The Journal of Supercomputing Special Issue manuscript No.
The original publication is available at www.link.springer.com.

Standardisation Advancements in the Area of Routing for Mobile Ad-hoc Networks

Tipu Arvind Ramrekha · Emmanouil Panaousis · Christos Politis

Published online: 12 October 2011

Abstract Mobile Ad hoc Networks (MANETs) are self-organized and fully distributed networks that rely on the collaboration of participating devices to route data from source to destination. The MANET paradigm is expected to enable ubiquitous mobile communication and thus the proliferation of pervasive applications. The MANET Working Group (WG) of the Internet Engineering Task Force (IETF) is responsible for standardizing an appropriate Internet Protocol (IP) based routing protocol functionality for both static (mesh) and dynamic (mobile) wireless ad hoc network topologies. In this paper, we provide a background on the possibility to use MANETs for enabling future pervasive internet and innovative ubiquitous services. We also describe the work achieved by the MANET WG thus far on the area of secure unicast and multicast routing for MANETs. We also examine non-IETF work on this area, chiefly based on adaptive and hybrid routing. The paper then presents comparative performance evaluations of discussed routing protocols. It is mainly observed that there is a need for adaptive hybrid routing approaches in order to support future ubiquitous and pervasive applications. Consequently, we finally present our conclusions.

Keywords Ubiquitous and pervasive networks · Standardisation advancements · Ad hoc networks · Adaptive hybrid routing · future internet services

1 Introduction

Mobile Ad hoc Networks (MANETs) consist of a set of self-organized communicating devices that may assume the role of a data source, destination or router. Data can be sent directly from source to destination if these are both within the same communication range. This range is defined by the enabling technology e.g. Zigbee (IEEE 802.15.4), Bluetooth (IEEE 802.15.1), Wifi (IEEE 802.11) and bespoke experimental MANET medium access (MAC) protocols. In the case where the source and destination nodes cannot directly connect to each other, intermediate nodes act as packet routers for multi-hoping data from a source to a destination. Hence, MANETs can be described as fully distributed, autonomous and cooperative communication networks that can be effectively setup and operated without the need for pre-established infrastructures. These peculiar MANET characteristics fit requirements for the deployment of several future ubiquitous applications, as presented in [1], such as pervasive applications providing services for tactical military, intelligent transportation, emergency response and broadband internet access in remote rural areas. Thus, MANETs could be usefully deployed as a peripheral future internet infrastructure as shown in Fig. 1.

For such deployments, wireless MANETs would enhance user mobility and remove any dependance on pre-existing infrastructures. At the same time such ubiquitous networks will maintain connectivity among users as well as between user devices and the internet to facilitate the deployment of pervasive applications such as in [2]. The successful deployment of such dynamic and self-organized networks mainly depends upon establishing a suitable routing protocol. For instance, routing mechanisms for MANET ubiquitous multimedia applications may have to satisfy certain application specific quality of service(QoS) requirements while at the same time being subject to dynamic constraints such as varying wireless link qualities along routes, link breakage

Address(es) of author(s) should be given

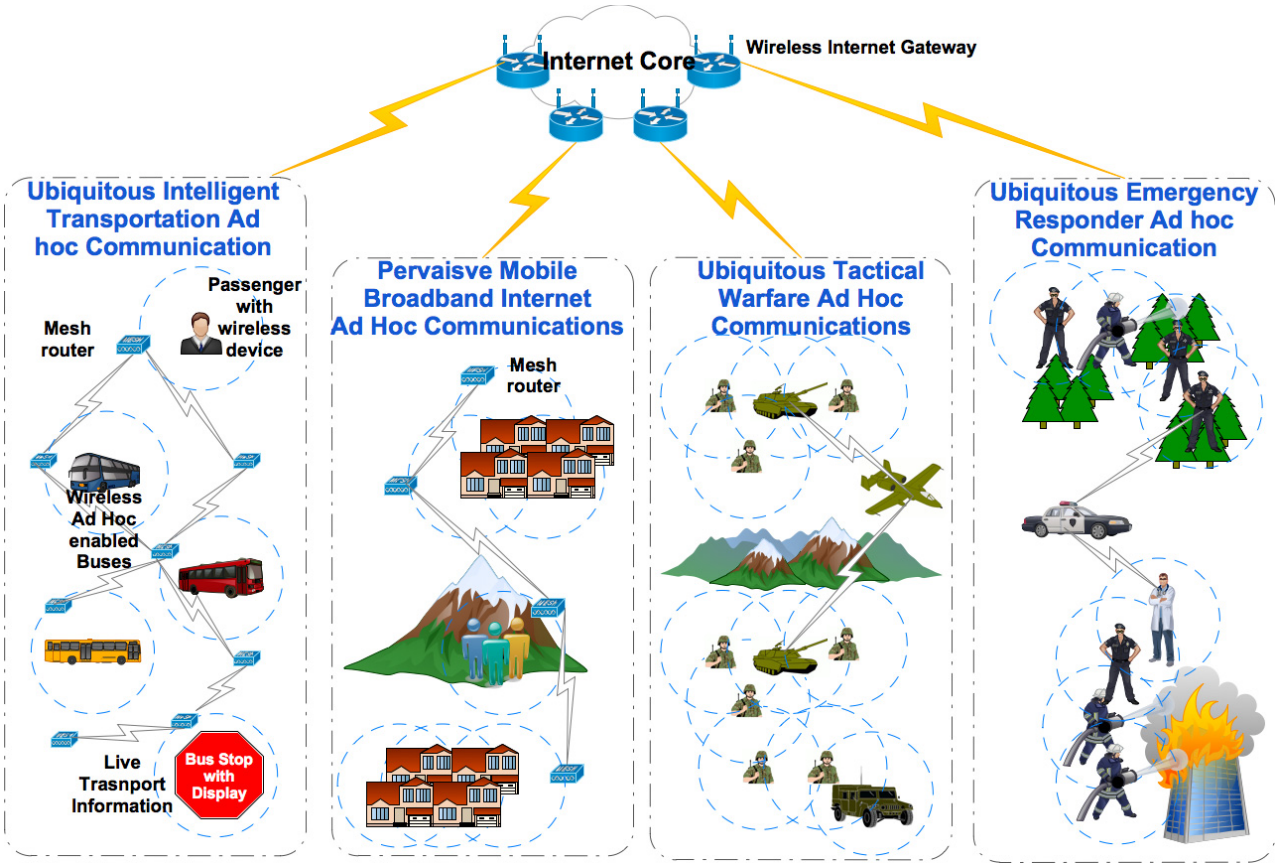


Fig. 1: Potential deployments of Ubiquitous Ad hoc networking

due to mobility of nodes and battery limitations of participating lightweight devices.

The MANET Working Group (WG) of the Internet Engineering Task Force (IETF), formed in 1997, are currently leading the standardisation activities for an appropriate Internet Protocol (IP) based routing protocol functionality for both static and dynamic wireless routing topologies. The establishment of the MANET WG has been a catalyst towards research in the field of MANET routing sparkling the creation of several scientific forums and the publication of thousands of scientific papers addressing related challenges and possible solutions. The protocols developed by the MANET WG are amongst the most adopted routing approaches towards implementation as discussed further in this paper. An overview of work that has been done by the MANET WG is illustrated in Fig. 2.

The remainder of this article is organized as follows. In section 2, we describe in more detail the requirement of MANETs for ubiquitous applications including possible impact of MANET in the future pervasive internet. We also discuss the IETF charter, specifications and routing recommendations by the MANET WG, Then, in section 3, we present the chartered development of proactive and reactive protocols. In the latter section, we additionally discuss WG activities on multicast routing and compulsory security considerations for MANET routing. This is followed by a discussion of non-chartered work related to MANET WG in section 4. We importantly evaluate and analyse the performance of the various discussed protocols in section 5. Finally we present conclusions in section 6.

2 Background

MANET routing protocols are mandatory towards enabling future MANET deployments within the context of future pervasive internet and ubiquitous communication services. It is likely that the future internet will consist of an Internet of Things (IoT) where pervasive machine to machine communications would be very popular. In such scenarios, IP based ad hoc communications between both sets of human and machine operated communication devices will be a facilitator towards ubiquitous information sharing. MANETs should also pave the way towards innovative and more effective communication services as mentioned in [1], [4], [5].

This will be mainly beneficial for users situated in areas with inadequate or no pre-existing communication infrastructures.

For instance, emergency responders often have to carry out rescue missions in remote sites or disaster locations where infrastructures maybe scarce, incapacitated or even nonexistent. In such cases, MANETs will provide an autonomous IP-based multimedia communication platform to enhance mission critical coordination efforts as being investigated in numerous large scale research projects [1]. MANETs can also be deployed as a tactical network in usually remote battlefields where ad hoc and autonomous communication setups are required. The DARPA project has developed programs [2] to study actionable implications for MANET design and deployment for ubiquitous rescuer communication.

Moreover, ad hoc networking in a mesh topological paradigm can be potentially very useful for commercial applications. Firstly, pervasive intelligent transportation systems could use MANETs for providing passengers with real-time travel information to improve cost effectiveness, efficiency and security compared to current transport systems. Also, ad hoc mesh networks has been deployed in some rural and scarcely populated urban regions for pervasive broadband internet connectivity. Thus even for low subscriber base regions, mesh networking could provide a viable alternative for metropolitan broadband networks, as it significantly reduces network installation costs wile offering pervasive internet connections. There are numerous other potential applications of MANETs for future ubiquitous services that are already being tested in a small scale including location specific tourist info-stations, automatic water meter readers and wildlife monitoring. A more comprehensive illustration of potential ubiquitous applications of ad hoc networking can be found in [1].

In the future, a standard routing protocol developed by the MANET WG should encourage a wider deployment of similar or novel applications to more geographical areas. Therefore, the work being carried out at the MANET WG may be regarded as a precursor towards the popular use of MANETs in the future internet of pervasive computing and ubiquitous data sharing. The role of Ad hoc networking should also facilitate the proliferation of more autonomous and distributed information system management that could foster quicker services and generally a better quality of life in ubiquitously connected communities.

[1] http://www.ict-peace.eu/

[2] http://www.darpa.mil/ipto/programs/itmanet/itmanet.asp

2.1 IETF MANET WG

Routing in a wireless MANET can be summarized as a multi-hop packet forwarding mechanism that can efficiently adapt to changes in the wireless network topology. In the realm of IETF, the WG charter describes the scope of work to be carried out. In that respect, the IETF MANET WG has been chartered for the aim as mentioned in section 1. Moreover, the MANET WG describes some important guidelines for the design of routing approaches. In general, lightweight routing approaches are preferred so that they can be applied on a wider range of hardwares and be suitable for different deployment environments.

Thus, designed MANET protocols have to be applicable to both peripheral pervasive networks attached to internet infrastructures and ubiquitous hybrid MANET-mesh fully autonomous infrastructures. Additionally, the developed protocols have to support both IP version 4 (IPv4) and IP version 6 (IPv6) while also considering routing security requirements and issues. Another goal of the WG is to develop a scoped forwarding protocol for efficient flooding of data packets to all cooperating MANET nodes as a simplified best effort multicast forwarding function by only considering routing layer design issues. The WG currently has two standards track routing protocol specifications namely the Reactive MANET Protocol (RMP) track and Proactive MANET Protocol (PMP) track. In the eventuality that RMRP and PMRP modules have significant commonalities, the WG may decide to converge these approaches into a hybrid protocol.

2.2 Challenges in wireless MANET routing

In addition to well-known wireless networking problems, MANETs present researchers with several peculiar routing challenges as described in [3], [4], [5]. One key routing challenge resides in the fact that routing paths in both static and dynamic wireless MANETs are subject to regular changes. These variances are often consequences of both user mobility and changes in wireless link quality between nodes that may be due to varying antenna coverage patterns, channel interferences and fading effects. Here, a very low link quality can be regarded as a broken link and result in unreachable routers and destinations. Some other constraints that can often cause route breakages between source and destinations include failure of battery operated nodes and security attacks in such fully distributed wireless network environments. The aforementioned occurrences are therefore important design issues that

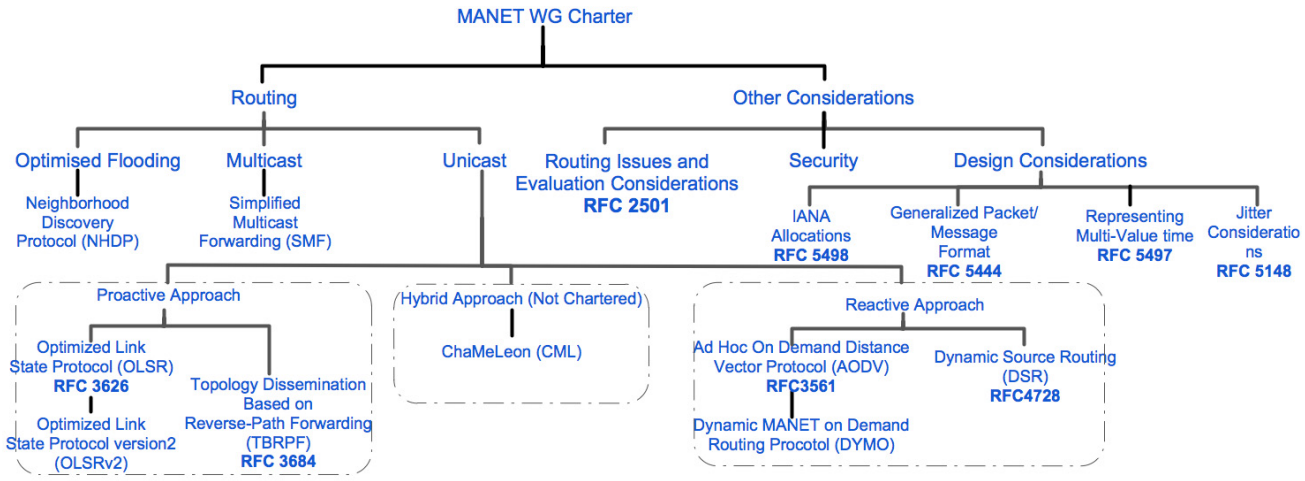


Fig. 2: An overview of Active work being undertaken by MANET WG

have to be addressed while designing a MANET routing protocol.

2.2.1 MANET Routing Issues and Evaluation Considerations (RFC 2501)

MANET routing protocol evaluation can be based upon certain qualitative and quantitative performance metrics as explained in RFC 2501 [3]. These metrics must be applicable to any routing protocol performance evaluation to indicate how well suited the protocol is for that particular test environment. According to MANET WG, a MANET routing protocol has to exhibit the following qualitative features:

- Fully distributed operation of routing algorithm.
- Loop-freedom to avoid same packets being repeatedly processed by set of nodes.
- Demand-based operation that can utilize network resources more efficiently but at the cost of increased route discovery delay.
- Proactive operation especially in contexts where delay intolerant networks with relatively good levels of network resources.
- Security mechanisms to ensure network-level and link-layer security.
- A Sleep period operation for energy conservation without any adverse consequences probably through link layer protocol coupling via a standardized interface.
- Unidirectional link support in wireless environments where bidirectional links are often scarce.

The authors in [3] also describe quantitative performance evaluation metrics for MANET routing protocols including:

- End-to-end data throughput and delay: these are measurements of the protocol effectiveness.
- Route establishment time: time required to establish route(s) when requested as is often the case in on-demand approaches.
- Routing overhead: a measure of efficiency of the protocol that may be expressed as the ratio of "Average number of control and data packets transmitted/data packet delivered".

Further emerging streaming applications that should form part of popular ubiquitous services [2], requires that the delay jitter (variance in end-to-end delay) be constrained to a minimum [6]. Therefore, delay jitter should also be considered as an important performance evaluation metric for MANET routing protocols.

The networking context or test environment is another determining factor in measuring the performance of routing protocols. It is important to vary some of the contexts during the evaluation of the protocol including network size, average number of neighbors of each node, topological rate of change, effective link quality (in terms of capacity and fraction of unidirectional links) and traffic patterns (such as non-uniform or bursty traffic patterns and number of traffic connections). In the rest of the article, the discussed protocols already possess the aforementioned characteristics, as elaborated by the MANET WG in [3].

2.3 Design Recommendations and Considerations

As a result of experience gained through implementation and testing, the WG has published several Internet-Drafts (I-Ds) and Request For Comments (RFCs) to specify recommended protocol design guidelines that

supplement the development of routing approaches presented in section 3. These are described next.

2.3.1 A Generalized MANET Packet/Message Format (RFC5444)

The work in [7] specifies the syntax of a packet format that is able to carry multiple messages required by MANET routing protocols. These messages are very useful for sharing routing information among MANET nodes. Each packet may consist of one or more messages, each in turn consisting of a message header, for message type identification and a message body, containing the actual route information. The RFC 5444 [7] only specify the syntax of such a packet and its messages as shown in Fig. 3 (a). Mainly, the specification include the packet format that may contain zero (in case that the packet header contains the route information) or more messages. The message header may, in turn, contain enough information for routers to perform processing and forwarding decisions. If required, the message body contains attributes corresponding to the message or message originator and address blocks or prefixes, with associated attributes. Here, an address block itself represents sets of addresses or address prefixes in a compact form with aggregated addresses.

It is important to note that a generalized type-length-value (TLV) format is used to represent these attributes where a given TLV can be associated with a packet, a message, or a single address block containing one or more addresses or address prefixes. It is also possible to include multiple TLVs where each TLV is associated with a packet or a message. Otherwise, each of the TLVs can be associated with the same, different, or overlapping sets of addresses or address prefixes in address blocks. The proposed generalized packet and message formats will be suitable for any protocol parsing logic, extensible to include new messages and TLVs, efficient by compacting information and by allowing message header processing for forwarding without the need to process the message body.

Interestingly, this specification was inspired and extended from the packet and message formatting used by the Optimized Link State Routing protocol (OLSR) [8]. In summary, a TLV allows the association of a value to either a packet or a message. While, in all cases, the data structure is identical, the position of the TLV within the packet determes its nature i.e. a “Packet TLV” in the packet header, a “Message TLV” in the TLV block, or an “Address Block TLV” in the TLV Block.

2.3.2 Jitter Considerations in MANETs (RFC5148)

Then,RFC 5148 [11] includes recommendations for the time randomisation of control traffic transmissions for MANET routing protocols in order to reduce the probability of transmission collisions. This process is termed as jittering. Particularly in the case of wireless MANETs, simultaneous packet transmissions may cause collisions and lost of part or all of the transmitted packets over the wireless medium before they even join the receiver queue. In such cases, principally, the Medium Access Control (MAC) protocol determine the extent of the resulting impact. This can range from increased delay in packet delivery to the complete loss of the packet. The document from [11] assumes that the above problem cannot be solved by layers below the network layer in the TCP/IP stack, thus requiring a network layer mechanism. Consequently, the jitter mechanism is proposed as the recommended solution either as part of an IP protocol for wireless networks or complementing a lower-layer mechanism.

The MANET routing protocols are especially prone to packet collisions because of regular scheduled transmission of routing messages by all nodes at equal time intervals, event-triggered messages by neighborhood nodes and message forwarding during routing. The use of the Jitter mechanism aims to inject a voluntary random bounded timing variation before packets are transmitted in order to desynchronize transmitters. In this way, overloading of the transmission medium and receivers could be avoided, decreasing the risk of collisions. This mechanism is deemed particularly useful for broadcast transmissions in MANET protocols. However, a poorly designed jitter mechanism can also create undesired delay jitter for end-to-end packet delivery and thus degrade protocol performance [6] for ubiquitous streaming services [2].

2.3.3 Representing Multi-Value Time in MANETs (RFC5497)

Moreover, a general and flexible TLV for representing time-values is described in [9]. In MANET routing, time-values such as intervals or durations can be very useful in protocol operations.The RFC 5497 [9] uses the generalized MANET packet/message format described above, to define two message TLVs and two Address Block TLVs. These TLVs may usefully represent validity and interval times for MANET routing protocols that need to express single time-values or a set of time-values where each time-value maybe associated with a range of hop counts.

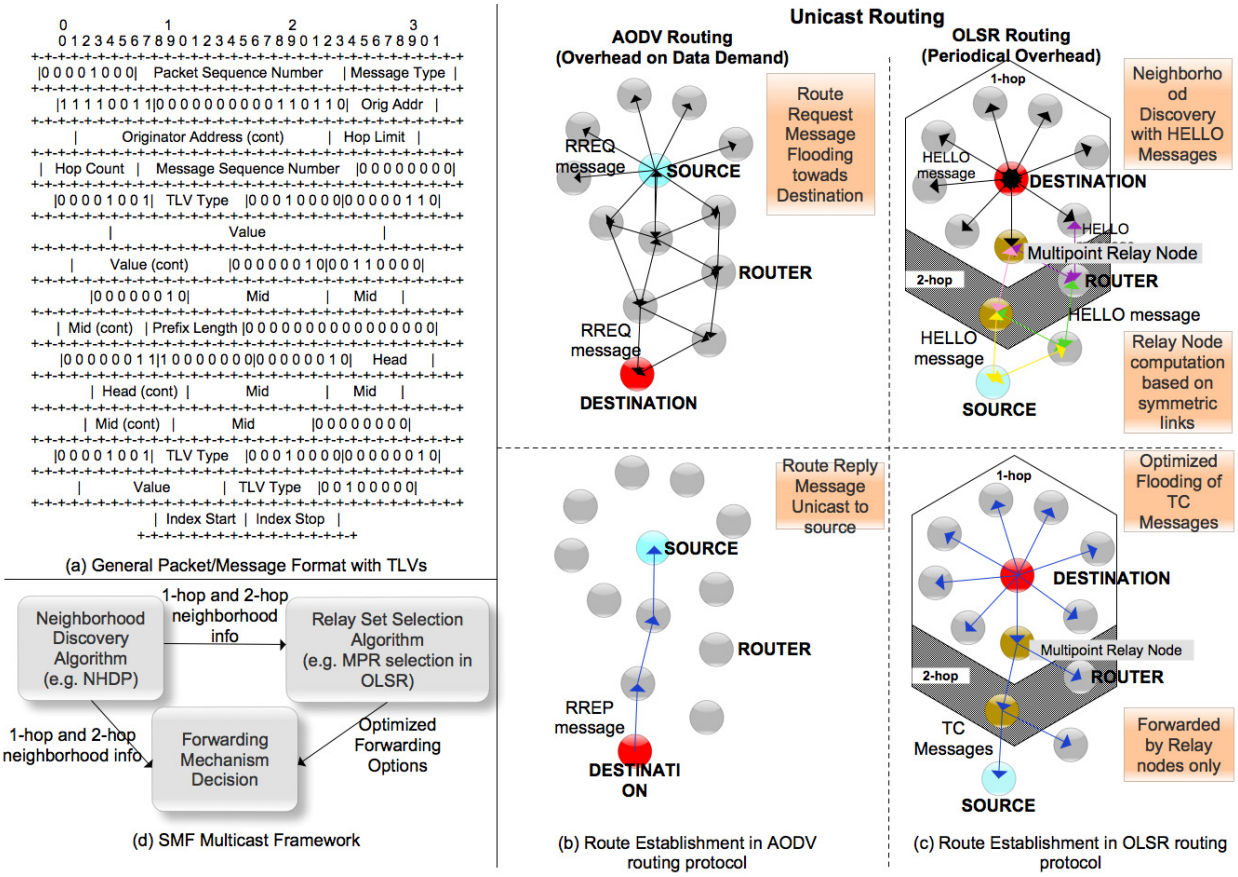


Fig. 3: Packet format and Chartered Routing protocols in MANET WG

This general time TLV structure allows a receiving node to determine single time-values if the hop count from the message originator node is known or if the Time TLV explicitly specifies a single time-value. The two message and address block TLV Types proposed in the document are "INTERVAL-TIME" and "VALIDITY-TIME". These messages and TLV types respectively specify the expected maximum time before another entity of the same type originating from the same node is received and the the entity information validity period after receipt. These are used by the routing protocols to indicate, for each message type, the expected time period between successive transmissions so that transmission rate can be varied as desired. Another attractive feature of such representations is its ability to reduce computational complexity by decreasing the number of bits transmitted in bandwidth-limited wireless MANETs where time TLVs usages do not require high-precision values of time. The 8-bit field encoded time-values allows for a range from small to large values of 1/1024 second to 45 days respectively. MANET routing protocols are also allowed to parameterize this range by modifying a single parameter to change the compacted encoding.

2.3.4 IANA Allocations for MANET Protocols (RFC5498)

Furthermore, the RFC 5498 [10] mentions about several common Internet Assigned Numbers Authority (IANA) allocations to be used by MANET protocols. The interoperable MANET routing protocols using these IANA allocations have to conform to the RFC 5444 [7] in order to use a common format that enables the unambiguous sharing of these IANA allocations. To send and receive MANET routing packets, MANET protocols require:

- UDP Port Number: the UDP port is entitled "manet" and allocated a value of 269.
- IP Protocol Number: the IP protocol number is 138 and is referred to as "manet".
- Link-Local Multicast Group Address: the multicast address to reach link-local (LL) MANET routers is termed "LL-MANET-Routers". For IPv4, the re-

quired link-local scope multicast address is 224.0.0.109 while for IPv6 the required address for LL-MANET-Routers is $FF02:0:0:0:0:0:0:6D$.

2.3.5 Management Considerations

Management considerations are very important MANET routing protocols as the IETF requires them to be manageable. Route change information is cooperatively obtained among MANET nodes and this is updated in the routing tables of each router. Though MANET routing protocols operate autonomously, it may be desirable to externally manage and monitor them in order to improve its performance resulting in a more stable perceived topology and reduced routing overhead. The WG has work in progress for the management frameworks for relevant objects and several Management Information Bases (MIBs) based on Simple Network Management Protocol (SNMP) [12], which is the most popular management protocol, have been proposed for the active WG protocols namely NHDP-MIB, OLSRv2-MIB, DYMO-MIB and SMF-MIB (see Table I for the relevant I-D). Due to the bandwidth-limitations and variable delays within wireless MANET data exchanges, polling is not a desirable option to retrieve object value associated timings as is usually employed by Network Management Systems [12]. Instead, a proxy, physically located close to the managed nodes, is utilised as described in the REPORT-MIB (see Table I for the relevant I-D). In this way, performance reports can be generated remotely using a process similar to the Remote Monitoring (RMON) [12] where the proxy would use local polling to obtain the required object values.

3 Advances in MANET WG Routing Protocols

In this section, we describe the various routing protocols that have been developed by the MANET working group along the RMP, PMP and multicasting tracks as well as essential associated security considerations. Briefly, the fist generation routing protocols were developed independently using the outlined design recommendations and guidelines in RFCs. However, through "lessons learnt" during development, a second generation protocol is currently awaiting for RFC status approval. The second generation protocols propose to use and extend the Neighborhood Discovery Protocol (NHDP) in order to obtain 2-hop network information wither on-demand or proactively. They also specify the usage of the new packet and message format from RFC 5444 [7].

3.1 Neighborhood Discovery Protocol (NHDP) (RFC-to-be 6130)

The NHDP draft (see Table I), or RFC-to-be 6130, is a symmetric 1-hop and 2-hop neighborhood discovery protocol for MANETs. This protocol requires each node to locally exchange HELLO messages so that each MANET router can detect the presence of bi-directional 1-hop and 2-hop connected neighbors. These messages are disseminated through packets as defined in [7]. The symmetric 1-hop neighborhood information is stored to determine direct connectivity to nodes while 2-hop symmetric neighborhood information is necessary for optimising flooding techniques. An example of a reduced flooding technique is the selection of relay sets to minimise the flooding of network wide link state advertisements as in OLSR [8]. Thus, the NHDP records symmetric 1-hop and 2-hop neighborhood information in repositories so that these are available for use by other routing protocols.

Besides, NHDP is designed to use link layer information if available as well as applicable and is based on the neighborhood discovery process utilized by OLSR. The NHDP protocol has added importance due to the fact that communication between two neighboring nodes may be uni-directional. Additionally, the dynamic nature of wireless communication implies that neighboring nodes even when sharing the same channel may still have different broadcast domains. Due to the dynamic nature of wireless MANET links discussed above, IP protocols need to gather such neighborhood information rapidly as generally no such information can be obtained from lower layers. The NHDP therefore updates each node with neighborhood changes, link bi-directionality and local topological information spanning up to 2-hops. It is important to note that the exchange of HELLO messages can be carried out proactively after a time interval or reactively when a change has taken place in a node's neighborhood table. At present, the NHDP has gained wide acceptance in the WG and is waiting approval, from its authors, to be declared as RFC 6130 in the near future.

3.2 Proactive Routing Track

The proactive routing approach, also known as table driven routing, consists of maintaining consistent and updated route information between all possible source-destination (S-D) pairs in the routing tables. Thus, routes between S-D pairs are always available reducing the latency in route establishment. Since a large amount of routing information is periodically disseminated and stored, the downside to such an approach

Table 1: Active Internet Drafts adopted by or related to MANET WG

I-D Title	Authors	I-D Type	Available online at:
MANET Neighborhood Discovery Protocol (NHDP) (Work in Progress)	T. Clausen, C. Dearlove J. Dean	WG	http://tools.ietf.org/id/ draft-ietf-manet-nhdp-14.txt
The Optimized Link State Routing Protocol version 2 (OLSRv2) (Work in Progress)	T. Clausen, C. Dearlove P. Jaquet	WG	http://tools.ietf.org/id/ draft-ietf-manet-olsrv2-11.tx
Simplified Multicast Forwarding (SMF) (Work in Progress)	J. Macker	WG	http://tools.ietf.org/id/ draft-ietf-manet-smf-10.txt
Dynamic MANET On-demand (DYMO) Routing (Work in Progress)	I. Chakeres, C. Perkins	WG	http://tools.ietf.org/id/ draft-ietf-manet-dymo-21.txt
Definition of Managed Objects for Performance Reporting (Work in Progress)	J. R. G. Cole, J. Macker A. Morton	WG	http://tools.ietf.org/id/ draft-ietf-manet-report-mib-00.txt
Definition of Managed Objects for the Neighborhood Discovery Protocol (Work in Progress)	U. Herberg, R. Cole I. Chakeres	WG	http://tools.ietf.org/id/ draft-ietf-manet-nhdp-mib-04.txt
Definition of Managed Objects for the Optimized Link State Routing Protocol version 2 (Work in Progress)	U. Herberg, R. Cole T. Clausen	WG	http://tools.ietf.org/id/ draft-ietf-manet-olsrv2-mib-02.txt
Definition of Managed Objects for the DYMO Manet Routing Protocol version 2 (Work in Progress)	S. Harnedy, R. Cole I. Chakeres	WG	http://tools.ietf.org/id/ draft-ietf-manet-dymo-mib-03.txt
Definition of Managed Objects for the Manet Simplified Multicast Framework Relay Set Process (Work in Progress)	R. Cole, J. Macker, B.Adamson, S. Harnedy	WG	http://tools.ietf.org/id/ draft-ietf-manet-smf-mib-01.txt
MANET Cryptographical Signature TLV Definition (Work in Progress)	U. Herberg, T. Clausen	WG	http://tools.ietf.org/id/ draft-ietf-manet-packetbb-sec-01.txt
Packet Sequence Number based ETX Metric for Mobile Ad Hoc Networks (Work in Progress)	H. Rogge, E. Baccelli A. Kaplan	Personal	http://tools.ietf.org/id/ draft-funkfeuer-manet-olsrv2-etx-01.txt
The ETX Objective Function for RPL (Work in Progress)	O. Gnawali, P. Levis	Personal	http://tools.ietf.org/id/ draft-gnawali-roll-etxof-01.txt
ChaMeLeon (CML): A hybrid and adaptive routing protocol for Emergency Situations (Work in Progress)	T. A. Ramrekha, E. Panaousis C. Politis	Personal	http://tools.ietf.org/id/ draft-ramrekha-manet-cml-01.txt
A Generic Cognitive Adaptive Module (CAM) for MANETs (Work in Progress)	T. A. Ramrekha, E. Panaousis C. Politis	Personal	http://tools.ietf.org/id/ draft-ramrekha-manet-cam-00.txt

is the high overhead of control packets and power consumption even when no data is being transmitted.

There are several WG published work and work in progress for such an approach. Firstly, the Topology Dissemination Based on Reverse-Path Forwarding (TBRPF) [13], last updated in 2004, is a proactive, link-state MANET routing protocol that was considered as an improvement over Open Shortest Path First (OSPF) routing protocol.

Then, OLSR [8] is one of the most popular protocols currently found in literature and experimental testbeds. It is a modified version of classical link state algorithm based on the requirements for MANET routing. The main optimization introduced by OLSR is the flooding message reduction technique using multipoint relays (MPRs). MPRs for each node are the set of minimum symmetrically connected 1-hop nodes that can symmetrically connect the source node to all 2-hop neighbors. Each node periodically issues HELLO messages to establish the MPR sets while periodic Topology Control (TC) messages are used to flood route information network wide. However, these TC messages are only forwarded by the MPRs in the network thus optimizing the flooding procedure. Each nodes receives these routing data at regular intervals of time to update neighborhood information and compute routes to all possible destinations. In addition, only MPRs generate link state messages further reducing routing overhead. OLSR had been designed to work independently from other protocols including underlying link-layer protocols. OLSR is

particularly well suited for MANETs with random and sporadic traffic as well as for deployments where the S-D pair regularly changes with time as no additional control traffic is required in such cases.

Also, the WG is currently working on a version 2 of OLSR called OLSRv2. OLSRv2 operates using the same basic algorithms and mechanisms as in OLSR. However, OLSRv2 uses a more efficient and flexible framework for control packet distribution and more simplified messages are exchanged. More specifically, OLSRv2 uses and extends NHDP for neighborhood discovery and uses the generalized packet/message format [7] as improvements over OLSR. The NHDP is extended by adding MPR Address Block TLV(s) that contains MPR selection of nodes and degree of willingness of nodes to be MPRs. A node can use this willingness value to decline to be a MPR while still participating as a router, source or destination. It is important to note that both OLSRv2 and OLSR, inherit its forwarding and relaying concept from the High Performance Radio LAN (HIPERLAN) MAC layer protocol standardized by the European Telecommunications Standards Institute (ETSI). Both versions of OLSR also conform with the guidelines and considerations mentioned in section 2.

3.3 Reactive Routing Track

On the other hand, a reactive routing approach, also known as on-demand routing, establishes and maintains routes between S-D pairs when requested by the data source node. Although such an approach generates routing overhead on an on-demand basis only, it nevertheless requires added latency for route discovery before routes are established. The Dynamic Source Routing Protocol (DSR) [14] is a well-known reactive protocol that utilises route discovery and route maintenance on-demand to route data from source to destinations. The particularity of DSR is that it allows the source to maintain several routes to specific destinations and select its preferred route that can be useful for load balancing and improved robustness.

The Ad hoc On-Demand Distance Vector (AODV) [15] routing protocol is one of the most well-known reactive protocols in literature. AODV uses an on-demand route discovery and maintenance algorithm for route establishment in unicast routing and is based on modified Bellman-Ford algorithm. The source node initiates route discovery by broadcasting Route Requests (RREQs). Intermediate nodes check if they have a route for the required destination before storing packet information in their routing table for reaching the source and flooding the RREQ further. If the routers have a valid route to the required destination, a Route Reply (RREP) is sent back to the source. Otherwise the destination eventually receives the RREQ, stores the source information in a routing table and sends a RREP through the reverse path. The source receives this reply message and data transmission occurs through the RREQ and RREP established paths. These messages are received via UDP, and the IP header are processed normally. A Time To Live (TTL) value within the packets is used to limit the dissemination radius of messages to a specific number of hops. The stored route information is valid for a timeout period after which the route discovery has to be re-initiated. The validity of a route is extended by the timeout period each time data is sent over that route. A Route Error (RERR) message is used to notify nodes that a link has been lost and that destinations are unreachable.

Then, the Dynamic MANET On-demand (DYMO) routing protocol(see Table I) is regarded as the second generation AODV and is a work in progress in the WG. The basic route discovery and route maintenance processes are similar to AODV. The DYMO protocol can be suitable for use in MANETs exhibiting a variety of mobility and traffic patterns by establishing routes on-demand and is more suitable for sparse networks. It also requires little processing from CPUs. The DYMO protocol differs from the AODV protocol in the sense that it considers the use of NHDP(see Table I) to detect bidirectional links in the neighbourhood ensuring establishment of bidirectional routes. This is a major improvement over AODV. These links are exclusively used for route discovery and route maintenance. DYMO also uses TLV(s) from the packet/message format described in [7] for generating and disseminating RREQ, RREP and RERR messages. As compared to AODV, DYMO allows for support of MIB, local route repairs, unicast links and accepts new improved routes even after routes establishment.

3.4 Multicast Routing

Furthermore, the WG is also working on a multicast routing approach. While the unicast routing can be described as a point-to-point i.e. source to destination data routing mechanism, the multicast routing protocol needs to carry out point-to-multipoint routing i.e. source to multiple destinations routing. Multicasting is useful for a group communication paradigm for various classes of applications within a MANET. Some examples of such applications include multimedia streaming, discovery or registration services and interactive group messaging. The Simplified Multicast Forwarding (SMF) (see Table I for the relevant I-D) is a matured

work in progress within the WG that attempt to satisfy the multicast MANET routing requirements. SMF also uses techniques for multicast duplicate packet detection (DPD) in its forwarding process. As described in section 3, OLSR uses an optimized flooding mechanisms for control messages based on relay sets. The SMF can be partly regarded as an extension to such an efficient flooding concept when applied to the data forwarding domain.

The determination and maintenance of a set of forwarding nodes generally requires dynamic neighborhood topology information that may be provided by a MANET unicast routing protocol or by NHDP operating in parallel with SMF. The NHDP is particularly useful in the absence of an existing MANET unicast protocol or lower layer interface information. The SMF draft also specifies alternative processes that can provide the necessary neighborhood information to support relay set selection. In particular, it emphasises on the requirements for neighborhood discovery with respect to the forwarding process and it finally discusses the relay set selection algorithms. The basic idea behind SMF is to provide a simple best-effort data forwarding mechanism based relying on relay sets flooding optimizations for regional data routing.

The latest version of the SMF I-D specifies the use of the NHDP to gather information so that a relay set selection algorithm can compute the required relays. SMF then uses this neighborhood information and the relays to efficiently multicast data packets to the required nodes. Here, Classical Flooding (CF) can be regarded as the simplest case of SMF multicasting and the use of neighborhood discovering (e.g. NHDP) and relay set selection algorithms are recommended but not required in that case. If used together with NHDP, it is recommended that the NHDP HELLO messages should include the "SMF RELAY ALG" TLV type for the explicit identification of SMF enabled nodes and their corresponding relay sets that are participating in the MANET.

A summary of the chartered routing approaches and the generalized packet format is illustrated in Fig. 3.

3.5 Security Considerations

The routing protocols examined and specified by the MANET WG, as described in the previous sections, are based on the assumption that routers behave legitimately. Secure operation of any MANET routing protocol is crucial due to the absence of a central authoritative infrastructure. In a MANET paradigm, routers and nodes are easily associated and have to cooperate with any other participating network entity including malicious ones. These can disrupt the route discovery routine and the data forwarding operations preventing the propagation of legitimate queries and routing updates. Furthermore, in a wireless MANET in which physical access to the medium is open to any router which relays within the transmission range of the nodes, wireless attacks might come from all directions in addition to the fact that wireless data transmission does not provide a clear line of defence, gateways and firewalls. Needless to say, routing protocols are more exposed to any malicious activity than the conventional infrastructure based networks. The paper [17] is a thorough work which examines the most well-known routing protocols in terms of security, identifying their limitations and analyzing different security solutions for these protocols.

Within the realm of the MANET WG, security issues are now being considered but this effort is not officially chartered. In the packetbb-sec I-D mentioned in Table I, authors envisage to assure network integrity by developing security extensions of the routing protocols, based on digital signatures. This I-D is currently considered as the MANET WG draft which defines a syntactical container for digital signatures and timestamps setting up registries for TLVs containing security related information. Such TLVs as described in section 2, can be associated to messages, packets and addresses in the same way as defined by [7].

Since the issue of security is only recently being addressed by the MANET WG, the current WG routing protocol related documents, specify security requirements without nevertheless directly mentioning about any extensions to support security. Future work could consider these limitations and add the required security extensions. In this manner, we will be able to envisage scenarios where only "admitted" routers will participate in any MANET routing protocol.

Last but not least, the MANET WG should consider drafts related to intrusion detection techniques designed for MANETs. These could be applied by all or certain type of routers and could target the detection of compromised nodes which are mostly insider attackers. Intrusion Detection Systems (IDS) for wireless ad-hoc networks [18] can be used as a second wall of defense. Nodes that are equipped with IDSs operate in *promiscuous* mode to continuously or periodically monitor the traffic sent or received by their neighbours in order to detect malicious packets. For instance, to overcome the harmful situation caused by a packet dropping attack, intrusion detection must be accomplished by a monitoring application such as [18] and [19]. According to these solutions when a packet is sent to a neighbour node, the sender expects to sense that the packet

has been forwarded by the relay node. To increase the detections accuracy; apart from the sender, all the relay node's neighbours can sense the wireless medium to confirm that the aforesaid retransmission occurred.

4 Non-chartered Routing Protocols

There are several interesting non-chartered works related to the MANET WG being carried out in literature and personal drafts in the areas of link error metric(ETX), hierarchical, hybrid, adaptive and multipath MANET routing protocols. These are potentially areas that could be chartered for future MANET WG work in order to create a third generation routing approaches.

One particular field of interest includes adaptive routing protocols based on hybrid approaches. Since MANETs are deployable for various ubiquitous mission critical[3] as well as commercial applications, routing protocols have to fulfil different application specific quality of service (QoS) requirements. In addition, each of proactive and reactive routing approaches, described in section 3, excels for different types of applications and network constraints as discussed in [3], [23], [21], [22].

The above discussion indicates the need for a hybrid routing approach that optimally utilises routing features from both chartered approaches adaptively based on the network context. The main emerging design challenges for adaptive routing protocols include finding mechanisms to gather network context information, establishing cohesive hybrid operations and identifying appropriate threshold values to initiate adaptive changes. Hence, such a protocol can use the best type of routing operation based on the network state in order to improve its performance and satisfy QoS requirements more effectively. ChaMeLeon (CML) (see information on CML I-D in Table I) is such an adaptive hybrid protocol that utilizes OLSR and AODV routing adaptively. In section 5, comparisons between OLSR and AODV show that OLSR displays better cost[4] performance for a particular delay[5] level in smaller networks while when considering the same evaluation criteria AODV performs better in larger network.

These results also indicate that the network threshold depends mainly on distribution of the network, size of the network and number of data connections between S-D pairs. Therefore, the 3-phase operation of CML, described in the I-D, was designed to adaptively route data according to the changing size of a networks as is usually the case in rescuer communication for disaster emergency situations. In this instance, the network threshold depends mainly on the changing network size assuming that the topology is uniformly distributed and the number of S-D connections is fixed.

Briefly, CML consists of a proactive phase (p-phase), reactive phase (r-phase) and oscillation phase (o-phase) suited for smaller networks, larger networks and network size fluctuations near the network size threshold value (oscillations) respectively. Each CML node in the MANET operates in the p-phase using OLSR, by default, and can thus monitor the network size by calculating the number of destinations in the routing table. In the r-phase where CML routes packet using AODV routing, the network size is estimated based on the number of hops of RREP packets. If the network size is found to have exceeded the network size threshold, CML switches to the o-phase only if the oscillation timer is expired, thus reducing effects of periodic oscillations. The o-phase has to continue the current r-phase or p-phase routing while also sampling two more network sizes (see CML I-D for more detail) in order to make sure that the monitored network size has actually changed as opposed to being an oscillation due to temporary node disconnection. If this network change is confirmed, the routing is switched from r-phase to p-phase or vice-versa depending on the network context. Finally, each node has the responsibility to flood CML Change Phase (CP) packets to alert other network nodes of such a phase change.

Additionally, the Cognitive and Adaptive Module (CAM) for MANET routing (see Table I for the relevant I-D) is a proposed design platform that should facilitate the implementation of hybrid adaptive routing protocols based on current work in the WG. CAM was based on [23] and it promotes segmentation of routing protocols into operating components and the standardisation of the components instead of the routing protocol as a whole. Chiefly, it is beneficial to have standard components for each application of MANETs due to the need to fulfilling scenario specific requirements. In this way, users or engineers will be able to create their own routing module and configure the adaptivity of their routing protocol up to a certain level of granularity as restricted by the standard components. In particular, the generalized packet format [7] and NHDP are good candidates for such standard components for defining packets and neighborhood discovery respectively. The users and engineers will then have high level interfaces that can be open or close as per requirements to configure the behaviour of routing protocols including hello intervals, TC intervals, network contexts and network thresholds according to their desired scenarios.

[3] http://www.ict-peace.eu/
[4] in terms of routing packet overhead
[5] in terms of end to end data delivery latency

Implementation	Features	Source
AODV		
Ad-hoc Support Library and AODV-UIU	API to implement ad-hoc routing protocols. Operating System (OS)	http://aslib.sourceforge.net/
Embedded AODV & TORA.	Embedded in the commercial NovaRoam mobile router	http://www.nova-eng.com/novaroam.html
AODV-UU	Implemented by Uppsala University for linux and crosscompiling for ARM/Mips based devices	http://core.it.uu.se/core/index.php/Main_Page
UoB-JAdhoc	Java based multi-platform implementation for Windows and Linux.	http://www.aodv.org/
OLSR		
OLSR daemon	Implementation for Nokia 770, iPhone (8GB model), Mac OS X Tiger, Debian Linux, Ubuntu Linux, Windows 2k/XP/Vista and Android HTC.	http://www.olsr.org/
OOLSR	C++ Implementation by INRIA for Linux and Windows.	http://hipercom.inria.fr/OOLSR/
NRL-OLSR	Naval Research Laboratory olsr implementation in C++ for Linux	http://cs.itd.nrl.navy.mil/work/olsr/index.php
Qolyester	OLSR implementation without any QoS feature by the QOLSR team.	http://qolsr.lri.fr/code/
DYMO		
NIST DYMO	Implementation of by National Institute of Standards and Technology (NIST) for Linux.	http://sourceforge.net/projects/nist-dymo/
DYMOUM	C++ implementation by MASIMUM for Linux.	http://masimum.dif.um.es/?Software:DYMOUM
DSR		
DSR-UU	DSR implementation for Linux and LinkSys WRT54G by Uppsala University.	http://core.it.uu.se/core/index.php/DSR-UU
SMF		
NRL-SMF	Naval Research Laboratory (NRL) PROTocol Engineering Advanced Networking (PROTEAN) Research Group for Linux, MacOS, BSD, Win32, and WinCE.	http://downloads.pf.itd.nrl.navy.mil/smf/

Fig. 4: Summary of implementations based on MANET WG RFCs

In addition, operational experience with wireless ad hoc community networks [6] has confirmed that the use of hop-count as routing metric leads to unsatisfactory net-

[6] Berlin and Vienna Wireless Community Networks (http://www.freifunk.net), Athens Wireless Community Network (http://awmn.net), Roma Wireless Community Network (http://www.ninux.org), Barcelona Wireless Commu-

work performance. Therefore, there is a need to devise a new metric for route selection that is easy to implement and results in satisfactory network performance. Hence, experiments with the ETX metric [20] were undertaken on the aforementioned networks a couple of years ago. The ETX metric of a link is the estimated number of transmissions required to successfully send a packet (each packet smaller than MTU) over that link, until an acknowledgement is received confirming that the packet has indeed been correctly transmitted.

It should be noted that the ETX metric is additive, i.e. the ETX metric of a path is the sum of the ETX metrics for each link on this path. The result of these experiments was that ETX was found to be sufficiently easy to implement while providing sufficiently good performance, and this metric has thus been used for daily operation on these wireless ad hoc community networks ever since, alongside OLSR [8]. Subsequently, some interest in standardizing the use of ETX for OLSRv2 has been shown, and work in progress such as the ETX I-D (see Table I for the relevant I-D) might be the first steps in this direction. Note that in the IETF, the interest in standardizing the use of the ETX metric is not confined to the MANET working group: preliminary work has also taken place within the ROLL working group to standardize the use of ETX within the RPL routing protocol for wireless sensor networks (see Table I).

5 Implementation and Performance Evaluation

5.1 Current Implementations of Protocols

There are well known freely available implementations of the routing protocols described in the sections above. A summary of some of these implementations is shown in Fig. 4. These implementations are freely available for experimentation and improvements. However, other proprietary implementations can also be found but they are not freely available and some are mostly being used for commercial ends.

5.2 Simulations

5.2.1 Scenario

As discussed above, proactive and reactive approaches each have its own merits for certain network contexts. Since it is very complex to properly understand effects of various network contexts on the routing performance in real life test environments, it is useful to use simulation based evaluations of protocols using models derived from their definitions in the RFCs. For the scope of this article, we choose to simulate the most popular researched protocol RFCs in literature. Therefore, we compare the performance of NHDP, AODV and OLSR. It is deemed important to research and evaluate NHDP as a soon to-be RFC of the MANET WG. Additionally, the IETF will recommend future protocols to use NHDP for local scoped routing or route maintenance. The Fig. 5b shows the performance evaluation results of OLSR and AODV based on the routing overhead [7] and average normalized average end-to-end data delivery delay [8]. Thus, the simulated scenario considers the qualitative and quantitative performance of these routing approaches for different network sizes with a uniformly distributed topology. In our scenarios, we investigate the effect of varying required number of route discoveries by AODV as a result of link breakages or need for different data connections. In that case, we assume that the source and destination nodes are located at the furthest possible points from each other while remaining connected in the aforementioned topology. Then, we also compare the overhead incurred by the investigated protocols when the HELLO_INTERVAL, TC_INTERVAL and TIMEOUT_INTERVAL are decreased in order to maintain the same level of delay guarantees. We simulate such a scenario based on the need to update routes at a higher rate due to rapidly changing network topologies due to varying conditions mentioned in section section 2.

5.2.2 Model

In this subsection, we describe the model that was considered for our evaluations. We assume that all the nodes forming the modelled MANET are uniformly distributed over a space of area A. The nodes are represented by a graph, $G = \{V, E\}$ and all nodes, n, in the network are denoted by the set of vertices $V = \{1....n\}$ and the links between nodes be represented by the set of edges $E = \{(i, j) : i, j \epsilon V\}$. A distance function $\Delta(i, j)$ gives the distance between vertices i and j in terms of number of hops required by a packet originating at node i to reach node j. Therefore, for $\forall(i, j)$ that are h-*hops* away from each other, $\Delta(i, j) = h$ where if $h = 1$, it implies that i, j are immediate or 1-*hop* neighbours. We also assume that all the packet sizes in the network have common headers and are of the same size as recommended in [7]. Thus, the normalised protocol overhead are derived based on the 1-hop neighbor nodes and the

nity Network (http://www.guifi.net), Boston Wireless Community Network (http://openairboston.net)

[7] in terms of control packets only i.e. excluding data packets

[8] including route establishment time delay

Table 2: Parameter values for simulation based evaluation of protocols

Parameter	**Value**	**Parameter**	**Value**
Simulated Protocol Usage Time	1 hour	Number of nodes	for n in [4; n++; 55]
Duration of discrete data connection	5 minutes	Number of Connections	2; 4; 6; 8; 10
Default HELLO_ INTERVAL	2 seconds	Reduced HELLO_ INTERVAL	1 second
Default TC_ INTERVAL	5 seconds	Reduced TC_ INTERVAL	3 seconds
Default TIMEOUT	3 seconds	Reduced TIMEOUT	1 second
Default MPR ratio	0.75	MPR ratio	0.25; 0.5; 0.9

value of n nodes for a given area A. In addition, a maximum normalised bound for end-to-end packet delivery delay can be approximated based on [24], [25], [26] and [29]. We use values reproduced in Table 2 for our simulations based on recommendations from RFC 3626 [8] and RFC 3561 [15].

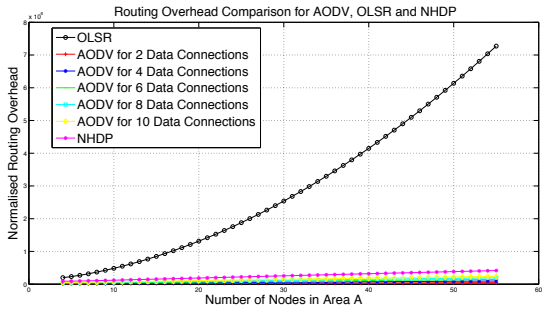
5.2.3 Results and Discussion

In this subsection, we describe and discuss the simulated evaluation results. It is important to note that the results of NHDP is based on a 2-hop data delivery scenario for delay and a 1-hop evaluation of the overhead cost for each node. It can be observed in Fig. 5a, that AODV overall produces lower normalised overhead (in terms of relative routing control data used by each protocol) than NHDP and OLSR. The overhead of AODV depends on the number of connections and increases proportionally to the latter parameter. NHDP can be regarded as the local overhead cost for each OLSR node and thus NHDP has less overhead than OLSR indicating that the TC messages used by OLSR produces exponential overhead. Additionally, the normalised overhead for all protocols increase as the size of the network increase, with the routing cost for OLSR increases exponentially in that case. From Fig. 5b, it can be seen that the normalized average delay for NHDP increases insignificantly as the network size increases as compared to both AODV and OLSR. The increase of normalised delay as a function of network size depends on the number of connections used, with a higher increasing gradient for higher number of connections. The increase in normalised delay for OLSR is independent on the number of data connections used. It is important to note that there is a netwrok size threshold beyond which AODV produces less delay that OLSR. This network size threshold, as observed in Fig. 5b, is dependent on the number of connections used in the networks and consequently the rate of increase of the AODV delay gradient.

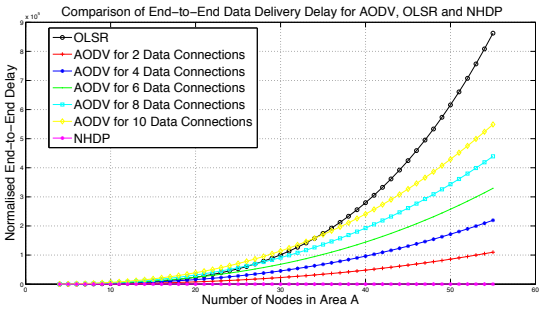
Then, in Fig. 5c and Fig. 5d, we investigate the effect of having different proportions of neighbour nodes as MPR nodes in the case of OLSR. MPR nodes are important for the optimisation of flooding mechanism that is prominent in OLSR for TC message dissemination. In cases where the link qualities in the network are poor or for sparsely distributed networks, a high ratio of MPR nodes will be required to form fully connected networks with reduced flooding using MPR. It can be seen that both the normalised overhead and normalised delay are dependent on the MPR ratio. A higher ratio results in higher overhead and delay. Furthermore these values increase exponentially for OLSR as the network size is increased. It is also observable that for smaller networks, the OLSR protocol has approximately the same performance irrespective of the MPR ratio. This small network size value is of the order of 10 nodes when the normalised overhead is considered and 20 nodes for normalised delay considerations.

Moreover, Fig. 5e and Fig. 5f considers the case of changing routes where a high route change of a second is considered. In such a case, in order to update routes in a timely manner, the intervals have to decreased in order to have faster route update periods as described in Table 2. It is observed that although the order of normalised routing overhead remains, in decreasing order, OLSR, NHDP and AODV, the normalised end-to-end delay performances change. NHDP deliver data to 2-hop neighbours and has the lowest average delay value. However, AODV has a higher delay for data delivery as compared to OLSR due to the increased TIMEOUT value. While in the case of OLSR, the delay is only due to medium access backoff time and queue wait time at each intermediate node, for AODV the route discovery time is significant. A lower timeout forces the source node to re-initiate route discoveries at a higher rate and thus injects a higher delay value to the network. This degradation in performance as compared to OLSR is even more noticeable for larger networks where the average number of intermediate hops towards potential destinations increase.

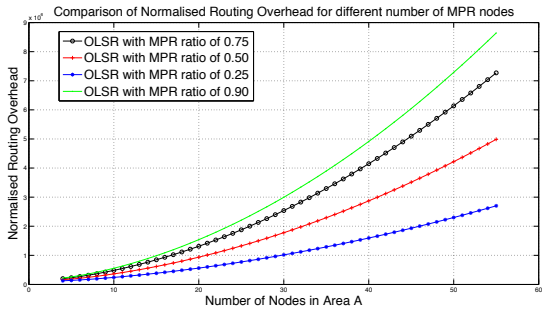
We finally analyse the efficiency of the protocols in Fig. 5g and Fig. 5h. Thus we evaluate the directions taken by the MANET WG i.e. the justification in the design of OLSRv2 and DYMO. We use the logarithm of



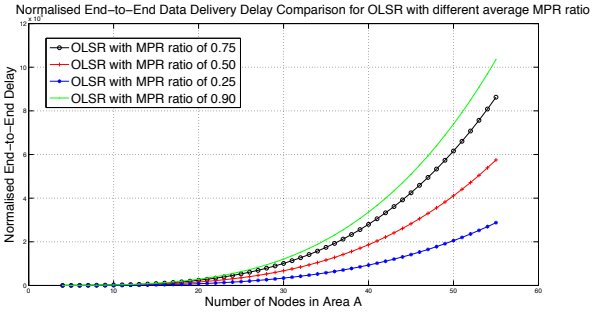
(a) Normalised routing overhead comparison



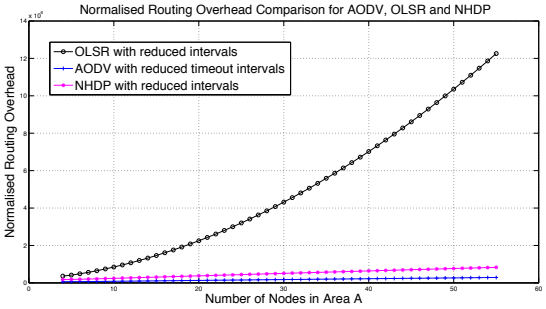
(b) Normalised end to end data delivery delay



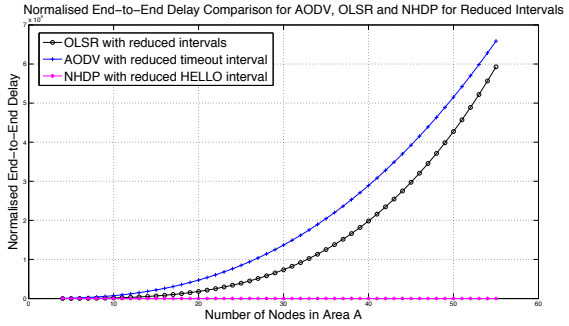
(c) Normalised routing overhead comparison for OLSR



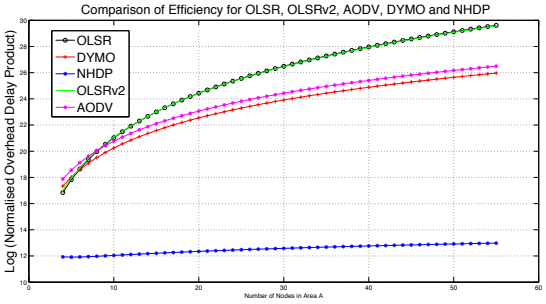
(d) Normalised end to end data delivery delay for OLSR



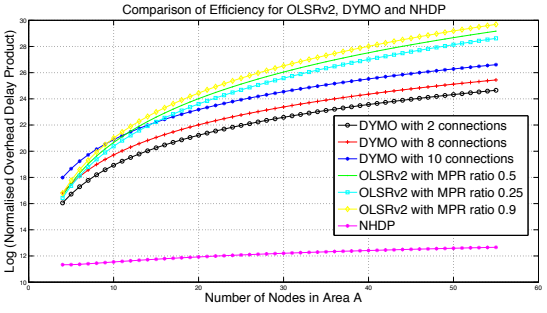
(e) Normalised routing overhead comparison



(f) Normalised end to end data delivery delay



(g) Efficiency in terms of log (Overhead x Delay product)



(h) Efficiency in terms of log (Overhead x Delay product)

Fig. 5: Performance Evaluation of OLSR, OLSRv2, AODV, DYMO and NHDP

the normalised delay-overhead product in order to estimate the efficiency of a protocol. This is because a relatively higher delay may be acceptable if the overhead is low but at the same time, higher overhead may be tol-

erated for relatively lower delay performance. Hence, a lower product indicates a better efficiency of the routing protocol and thus better performance as recommended in RFC 2501 [3]. It can be observed in Fig. 5g that OLSR is more efficient than AODV for smaller networks of less than 10 nodes whereas AODV is the preferred protocol for larger networks based on the default parameter values in Table 2. Here, it is clearly noticeable that NHDP is most efficient for 2-hop route information maintenance and data routing throughout the investigated range of network sizes. Hence, as supported by our above discussions, the MANET WG has proceeded in the right direction by integrating NHDP as the basis of OLSRv2 and DYMO as a second generation for OLSR and AODV respectively. It can be seen that OLSRv2 has slightly better efficiency than OLSR with the benefit of having variable parameters of HELLO_ INTERVAL and TC_ INTERVAL as well as a more flexible packet format. In the case of DYMO, a significant improvement in efficiency can be observed by using NHDP instead of re-initiating route discoveries at TIMEOUT intervals. Although it produces more overhead than AODV, DYMO benefits from much improved delay performance as it no longer endures delays due to route discoveries unless routes are changed during transmission as indicated by the reactive mode NHDP component. In Fig. 5h, we confirm the fact that even though DYMO and OLSRv2 have improved efficiencies, DYMO still perform better for larger network size than OLSRv2. The threshold network size beyond which this occurs depends on the number of connections and MPR ratio. For a reasonable scenario, where 10 connections are used and the MPR ratio of neighbours is 0.25, the network size threshold resides in the order of 15 nodes.

Hence, it is not effective to utilize different protocols depending on the changing context of the network and also not efficient (as discussed above) to use one given protocol approach for all network contexts. Therefore, a logical solution is to combine both approaches into a hybrid routing protocol that will adaptively use the most efficient routing approach based on the network conditions and traffic requirements. The proposed CML protocol (see Table I), is such a hybrid adaptive protocol as described in section 4. Such type of work is not yet chartered at the MANET WG but can be an interesting avenue for future charters i.e. hybrid adaptive protocols can pave the way for third generation MANET routing protocols that will be more suitable for a wider range of ubiquitous applications. However, adaptive hybrid routing approaches present a number of emerging challenges as presented in section 4 and therefore the CML protocol is still a work in progress. Furthermore, CML does require additional routing overhead and adds slightly more packet processing delay as compared to AODV and OLSR while being more suitable than both approaches when considered for a wider context range [27]. The same should be applicable to DYMO and OLSRv2 if the CML approach is applied to these second generation protocols.

6 Conclusion

The MANET paradigm provides a novel approach towards IP-based data exchange whereby users will be able to ubiquitously exchange information. These autonomous networks can be deployed either as a peripheral network connected to the internet or as a purely peer-to-peer network, thus, paving the way for pervasive communication services for the future internet. The MANET WG has carried out significant pioneering work in encouraging research and development of MANET routing protocols to encourage real life MANET deployments.

Two IETF chartered routing protocols, namely OLSR and AODV (including their second generation counterparts OLSRv2 and DYMO respectively) stand out as the popular candidates towards standardisation. However, hybrid adaptive routing approaches have the potential to improve the performance of current adopted protocols and therefore represent interesting candidates for future work within the WG (as a third generation routing approach). Such routing protocols may trigger a popular acceptance of MANETs for a wider range of commercial and governmental communication services, thus making such applications pervasive. Such an appraoch is also adopted in [28]. Last but not least, due to the autonomous, distributed and wireless nature of MANETs, security mechanisms must be standardized to guarantee an appropriate trust level to any prospective user.

References

1. Bruno R, Conti M, Gregori E (2005) Mesh networks: commodity multihop ad hoc networks. IEEE Commun Mag 43(3):123131
2. Braun D, Buford J, Fish R, Gelman A, Kaplan A, Khandelwal R, Narayanan S, Shim E, Yu H (2008) UP2P: a peer-to-peer overlay architecture for ubiquitous communications and networking. IEEE Commun Mag 46(12):3239
3. Corson S, Macker J (1999) Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations. Informational, [Online]. Available: `http://www.ietf.org/rfc/rfc2501.txt`
4. Burbank JL, Chimento PF, Haberman BK, Kasch WT (2006) Key challenges of military tactical networking and

the elusive promise of MANET technology. IEEE Commun Mag 44(11):3945
5. Conti M, Giordano S (2007) Multihop ad hoc networking: the reality. IEEE Commun Mag 45(4):8895
6. Chan S-P, Kok C, Wong AK (2005) Multimedia streaming gateway with jitter detection. IEEE Trans Multimed 7(3):585592
7. Clausen T, Dearlove C, Dean J, Adjih C (2009) RFC5444: generalized mobile ad hoc network (MANET) packet/message format. Std. track, [Online]. Available: `http://www.ietf.org/rfc/rfc5444.txt`
8. Clausen T, Jacquet P (2003) RFC3626: optimized link state routing protocol (OLSR). Experimental, [Online]. Available: `http://www.ietf.org/rfc/rfc3626.txt`
9. Clausen T, Dearlove C (2009) RFC5497: representing multi-value time in mobile ad hoc networks (MANETs). Std. track, [Online]. Available: `http://www.ietf.org/rfc/rfc5497.txt`
10. Chakeres I (2009) RFC5498: IANA allocations for mobile ad hoc network (MANET) protocols. Std. track, [Online]. Available: `http://www.ietf.org/rfc/rfc5498.txt`
11. Clausen T, Dearlove C, Adamson B (2008) RFC5148: jitter considerations in mobile ad hoc networks (MANETs). Informational, [Online]. Available: `http://www.ietf.org/rfc/rfc5148.txt`
12. Hajji H (2005) Statistical analysis of network traffic for adaptive faults detection. IEEE Trans Neural Netw 16(5):10531063
13. Ogier R, Templin F, Lewis M (2004) Topology dissemination based on reverse-path forwarding (TBRPF). Experimental, [Online]. Available: `http://www.ietf.org/rfc/rfc3684.txt`
14. Johnson D, Hu Y, Maltz D (2007) The dynamic source routing protocol (DSR). Experimental, [Online]. Available: `http://www.ietf.org/rfc/rfc4728.txt`
15. Perkins C, Belding-Royer E, Das S (2003) RFC3561: ad hoc on-demand distance vector (AODV) routing. Experimental, [Online]. Available: `http://www.ietf.org/rfc/rfc3561.txt`
16. Clausen T, Dearlove C, Dean J (2011) RFC6130: MANET neighborhood discovery protocol (NHDP). Std. track, [Online]. Available: `http://www.ietf.org/rfc/rfc6130.txt`
17. Abusalah L, Khokhar A, Guizani M (2008) A survey of secure mobile ad hoc routing protocols. IEEE Commun Surv Tutor 10(4):7893
18. Zhang Y, Lee W (2000) Intrusion detection in wireless ad-hoc networks. In: Proc ACM MOBIHOC 2000, pp. 275283
19. Yu W, Sun Y, Liu KJR (2005) HADOF: defense against routing disruptions in mobile ad hoc networks. In: Proc IEEE INFOCOM 2005, vol 2, pp 12521261
20. De Couto D, Aguayo D, Bicket J, Morris R (2003) A high-throughput path metric for multi-hop wireless routing. In: Proc ninth annual international conf. on mobile computing and networking. ACM Mobicom, vol 3
21. Pathak H, Dutta R (2010) A survey of network design problems and joint design approaches in wireless mesh networks. IEEE Commun Surv Tutor PP(99):133
22. Akyildiz IF, Wang X, Wang W (2005) Wireless mesh networks: a survey. Comput Netw 47(4):445487
23. Samar P, Pearlman MR, Haas ZJ (2004) Independent zone routing: an adaptive hybrid routing framework for ad hoc wireless networks. IEEE/ACM Trans Netw 12(4): 595608
24. Bisnik N, Abouzeid A (2009) Queuing network models for delay analysis of multihop wireless ad hoc networks. Ad Hoc Netw 7(1):7997
25. Groenevelt R, Nain P, Koole G (2005) The message delay in mobile ad hoc networks. Perform Eval 62:210228
26. Wang Z, Crowcroft J (1996) Quality-of-service routing for supporting multimedia applications. IEEE J Sel Areas Commun 14:12281234
27. Ramrekha TA, Politis C (2010) A hybrid adaptive routing protocol for extreme emergency ad hoc communication. In: Proceedings of 19th IEEE International Conference Computer Communications And Networks (ICCCN), pp 16, 25 August 2010
28. Chai WK, Wang N, Psaras I, Pavlou G, Wang C, Garcia de Blas G, Ramon-Salguero FJ, Liang L, Spirou S, Beben A, Hadjioannou E (2011) Curling: content-ubiquitous resolution and delivery infrastructure for next-generation services. IEEE Commun Mag 49(3):112120
29. Ramrekha TA, Millar GP, Politis C (2011) A model for designing scalable and efficient adaptive routing approaches in emergency ad hoc communications. In: IEEE Symposium on Computers and Communications (ISCC), pp 916-923, 28 June1 July 2011