An Adaptive QoS Routing Solution for MANET Based Multimedia Communications in Emergency Cases

Tipu Arvind Ramrekha and Christos Politis

Kingston University, London, KT1 2EE, UK
{a.ramrekha,c.politis}@kingston.ac.uk

Abstract. The Mobile Ad hoc Networks (MANET) is a wireless network deprived of any fixed central authoritative routing entity. It relies entirely on collaborating nodes forwarding packets from source to destination. This paper describes the design, implementation and performance evaluation of CHAMELEON, an adaptive Quality of Service (QoS) routing solution, with improved delay and jitter performances, enabling multimedia communication for MANETs in extreme emergency situations such as forest fire and terrorist attacks as defined in the PEACE[1] project. CHAMELEON is designed to adapt its routing behaviour according to the size of a MANET. The reactive Ad Hoc on-Demand Distance Vector Routing (AODV) and proactive Optimized Link State Routing (OLSR) protocols are deemed appropriate for CHAMELEON through their performance evaluation in terms of delay and jitter for different MANET sizes in a building fire emergency scenario. CHAMELEON is then implemented in NS-2 and evaluated similarly. The paper concludes with a summary of findings so far and intended future work.

Keywords: MANET, emergency communication, quality of service, wireless networks, NS-2, adaptive routing.

1 Introduction

There is a definite rise in popularity for portable wireless devices which are equipped for multimedia communication. This trend is likely to mould the next generation network architecture as described by [1] and illustrated in fig. 1, where such highly mobile wireless multimedia devices will be preponderant in society. Therefore, in such a context, the IP Multimedia Subsystem (IMS) as proposed by the 3rd Generation Partnership Project (3GPP) [2] has added importance. The IMS plans to provide facilities for possible high quality IP based multimedia communication in case of emergency scenarios. In many emergency scenarios, such as natural or manmade disasters, the rescuers will have difficulty using traditional legacy networks due to destruction or collapse of infrastructure in such events or in case of remote disaster locations, the non-existence of any cost effective means of communication.

The MANET [4] is defined as a wireless network consisting of a group of at least two wireless mobile nodes which can either communicate directly to each other

[1] PEACE is a partly funded EU project. For more info visit: http://www.ict-peace.eu/

F. Granelli et al. (Eds.): MOBILIGHT 2009, LNICST 13, pp. 74–84, 2009.

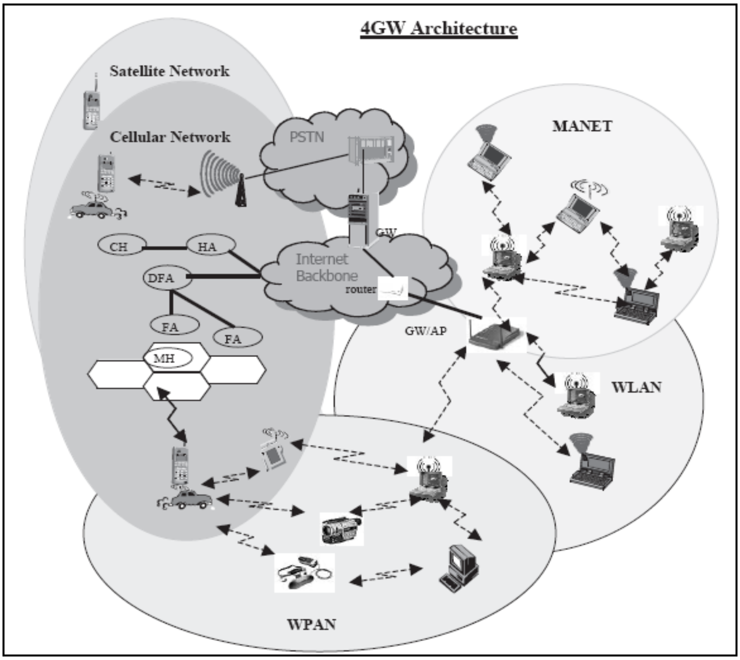

Fig. 1. Next generation network architecture illustrating the integration of *MANET* [3]

through a wireless interface or communicate through the forwarding of packets through other mobile nodes within the same group. Hence, a node in the MANET should essentially collaborate as a router of packets while also having the possibility of acting as a sender or receiver. The mobility of the nodes is a very useful feature for users but result in a very dynamic topology where routing of packets can be complex.

The nature of MANET makes it suitable to be utilised in the context of an Emergency for all rescue teams. The network layer Quality of Service (QoS) is critical for multimedia communication and encompasses several issues which need consideration [5] due to the topological dynamism of the MANET. The QoS of IP based multimedia communications can therefore be decisive in the effectiveness and efficiency of rescue missions in extreme emergency cases as described in PEACE project.

The project considers the provisioning of both day-to –day and extreme emergency communications in next generation all-IP networks. In the case of extreme emergency, it investigates the possibility for rescuers to use mobile devices such as PDAs for ad-hoc multimedia communication because in such scenarios, including natural and manmade disasters, the rescuers will have difficulty using traditional legacy networks due to destruction or collapse of infrastructure or in case of remote disaster locations, the non-existence of any cost effective means of communication.

The paper is organised as follows. In section 2, a summary of the various types of routing protocols for MANET is provided along with a small discussion on their merits. A more detailed explanation of AODV and OLSR routing protocols is provided in Section 3 together with their performance evaluation in NS-2 for a fire emergency scenario. Section 4 describes the CHAMELEON routing protocol and compares its performance against both OLSR and AODV. Finally section 5 contains conclusions from the findings in this paper and future work.

2 Background

The Internet Engineering Task Force (IETF) is responsible for the research and development of various Internet protocols and it has a working group called manet WG [6] which has the responsibility to standardise IP routing protocols for the purpose of static and dynamic MANET topologies. There are numerous categories of routing protocols which are designed for the MANET as described in [7], [3] and [4].

2.1 MANET Routing Approaches

The main MANET routing approaches are described in this section. A proactive approach is derived from the distance vector and link state routing approaches for wired internet. Each node stores a possible path to all possible destination nodes at any given time through a mixture of periodic and event triggered signalling mechanisms. A reactive approach is also described as the on-demand approach where routes are updated in MANET when required and not throughout its lifetime thus diminishing the overhead due to frequent message flooding. Then, geographical approaches use the proactive or reactive techniques described above adding geographical information to help the routing in the form of actual geographic coordinates (GPS) or relative to a fixed coordinate system. Also, the hybrid approach is an approach usually comprising of a mixture of proactivity and reactivity displayed by the routing protocol depending on certain situations.

2.2 Comparing Routing Approaches

The MANET, as described in the above sections, is a dynamic network. The approaches described above apart from the hybrid approach offer a specific solution to a possibly changing problem of routing in a dynamic topology of mobile nodes. A hybrid approach on the other hand can propose a more adaptive solution.

A reliable hybrid protocol could be constructed by using protocols which are being considered by the IETF. The Dynamic Source Routing (DSR), AODV, OLSR, and Topology Broadcast Based on Reverse-Path Forwarding (TBRPF) protocols, summarised in table 1 below, have evolved into a Request for Comment (RFC) through the IETF. However, research [8] has shown that AODV and OLSR are the two protocols which are most attractive for a hybrid solution in the case of a QoS routing solution for multimedia transmission.

Table 1. A Summary of RFC routing protocols being considered by IETF

Type	Reactive	Proactive
Source routing	DSR	OLSR
Hop-by-hop routing	TORA, AODV	DSDV, TBRF

3 Comparing AODV and OLSR

This section will investigate the performance of two routing protocols in MANET. The protocols are in the RFC stage at the IETF and therefore have the potential of developing into standardised protocols.

3.1 Ad Hoc on-Demand Distance Vector (AODV) Routing

The AODV Routing Protocol [9] provides a reactive approach towards routing. Route discovery is carried out by first sending a MANET wide broadcast request to search for the destination node and then receiving a unicast reply with the required path to the destination node. AODV nodes maintain a route table containing next hop routing information for a given destination and per hope sequence numbers nodes is stored. Each cached value in the table has an associated lifetime before expiration if unused.

3.2 Optimized Link State Routing (OLSR)

The OLSR protocol [10] is a variant of traditional link state routing for MANET. OLSR has multipoint relays (MPR) which reduces flooding and link state update overhead. Each node computes its own MPR from set of neighbouring nodes, the MPR Selectors. The MPR Selectors are the minimum set of single hop bidirectional linked neighbours that can connect the source to the maximum number of two hop bidirectional linked neighbours. They are the only nodes that rebroadcast a broadcast message from the sender. The sender also only exchange link state messages with its MPR selectors. Topology control (TC) messages are used to propagate topology information in MANET. The TC message are destined for MPR selectors only which is the only set of node advertised in the network. Nodes then accordingly rectify their routing tables through shortest path first algorithms such as refined Dijkstra's algorithms.

3.3 Emergency Scenario

The scenario considered is a fire situation in the Faculty of Computing and Information Systems (Sopwith building) at Kingston University, London and will be used for evaluating the performances of AODV, OLSR and CHAMELEON. There will be rescuers equipped with wireless multimedia transmission enabled portable devices, represented as mobile nodes, in the building for the emergency situation. The building has an area of 30m x 50m. The initial positions of the nodes are randomly distributed over the building. The movement of each node is random, but with a pre-configured speed of 1.5m/s and a maximum of 2.0m/s. They are assumed to have a pause time of 30s at random to take actions on the fire situation. The nodes start moving in random directions again after the pause and this movement pattern continues until simulation time ends. The simulations will be run for five scenario sets which include 2, 5, 10, 20, 50 and 90 who transmit both TCP and UDP packets to their colleagues i.e. a varying number of rescuers to demonstrate the reaction of routing protocols with respect to overall MANET size including traffic increase. The parameters used for simulating such an environment in NS-2 is summarised in table 2 below.

Table 2. Simulation parameters used for performance evaluation of AODV, OLSR and CHAMELEON protocols

Parameter	Value	Parameter	Value
TCP Packet Size	572 bytes	Simulation area	30m x 50m
TCP data rate	128 kbps	Data Traffic	FTP and CBR
TCP window	20	MAC trans. range	NS default for 802.11 option
TCP max. packets	10000	Simulation time	300s for 2 nodes 360s for 5, 10, 20 nodes 300s for 50, 70, 90 nodes
UDP Packet Size	512 bytes	OLSR setting	Default[11]
UDP data rate	64kbits/s	AODV setting	NS Default
UDP max. packets	10000	Mobility Model	Random
TCP Packet Size	572 bytes	Simulation area	30m x 50m
TCP data rate	128 kbps	Data Traffic	FTP and CBR

3.4 Comparative Results and Discussion

Delay performance comparison for UDP traffic link. Delay was considered on an end to end basis. The graph in fig. 2 shows that delay increases with an increase in number of nodes in the network. The OLSR protocol can be observed to have similar delay properties for the first ten nodes while its performance degrades for larger networks where the AODV protocol displays lower delay time. Also, the delay for AODV UDP packets itself decreases for number of nodes greater than 20 most probably because of non-expiry of route timeouts as described in section 2.

Jitter performance comparison for UDP traffic link. The graph in fig. 3 clearly shows that, for UDP traffic, OLSR has lower jitter magnitude than AODV for MANET sizes of less than 10 nodes while AODV is a better routing protocol for MANET sizes of more than 10 nodes. Consequently, it can be deduced from earlier results in this section that the proactive behaviour of OLSR is better than the reactive behaviour of AODV for MANET sizes of less than 10. Nevertheless, the performance of AODV is much better, for delay and jitter, for MANET sizes of more than 10. The resulting routing protocol will then be able to sustain a lower delay and jitter value irrespective of the number of nodes in such a MANET of size range between 2 and 90.

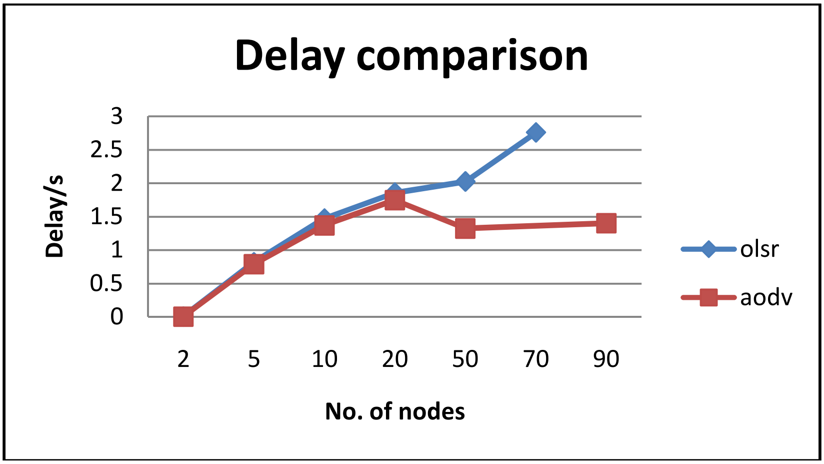

Fig. 2. Delay comparison between OLSR and AODV for varying MANET size for UDP links

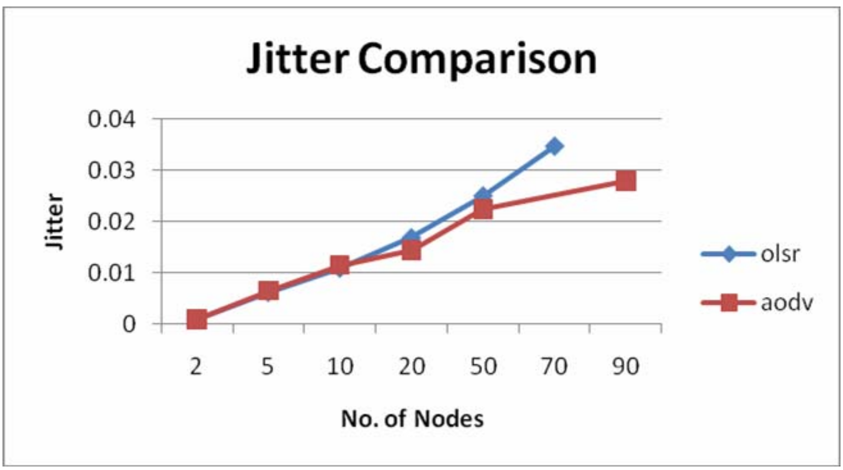

Fig. 3. Jitter comparison between OLSR and AODV for varying MANET size for UDP links

4 CHAMELEON

The CHAMELEON is a QoS routing protocol for variable size MANET in Emergency cases such as the fire situation in this paper.

4.1 CHAMELEON Algorithm

The hybrid protocol will have two modes of operations which are the proactive mode and the reactive mode. The proactive mode of operation will operate for a MANET size of up to 10 nodes and the reactive mode will operate for bigger sized MANETs

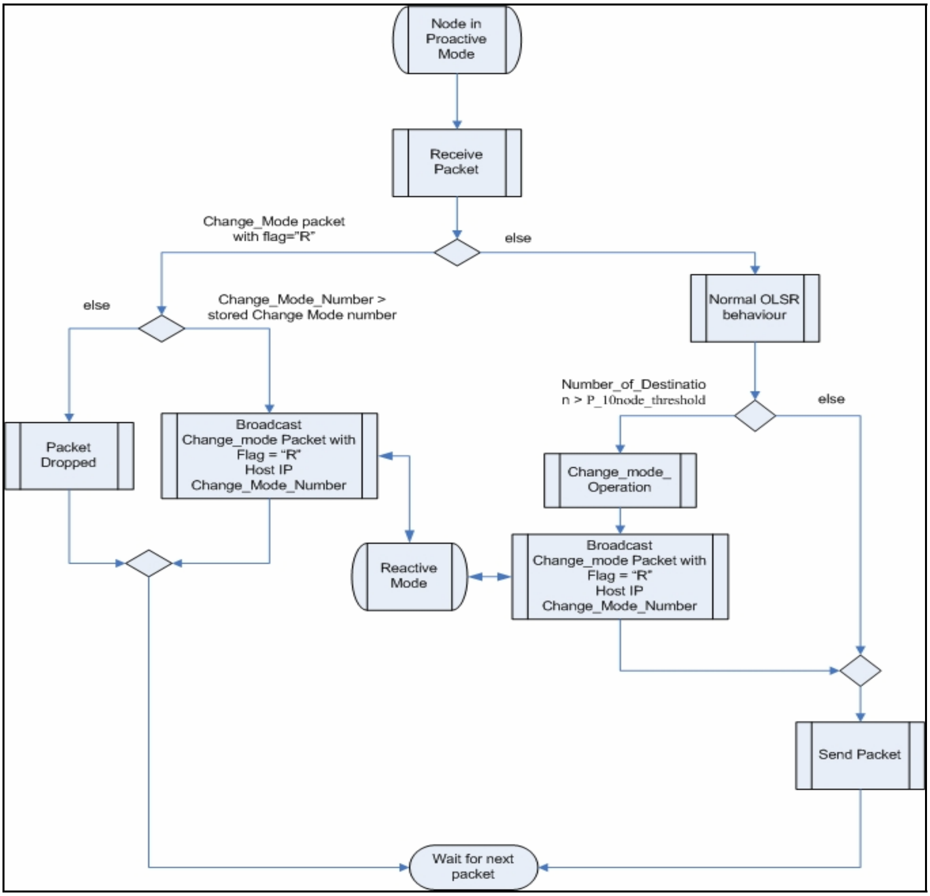

Fig. 4. CHAMELEON algorithm flowchart

of size greater than 10. The reactive mode operates in a similar fashion to OLSR with minor modifications on some features while the reactive mode operates in a similar fashion to AODV. A Change_Mode packet is introduced in the protocol. It is responsible for signalling neighbours through broadcasts that a threshold has been exceeded and behaviour has to be changed accordingly. Here, the presence of more than 10 nodes in the MANET is detected as exceeding the threshold and the protocol needs to shift from a proactive to a reactive routing behaviour as shown in fig. 4. The 10 node threshold is detected by using the P_10node_threshold value, which is equal to the value of the number of host stored in the OLSR routing tables.

A node can change to a reactive behaviour either by receiving a non-looped Change_mode packet with a flag 'R' or through detecting an exceeded P_10 node_threshold value from its routing table after computations when information from Hello and TC packets are received. The node which thus detects more than 10 nodes in the network first, broadcasts the Change_Mode_Packets which are valid for one-hop only. The Change_Mode packet is only considered in the case where the mode of operation is still proactive. The change in behaviour mode is carried out before the next packet to be sent is created to maximise efficiency. The algorithm for CHAMELEON requires that both the reactive and proactive structures are maintained simultaneously.

4.2 Results

The simulation results of CHAMELEON implemented through NS-2 and run for the same scenario as in table 2 are shown in fig. 5 for delay results and fig. 6 for jitter results respectively. It can be observed from fig. 5 below that the delay results for

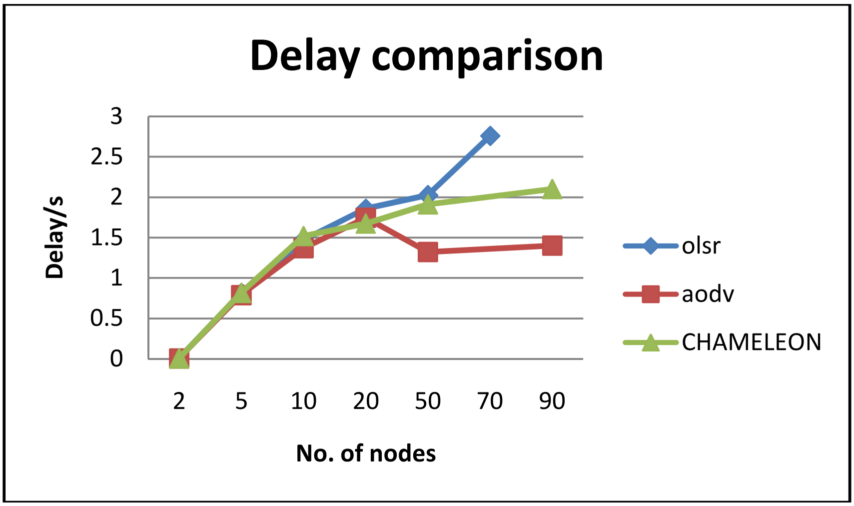

Fig. 5. Delay comparison results for CHAMELEON in UDP links for varying MANET sizes

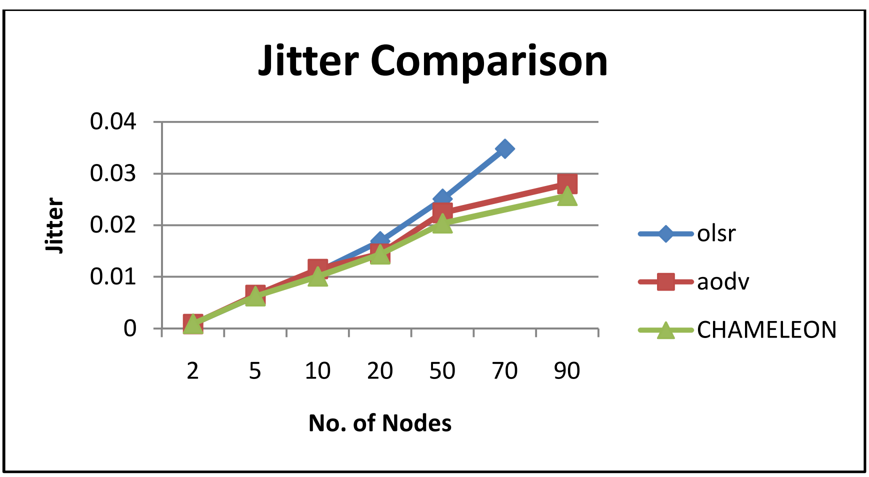

Fig. 6. Jitter comparison results for CHAMELEON in UDP links for varying MANET sizes

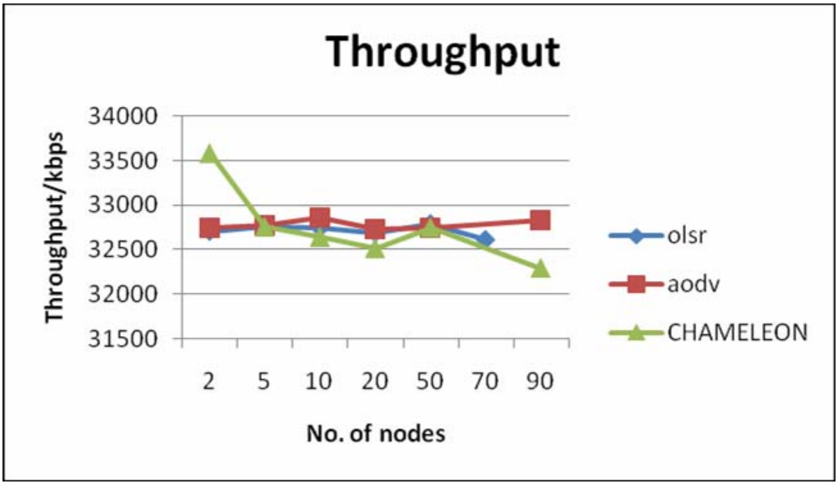

Fig. 7. Throughput comparison results for CHAMELEON in UDP links for varying MANET sizes

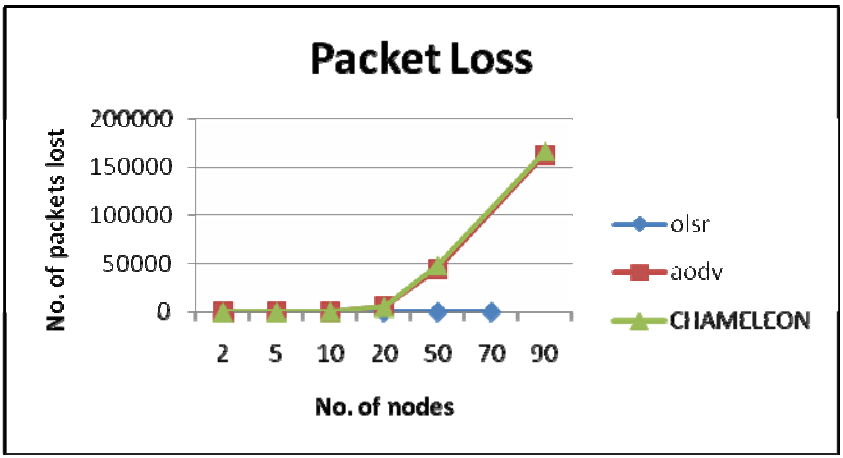

Fig. 8. Packet loss comparison results for CHAMELEON in UDP links for varying MANET sizes

CHAMELEON shows that its delay is similar to AODV and OLSR for MANET sizes of up to 10 nodes. For a MANET size of more than 10 nodes, the CHAMELEON delay is less than OLSR delay and slightly more than AODV delay. However, as shown in fig. 6 below, the jitter in CHAMELEON is less than both AODV and OLSR for the whole range of MANET size investigated.

Further results, as shown in fig. 7 demonstrate that CHAMELEON has an approximate average throughput of 32kbps. This throughput is comparable to the throughputs of both AODV and OLSR protocols and has a low variance irrespective of the number of nodes in the network. Therefore, voice over IP (VOIP) communication could be considered in such a network. Nevertheless, a codec such as ‘G.729 (A)’ would have to be used for good quality VOIP communication.

However, CHAMELEON has the disadvantage of displaying a similar trend to the AODV protocol in terms of packet losses for large networks in the case of the simulated building fire emergency scenario, as shown in fig. 8. OLSR has a relatively good performance with respect to packet losses in the same scenario. Applications enabling file transfers and using CHAMELEON or AODV for routing would therefore have bad performance as these applications require data transmission with minimal data loss.

5 Conclusion and Future Work

The findings in this paper show that a hybrid approach for providing a QoS solution for MANET routing can be beneficial. The results in section 4 show that CHAMELEON has an overall improved delay and jitter performance over both AODV and OLSR routing protocols over the range of investigated MANET sizes. The slightly greater average delay as compared to that of the AODV protocol can be explained by the fact that the CHAMELEON algorithm comprises of additional *Change_mode* packet processing time and behaviour shifting time delays. Since the performance results show improved overall delay and jitter performances, CHAMELEON can provide better QoS for multimedia communications over a larger MANET size range in case of such emergency scenarios as compared to AODV and OLSR respectively.

Future work includes the need to secure the CHAMELEON routing protocol against the risk of attacks in MANET used for emergency situations as proposed in [12]. The performance of the protocol should also be investigated for a larger set of scenarios. The algorithm for CHAMELEON can be refined to minimise processing delay so that its overall routing delay time can be decreased as compared to that of both AODV and OLSR. Also, further study on CHAMELEON could be carried out to identify the cause of packet losses and consequently measures could be derived to minimise packet loss to improve the QoS further.

Acknowledgments. The authors wish to acknowledge the support of the ICT European Research Programme and all the partners in PEACE: PDMF&C, Instituto de Telecomunicaes, FhG Fokus, University of Patra, Thales, Telefonica, CeBit.

References

1. Basagni, S., et al.: Mobile Ad Hoc Networking. Wiley-IEEE press (2004) ISBN: 978-0-471-37313-1
2. 3GPP Specification: IP Multimedia Subsystem (IMS) emergency sessions (2008), `http://www.3gpp.org/FTP/Specs/html-info/23167.htm` (accessed on July 31, 2008)
3. Mishra, A.: Security and Quality of Service in Ad Hoc Netwroks, Johns Hopkins University, United States of America. Cambridge University Press, New York (2008)
4. Conti, M., Giordano, S.: Multihop Ad Hoc Networking: The Theory. IEEE Communications Magazine 45(4), 78–86 (2007)

5. Liu, J., Chlamtac, I.: Mobile Ad-Hoc Networking with a View of 4G Wireless: Imperatives and Challenges. In: Basagni, S., Conti, M., Giordano, S. (eds.) Mobile Ad Hoc Networking, pp. 1–47. Wiley-IEEE Press, USA (2004)
6. IETF Secretariat: Mobile Ad-hoc Networks (manet) (2008), http://www.ietf.org/html.charters/manet-charter.html (accessed on July 1, 2008)
7. Belding-Royer, E.M.: Routing Approaches in Mobile Ad Hoc Networks. In: Basagni, S., Conti, M., Giordano, S. (eds.) Mobile Ad Hoc Networking, pp. 275–301. Wiley-IEEE press, USA (2004)
8. Huhtonen, A.: Comparing AODV and OLSR Routing Protocols. Seminar on Internetworking, Sjökulla, April 26-27 (2004)
9. Perkins, C.E., Royer, E.M.: The Ad Hoc On-Demand Distance Vector Protocol. In: Perkins, C.E. (ed.) Ad Hoc Networking, pp. 173–219. Addison-Wesley, Reading (2000)
10. Clausen, T., Jacquet, P., Laouiti, A., Muhlethaler, P., Qayyum, A., Viennot, L.: Optimized Link State Routing Protocol. In: Proceedings of IEEE INMI, Lahore, Pakistan (December 2001)
11. MASIMUM: Documentation and information related to UM-OLSR software (2008), http://masimum.dif.um.es/?Software:UM-OLSR (accessed on July 31, 2008)
12. Panaousis, E.A., Politis, C.: Towards Secure Ad-Hoc Communications in Extreme Emergency Case. In: WWRF/22nd meeting, May 2009, Paris (to be published) (2009)