Increasing Reliability in Large Scale Ad-hoc Networks

David Palma and Marilia Curado

Department of Informatics Engineering
Centre for Informatics and Systems
University of Coimbra (CISUC)
palma@dei.uc.pt, marilia@dei.uc.pt

Abstract. A new routing metric aimed at increasing reliability in large scale wireless ad-hoc networks is proposed and used to classify existing gateways, not only by their hop count but also by their stability and validity. Using a Deferred Routing Protocol in the performed simulations the proposed metric has 15% more traffic deliveries when compared with a simple hop count metric. These results motivate the usage of adequate routing metrics for large scale networks, as they make routing protocols more stable and reliable, allowing the spread of wireless ad-hoc networks in demanding scenarios such as emergency and rescue.

1 Introduction

The concept of creating mobile ad-hoc networks has been motivating the development of new routing protocols as well as the definition of new possible scenarios for these flexible and robust networks. However, even though the technology advances have provided a massification of wireless capable devices, ad-hoc networks are still little used [1]. One of the most focused scenarios for such networks is the disaster/rescue scenario where infra-structures may not be available thus requiring an ad-hoc network solution where all the involved authorities, for instance army, police, fire department, medical staff, can share important and critical information in real-time [2][3].

Currently there are many ad-hoc routing protocols such as the standardised Optimized Link State Routing Protocol (OLSR) [4], and the Dynamic MANET On-demand (DYMO) Routing [5], which respectively propose a proactive and reactive routing approach for managing their routing tables. Other contributions present additional routing and clustering schemes with the purpose of ensuring scalable routing. This aspect is significantly important since more and more wireless devices are expected to be used in any particular scenario, even on a daily basis [1]. Some examples of work regarding scalable routing involve the definition of clusters and hierarchies [6][7], or the modification of well known protocols such as OLSR [8].

Most of the existing schemes that target scalable routing depend on some sort of Gateway nodes which are responsible for exchanging data between different

network partitions. Often, routing protocols determine the end-to-end path, and typically there is no special concern about these nodes when they exist, being considered as any other node in the path. However, the choice of an adequate Gateway node in a path may improve the overall network performance even if it means increasing the path's length [9]. This aspect is particularly more significant if a routing protocol is not completely aware of the entire network's topology, relying on condensed routing information such as DASH [10].

This recent approach for scalable routing in ad-hoc networks will be briefly presented in the next section, motivating the definition of a new gateway routing metric suitable for Deferred Routing protocols, aiming at increased network reliability by choosing the most suitable gateways. In section 3 the performance of the proposed metric will be evaluated in a possible scenario for rescue operations. The final section summarises the results obtained from the presented work and provides insights for future work.

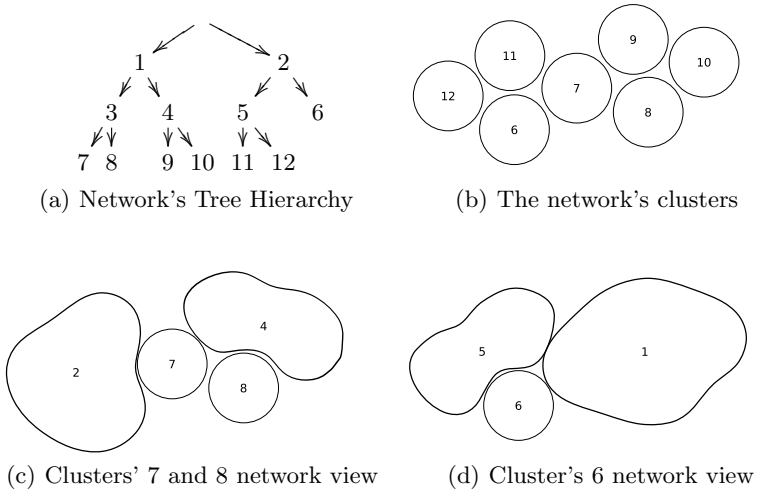
2 MATE: Metric for gAteway selecTion in dEferred routing

Maintaining consistent views of a network's routing tables is typically a challenge and failing with an appropriate routing metric to do so may result in undesirable loops [11]. Even though many approaches have been taken by different routing metrics [9][12] and protocols [4][13][5], in wireless networks, the formation of loops (despite being mainly temporary) is more common than in wired networks. This problem is much more noticeable with larger networks and specific measures have to be taken to avoid so, ensuring routing reliability.

As previously mentioned, there are several routing approaches aiming at being scalable which rely on clustering, hierarchies or, more recently, deferred routing. This last routing proposal strongly depends on an accurate and unique choice of Gateway nodes per cluster since it does not perform a path calculation throughout the existing clusters, as it will be explained in the following section.

2.1 Understanding Deferred Routing

The most common clustered routing approaches maintain information about all the clusters and the existing paths to reach such clusters. However, this still incurs large overheads and thus, a new approach where routing is Deferred to each cluster, has been proposed [10]. This approach only keeps information about the gateways capable of reaching each cluster and the number of "Cluster Hops" to do so (the actual number of node hops is not maintained since it is a large amount of volatile information which is not frequently necessary). Similarly to a post office, the postman responsible for delivering a letter, only does so until a specific point of his working area. He leaves the letter in specific points, depending whether it is a local, regional or international delivery, and is completely unaware of how to reach the final destination, since it will be someone else's job, closer to the final destination, to do so. Deferred Routing follows the



(a) Network's Tree Hierarchy (b) The network's clusters

(c) Clusters' 7 and 8 network view (d) Cluster's 6 network view

Fig. 1. Possible network perspectives for tree hierarchy (a), (c) and (d)

same approach as the mail delivering process, the most significant difference being the fact that no specific delivery points (Gateways) are previously defined, thus requiring an efficient solution to choose the most suitable one.

In routing, the most common metric used for determining paths is the "hop count" metric, where the shortest path is usually the most suitable one. Even though Deferred Routing does not consider path calculation from source to destination, the required number of "Cluster Hops" from end to end could be used in order to choose the most suitable Gateway. However, due to information aggregation in a large scale network, several gateways may have the exact same number of "Cluster Hops" thus leading to possible ambiguous views of the routing tables, resulting in network loops. This motivates the development of a new routing protocol capable of increasing routing reliability for Deferred Routing Protocols, which still lack such a solution.

2.2 The DASH protocol

The DASH routing protocol stands for Deferred Aggregated routing for Scalable ad-Hoc networks, where the wireless ad-hoc network is organised into a tree hierarchy of clusters, identified by their context. This protocol follows the Deferred Routing paradigm performing similarly to typical routing protocols within clusters, and postponing inter-cluster routing decisions to neighbour clusters closer to the destination. This behaviour mimics the postman's job previously described, and it further uses a virtual cluster aggregation scheme, using different network perspectives, allowing the DASH protocol to maintain its routing overhead very small. A possible network perspective when using DASH is depicted in figure 2.2,

where clusters with the identifications 7 and 8 (cluster IDs), as siblings have the same network perspective, and are unaware of clusters 9 and 10, which are seen as cluster 4, and of the remaining clusters, since they are hierarchically distant, and are only seen as cluster 1. Following the post office and postman paradigm, in DASH, a node within a cluster, just like the postman, knows how to deliver a packet to a destination in its working area (i.e. its cluster), other packets are forwarded to Gateway nodes, which on their turn handle the packet to nodes in clusters "closer" to the destination node, until the destination's cluster is reached.

In the DASH protocol, a node is considered a Gateway when it is able to reach other contexts (or clusters), announcing it to the other nodes within its own cluster. The Gateway nodes, by "overhearing" their neighbours' routing information also consider themselves indirect Gateways to clusters which they are not neighbours with, increasing their Cluster Hop Count connectivity by one. Such approach allows DASH's nodes to choose the necessary nodes to reach other clusters, but lacks a robust scheme to guarantee that this choice is not ambiguous between nodes within the same cluster. This aspect was previously mentioned regarding Deferred Routing, as the propagation of Gateway information in a large scale network is prone to delays and lost routing packets, leading to routing inconsistencies and poor reliability.

By defining a new routing metric which complements the number of cluster hops with additional and relevant information, more reliable and consensual network views could be achieved. Focusing on DASH and consequently on Deferred Routing, the choice of a suitable Gateway throughout different clusters should consider using the most stable gateway and take into account the reliability of the existing information. These two aspects can easily be obtained from the existing gateways in the network. The "age" of a gateway is a property that reflects how stable a node is as gateway, being more stable for each epoch as gateway (i.e. every time a gateway node's information is updated/refreshed, its age increases). In addition to this information, it is important to be aware of how valid the existing information is, since when a node receives information about a gateway, it may be about to expire or it might just have been sent.

Taking into account the number of "Cluster Hops", a gateway's "age" and the validity of the existing information, which may be more or less up-to-date, a suitable metric for reliable routing may be derived.

2.3 The Proposed Gateway Metric, MATE

As previously mentioned, a routing metric capable of handling the number of "Cluster Hops", a gateway's "age" and the validity of such information would allow robust routing in large scale networks. However, in addition to the three defined parameters, it is also important to understand what they represent and how they can be used simultaneously. For instance, considering the number of cluster hops, one may infer that the difference between 2 and 3 hops is more significant than the difference between 12 and 13 hops, depending on the network size. Instead of having a linear function for the number of hops, the difference

between the number of hops may be mapped to a sigmoid function with a predefined threshold hop_{th}. The hop parcel (hop_{par}) of the metric is defined in equation 1.

$$hop_{par} = \frac{1}{1+e^{hop_{th}-x}} \tag{1}$$

The "age" of a gateway may be representative of its stability, nevertheless, when comparing two gateways, their age difference must be correctly understood, just like for the number of cluster hops. This property depends on the number of refreshes/updates that a node receives from a neighbour node in a different cluster, increasing its age by 1 for each advertisement. Consequently, a gateway with an age of 3, is still "young" but it should represent more stability than another gateway with less age. However, when considering "older" Gateways, the difference between their ages should not be so representative since they have been already stable for a long period of time, such that two Gateways with an age of 40 and 43 will have a similar stability factor. This behaviour can be represented by the metric's age parcel, in equation 2. A routing protocol which also considers stability is presented in [14], where route stability is considered above the path hop count. Despite using different metrics for link stability, this protocol still suffers from typical on-demand protocols disadvantages such as flooding and path retrieval delays, not being suitable for large-scale networks.

$$age_{par} = \frac{1}{\sqrt{x}} \tag{2}$$

Common routing protocols keep the gathered network information for a limited amount of time, and rely on updates to this information such that it does not expire. Generally speaking, the most recent information should reflect the most up-to-date perspective of the network, however, due to network delays, newly created information may not have been propagated throughout the entire network, creating inconsistencies. In order to avoid this, information "validity" should be analysed taking into account its expiration time. To achieve this behaviour, the expiration time should be modelled into a function, such that at the threshold $validity_{th}$ represents the most valid information. Moreover, since time is continuous and it is not desirable that minor differences in time produce different results, the expiration time should also be considered as a discrete variable. The corresponding part of the metric which concerns validity is shown in equation 3.

$$val_{par} = \frac{((MAX_{expiry}-validity_{th})-x)^2}{(MAX_{expiry}-validity_{th})^2} \tag{3}$$

The weighted function of these three parameters, each one mapped to an adequate function of its own, should produce a relevant metric capable of providing consistent views of routing tables in large scale networks, even when using deferred routing which only maintains limited information, as presented in

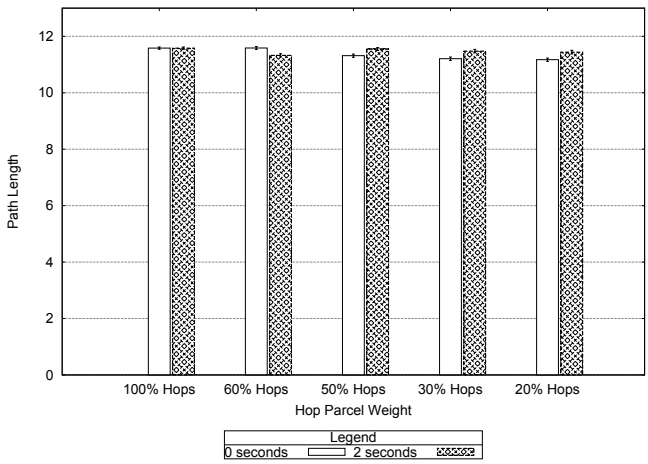


Fig. 2. Average Path Length

equation 4. The maximum value for the metric will be 1, representing the worst possible value for a gateway.

$$MATE = w_{hop} \times hop_{par} + w_{age} \times age_{par} + w_{val} \times val_{par} \tag{4}$$

Furthermore, the metric can be adjusted to specific networks by changing $w_{hop}, w_{age}, w_{val}$ weights, as well as by tweaking the existing thresholds, tuning the results according to the existing scenarios. In the following section a plausible rescue scenario is simulated using different weights for the concerned parameters.

3 Performance Evaluation

In order to properly evaluate the quality of MATE and how it affects the performance of a Deferred Routing Protocol, several simulations were performed varying the different parameters of the routing metric. A large scale network of 312 wireless nodes was used to represent a possible rescue scenario with two main working rescue teams. In order to address typical large scale routing protocols, the network was divided into 8 clusters of 39 nodes each, assuming that a single team is composed of 4 clusters, allowing it to cover a significant disaster area.

The used Deferred Routing Protocol was DASH [10], and the Cluster IDs were defined according to the teams' contexts, such that the DASH protocol's capabilities were fully used. The rescue teams in the scenario were disposed in the shape of a "V", as if there was an obstacle separating them, for instance in a tunnel, where debris force rescue teams to be separated. In order to simulate the possible data traffic used by rescue teams, 2 Constant Bit Rate (CBR) video flows were established in each team (with a total of 4 video flows), where the

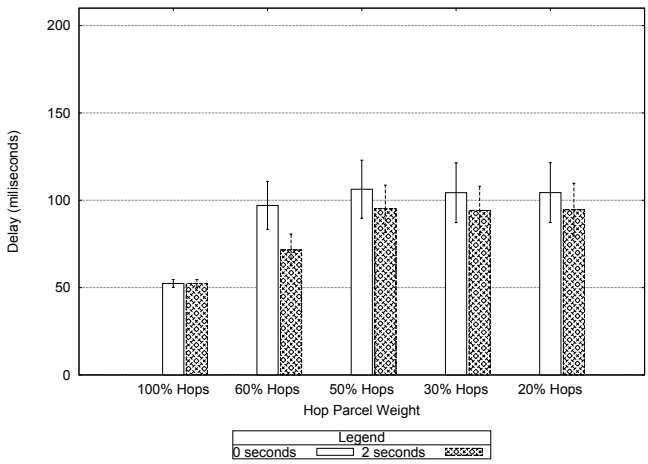


Fig. 3. Average End-to-end Delay

source nodes were in the front of the rescue team, reporting visual data to the control centre, which is set in the back, such that the destination nodes are as far as possible from the source. Each video flow had a CBR of 200kbit/s, which should be more than enough to establish a video-conference between source and destination [15], allowing the rescue teams to send video images to the control centre and to receive detailed information on how to proceed in critical situations which might require step-by-step instructions from experts (for instance medical assistance).

All the presented results are for the DASH protocol with and without the MATE metric, in order to correctly assess the contribution of this work, comparing both performances. No other routing protocols are shown in the given results as they would not be related with the metric subject, but with the routing approach followed by DASH. However, some experiments using the OLSR protocol revealed much more routing traffic (up to 50 times more), and worst traffic delivery.

3.1 Simulation Results

The simulations were ran in the OPNET Modeler Wireless Simulator [16], with a total of 30 runs per scenario, always using different seed values and the Linear-Congruential Random Number Generator Algorithm. Moreover, all the presented graphs show a 95% confidence interval for the results, obtained from the central limit theorem which states that, regardless of a random variable's actual distribution, as the number of samples (i.e. runs) grows larger, the random variable has a distribution that approaches that of a normal random variable with mean m, the same mean as the random variable itself. All the wireless

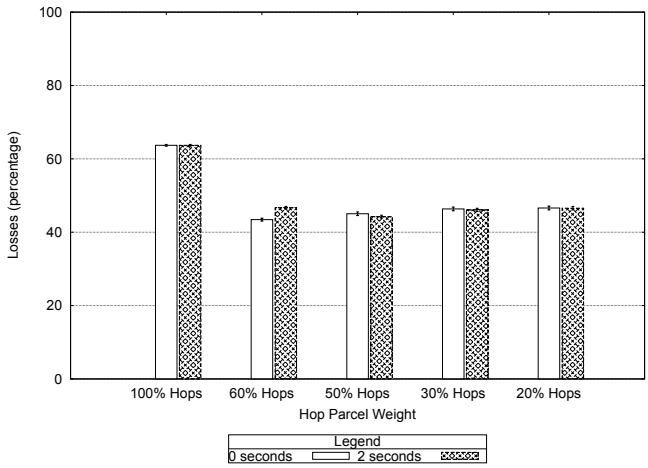


Fig. 4. Average Percentage of Traffic Losses

nodes follow the IEEE 802.11g standard [17], having a range of 30 meters which should correspond to a realistic range of common wireless cards [18][19].

The following results show the network performance regarding different parameters. To avoid any interference of specific mobility patterns, all the nodes are static. Regarding the hop and validity thresholds ($hop_{th}, validity_{th}$), the hop threshold was kept fixed in all simulations (4 hops) and the validity threshold was set to 0 and 2 seconds in order to understand how the propagation of information may influence the network's reliability. All the results will show the obtained performance when the weight of the number of hops is changed in the metric. The weight of the information's validity is always set to 20% and the gateway's age weight will correspond to the remaining between the other two parameters. In the results, the column corresponding to 100% weight reflects the typically used hop count metric (i.e. ignores the proposed metric).

Path Length One important aspect to be verified in the MATE approach, is the used number of hops from source to destination (i.e. path length). Figure 2 presents the results obtained, showing that there is no significant differences between all the shown variations of the metric, not even when compared with the typical hop count metric. This certainly motivates further results since MATE has at least the same performance as the hop count metric in the only aspect that this last one is aimed to.

Average Delay The registered end-to-end delay is depicted in figure 3, where the only existing difference, which is not very significant, occurs between the paths used by the hop count metric and the ones provided by MATE. At a glance it might seem that the suggested metric has a worse performance, however, these results can easily be explained by analysing them in conjunction with the

Table 1. Traffic Losses with Mobility

Mobility	Metric	
losses	Hop	MATE
%	82%	69%

Table 2. Traffic Losses for different size packets

Packet Size	Metric	
(bits)	Hop	MATE
1000	24%	6%
2000	31%	18%
4000	37%	23%

percentage of traffic losses. Since the hop count metric has less delivered traffic, the network is less congestioned thus having a smaller delay. When comparing the results obtained with the proposed metric, there is a noticeable difference between the results with a validity threshold of 0 and 2 seconds, showing a smaller delay for the latter, probably due to a valid gateway choice.

Traffic Losses When considering the amount of traffic losses, shown in figure 4, it is clear that there are many. This may indicate that an ad-hoc network with the given configuration may not be suitable to handle such demanding traffic flows. However, similarly to the previously analysed results, the only significant difference between the given variations of the metric is for a 100% hop weight, which has a 15% worse performance when compared to the results obtained with the new metric. Even though the remaining results do not present a major difference between themselves, the best performance was achieved with a hop weight of 60% with 0 seconds attributed to the validity threshold.

Complementary Results Further results were obtained for the same scenario previously presented, using the Random Waypoint Model as the default mobility pattern for each node, inside its cluster. The node's speed uniformly varies from 0 up to 10 meters per second, suitable for human or vehicle movement, and where a pause time of 100 seconds is set. These results are depicted in table 1, revealing that by using the metric with 60% weight for the hop parameter, the obtained losses decrease by 13% when compared to a typical hop count metric, sustaining the same results previously registered without mobility.

Moreover, even though the DASH protocol's specification is out of the scope of this work, the significant traffic losses raised some questions about its efficiency. Thus, extra simulations were performed to analyse the reason of the obtained losses. A preliminary analysis revealed losses mainly due to the wireless physical layer, presenting a large number of dropped packets as a result of consistently failed retransmissions.

In order to ensure that the above results depend mainly on the wireless technology, additional simulations were performed using CBRs of 100kbit/s with smaller packets of 1 and 2 kbit at a rate of 100 and 50 packets per second respectively. These results are presented in Table 2. Additionally, new simulations using a higher retransmission threshold, while keeping the 4bkit packets and CBRs of 200kbit/s as in the performance evaluation, confirm that almost every registered losses were technology dependent and not related with routing problems, since the number of losses significantly reduces. Also, these results reinforce that MATE can effectively improve large scale networks' reliability.

4 Conclusion

A new routing metric focused on improving routing in large scale ad-hoc networks, MATE, has been proposed. This metric combines not only the hop count, but also stability and validity of gateway nodes within clusters. The performance improvement of using the MATE approach has been demonstrated by simulating a large rescue operation scenario, where a routing Deferred Scheme, the DASH protocol, was used to perform routing decisions. When comparing the choice of a gateway by simply using the typical hop count metric against the proposed metric, it is possible to see that an improvement of 15% regarding traffic delivery is achieved by using also stability and validity parameters. These results contribute to further motivate the deployment of ad-hoc networks in challenging scenarios, showing that the usage of an appropriate routing metric focused on a robust routing protocol can improve the overall performance.

In this work a static ad-hoc network was mainly used, in order to avoid the interference of mobility models' specific patterns. However, some preliminary results with mobile nodes were also obtained, suggesting that, in a future work, it would be interesting to analyse how the tuning of the metric could improve the network's performance in different mobility scenarios, as well as with a different number of nodes. Moreover, future results could benefit from the usage of more appropriate traffic flows, according to specific applications focused on the used scenario.

Acknowledgement

This work was supported by the Portuguese National Foundation for Science and Technology (FCT) through a PhD Scholarship (SFRH / BD / 43790 / 2008) and by the National Project MORFEU. The authors would like to thank the OPNET University Program for the licenses provided for the OPNET Modeler Wireless Suite®.

References

1. Cimmino, A., Donadio, P.: Overall requirements for global information multimedia communication village 10th strategic workshop. Wireless Personal Communications **49**(3) (May 2009) 311–319

2. Sugiyama, H., Tsujioka, T., Murata, M.: Integrated operations of multi-robot rescue system with ad hoc networking. In: Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology, 2009. Wireless VITAE 2009. 1st International Conference on. (may 2009) 535 –539
3. Khoukhi, L., Cherkaoui, S., Gaiti, D.: Managing rescue and relief operations using wireless mobile ad hoc technology, the best way? In: Local Computer Networks, 2009. LCN 2009. IEEE 34th Conference on. (oct. 2009) 708 –713
4. Clausen, T., Jacquet, P.: Optimized link state routing protocol (olsr). RFC 3626, Internet Engineering Task Force (October 2003)
5. Chakeres, Perkins, C.: Dynamic manet on-demand (dymo) routing. Work in progress, internet-draft, Internet Engineering Task Force (March 2010)
6. Villasenor-Gonzalez, L., Ge, Y., Lament, L.: HOLSR: a hierarchical proactive routing mechanism for mobile ad hoc networks. Communications Magazine, IEEE **43**(7) (2005) 118–125
7. Eriksson, J., Faloutsos, M., Krishnamurthy, S.V.: Dart: Dynamic address routing for scalable ad hoc and mesh networks. Networking, IEEE/ACM Transactions on **15** (2007) 119–132
8. Canourgues, L., Lephay, J., Soyer, L., Beylot, A.: A scalable adaptation of the OLSR protocol for large clustered mobile ad hoc networks. Advances in Ad Hoc Networking (2008)
9. Zhou, Y., Chung, S.H., Yang, L., jin Choi, H.: A link-quality aware routing metric for multi-hop wireless network. In: Communication Software and Networks, 2009. ICCSN '09. International Conference on. (February 2009) 390 –394
10. Palma, D., Curado, M.: DASH, deferred aggregated routing for scalable ad-hoc networks. Submited to MSWiM'10, The 13-th International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems 2010 (2010)
11. Yang, Y., Wang, J.: Design guidelines for routing metrics in multihop wireless networks. In: INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. (April 2008) 1615 –1623
12. Rahman, M., Azad, M., Anwar, F.: Intergating multiple metrics to improve the performance of a routing protocol over wireless mesh networks. In: 2009 International Conference on Signal Processing Systems. (may 2009) 784 –787
13. Perkins, C.E., Belding-Royer, E.M., Das, S.R.: Ad hoc on-demand distance vector (aodv) routing. RFC Experimental 3561, Internet Engineering Task Force (July 2003)
14. Toh, C.K.: A novel distributed routing protocol to support ad hoc mobile computing. In: Proc. IEEE 15th Annual International Phoenix Conference on Computers and Communications, IEEE IPCCC 1996, March 27-29, Phoenix, AZ, USA, IEEE, IEEE (March 1996) 480–486
15. On2 Technologies, I.: On2's truemotion vp7 video codec. White paper, On2's (July 2008)
16. OPNET Technologies, I.: Opnet simulator http://www.opnet.com/.
17. Ortiz, S.: IEEE 802.11n: The road ahead. IEEE Computer **42**(7) (2009) 13–15
18. Anastasi, G., Borgia, E., Conti, M., Gregori, E.: Wi-fi in ad hoc mode: A measurement study. Pervasive Computing and Communications, IEEE International Conference on (2004) 145
19. Xing, B., Seada, K., Venkatasubramanian, N.: An experimental study on wi-fi ad-hoc mode for mobile device-to-device video delivery. In: INFOCOM Workshops 2009, IEEE. (April 2009) 1 –6