QoS Ad Hoc Routing Protocol Analysis in Civil Safety Context

Sylwia Romaszko, Jean Carle

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

QoS Ad Hoc Routing Protocol Analysis in Civil Safety Context

Sylwia A. ROMASZKO — Jean CARLE

N° 7358

Juillet 2010

ISSN 0249-6399 ISRN INRIA/RR--7358--FR+ENG

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA

centre de recherche
LILLE - NORD EUROPE

QoS Ad Hoc Routing Protocol Analysis in Civil Safety Context

Sylwia A. Romaszko, Jean Carle

Theme :
Équipes-Projets POPS

Rapport de recherche n° 7358 — Juillet 2010 — 7 pages

Abstract: In this paper, we have conducted an investigation of quality of service (QoS) approaches supporting a ad hoc routing protocol in civil safety context. We have proposed different schemes of the QoS path selection among multiple paths in order to find the most suitable in our context. We analyze an influence of the route path information and per-hop information. This performance analysis shows us which method is adequate in civil safety environment.

Key-words: ad hoc networks, routing protocol, civil safety environnement

Centre de recherche INRIA Lille – Nord Europe
Parc Scientifique de la Haute Borne
40, avenue Halley, 59650 Villeneuve d'Ascq
Téléphone : +33 3 59 57 78 00 — Télécopie : +33 3 59 57 78 50

Analyse de protocole de routage ad hoc avec QoS pour la sécurité civile

Résumé : Dans cet article, nous menons une étude sur les approches qualité de service (QoS) sur les protocoles de routage en réseau ad hoc dans le contexte de la sécurité civile. Nous proposons différentes méthodes de sélection de chemins pour trouver le plus adapté à notre contexte. Nous analysons l'influence d'une recherche de route par la source ou par sauts. Cette étude des performances nous montre quelle est la méthode la plus adaptée à un environnement pour la sécurité civile.

Mots-clés : réseaux ad hoc, protocole de routage, sécurité civil

QoS Ad Hoc Routing Protocol Analysis in Civil Safety Context

Sylwia Romaszko, Jean Carle
IRCICA/LIFL University of Lille 1
CNRS UMR 8022, INRIA Lille - Nord Europe, France
Email: {first name.name}@lifl.fr

***Abstract*— In this paper, we have conducted an investigation of quality of service (QoS) approaches supporting a routing protocol in civil safety context. We have proposed different schemes of the QoS path selection among multiple paths in order to find the most suitable in our context. We analyze an influence of the route path information and per-hop information. This performance analysis shows us which method is adequate in civil safety environment.**

I. Introduction

This work is performed within a project that focuses on heterogeneous networks in the context of civil safety. Such network contains mobile and static nodes. Some nodes have the ability to monitor the environment and some so-called *sink* nodes forward data outside the network. Such networks could be used in a safety operation context e.g. a fireman uses radio systems and sensors to monitor its human biological constant by remote systems allowing the leader to be informed of his health or firemen could put sensors for environmental monitoring like temperature changes, presence of toxic gases or even detecting life in a building fully covered by smoke. In our context, we have a mobile ad hoc network with some sensor networking capacity. In this context, this paper focuses on a quality of service analysis.

The remainder of the paper is organized as follows. In Section II, we define the problem, explanation of our choice and we described the foundations of our research, and related work. In Section III, we describe our QoS methods. In Section IV, performance evaluation is presented. Finally, concluding remarks are formulated in the last section.

II. Problem definition and foundations

In the previous work [6], we have searched an answer which reactive routing protocol behaves the best in the civil safety context. In this context, we often need multimedia streams such as audio, video and sensing capacity. We have selected three different approaches, namely, on-demand routing method where the AODV routing scheme [1] is chosen as the reference, the Gradient protocol [2] design for use in sensor networks, and the cluster based method created in order to perform this analysis. We have concluded that AODV protocol outperforms other schemes in different scenarios where having static or mobile nodes and multiple sinks. Therefore, we took this approach as a reference in this paper, adapting it to the protocol considering QoS requirements. Here, we point out that the existing QoS-AODV [3][4] has completely different approach and assumptions than our scheme. In the existing QoS-AODV the quality of service requirements enables only the route, which satisfies, thus RREQ is not rebroadcasted if it is not a case. This also means that if there is no route which guarantee QoS the data cannot be send. In our context this is unacceptable, since when a fireman wants to send a data message, the message must be send via any existing route but it will be the best when this route meets the best (while selecting from multiple routes) QoS requirements; if there is no route which guarantees QoS, the data must be sent anyway.

In the next section, we highlight the main concepts of the origin AODV approach. In order to compare different QoS path selection approaches to choose a multi-constrained path, we have decided to choose an approach that is already used in a number real systems, namely, Enhanced Interior Gateway Routing Protocol (EIGRP) CISCO method [7], which we present in the last section II-B of this chapter.

A. AODV protocol

In AODV (Ad hoc On Demand Distance Vector) protocol [1], when a source S requires to send a message to a destination node D, a route discovery process is initiated by broadcasting a route request (RREQ). Each intermediate node temporarily records the 1-hop information about this communication in its routing table. When the destination is found, a route reply message (RREP) is sent back (unicast mode) to S. RREP can be sent by the destination directly, or by an intermediate node if the destination node is already registered in its routing table. In any case, each node receiving the RREP enables the route for a fixed time, allowing data to be forwarded between S and D. If another RREP is received, then the path information is updated accordingly. When a node detects a link failure, it sends a route error message (RERR) back to the source.

B. CISCO method

Enhanced Interior Gateway Routing Protocol (EIGRP) considers the minimum bandwidth on the path to a destination and the total delay in order to compute QoS routing metrics. Other metrics can be also configured, however this is not recommended by Cisco, since it causes routing loops in the network [7]. EIGRP determines the total metric of the network using this formula: $metric = [K_1 * bandwidth + \frac{(K_2 * bandwidth)}{(256 - load)} + K_3 * delay] * [\frac{K_5}{(reliability + K_4)}]$, where K_n

$(1 \leq n \leq 5)$ values must be planned carefully in order to avoid that the network fails to converge, and other values must be scaled first. The default K_n values are: $K1 = K3 = 1$, and $K2 = K4 = K5 = 0$, hence simplified formula:

$$metric = bandwidth + delay \quad (1)$$

Let us analyze an example depicted in Fig. 1. If gateway **one** is estimating the best path to Network A, it checks the route via *four* (with 56Kb minimum bandwidth and 2200 μs total delay) and via *three* (with 128 Kb minimum bandwidth and 1200 μs delay). Gateway **one** selects the path with the *lowest*

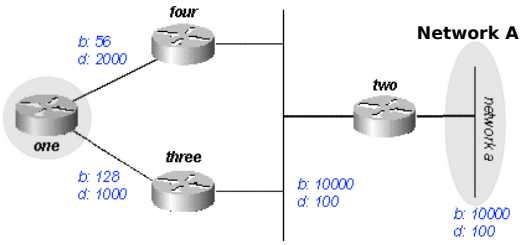

Fig. 1. EIGRP example [7]

computed metric. To do this, first of all, the bandwidth and delay metrics must be scaled by using the following formulas: $bandwidth = (\frac{10000000}{bandwidth(i)}) * 256$, where $bandwidth(i)$ is the lowest bandwidth of all outgoing interfaces on the route to the destination network, $delay = delay(i) * 256$, where $delay(i)$ is the sum of the delays configured on the interfaces on the route to the destination network.

According to the Formula (1), the total cost through gateway **three** is $(\frac{10000000}{128} + 1200) * 256 = 20307200$ (note, that floating point math is not performed, a result at each stage rounds down to the nearest integer) and the total cost through gateway **four** is $(\frac{10000000}{56} + 2200) * 256 = 46277376$. Since the computed metric of the route through gateway **three** is lower than that of gateway four, gateway one chooses this route.

III. Quality of Service Algorithm/s

The quality of service extension added to the existing AODV protocol has a goal to keep multiple paths with QoS information in the routing table in order to choose the most optimal path if possible. The discovery stage is partly affected by this extension. From one side, no QoS requirements are maintained in the request control message. From another side, replies are sent via the faster route in order to reach an originator as soon as possible and they also maintain QoS information. RREP messages can contain information about the minimum available bandwidth on the route to originator of RREQ, available bandwidth, latency, and bit error rate of the route (from source to destination). Depending on the QoS selection path method (see section III-A), some information are not used/kept in RREP message (see details later), e.g.: if we just use the Cisco method, described in the previous section, RREP maintains the minimum available bandwidth and the route latency only.

A. Guidelines of QoS path selection

There are different approaches designed in order to search the most optimal path. In this section, just the guidelines of possible choices are shortly given, where in the next sections details about the whole process can be found. Figure 2 depicts different possible schemes for QoS data path selection. In

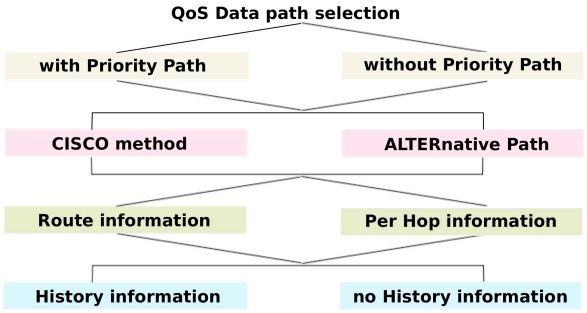

Fig. 2. QoS Data path selection tree

the first place, the priority path (PP) option can be chosen, thus, whether nodes maintain and consider the given priority ('voice', 'video', 'data') for the path. Unlike it is done in QoS-AODV [3], no QoS requirements are maintained in the RREQ message, we do not specify in the message which maximum or minimum value of QoS constraint we need. In RREQ, we keep information only about the priority we will need to send a data message with. Hence, we are searching the path, which can satisfy the minimum/maximum tolerable QoS requirements for transmitting either 'voice', or 'video' or 'data' packet. The bandwidth, latency and Bit Error Rate (BER) criteria are taken into account while selecting the link priority. In order to collect this information, RREP must contain statistics about these three metrics, and of course the number of hops to destination. Table I shows maximum/minimum required (tolerable) values of bandwidth, latency and BER for particular type of traffic. These values can be changed depending on the application or scenario we need.

TABLE I

Min/Max required values for multimedia traffic

Traffic	Bandwidth	Latency	BER
Voice	64 kb	300 ms	10^{-3}
Video	512 kb	300 ms	10^{-5}
Data	12 kb	NA	10^{-9}

If, either the priority path (PP) is chosen but no adequate priority path found, or no priority path is chosen, then the aforementioned Cisco method or ALTERnative path algorithm (ALTER) are executed (see section III-C). Both methods can rely on, either route information (from source to destination), or per hop (one-hop) information. Finally, this information can be, either instantaneous only, or taking the history into account.

Since nodes maintain multiple paths to the same destination, nodes can send RREP based on, either the *shortest route*, or the route with the *lowest latency*, or the *Hops-Latency*

(HL) algorithm is executed deciding whether to choose the path with the shortest route or with the lowest latency. When latency must be taken into account the history information or instantaneous information are considered.

Depending on the chosen algorithm different information regarding the needs is maintained in the routing table, likewise different information is attached to control messages. When choosing the PP option in the first stage, the local metrics information must be kept and forwarded in the RREP packet; otherwise only one-hop information is needed, so no extra QoS information must be inserted to RREPs. If the Cisco method is chosen in the second stage, then only the minimum available bandwidth and the route latency must be added to the RREP packet. In case of the ALTERpath selection algorithm the chosen local metrics (details in the next section) must be placed in replies. Naturally all route information does not need to be added to RREP packets if the Cisco or ALTER methods are executed with 'Per Hop information' choice.

B. Routing table information, updates and processing

Each node maintains a routing table with the ordinary AODV routing information, local metrics information. Depending on the used scheme (section III-A) additional information could be kept: priority information of the active routes and 1-hop priority information, Cisco estimations of the active routes and 1-hop connections. In order to update the local information, each node in a network is exchanging *Hello* messages as in the ordinary AODV [1]. However, in our protocol/s, upon reception of a *Hello* message, nodes estimate local metrics and update their routing table information, also concerning the priority to the next hop and the Cisco estimations (if applicable). Upon reception of control packets, likewise data messages, the routing table information is also updated. If a node is not the intended next hop of the reply message, or this message has been already processed, the message is rejected without any updates.

Taking into account that our QoS schemes keep multiple paths in the routing table, there is a need for an additional mechanism taking care of cleaning and updating the routing table entries. A limit must be defined indicating the maximum number of paths to the same destination, called *paths threshold*. If a new path is discovered (upon reception of a packet) and the maximum number of paths to this destination has reached the paths threshold, the *worst path* to this destination must be removed first in order to add a new fresh one.

In order to find the worst path the *FindTheWorstPath* function is processed. First, the activation of the path is verified. If there is one path inactive and others are active, the inactive route is pronounced as the worst and it is removed from the table. If two paths are inactive or no path is inactive the expiration time is checked. The path with the shortest expiration time is removed from the table. This way oldest routes are removed first when there is a new route discovered and the number of routes to the particular destination reached the paths threshold.

In our approach nodes do not discard any messages as it happens in QoS-AODV [3]. If a node which received RREQ, has a path to the destination, however it does not provide the required priority (if checking the link priority is applicable), the node answers anyway with adequate information (e.g., available bandwidth, latency, BER) about the route to the destination. After receiving RREP/s the originator of RREQ estimates and decides which route is the most optimal (although it can happen that neither of them guarantees QoS) according to the QoS algorithm and it transmits a data packet. Each node forwarding data can decide which route to the destination is the most optimal according to the QoS algorithm. It can happen that although the originator had no path with a right priority, one of the forwarders has meanwhile learned about such route. Finally, although the originator had no QoS guarantee for this data packet, the packet may reach the destination meeting QoS constraints. Since nodes can maintain multiple paths to the source and to the destination the forwarder of the data message can change a "fate" of so-called "data packet without QoS guarantee".

We distinguish two different parts of QoS extension: selecting the best possible route for data packets, and selecting the best possible path for the reply (RREP) packet. These parts will be explained now.

C. Selection the most optimal path for DATA

While a source or a forwarder node must transmit a data packet and knows multiple routes, it processes the intelligent QoS algorithm first if the priority path (PP) option was chosen in the first stage. We say 'intelligent' since when the PP method does not satisfy the QoS constraints or there are found more paths with the required priority, the algorithm tries to search the best possible path.

In the *first step* the priority of the path is checked to know if it exists any route with a right priority (thus, either 'voice' or 'video' or 'data') according to the simple IF-ELSE rules (with regard to min/max required values from Tab. I) for the voice, video, data:

$$\textbf{if } (BER < BER_{voice}) \textbf{ and } (LAT < LAT_{voice}) \textbf{ and } (BD > BD_{voice}) \quad priority = p_{voice}; \tag{2}$$

$$\textbf{if } (BER < BER_{video}) \textbf{ and } (LAT < LAT_{video}) \textbf{ and } (BD > BD_{video}) \quad priority = p_{video}; \tag{3}$$

$$\textbf{if } (BER < BER_{data} \textbf{ and } BD > BD_{data}) \quad priority = p_{data}; \tag{4}$$

where BD is bandwidth, LAT latency, and $p_{\{voice,\, video,\, \text{or}\, data\}}$ represents particular link priority.

If there is one of such paths with the required priority, then the node transmits the data packet via this route (next hop on this route). If there are two or more such paths with the right priority, then in the second step the Cisco algorithm (Section II-B) is executed to choose the most optimal one (among the 'priority' paths found in the first step), thus the minimum available bandwidth on the route, and latency of whole route are taken into account.

If, either there is no path with the right priority, or the PP method was not chosen, two different approaches can be

executed (second step): the Cisco algorithm (used as above) or the algorithm searching the alternative path (ALTERnative path algorithm) based on the most important metric for this required priority link. We assume that the latency is the most important metric for 'voice' packet, the bandwidth is the most important metric for the 'video' packets, and finally the BER is the most important metric for 'data' packet.
There is also considered the possibility that multiple paths can have the same 'main' value (first the most important metric), then ALTER is processed again (third step) but with the use of the second most important metric value which is, bandwidth for 'voice', latency for 'video', and bandwidth for 'data'. Depending on the required priority, the needed local information metrics must be added to RREP messages (information about available bandwidth and latency in case of 'voice' and 'video' link priority, and BER and bandwidth information in case of 'data' link priority).

D. Selection the fastest path for RREP

When sending RREP message, the originator or forwarders execute the ALTER algorithm in order to find the most optimal path for this control packet. Here, the most optimal means the fastest path in order to inform the RREQ originator about existing path to the destination. Thus, either having the smallest number of hops to the source, or the shortest latency. The idea behind is to adjust the algorithm to the civil safety context, where a prompt answer can be very precious. ALTER is based on, either the number of hops to the source, or the latency, or the Hops-Latency (HL) algorithm. The HL algorithm estimates whether a difference in the latency between the path chosen based on the number of hops ('hops path') and the path chosen based on the shortest latency ('latency path') is significant; If it is the case, the latency of the 'hops path' is much larger than latency of the 'latency path' (difference is larger than the predefined threshold), then the 'latency path' is chosen, otherwise the 'hops path' is chosen.
When selecting a path, the second step is executed while it occurs that there are two paths to the source with the same number of hops or the same latency. In this step ALTER is processed again based on the 'second metric', which is the latency if the number of hops was the first metric (in the first step), or the number of hops if the latency was the first metric. This way, we make sure that the path is not chosen randomly, only based on estimations.

IV. Performance evaluation

The AODV protocol and all quality of service approaches have been implemented and compared under the Mobility Framework 2 (MF) [9] in the OMNET++ version 4 network simulator [8]. The following performance metrics are used: *ratio of total number of data packets received over data sent (R/S ratio), the number of packets received that met QoS requirements, ratio of the number of data packet received that met QoS requirements over the total number of data packets received (we call it 'priority path' performance), total number of control messages sent, average aggregate goodput and latency obtained by all sinks*. We defined the latency as the time between the sending of the data by the source and its arrival at the final destination, in respect to the number of samples, thus $\frac{Latency_i \ Samples_i}{\sum Samples_i}$. There is no way of knowing the bandwidth, therefore, we measure the goodput to estimate the bandwidth. The goodput is specified as the number of bytes received over the time spent to transmit this packet in respect to the number of samples, thus $\frac{Throughput_i \ Samples_i}{\sum Samples_i}$.
Tab. II shows the general parameters used in simulations. We

TABLE II
SIMULATIONS PARAMETERS

Parameter	Values
txPower	350 m
Payload size (bytes)	4608
Sending interval (ms)	0.0703125
MAC bitrate (bps)	10485760
MAC layer	Dummy with queue=10 pkts
HL threshold	0.01
paths threshold	1 *(AODV)*, 2, 3
Hello interval (s)	1
Allowed Hello Loss (s)	2

have defined a scenario in a 1000×1000 m^2 area with 20 static nodes and 4 sinks. The 4 sinks are placed in the corners of the area. The area is split in 4 equal squares, nodes are randomly deployed, 5 in each square. The nodes-sources from each square are sending packets to the farthest sink, so the top-left nodes are sending to the sink which lies in the bottom-right corner (top-left corner) , etc.
In this paper, we show simulations for static networks only (not enough place here for mobile scenarios). We aim to analyze the behavior and an importance of some settings in a network without mobility. All the nodes are sources sending to the farthest sinks (in the opposite square of the area) thus, traffic load is high, nodes need to keep a lot of information in the routing table, which from one side could be advantageous but too much information is not so good as well. In this simulation, the active route time-out (ART) is set to 3 seconds as defined by default in the AODV protocol.
Fig. 3 depicts the total number of packets received ("RCVD") by the sinks. In this figure, "PP" represents selection of the

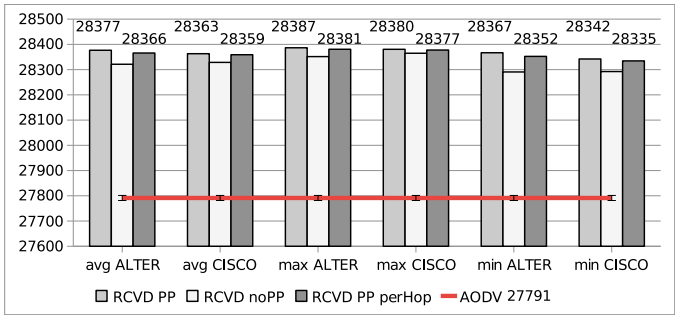

Fig. 3. Total number packets received; 20 static nodes and 4 sinks

priority path option, where "noPP" means that the Cisco or ALTER algorithm is executed at once. By the default

the schemes use the route information, otherwise, "perHop" comment added. The bars depict the QoS methods, where the line shows the AODV performance. Moreover, the bars show the *average* performance, the *best* performance ("MAX") and the *worst* performance ("MIN") of the Cisco and ALTER method. The average, best and worst performance consider the performance of intermediate average performances with different settings (2 or 3 multiple paths, history or only instantaneous information, and selection of either 'hops path', or 'latency path' or HL algorithm).

The figure shows that using any of QoS method lets to receive much more packets than using AODV: AODV receives 27791 packets whereas all other compared schemes receive more than 28300 packets. This observation is not surprising, since having multiple paths nodes do not waste time to send requests and the number of errors messages is significantly decreased as well (QoS schemes send around 65% less error packets RERR). Notice, that without PP choice the number of total packets received is degraded, whereas the route or per hop information does not really change the performance. However, if we look at Fig. 4 showing the number packets received by the sinks with the required QoS constraints ("pRCVD"), we can notice that using just per hop information can be advantageous. Notice,

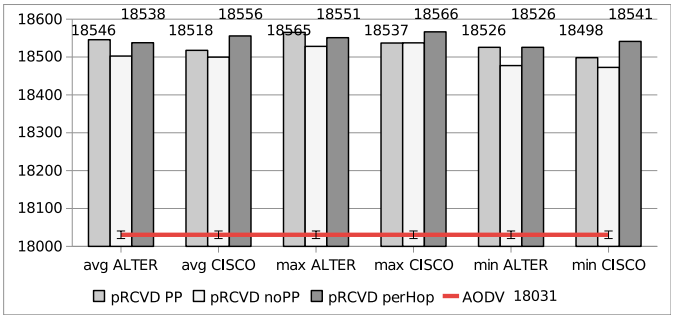

Fig. 4. Packets received with the required priority; 20 nodes and 4 sinks

the number of 'priority' packets received by AODV (18031) is much less than that received by QoS schemes (more than 18500), even while we analyze only the minimum performance of QoS schemes. The PP choice in the first step of Data route selection is noticeable advantageous in a static scenario.

Analyzing the individual performance of each scheme, we observe that while using PP, both the ALTER algorithm and the Cisco, perform the best having 3 multiple paths based on the information without history, and using the HL algorithm while searching the best path for RREP; whereas the ALTER scheme has slightly better performance than the Cisco method. ALTER receives a total of 28400 packets, where 18585 met the QoS requirements, while Cisco receives more packets (28385) in total, but fewer (18529) are satisfying the QoS constraints. Moreover, ALTER sends much less control packets (2314) than Cisco (2658). It is interesting to add that the general aggregate Cisco goodput reaches 1582 Kbps, where ALTER obtains 1568 Kbps (where latency performance is similar), which means that Cisco chooses more paths with higher bandwidth than ALTER.

Moreover, we see again that using the PP option in the first step improves the performance. Observe, that Cisco using only per hop information obtains the best 'priority path' performance (0.6549 receiving, whereas for AODV is 0.6488). However, the general aggregate goodput performance is degraded till 1425 Kbps. The route or per hop information has less influence on the ALTER method, since the 'priority path' is slightly increased, whereas, the general aggregate goodput performance slightly decreased (till 1548.5 Kbps). However, while using per hop information, both ALTER and CISCO act better while using 'hops' paths for RREPs.

General analysis of different settings: the number of multiple paths (2 and 3 simulated), history information, and the scheme chosen for RREPs, shows that, the choice of 3 paths increases R/S ratio for both methods (ALTER and Cisco), decreases latency increasing goodput, and naturally decreases the number of control packets. With respect to the 'priority path' performance the Cisco follows the patron, where ALTER performs better with 2 multiple paths. We can also observe that history information has no high importance, but we point out here, that we did not take into account EWMA (Exponential Weighted Mean Average) which we will be part of our future analysis.

ACKNOWLEDGMENT

This work was supported by a grant from French National Research Agency RISC.

V. CONCLUSION

In this paper we have investigated quality of service approaches supporting a routing protocol in civil safety context. We have proposed different schemes of the QoS path selection among multiple paths in order to find the most suitable in our context. Simulations show that QoS schemes can increase the packet delivery performance but also packets received with QoS guarantee, decreasing overhead significantly.

REFERENCES

[1] C. Perkins, E. Royer and S. Das *RFC 3561 – Ad hoc On-Demand Distance Vector (AODV) Routing*, Nokia Research Center, University of California, University of Cincinnati, July 2003.

[2] F. Khadar and T. Razafindralambo, *Performance Evaluation of Gradient Routing Strategies for Wireless Sensor Networks*, Proc. IFIP Networking 2009, Aachen, Germany, 2009.

[3] C. Perkins, E. Royer, and S. Das, *Quality of Service for Ad hoc On-Demand Vector Routing, draft-ietf-manet-aodvqos-00.txt*, Mobile Ad Hoc Networking Working Group, Internet Draft, July 2000.

[4] J. Mungara, S.-P. Setti, and G. Vasanth, *New Model for Quality of Service in Mobile Ad Hoc Network*, International Journal of Computer Science and Network Security (IJCSNS), Vol. 9 No. 12, Dec. 2009.

[5] N.I.Md Enzai, F. Anwar, and O. Mahmoud, *Evaluation study of QoS-enabled AODV*, International Conference on Computer and Communication Engineering, Malaysia, May 2008.

[6] S. Romaszko, J. Carle, and F. Nolot, *Ad hoc Routing Protocol Analysis in Civil Safety Context*, IFIP Mediterranean Ad Hoc Networking workshop (Med-Hoc-Net 2010), Juan-les-Pins, France, June 2010.

[7] Cisco Systems, Inc. http://www.cisco.com

[8] The OMNeT++ modular, component-based C++ simulation library and framework: http://www.omnetpp.org

[9] Mobility Framework (MF) for OMNeT++: http://mobility-fw.sourceforge.net

Centre de recherche INRIA Lille – Nord Europe
Parc Scientifique de la Haute Borne - 40, avenue Halley - 59650 Villeneuve d'Ascq (France)

Centre de recherche INRIA Bordeaux – Sud Ouest : Domaine Universitaire - 351, cours de la Libération - 33405 Talence Cedex
Centre de recherche INRIA Grenoble – Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier
Centre de recherche INRIA Nancy – Grand Est : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex
Centre de recherche INRIA Paris – Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex
Centre de recherche INRIA Rennes – Bretagne Atlantique : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex
Centre de recherche INRIA Saclay – Île-de-France : Parc Orsay Université - ZAC des Vignes : 4, rue Jacques Monod - 91893 Orsay Cedex
Centre de recherche INRIA Sophia Antipolis – Méditerranée : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399