New Capabilities in Security and QoS Using the Updated MANET Routing Protocol OLSRv2

Christopher Dearlove
BAE Systems Advanced Technology Centre,
West Hanningfield Road, Great Baddow,
Chelmsford, CM2 8HN, UK.

chris.dearlove@baesystems.com

ABSTRACT

Mobile ad hoc networks (MANETs) are a good fit to a number of military and public safety scenarios in which security and quality of service (QoS) are important. Optimised Link State Routing (OLSR) is a widely used proactive ad hoc routing protocol; a successor version 2 (OLSRv2) is being developed as a Standards Track protocol by the Internet Engineering Task Force (IETF). Improvements in OLSRv2 are detailed and matched to specific weaknesses of OLSRv1. How two of these improvements, a flexible packet/message format and the use of link metrics, enable improvements in security and quality of service in an OLSRv2-based MANET is described.

1.0 INTRODUCTION

Mobile ad hoc networks (MANETs) are self-organising, self-healing, networks in which wireless devices overcome range and other propagation issues by cooperating to relay information, typically IP (Internet Protocol) packets, from the source to the destination when they are out of direct contact.

MANETs are a good fit to a number of military, and public safety, scenarios, where the issues are of rapid deployment and maintaining connectivity even in difficult environments. Examples include:

- Soldiers on deployment, both in vehicles and dismounted.
- Extended range operation of UAVs (Unmanned Aerial Vehicles) and use of UAVs and other aerial platforms as communications relays.
- Use to provide communications coverage of aircraft hangars and flight decks.
- Emergency services deployed into unknown and complex radio propagation environments such as underground railway stations and tunnels.
- Sensor networks, and dual-purpose sensor and communications networks.

In such scenarios, two issues are of particular importance: security and quality of service (QoS). Specific features of each of these are addressed: for security the integrity of the cooperative routing and the confidentiality of information in the network, and for QoS routing using the most appropriate links, not just the fewest links, by taking account of relevant link properties (e.g. bandwidth or latency as required).

The Optimised Link State Routing (OLSR) is the most widely used proactive ad hoc routing protocol (AHRP). It is specified in [1], an Experimental RFC, developed by the MANET WG of the Internet Engineering Task Force (IETF).

The MANET WG is now developing version 2 of OLSR (OLSRv2) as a Standards Track Internet protocol, building on the success of OLSRv1 while improving on it. OLSRv2 can be used to create networks over a wide range of bearers, creating a single ad hoc network, which can be over a

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **SEP 2010**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **New Capabilities in Security and QoS Using the Updated MANET Routing Protocol OLSRv2**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **BAE Systems Advanced Technology Centre, West Hanningfield Road, Great Baddow, Chelmsford, CM2 8HN, UK.**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

See also ADA568727. Military Communications and Networks (Communications et reseaux militaires). RTO-MP-IST-092

14. ABSTRACT

Mobile ad hoc networks (MANETs) are a good fit to a number of military and public safety scenarios in which security and quality of service (QoS) are important. Optimised Link State Routing (OLSR) is a widely used proactive ad hoc routing protocol; a successor version 2 (OLSRv2) is being developed as a Standards Track protocol by the Internet Engineering Task Force (IETF). Improvements in OLSRv2 are detailed and matched to specific weaknesses of OLSRv1. How two of these improvements, a flexible packet/message format and the use of link metrics, enable improvements in security and quality of service in an OLSRv2-based MANET is described.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT **SAR**	18. NUMBER OF PAGES **25**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

heterogeneous mixture of wireless, and wired, bearers. As an IETF standard, it will be possible to create interworking networks with mixed vendor products, avoiding supplier lock-in.

OLSRv2 is currently specified by the RFCs and Internet Drafts [2] to [6], with some additional material to be incorporated described in a further Internet Draft [7]. The relationships between these components are described below, but in particular they include a packet/message format specification [2] and a NeighbourHood Discovery Protocol (NHDP) [3].

Section 2 of this paper contains a summary of key aspects of the design rationale for OLSRv2. The rationale starts with a summary of what is now considered version 1 of OLSR (OLSRv1), its features and problems, and how OLSRv2 improves on OLSRv1. Section 3 of this paper then discusses the new capabilities available to an ad hoc network when using OLSRv2 rather than OLSRv1, with particular reference to security and QoS.

2.0 OLSRV1 AND OLSRV2

2.1 Key Features of OLSRv1

The key features of OLSRv1, as defined by [1], are:

- It is a proactive routing protocol for use in mobile ad hoc networks, enabling decentralised, cooperative, multi-hop routing in what is typically a wireless network.
- It is intended for routing in IP networks, using control messages sent using UDP (User Datagram Protocol). It can be used with either IPv4 or IPv6 addresses.
- It is a link state protocol, in which link state information, determined locally by each router and its neighbours by an exchange of HELLO messages, is propagated through the network, so that all routers maintain routes to all other routers. Information on usable bidirectional links is propagated non-locally in Topology Control (TC) messages.
- Each router elects a subset of its one hop neighbours, which “cover” the router’s two hop neighbourhood, as MultiPoint Relays (MPRs). This two hop neighbourhood is determined directly from the one hop neighbourhood information in HELLO messages.
- MPRs are used to optimise the control message overhead. First they allow a reduction in the link state information that is required by routers, thus allowing a reduction in both the size and number of TC messages. Second they allow an optimised flooding of messages, including TC messages.
- The reduced link state information available to each router still allows minimum hop paths to be constructed to all destinations.
- A router can have multiple interfaces, each assumed to have a single, unique, address. Multiple interface information has to be flooded through the network using Multiple Interface Declaration (MID) messages.
- A router can advertise that it is a gateway to a network, which may be either hosted on the same device or externally attached. This information is included in a Host and Network Association (HNA) message, which is also flooded through the network.
- The protocol is extensible by the addition of new messages. New message types can be specified and may be flooded using MPRs in the same way that TC, MID and HNA messages are.

- Flooding may be range limited (number of hops). This allows, in principle, the use of techniques to reduce control traffic, such as variable range flooding, as used by Fisheye State Routing (FSR) [8] and Hazy Sighted Link State (HSLS) routing [9].
- Each router may be independently parameterised with regard to message intervals and other protocol parameters.

2.2 Limitations of OLSRv1

However there are some limitations of OLSRv1:

(a) **Message formats are fixed.** It is not possible to, for example, add information directly to a HELLO message to represent some other information about neighbours.

(b) **Routing is only by minimum hop paths.** It is not possible to, for example, prefer a path consisting of three good links over one consisting of two poor links. An optional link quality process may allow a local decision not to allow a poor link to be used at all, but this is a much more limited feature.

(c) **No advantage is taken of commonalities in the addresses used.** These happen when addresses belonging to the same subnet are used. In addition, IPv4 subnets are reported in HNA messages using a 32 bit address mask, rather than using a more efficient prefix length, and reporting of IPv6 subnets is not well specified.

(d) **The addressing model may be inappropriate.** This model is of a single, unique, address per interface. However a router may (especially using IPv6) want to configure more than one address on an interface. Alternatively a router may wish to use the same address on more than one interface, where this can be made to work.

(e) **A router with multiple interfaces must send MID messages that flood the complete network.** This is inefficient, even with OLSR's optimised flooding. Single interface routers do not need to send flooded messages unless selected as an MPR, but multiple interface routers must send messages that are flooded through the network. If multiple addresses were allowed on an interface then even routers with a single interface, but with more than one address, would need to flood messages. The use of HNA messages to advertise locally hosted networks also requires additional flooded messages.

(f) **External networks advertised using HNA messages have no associated hop count.** They are thus assumed to be at the same distance from any advertising router. An example of the possible use of such a hop count is described in [10].

(g) **HNA messages do not have the flexibility of TC messages.** The latter have a "cancellation" option whereby reception of a later TC message that does not contain that link immediately stops the use of that link by the receiving router. This includes the option of an empty TC message to cancel all links from the sending router. HNA messages do not have this cancellation capability, they rely on information "timing out".

(h) **The TC message cancellation process is slightly flawed.** As cancellation of all links by a router using an empty TC message is not recorded by a recipient router, a reordering of a TC message and a later empty TC message can result in incorrectly "resurrecting" a cancelled link.

(i) **Problems can also occur when using TC message fragmentation.** A single fragment cancels all older link information, even if that information is to be retained, but is reported in a separate fragment. At best this could result in a "glitch" between fragments, at worst a significant loss of connectivity, breaking the intent of the protocol to be robust against single message loss.

(j) **The implementation of Fisheye/HSLS in OLSRv1 is imperfect.** An OLSRv1 message has a single interval time, and a single validity time. However using the Fisheye/HSLS approach, messages are sent with different maximum ranges, which means that the apparent message interval is different at different ranges, and the required validity time should therefore also differ.

(k) **The protocol does not specify if and how parameters may be dynamic.** Whether a router should be allowed to change its parameters, and if it does how exactly message processing should accommodate this, is not described in [1]. Allowing a router to freely change parameters permits behaviour such as exponentially backing off message sending in static conditions.

(l) **A router is forced to have the same parameters for all interfaces.** Thus even if a router has, for example, a stable interface and an unstable interface, it must use a single HELLO message interval, and a single validity time for information in all HELLO messages.

(m) **HELLO and TC messages should be re-sent whenever the local neighbourhood changes.** There is no recommendation of a tradeoff between this and keeping the message sending rate bounded so as to manage message flow. This could be done by, for example, introducing a minimum message interval as well as the normal (maximum) message interval. This behaviour is compatible with OLSRv1, and has been used with it [11], but is not included in [1].

(n) **Features useful for other protocols are not made easily available.** Some of the features of OLSRv1, in particular its neighbourhood discovery, could be of value to other protocols. This is partly catered for in that OLSRv1 can be used to efficiently flood new messages. However that requires them to be formatted as OLSRv1 messages, and also does not allow other protocols to use information from OLSRv1.

2.3 New Features of OLSRv2

All of the limitations of OLSRv1 described in the previous section have inspired features of OLSRv2 that improve on OLSRv1. These improvements are summarised in the following points, each of which finishes with an indication of which of the limitations the improvement addresses. These improvements also do more than just improve on or remove the limitations.

- **A new, flexible, packet and message format has been defined.** It is sufficiently general that it has been separated from OLSRv2 into an additional specification, a Proposed Standard RFC [2]. As in OLSRv1, [2] allows multiple messages to be included in a single packet, which will typically form the body of a single UDP or IP datagram. Examples of the packet and message formats are shown in Figure 1:

-

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|0|0|0|1|1|Rsv|    Packet Sequence Number     |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+               |
|                                                               |
|                        Packet TLV Block                       |
|                                                               |
|                                +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                               |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
|                                                               |
|                            Message                            |
|                                                               |
|                                                +-+-+-+-+-+-+-+-+
|                                               |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+               |
|                                                               |
:                              ...                              :
|                                                               |
|                                +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                               |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
|                                                               |
|                            Message                            |
|                                                +-+-+-+-+-+-+-+-+
|                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Message Type  |1|1|1|1|  MAL  |          Message Size         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Originator Address                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Hop Limit   |   Hop Count   |    Message Sequence Number    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                       Message TLV Block                       |
|                                                +-+-+-+-+-+-+-+-+
|                                               |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+               |
|                                                               |
|                         Address Block                         |
|                                                               |
|               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               |                                               |
+-+-+-+-+-+-+-+-+                                               |
|                    Address Block TLV Block                    |
|                                                               |
|                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                               |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
|                                                               |
:                              ...                              :
|                                                               |
|                                                +-+-+-+-+-+-+-+-+
|                                               |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+               |
|                                                               |
|                         Address Block                         |
|                                                               |
|                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                               |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
|                                                               |
|                    Address Block TLV Block                    |
|                                                               |
|                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: Example packet and message formats

These messages do not have to all be OLSRv2 messages, they can be from any protocol built on [2], which defines a multi-protocol multiplexing approach with additional details in [12]. Specific non-OLSRv2 examples using this format are the IETF MANET protocols DYMO [13] and SMF [14]. Limitations addressed: (a).

- **The new message format permits efficient encoding of addresses.** A message can include multiple addresses in one or more address blocks, which each permit compression of common address initial and/or final octets. This is done purely based on common values, without consideration as to any structural meaning of the common octets, such as a subnet. Addresses can have a specified length, which while typically 4 octets (for IPv4) or 16 octets (for IPv6) may be of any number of octets from 1 to 16. The address block also allows the specification of a prefix length (subnet masks are not used) so that IPv6 addresses, in particular, can be significantly more efficient. Limitations addressed: (c).
- **The new packet and message format allows flexible addition of attributes.** These are encoded as TLVs (Type, Length, Value entities) applied to individual addresses or groups of addresses in a message, or to a message or a packet as a whole. This allows “internal extensibility” of a message, as new TLVs may be later defined and added to a message, but will be ignored by unextended instances of the protocol. A suggestion as to how to use a packet or message TLV for security purposes is described in an appendix to [2]. Limitations addressed: (a).
- **Four reusable components have been separately published.** This makes a total of five documents that define OLSRv2. [2] defines the packet/message format. [3] defines the NeighbourHood Discovery Protocol (NHDP), which contains the HELLO message driven part of OLSRv2, other than MPRs, through which a router identifies its one and two hop neighbours. [5] contains the definition of TLVs to include a hop count dependent time in a message. [6] describes the use of jitter, intentional random delays to avoid packet collisions, a codification and extension of the similar mechanism in OLSRv1. The overall specification of OLSRv2 is [4], which includes the other specifications by reference. These form five of the eight main IETF MANET WG documents that are based on [2], the others being [12] to [14]. Their relationships are shown in Figure 2:

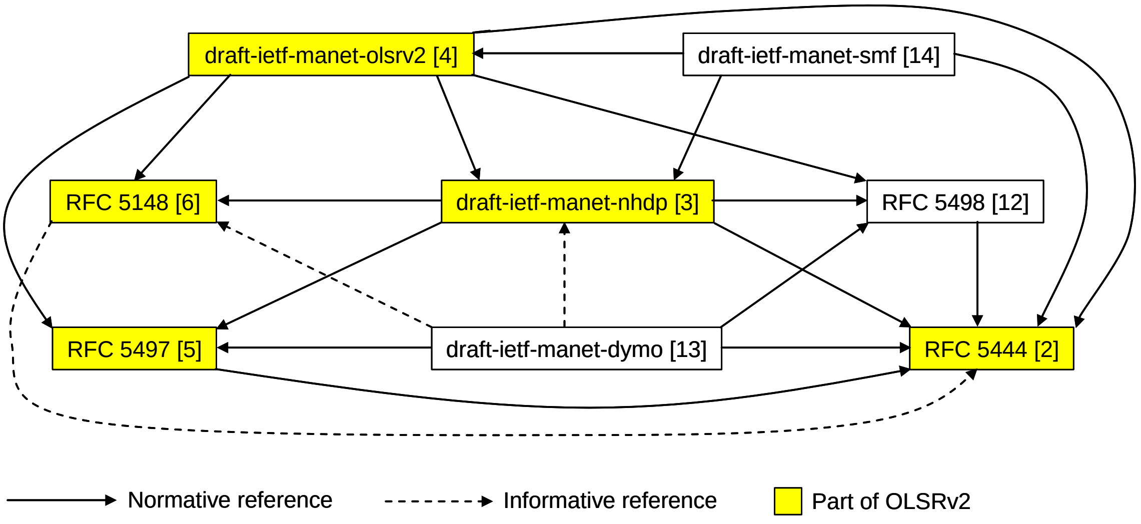

draft-ietf-manet-olsrv2 [4]
draft-ietf-manet-smf [14]
RFC 5148 [6]
draft-ietf-manet-nhdp [3]
RFC 5498 [12]
RFC 5497 [5]
draft-ietf-manet-dymo [13]
RFC 5444 [2]
Normative reference
Informative reference
Part of OLSRv2

Figure 2: IETF MANET WG documents and OLSRv2

Limitations addressed: (a).

- **A protocol can use NHDP and an alternative to MPRs.** An example is the use of a Connected Dominating Set (CDS) rather than MPRs for flooding; a protocol that includes the option to do so is the Simplified Multicast Forwarding (SMF) protocol [14]. This is in part possible because NHDP has been specified as not just including the non-MPR HELLO message part of OLSRv2, but also in making information available to, and extensible by, other protocols that use NHDP. Limitations addressed: (n).
- **All parameters are fully dynamic.** Parameters can be changed at any time, thus allowing, for example, backing off message intervals if the network appears to be static. Parameters are divided between interface parameters, which can be independently set on each participating interface, and router parameters, which have a single value for that router, but may be different on different routers. Limitations addressed: (k), (l).
- **Message flooding includes variable message hop limits.** This allows full implementation of the Fisheye/HSLS concept. The hop count dependent multiple time TLV included in [5] allows the correct implementation without the faults in OLSRv1. Limitations addressed: (j).
- **Routers have additional multiple address options.** NHDP allows multiple addresses per interface which may be individually specified, use an address plus an address prefix length specification, or use a combination of these. This has allowed the abolition of the MID message, and also allowed some locally hosted networks to be reported in HELLO messages rather than HNA messages. Limitations addressed: (d), (e).
- **A router is allowed to use the same address on more than one interface.** This is if, and only if, there is no interface on another router that can hear and/or be heard by interfaces with a common address. Limitations addressed: (d).
- **The HNA message has been removed.** Network addresses that were previously reported in HNA messages are now either reported as non-participating interface addresses in HELLO messages or reported, with an added hop count, in TC messages, possibly by more than one router. Limitations addressed: (f), (g).

- **TC messages are no longer fragmented.** Instead a TC message may be incomplete, allowing an addition, but not removal, of some link state information. The problems associated with TC fragmentation are solved because information is only added, and the problems with empty TC message reordering have also been resolved. Limitations addressed: (h), (i).
- **Minimum message sending intervals are specified.** This is done for each message type (HELLO and TC), allowing better management of control message flow, as a tradeoff with keeping information up to date. Limitations addressed: (m).
- **The use of link metrics will be included in OLSRv2.** An Internet Draft [7] indicating how to do so has been published, and it has been agreed to add such link metrics to OLSRv2, using the TLV mechanism. Limitations addressed: (b).

3.0 NEW CAPABILITIES USING OLSRV2

3.1 Security

3.1.1 Overview

A recommended security framework is presented in the packet and message format specification [2]. This assumes that packets are one hop constructs and messages whose contents are unchanged when forwarded. These conditions are satisfied by OLSRv2, and thus the security framework applies to OLSRv2, but also has a wider applicability. The framework addresses both the issues of network integrity, by the authentication of packets or messages, and confidentiality. These are discussed in the following sections. Issues of availability, where OLSRv2 offers similar capabilities to OLSRv2, are not considered here.

3.1.2 Integrity

A straightforward capability that is suggested, but not fully specified, in [2] is the addition of a TLV including a cryptographic signature that will allow the authentication of the received information. The objective is to ensure the integrity of the ad hoc network, that only authorised routers can join the network because unauthorised routers will have their HELLO and TC messages rejected. Some key points are:

- There are two possible entities to which such a signature TLV could be added, the packet, or the message. In either case the signature (in the TLV value field) will need to be calculated based on the packet or message without this TLV, and verified after removal of this TLV from a received packet or message.
- The simpler option is to use a packet TLV to sign an entire packet. Packets are, according to the intended usage of [2], a single-hop construct. Thus the process is simply one of adding a signature packet TLV as the last action before sending the packet, and on reception removing it and verifying the packet, discarding the packet if it has no such TLV, or the signature does not match.
- Use of message TLVs is more complicated. The intended usage of [2] is that messages may travel multiple hops, being forwarded unchanged other than the hop limit and/or hop count fields in the message header. Messages could be re-signed each hop, but in that case packet signatures do what is wanted more efficiently. Messages are thus appropriately signed at the message originator, verified by each receiver, and forwarded with the signature unchanged. The signature cannot cover any hop count or hop limit fields (they must be set to zero to calculate the signature).

- There needs to be a security association between the packet or message originator and each router that verifies the signature. For TC messages this may mean every other router in the network. This also needs to be based on some pre-configuration of all such routers, as otherwise an unauthorised device trying to infiltrate the network could do exactly the same as an authorised device. The simplest form of pre-configuration is to install a single shared secret in all authorised routers. A possibly better approach is discussed later in this section.

There are advantages of each of the packet and message signature approaches, both theoretical (what chains of trust are relied on) and practical. Comparing their overheads depends on the network size and density, and on how aggressively messages are aggregated into packets.

One advantage of OLSRv2, directly due to the flexible packet/message format [2] that it uses, is that each signature can be combined with the entity that it is signing, so that the two can be guaranteed to arrive together. This was not the case for OLSRv1, where a message's signature had to be in a separate message and there was no guarantee that the two could be kept together [15]. This was a motivating example in the development of [2] as part of OLSRv2, see [10].

As noted above, the security pre-configuration of the routers could be using a single shared secret. Ad hoc networks are however often deployed where they are vulnerable to capture of their routing devices. With a single shared secret, capture of one such device compromises all devices. An alternative is thus desirable. The alternative also should have the characteristics of not deploying an authority (for example a certificate authority) in the network, where it also would be vulnerable, and to make little impact on the characteristics that make an ad hoc network desirable, that of being a decentralised, minimally planned network.

A candidate for such an approach to authentication is using Identity Based Encryption (IBE). A use of IBE with OLSRv1 is described in [10]. As well as the change to OLSRv2, the specific details of the IBE described there can be improved on, but still having the following characteristics:

- There will be an IBE authority, which is maintained in a secure location, not part of the ad hoc network. Note that this authority could be, for example, simply a laptop computer.
- Each device, before being deployed in the ad hoc network, is configured by secure connection to the authority.
- Each device does not need to be informed of the identities, or even the existence of, other devices in the network. This also allows (provided the authority is maintained) devices to be added later to the network, without planning this addition.
- Compromise of a device only allows that device to be copied. This is where there is an advantage in message signatures, in that only an invalid neighbourhood around the compromised device can be forged.
- The simplest identity, and one that adds no identity overhead to packets or messages, is using the router's originator IP address as its identity.
- That identity can however be extended. A useful extension is that when configured by the authority a router is also allocated an expiry time, which is added to its identity (it needs to be reported in the signature TLV, or in an accompanying identity TLV). This means that a captured device's value is time-limited. However it also means that devices need to be re-connected to the authority before their expiry time. Devices also need a time source, but this can be of limited accuracy.

Of course no approach is perfect, and one limitation of this use of IBE is that the authority has complete information as to all routers' private information, unlike a conventional public key cryptography (PKC) scheme where users can choose their own private keys. However the IBE approach may be suitable for a military network where such issues are less significant.

Another issue is that IBE is computationally expensive. With moderate processing power it can be implemented in real time for real key lengths (an advance on [10]) at the expected frequency of OLSRv2 packets or messages in a moderate sized network. However it opens the possibility of a denial of service (DoS) attack by an adversary that can create many packets or messages with correctly formatted, but invalid, signatures that have to be verified. However, in most ad hoc networks, rapid message sending can be used to create a jamming effect, without needing to overload the signature verification.

3.1.3 Confidentiality

A side-effect of the IBE process discussed in the previous section is that a router can create a secret specific to, and shared with, each other router, even if it is aware of that other router only due to it being reported in a third router's TC messages. These shared secrets can be used as the basis on which to build a traffic confidentiality process. This can construct session keys for specific traffic flows, rather than use the shared secret key directly.

Confidentiality of the OLSRv2 signalling is however more difficult. While [2] discusses how to use encryption of packets or messages (essentially by replacing the whole packet or message by a single TLV whose value is the encrypted true packet or message) this relies on a security association between source and destination. OLSRv2 messages are however one to many, and except for a shared secret key (with its previously noted disadvantages) such a security association is difficult to set up. This is particularly so as authentication is required when the ad hoc network routing is not in place - the OLSRv2 messages that are to be encrypted are what sets up that routing. How to provide some measure of confidentiality of routing remains an open question. Routing signalling confidentiality is not essential, unlike routing signalling integrity and traffic confidentiality, but would prevent various forms of traffic analysis and leakage of other potentially useful information.

3.2 Quality of Service

The major improvement that will be added to OLSRv2 is the addition of link metrics. Link metrics are widely used in link state protocols, and have been used in non-standard extensions to OLSRv1.

Using link metrics, traffic can be sent using, for example, three good links rather than two poor links. OLSRv1, which relies on minimum hop routing, cannot do this, see Figure 3:

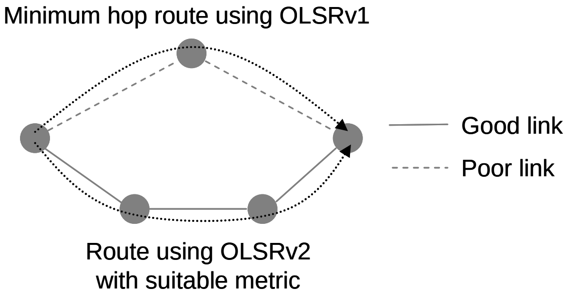


Figure 3: QoS routing using link metrics

OLSRv1 can force the use of the preferred route using its "link quality" mechanism, removing links that a router assesses as below a certain quality threshold. However this prevents their use at all, even if there is no alternative. This mechanism is retained in NHDP, both because NHDP may be used outside OLSRv2, and because the mechanism has some specific applications. In particular the link quality mechanism may be used when creating ad hoc networks over IEEE 802.11 due to the physical differences between unicast and local broadcast characteristics, see [16] for details.

In some cases, a significant gain can be easily realised using metrics. One such case is a ground-based ad hoc network with an aerial relay, possibly a UAV. Minimum hop routing will result in most traffic being sent on a two hop route via the UAV. This would overload that link, and significantly degrade the general quality of service of communications, in particular available throughput, and probably also latency. Instead use of links via the UAV should be reserved for cases where it offers a substantial gain, especially when it links two otherwise disconnected components of the network. This is easily accomplished by giving the links via the UAV a larger metric value, as shown in Figure 4:

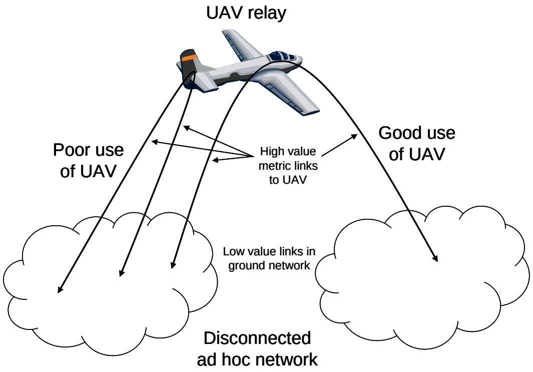

UAV relay
Poor use of UAV
High value metric links to UAV
Good use of UAV
Low value links in ground network
Disconnected ad hoc network

Figure 4: Metric use with UAV relay

More generally, how to allocate metrics to links is a difficult problem. Metrics can be based on physical characteristics of links such as delay or bandwidth, or can be more dynamic, taking into account network use. Metrics can also be more abstract, possibly allocated by some optimisation process, although decentralising that to run in an ad hoc network is not a simple process. A poor choice of metric allocation process can however make matters worse, and an over-dynamic process may fail to provide the stability that is needed for routing, as each metric change has a similar effect to network topology changes due to mobility.

Decisions on how to set metric values are outside the scope of OLSRv2, which will, as described in [7], just specify the nature of metrics (directional and additive), the necessary TLVs to report metrics, how to record metric information, and how to use it to find routes.

The TLV mechanism will however allow the specification of particular metric types, the routers in a network selecting which metric type they are using. A fairly straightforward extension to OLSRv2 could be created to allow a multi-topology routing fabric to be created, routing different types of packet differently, where a likely interpretation of packet type would be DiffServ Code Point (DSCP) [17].

Link metrics are the main mechanism added to OLSRv2 that can be used for quality of service purposes. OLSRv2 is of course compatible with various other QoS mechanisms that are however outside it, for example the use of various class-based and/or active packet queue management techniques. If considering such, then note that OLSRv2’s own packets are essential to the operation of the network, and while they are likely to be both delay and loss tolerant, both of these are only up to a point. They also are likely to be a low proportion of all packets, and thus safe and proper candidates for being assigned a high priority.

3.3 Other Capabilities

The consequences of some of the new capabilities added to OLSRv2 as noted in Section 2.3 above may need some additional explanation in order to see some of the possibilities that they add when using OLSRv2.

- The Fisheye/HSLS concept can be used to improve network scalability, and hence to increase the sizes of networks that can be deployed. This has been demonstrated for OLSRv1 in [18].
- Dynamic parameters can be controlled by an intelligent process that, for example, recognises that the local neighbourhood is stable and backs off sending periodic messages by increasing interval parameters, or recognises an increase in vehicle speed and reduces its interval parameters. Dynamic parameters also help improve the scalability of OLSRv2 by not requiring worst case fixed message intervals.
- Further flexibility in management of message sending is provided by the specification of minimum intervals (although these are, in effect, optional, as they may be set to zero). Their main function is to allow setting a longer periodic interval while still being able to be sure that updates are sent when needed more frequently (by enabling messages responding to neighbourhood changes) but ensuring that message overheads are kept under control (due to the minimum interval). By setting a very long periodic interval, the neighbourhood discovery protocol can even be made to perform as a reactive protocol.
- Per-interface parameters allow a router to operate efficiently even when it has interfaces with significantly different characteristics. An example is a router with an IEEE 802.11 interface and an Ethernet interface, the latter perhaps attaching to a similar router using a different wireless channel. A router need not send as frequent HELLO messages over the Ethernet link; it may suffice to send such messages only when it needs to report a change in its wireless neighbours.
- When a router has an Ethernet connection, it may not even be necessary to send an initial HELLO message to establish that link. NHDP, and hence OLSRv2, can handle this case because they permit a router to update the Information Bases maintained by NHDP/OLSRv2 directly. A router can use this freedom when other forms of cross-layer information are available. A complete freedom to update the Information Bases could however be dangerous, so both protocols specify constraints on what may be done to the Information Bases; if these are viewed in an object-oriented manner then the constraints are the class invariants. They include rules such as that if a router has a recorded neighbour (a Neighbour Tuple) then it must have at least one matching recorded link (a Link Tuple).

In all of these cases, OLSRv2 provides the capability, but how to get best value from the capability, and what extra intelligence to use, is up to the implementer or user. An important feature in all of these cases is that routers can fully interwork even when using different combinations of these capabilities, or none of them.

While they should interwork, not all OLSRv2 implementations will be equal. In order to allow the creation of more efficient messages, [2] contains various options for inclusion of data, in particular how to use TLVs. An implementation can, for example, use a simple heuristic that produces reasonable efficiency messages (usually more efficient than for OLSRv1 when using addresses that compress) or a more complicated analysis that produces the most efficient possible messages.

Another area where implementations can make a significant difference is in intelligent combination of the use of jittering [6] with the construction of multi-message packets, where as long as packets do not become too large, there are, for most systems, significant advantages in sending messages in as few packets as possible, saving repeated headers and other overheads from the packet/message format [2], and from UDP, IP, MAC and the physical layer.

4.0 CONCLUSIONS

This paper has described version 2 of the Optimised Link State Routing protocol (OLSRv2), the Standards Track successor to the widely-used proactive MANET routing protocol OLSR (now OLSRv1), and how features in OLSRv2 have been designed to improve on OLSRv1. In particular it has been noted how the flexible packet/message format designed for OLSRv2, but also used by other IETF MANET protocols, enables improved security functionality, and how the addition of link metrics to OLSRv2 allows better routing decisions, that can be used to improve the quality of service (QoS) in a OLSRv2-based MANET. These are both capabilities particularly required by military and public safety uses of MANETs.

5.0 ACKNOWLEDGEMENTS

The author thanks his co-authors of the components [2] to [7] of OLSRv2, especially Thomas Clausen (Ecole Polytechnique), co-author of all six, and also Brian Adamson (NRL), Cedric Adjih (INRIA), Justin Dean (NRL) and Philippe Jacquet (INRIA).

The author would also like to thank his colleagues at the BAE Systems Advanced Technology Centre who have helped with various aspects of OLSRv2 and related ad hoc networking matters, in particular Alan Cullen, Peter Smith and Kevin Wainwright.

5.0 REFERENCES

[1] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, October 2003.

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

[3] T. Clausen, C. Dearlove and J. Dean, "MANET Neighborhood Discovery Protocol (NHDP)", draft-ietf-manet-nhdp-14, Internet Draft (work in progress), July 2010.

[4] T. Clausen, C. Dearlove and P. Jacquet, "The Optimized Link-State Routing Protocol version 2", draft-ietf-manet-olsrv2-11, Internet Draft (work in progress), April 2010.

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

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

[7] C. Dearlove, T. Clausen and P. Jacquet, "Link Metrics for OLSRv2", draft-dearlove-olsrv2-metrics-05, Internet Draft (work in progress), June 2010.

[8] G. Pei, M. Gerla and T-W. Chen, "Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks", IEEE International Conference on Communications (ICC 2000), Volume I, pp. 70-74, June 2000.

[9] C. Santiváñez and R. Ramanthan, "Hazy Sighted Link State (HSLS): A Scalable Link state Algorithm", BBN Technical Memorandum No. 1301, March 2003.

[10] C. Dearlove, "OLSR Developments and Extensions", 2nd OLSR Interoperability Workshop, Paris, July 2005, http://interop.thomasclausen.org/Interop05/Papers/Papers/paper-01.pdf

[11] C. Dearlove, "OLSR Simulation, Implementation and Ad Hoc Sensor Network Application", 1st OLSR Interoperability Workshop, San Diego, August 2004, http://interop.thomasclausen.org/Interop04/Papers/Papers/Dearlove.pdf

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

[13] I. Chakeres and C. Perkins, "Dynamic MANET On-demand (DYMO) Routing", draft-ietf-manet-dymo-21, Internet Draft (work in progress), July 2010.

[14] J. Macker, "Simplified Multicast Forwarding for MANET", draft-ietf-manet-smf-10, Internet Draft (work in progress), March 2010.

[15] C. Adjih, T. Clausen, A. Laouiti, P. Mühlethaler and D. Raffo, "Securing the OLSR Protocol", 2nd IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), Mahdia, June 2003.

[16] H. Lundgren, E. Nordström and C. Tschudin, "The Gray Zone Problem in IEEE 802.11b Based Ad Hoc Networks", ACM SIGMOBILE Mobile Computing and Communications Review, Volume 6, Issue 3, pp. 104-105, July 2002.

[17] K. Nichols, S. Blake, F. Baker and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.

[18] C. Adjih, E. Baccelli, T. Clausen, P. Jacquet and G. Rodolakis, "Fish Eye OLSR Scaling Properties", IEEE Journal of Communications and Networks, Volume 6; Part 4, pp. 343-351, December 2004.

BAE SYSTEMS

New Capabilities in Security and QoS Using the Updated MANET Routing Protocol OLSRv2

Christopher Dearlove chris.dearlove@baesystems.com

Overview

Introduction:

- Mobile ad hoc networks (MANETs)
- Optimised Link State Routing (OLSR)
- New features in OLSR version 2 (OLSRv2)

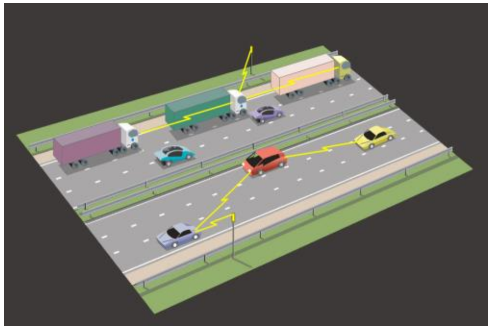
Packet/message format and security:

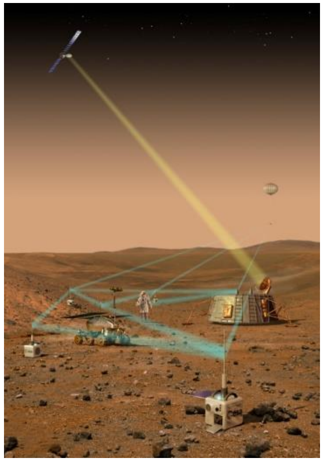
- Generalised packet and message format
- Packet/message authentication signatures
- Use of Identity Based Encryption (IBE)

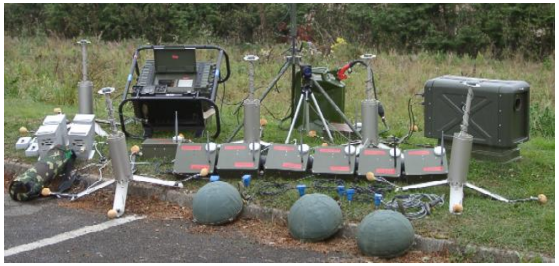
Link metrics and QoS:

- Link metrics
- Quality of Service (QoS)

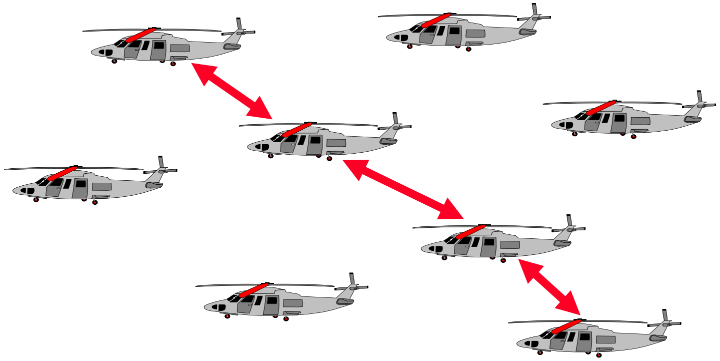
Conclusions







MANETs



Mobile ad hoc networks (MANETs):

- Connect wireless devices into a network.
- Cooperative, relays packets when out of direct contact.
- Self-organising and self-healing.

MANETs are a good fit to many military, and public safety, scenarios:

- Soldiers in vehicles and dismounted.
- Aerial platforms as communications relays.
- Communications coverage of aircraft hangars and flight decks.
- Emergency services in underground railway stations, tunnels, etc.
- Sensor networks, and dual-purpose sensor/communications networks.

Optimized Link State Routing (OLSR)

OLSR is a widely used MANET routing protocol:

- Finds the relays to get packets to their destinations.
- Proactive link state routing protocol.
    - ♦ Discovers links, keeps a current topology graph, uses it to find routes.
- Optimisation based on definition and use of Multi-Point Relays (MPRs).
    - ♦ Minimises message flooding overheads, enables use of partial topology.

OLSR is good, but not perfect. The IETF (Internet Engineering Task Force) is working on standardising OLSR version 2 (OLSRv2).

- OLSRv2 retains the key features of OLSRv1, such as MPRs.
- Improvements from OLSRv1 to OLSRv2 are described in paper.

Major New Features in OLSRv2

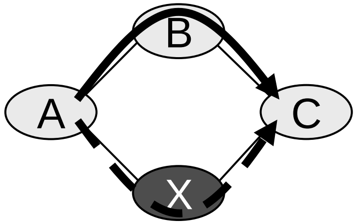
Modular protocol, with three major components:

- OLSRv2, including other components by reference.
- NeighbourHood Discovery Protocol (NHDP).
- Generalised packet and message format (RFC 5444):
  - ♦ Multi-message packet.
  - ♦ Message header enables fast decision whether to process and/or forward.
  - ♦ Message body contains addresses, e.g. of self or neighbour, compressed.
  - ♦ Packets, messages, and addresses can have attributes added.
  - ♦ Attributes use a Type-Length-Value (TLV) structure.
  - ♦ Attributes used by OLSRv2 for validity time, link status, MPR signalling, etc.

Links to have metrics, not just hop count

- Reported using TLVs.
- Shortest path routing using additive directional link metrics.

Packet/Message Authentication Signatures



A major security issue in MANETs is network integrity.

- Hostile devices can impersonate legitimate devices.
  - Can use same protocols, copied or false identities, etc.
- Hostile devices can e.g. become relays, but not forward traffic packets.

Major step is to authenticate routing packets/messages.

- Can be achieved using packet/message cryptographic signatures.
- Reject packets/messages without valid signature.
- Hostile devices cannot become relays, etc.

OLSRv2 allows signatures to be attached as packet/message TLVs.

- OLSRv1 immutable packet/message format causes signature problems.

Signature Key Management and Identity Based Encryption

Simplest approach is to pre-configure all devices with single shared secret.

- If one device is compromised, all are.

Better approach would be for each device to have a unique secret.

Can be done with conventional Public Key Cryptography (PKC):

- Needs pre-configuration about each device in all devices, vulnerable certificate authority, or certificates in messages.

Another solution is using Identity Based Encryption (IBE):

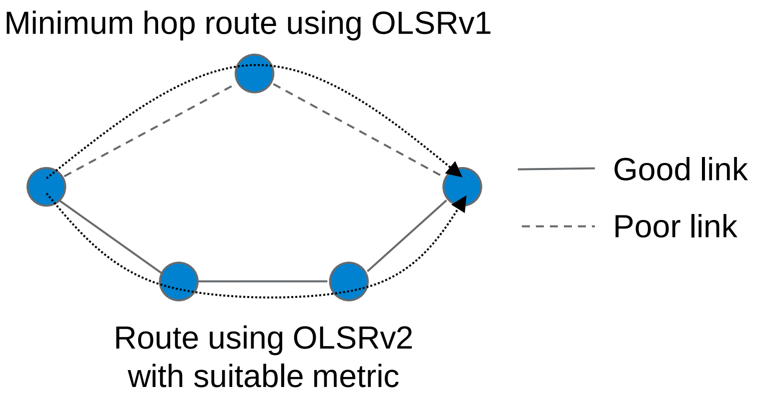
- Variant of PKC where public key is identity – can use IP address.
- Each device is uniquely pre-configured prior to deployment.
    - ♦ No knowledge of other devices. More can be added later, unplanned.
- Computationally expensive, but for routing can be done in real time.
- Can create shared secrets for traffic encryption with no extra signalling.
- Good fit to unplanned, decentralised, ad hoc network.

Link Metrics

OLSRv1 only finds minimum hop routes.

- Often not best, e.g. three good links may be better than two poor links.

OLSRv2 will include link metrics, to allow use of better routes.



Meaning of metric (bandwidth, delay etc.) is outside scope of OLSRv2.

- Alternative metric types can be defined later without changing OLSRv2.

Link Metrics and Quality of Service

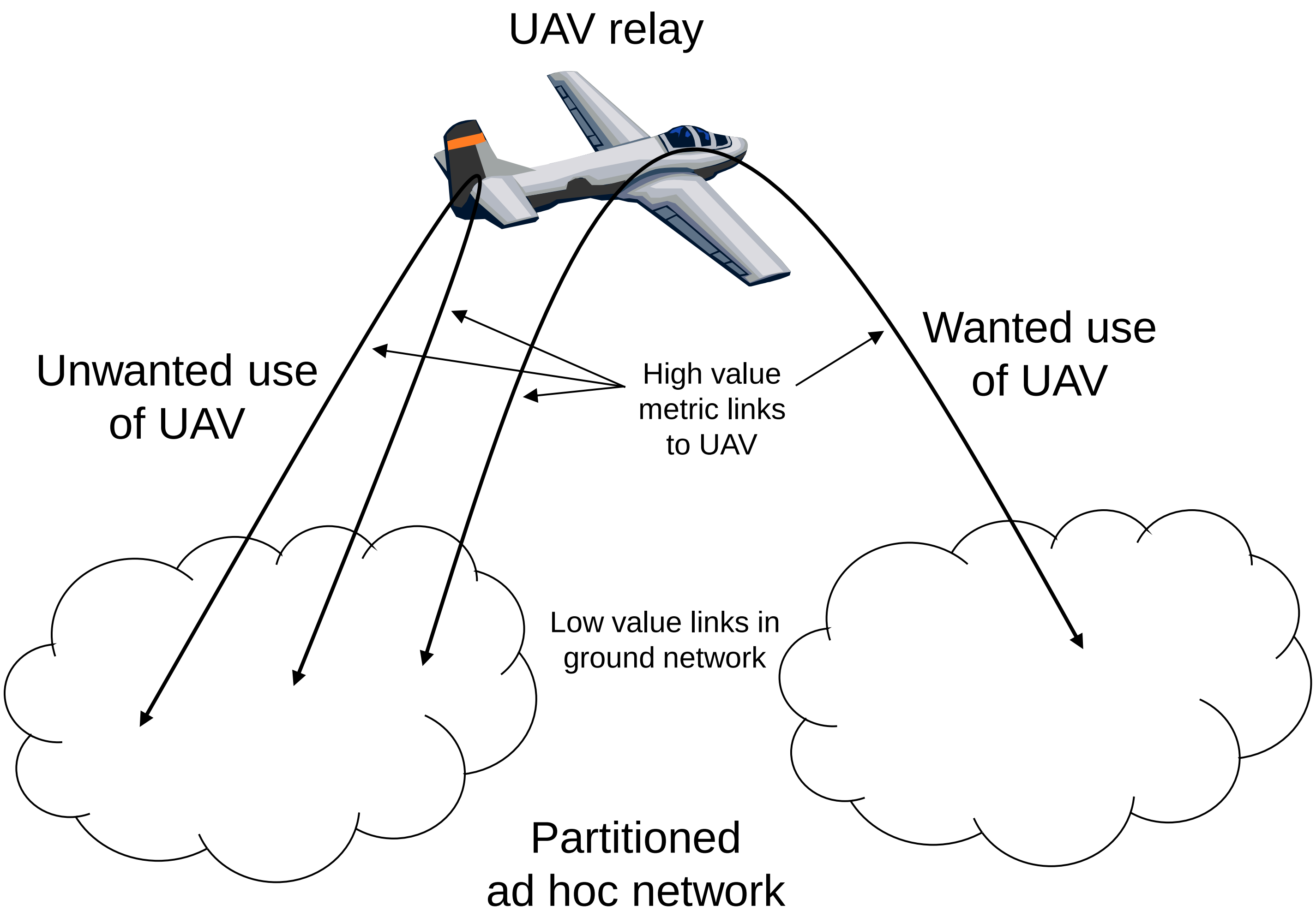
Link metrics can be a critical feature to support Quality of Service (QoS) in a MANET:

- Wireless networks often have poor, and variable, links.
- Link metric is directional, as radio link properties may be.
- Network layer routing enables heterogeneous MANETs, which have greater need to use the most appropriate links.
- Link metric type may be chosen as appropriate to network and traffic.
  - Examples: bandwidth, delay, loss rate, preservation of limited resource (e.g. battery power).
- Link metric must be specified so as to be additive.
  - Examples: logarithm of loss rate, suggested approximations for bandwidth.

Use alongside other QoS mechanisms:

- Reservation, prioritisation, queue management, flow control, etc.

An Example



UAV relay

Unwanted use of UAV

High value metric links to UAV

Wanted use of UAV

Low value links in ground network

Partitioned ad hoc network

BAE SYSTEMS

Conclusions

OLSRv2

- Improves on OLSRv1:
  - ♦ Generalised packet/message format aids extensibility.
  - ♦ Link metrics.
  - ♦ Numerous other improvements.
- Major improvements directly facilitate improvements against key requirements for military application of MANETs:
  - ♦ Security (network integrity) using packet/message signatures.
  - ♦ Quality of service.
- Standards Track in IETF.