associated with a MANET router or with MANET interface (e.g. route request table, IIB, RIB, FIB, MIB).

RIB Entry:
The RIB entry is a conceptual data structure. Implementations may use any internal representation that conforms to the semantics of a route as specified in the router specification.

## 3. IP Considerations and Terminology

All MANET nodes MUST implement IP and all MANET routers MUST run/implement at least one MANET routing protocol. The terminologies described in this document can be used for IPv4-MANET and IPv6-MANET. The IPv4 addresses MAY be used in IPv6 packets but IPv6 addresses MUST not be in IPv4 packets.

IP address:
IPv4 addresses or IPv6 addresses.

IP Packet:
The packet header plus payload as specified in [RFC791] and [RFC2460] for IPv4 and IPv6 respectively. It can encapsulate RFC5444 packets as specified by RFC5498.

Mobile IP considerations:
Mobile IP terms are provided in [RFC6275], and this technology assists nodes while connected through the Internet domain(s). MANET is an infrastructure-less network that is able to communicate with the Internet (i.e. an IP infrastructure network).

## 4. Security Consideration and Terminology

It is RECOMMENDED that MANET routing protocols consider security issues because the MANET's transmission medium is wireless which make it vulnerable to attacks [ANJUM][RFC4593]. In some situations the routing information while traversing the MANET MAY be used by an intruder node, to obtain MANET data traffic or/and attack the MANET [HERBERG]. Forwarding protocols that use DPD techniques MAY be vulnerable to DoS attacks such as [RFC6621]. MANETs MAY be secured by using IPsec, AH, DAD, and ESP techniques, and other. However, it is RECOMMENDED that MANET detects attackers and possible threats.

The following are some terminology related to MANET threats and security.

Attacker: A node, present in the network and which intentionally seeks to compromise information based in MANET router(s). The Attacker MAY be a compromised MANET router if obtained MANET identity or routing information.

Compromised MANET Router: An attacker router, present in MANET and which generates syntactically correct routing control messages. Control messages emitted by compromised router(s) may contain additional information, or omit information, as compared to a control message generated by a non-compromised router located in the same MANET topological position.

Legitimate MANET Router: A MANET router, which is not a Compromised MANET Router.

Jamming Attack:
The attacker transmits massive amounts of interfering radio traffic, which will prevent legitimate traffic (e.g., routing and data traffic) on all or part of the MANET. Indirect jamming attacks MAY occur by influencing Legitimate MANET Router to transmit unnecessary information.

Eavesdropping:
Obtaining a copy by the attacker of the transmitted MANET routing information or the transmitted data information from its neighbor's transmitted radio packet. Attacker's processes MANY be used by attacker to mislead routing. Eavesdropping does not pose a direct threat to the MANET or to its routing.

Identity Spoofing:
Attacker sends routing messages, pretending to have the MANET identity of another node.

Link Spoofing:
Compromised MANET router sends routing messages to neighbor node(s) providing incorrect set of link information.

Replay Attack:
A Compromised router in one MANET region records control traffic information and replays the recorded information in a different MANET region (this type of attack is also called the Wormhole attack).

Broadcast Storm:
Compromised MANET router may attack the MANET by attempting to change the MANET flooding algorithm(s) to increase routing overheads or/and to increase the route discovery delay. Broadcast storm degrades the data

traffic delivery and MANET performance.

Falsification in MANET:
The compromised MANET router sends false routing information into MANET. False routing information received in MANET, MAY create unrealistic information bases.

ICMP Attacks:
The generation of ICMPv6 error messages may be used by compromised MANET router to attempt DoS attacks by sending an error-causing source routing header in back-to-back datagrams. As the ICMP messages are passed to the upper-layer processes, it is possible to perform attacks on the upper layer protocols (e.g., UDP, TCP). Protocols at the upper layers are RECOMMENDED to perform some form of validation to ICMP messages (using the information contained in the payload of the ICMP message) before acting upon them.

Source Routing Attacks: TBD

## 5. IANA Considerations

This document has no request to IANA.

## 6. Acknowledgments

This work has used/modified terms of the following documents: RFC2462, RFC2501, RFC3561, RFC3626, RFC3753, RFC4728, RFC4861, RFC5444, RFC6130, RFC6621, [AODVv2], [OLSRv2], and [HERBERG], thanking all authors. The author would like to thank who inspired to take over the work from their discussions as; Charlie Perkins, Christopher Dearlover, and Teco Bo. The author would like to gratefully acknowledge to the MANET WG for all contributions.

## 7. References

### 7.1. Normative References

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

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[RFC2501] Macker, J. and S. Corson, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", RFC 2501, January 1999.

[RFC3561] Perkins, C., Belding-Royer, E., and Das S., "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, July 2003.

[RFC3626] Clausen, T. and P. Jacquet, "The Optimized Link State Routing Protocol", RFC 3626, October 2003.

[RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

[RFC5095] Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, December 2007.

[RFC5444] Clausen, T., Dean, J., Dearlove, C., and Adjih, C. "Generalized MANET Packet/Message Format", RFC 5444, February 2009.

[RFC5497] Clausen, T. and C. Dearlove, "Representing multi-value time in MANETs", RFC 5497, March 2009.

[RFC6554] Hui, J., Vasseur, JP., Culler, D., and V. Manral, "An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6554, March 2012.

[RFC4593] Barbir, A., Murphy, S., and Yang, Y., "Generic Threats to Routing Protocols", Oct, 2006.

[RFC5498] Chakeres, I., "IANA Allocations for MANET Protocols", RFC 5498, March 2009.

[HERBERG] Herberg, U., Yi, J., Clausen, T.,"Security Threats for NHDP", Work in progress, March, 2012.

## 7.2.Informative References

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

## Author Address

Abdussalam Nuri Baryun
University of Glamorgan (UoG)
Treforest, CF37 1DL, UK
Email: abdussalambaryun@gmail.com