Improving Performance on Mobile Ad hoc Networks by Using Proxy Service

G. E. RIZOS
University of Peloponnese
Department of Computer Science and Technology
GR-221 00 Tripolis GREECE
georizos@uop.gr

D. C. VASILIADIS
University of Peloponnese
Department of Computer Science and Technology
GR-221 00 Tripolis GREECE
dvas@uop.gr

E. STERGIOY
ATEI of Epirus
GR-471 00 Arta GREECE
ster@teiep.gr

Abstract: In this paper, we present the role of proxy service in a MANET environment. MANET is specifically characterized by high mobility of network nodes and frequent changes of direct visibility. High dynamicity affects the design and implementation of distributed applications by significantly increasing their complexity, to consider not only routing and node configuration issues, but also the possible mobility of software components and the loss of direct connectivity during service provisioning. The proxy role is assigned dynamically in a completely decentralized way. Proxies exploit code mobility to install only when and where needed. In this work, we estimate and compare the performance of routing protocols for ad-hoc networks, namely Ad Hoc On-Demand Distance Vector protocol (AODV) and Dynamic Source Routing (DSR). We use the file transfer protocol to measure the performance of our model. The protocol provides file downloading from a dynamically discovered service component available in a MANET locality, even if the server moves during file transfer

Keywords: Mobile Ad Hoc Networks (MANET), routing protocols, AODV, DSR, Service PROXY, file transfer protocol.

1. Introduction

Wireless systems have recently become more and more popular, mainly because of their offered capability of supporting continuous mobility while accessing services. The spreading of wireless solutions is significantly changing also the way to conceive and design distributed services. On the one hand, the new features introduced by the wireless network infrastructure suggest application developers to create location-aware services [1].

In a wireless network, all nodes are not always within transmission range. The hidden node and the exposed node are two problems that are solved with a collision avoidance mechanism and figure 1 illustrates the problems.

The *hidden terminal* problem occurs because the radio network, as opposed to other networks, such as a LAN, for instance, does not guarantee high degree of connectivity. Thus, two nodes, which maintain connectivity to a third node, do not, necessarily, can hear each other.

In general, the *hidden terminal* problem reduces the capacity of a network due to increasing the number of collisions, while the *exposed terminal* problem reduces the network capacity due to the unnecessarily deferring nodes from transmitting.

On the other hand, the necessity of rapid, flexible and temporary connections between heterogeneous wireless devices is motivating the research for Mobile Ad hoc Networks (MANET). Any node in a MANET can move at any time; therefore, topological variations force the continuous reorganization of the network, which must occur in an autonomous, spontaneous and transparent way [2]. MANET's are capable of operating without infrastructure support, because each node is autonomous and can collaborate with the others to enable information delivery.

The term "ad hoc" could mean different things in different contexts. The common meaning within the network community is that this term refers to a multi-hop wireless network. In 802.11 vocabularies ad hoc refers to the lack of infrastructure, allowing direct communication between stations. Mobile ad hoc network (MANET) [3] is another term defining a network that may operate in isolation or may have a gateway to a fixed network.

The rest of the paper is organized as follows. In section 2 an overview of Mobile Ad Hoc Networks is presented. Section 3 outlines the Routing Protocols for Ad Hoc Networks and section 4 the related work. Section 5 presents the network model and section 6 the design of our model and section 7 performance analysis results. Finally, in section 8 conclusions are drawn.

2. Mobile Ad Hoc Networks: Overview

MANET identify a specific type of wireless network without requiring any kind of statically deployed support infrastructure, but permitting any node autonomy and cooperation to service delivery by forwarding messages along multi-hop paths.

An ad hoc network is a small network without any fixed network infrastructure. They often have wireless or temporary plug-in connections. In Latin, ad hoc literally means "for this", further meaning "for this purpose only". Ad hoc networks are formed when two or more units (hosts) are in proximity of each other. Two ad hoc networks may also merge to become one at any time, and one ad hoc network may partition into two. Ad hoc networks require multi-hop routing (using routing algorithms such as AODV or DSR). Multi-hop routing is necessary since the participating devices in these networks have limited coverage areas and in order to reach a node (not in direct proximity) multiple network hops are required. In a mobile ad hoc network each unit acts as a router, forwarding packets to other units. No central administration is necessary to establish a working ad hoc network, since all participating units help one another.

The characteristics of a mobile ad hoc network (MANET) are the lack of fixed and wired network infrastructure. Static IP addresses, used in the traditional client-server model, are inconvenient to use in a MANET because of the dynamic network topology. The mobile hosts in a MANET can dynamically join or leave the network at any time, and units can move from one network domain to another. The joining and leaving is both due to user control and/or to user movement outside the radio signal coverage. This means that the network connectivity can be suddenly and intermittently stopped. Examples of devices that can be used in a MANET are cellular phones, PDAs (Personal Digital Assistant) etc. Such devices have limited resources considering available main memory, mass memory, CPU speed and battery power, and therefore the resources need to be used as effectively as possible. Furthermore the bandwidth is typically smaller than the bandwidth available in fixed networks [4, 30].

MANET is based upon autonomy and fast deployment, at the cost of continuous re-organizations due to frequent and unpredictable node movements. MANET applications can be profitably deployed in several different environments, from hostile grounds/disaster-recovering scenarios where a network infrastructure typically does not exist or has been destroyed (military and search-and-rescue operations), to contexts where the rapidity of the network deployment process is paramount (during a conference in a convention hall). It is possible to identify three different classes of MANET, with different degrees of complexity, by considering the physical dimensions and the number of participating nodes: sensor networks are low power, low range, and suit simple monitoring operations, e.g., on buildings and transportation structures [4]; Bluetooth-based MANET are small and quite static networks, also identified as Personal Area Networks (PAN), designed mainly to let printers and cell phones communicate when in direct and mutual visibility range [5]; IEEE 802.11-based MANET can consist of a large number of nodes, even geographically distributed, and generally widen to support multi-hop path routing [6].

To handle routing in wireless multi-hop networks, specific routing protocols are developed. They are classified as either proactive (table driven) or reactive (on demand) protocols. The proactive protocols maintain a route table at each node in the same manner as fixed network routing protocols (e.g. RIP, OSPF) [7, 8]. An example is the Destination-Sequence Distance-Vector (DSDV) [9] routing protocol that lists the available destinations and their hop counts. DSDV transmits routing updates periodically and based on events and uses sequence number for preventing routing loops. Another example of proactive routing is the Cluster Switch Gateway Routing (CSGR) [10] protocol that adds a hierarchical structure to DSDV with cluster heads forming a wireless backbone. Optimized Link State Routing (OLSR) [11] reduces the flooding overhead in the route update process by introducing multipoint relays (MPRs). MPRs are selected nodes which generate and forward the updates. A MPR may choose to report only links between itself and its selected MPRs.

The reactive routing protocols have an advantage of not having the overhead of periodically routing updates. This leads on the other hand to the need for a route discovery process. In the process route requests (RREQ) are broadcast throughout the network and the destination answers with a route reply (RREP) as illustrated by figure 2.

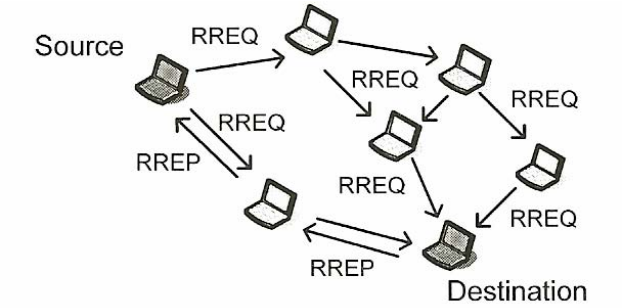

Fig.2. AODV reactive routing with route discovery

Dynamic Source Routing (DSR) [12] is an on-demand protocol that uses source routes for each destination. The route discovery process requires intermediate nodes to attach their address before rebroadcasting the RREQ. The destinations RREP could use the reverse route of the RREQ or be piggybacked on a new RREQ broadcast for the source. Promiscuous listening enables route caching and route shortening. Ad Hoc On-Demand Distance Vector (AODV) [13] is a distance vector protocol that establishes reverse routes in the route discovery process. A RREP is unicast back to the source creating the forwarding route towards the destination. The RREP could be sent from the destination or, if allowed by the source, from an intermediate node having a route to the destination.

3. Routing Protocols for Ad Hoc Networks

Traditionally, the network routing protocols could be divided into *proactive protocols* and *reactive* protocols. Proactive protocols continuously learn the topology of the network by exchanging topological information among the network nodes. Thus, when there is a need for a route to a destination, such route information is available immediately.

The main issue with the application of proactive protocols to the ad hoc networking environment stems from the fact, that as the topology continuously changes, the cost of updating the topological information may be prohibitively high. Moreover, if the network activity is low, the information about the actual topology is may even not be used and the investment of limited transmission and computing resources in maintaining the topology is lost.

On the other "end of the spectrum" are the *reactive* routing protocols, which are based on some type of "query-reply" dialog. Reactive protocols do not attempt to continuously maintain the up-to-date topology of the network. Rather, when the need arises, a reactive protocol invokes a procedure to find a route to the destination; such a procedure involves some sort of flooding the network with the route query. As such, such protocols are often also referred to as *on demand.*

Examples of reactive protocols include the Temporally Ordered Routing Algorithm (TORA) the *Dynamic Source Routing (DSR)* and *Ad hoc On Demand Distance Vector (AODV)* [13]. In *TORA*, the route replies use controlled flooding to distribute the routing information through a form of a Directed Acyclic Graph (DAG), which is rooted at the destination. The DSR and the AODV protocols, on the other hand, use unicast to route the reply back to the source of the routing query, along the reverse path of the query packet. The reversed path is "inscribed" into the query packet as "accumulated" route in the DSR and is used for source routing. In AODV, the path information is stored as the "next hop" within the nodes on the path. Although the reactive approach can lead to less control traffic, as compared with proactive Distance Vector or Link State schemes, in particular when the network activity is low and the topological changes frequent, the amount of traffic is can still be significant at times. Moreover, due to the network-wide flooding, the delay associated with reactive route discovery may be considerable as well.

3.1.1 Ad Hoc On-Demand Distance Vector Routing (AODV)

Ad hoc On-demand Distance Vector Routing (AODV) is an improvement algorithm of DSDV designed for wireless networks. To send a message, the data source initiates a path-discovery process in order to find the route. The route request packet (REQ) is flooded to the network and the intermediate nodes record the neighbour from which they get the REQ first, in order to establish reverse paths back to the source. When the REQ arrives at the destination, it then sends back a route reply (REP) to the source following those reverse paths. AODV needs symmetric links; otherwise the REP may not be able to reach the source and AODV would fail.

AODV [13] incorporates the destination sequence number technique of *Destination-Sequenced Distance-Vector Routing (DSDV)* routing into an on-demand protocol. (DSDV is discussed in the sequel.)

Each node keeps a next-hop routing table containing the destinations to which it currently has a route.

A route expires if it is not used or reactivated for a threshold amount of time. If a source has no route

to a destination, it broadcasts a route request (RREQ) packet using an *expanding ring search* procedure, starting from a small Time-To-Live value (maximum hop count) for the RREQ, and increasing it if the destination is not found. The RREQ contains the last seen sequence number of the destination, as well as the source node's current sequence number. Any node that receives the RREQ updates its next-hop table entries with respect to the source node. A node that has a route to the destination with a higher sequence number than the one specified in the RREQ unicasts a route reply (RREP) packet back to the source. Upon receiving the RREP packet, each intermediate node along the RREP routes updates its next-hop table entries with respect to the destination node, dropping the redundant RREP packets and those RREP packets with a lower destination sequence number than one previously seen.

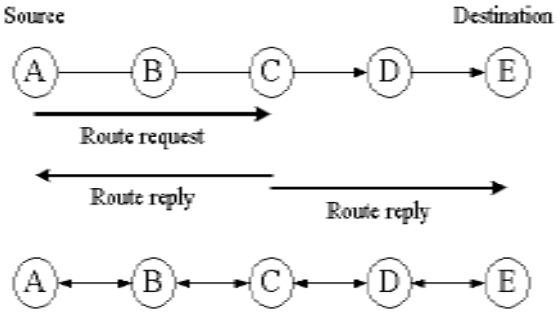

Fig.3. AODV protocol

When an intermediate node discovers a broken link in an active route, it broadcasts a route error (RERR) packet to its neighbors, which in turn propagate the RERR packet up-stream towards all nodes that have an active route using the broken link. The affected source can then re-initiate route discovery if the route is still needed.

*3.1.2 Dynamic Source Routing (*DSR*)*

Dynamic Source Routing (DSR) eliminates the symmetric-link assumption held in AODV. When a sender has a message to send, a REQ is generated and flooded into the network. DSR is different from AODV, which records the route in the intermediate nodes, in that it holds all the route information in the REP packet. When the REQ arrive at the destination, the latter then has the whole route information from the source to the destination. The destination then floods another packet, the REP message, into the network. REP carries two bits of information, the REQ received by the destination and the route information thus far. When this REP arrives to the source node, the source will have both the whole route to the destination (carried by REQ) and the route from the destination back to the source (carried by REP).

DSR [14] is a source routing on-demand protocol with various efficiency improvements.

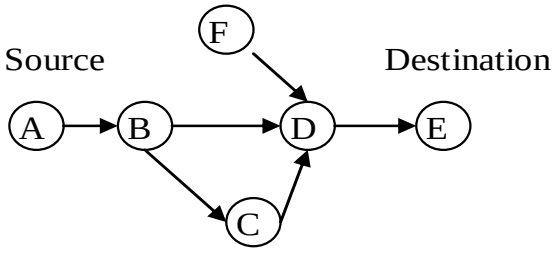

Fig.4. DSR protocol

In DSR, each node keeps a *route cache* that contains full paths to known destinations. If a source has no route to a destination, it broadcasts a route request packet to its neighbors. Any node receiving the route request packet and without a route to the destination appends it's own ID to the packet and re-broadcasts the packet. If a node receiving the route request packet has a route to the destination, the node replies to the source with a concatenation of the path from the source to itself and the path from itself to the destination. If the node already has a route to the source, the route reply packet will be sent over that route. Otherwise, depending on the underlining assumption of the directionality of links, the route reply packet can be sent over the reversed source-to-node path, or piggy-backed in the node's route request packet for the source.

When an intermediate node discovers a broken link in an active route, it sends a route error packet to the source, which may re-initiate route discovery if an alternate route is not available.

DSR makes very aggressive use of source routing and route caching. It does not require any mechanism for detecting routing loops. Additionally forwarding nodes cache the source routes found in forwarded packets for possible future usage. The authors of the protocol have proposed additional optimizations, which they have evaluated and found them to be effective. These optimizations are described in [19] and are, in brief:

(i) *Salvaging*: An intermediate node can use an alternate route from its own cache, when a data packet meets a failed link on its source route.

(ii) *Gratuitous route repair*: A source node receiving a RERR packet piggybacks the RERR in the following RREQ. This helps clean up the caches

of other nodes in the network that may have the failed link in one of the cached source routes.

(iii) *Promiscuous listening*: When a node overhears a packet not addressed to itself, it checks if the packet could be routed via itself to gain a shorter route. If so, the node sends a *gratuitous* RREP to the source of the route with this new, better route. Aside from this, promiscuous listening helps a node to learn different routes without directly participating in the routing process.

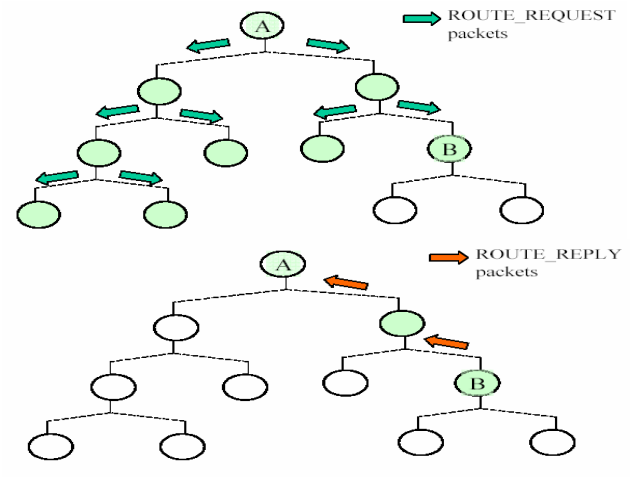

Fig.5. Multicasting Protocol DSR

DSR has efficiency improving features. One of such features is the *promiscuous* mode, in which a node listens to route request, reply, or error messages not intended to itself and updates its route cache correspondingly. Another DSR feature is the *expanding ring search* procedure, in which the route request packets are sent with a maximum hop count, which can be increased if the destination is not found within the hop-count limit. Finally, adding *jitter* in sending the route reply messages to prevent *route reply storms* and *packet salvaging* to extract correct routes from route error packets are yet two other features that improve DSR performance.

4. Related Work

From the point of view of multi-hop routing protocols, several recent proposals have presented original solutions. If two MANET nodes, not in direct communication range, need to exchange messages, they have to rely on the forwarding ability of nodes located in the intermediate area. Several aspects make this forwarding problem hard to solve effectively in MANET: the dynamic topology makes most traditional routing algorithms not applicable; assigning the router role to any MANET node, although apparently natural in this context, may put an intolerable computational burden on unprepared devices; the wireless propagation implies undefined coverage areas that dynamically change, and the available bandwidth is limited, also because of possibly high error rates due to interferences [11].

In [12], different possible aspects to consider when providing taxonomy of MANET routing protocols have been identified: which routing information is exchanged, when and how this information is exchanged, when and how routing paths are built. Here we propose to combine principles suggested by different researches ([16], [17], [18], [19], [20], [21]), to classify routing solutions in position-based ones, which exploit the knowledge about the geographic localization of the receiver, and topology-based ones, which consider the network as a link sequence. The latter can be split up in table-driven, on-demand and hybrid approaches.

Among topology-based solutions, traditional table-driven protocols (distance vector and link state families of algorithms) have demonstrated to be inefficient due to the low bandwidth and the frequent topology changes typical of MANET. On-demand protocols create a route only when 4 required by the source node. The communication requires a first phase in which the sender has to find a route to the destination; while topology conditions are considered unchanged; the calculated route is maintained valid. Hybrid protocols [15], instead, take advantage of traditional table-driven routing schemes into local communication contexts, and combine them with on-demand solutions for non-local routing.

5. The model

Figure 6 shows a service model for ad hoc users. The service of proxy that is implemented in an ad hoc gateway indicates the available services provided by the access networks to ad hoc users. A service client of an ad hoc user associates with the service of proxy in order to use the IP services in the access networks.

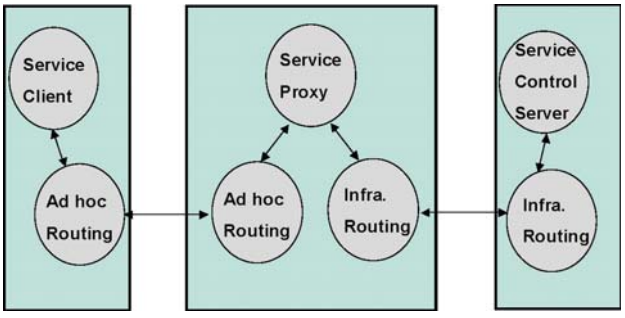

Fig.6. A service-model: Client-Proxy-Server

We use a model based on a couple of MANET localities with a few nodes (IEEE 802.11b-compliant portable devices that exploit the WiFi ad hoc connectivity mode). To better evaluate the behaviour of the system under actual operating conditions, we have deployed it over two different types of devices, Hp laptops and iPAQ PDAs. The multi-hop message delivery was obtained by employing a routing protocol AODV first and then the routing protocol DSR, implemented on the Linux kernel.

6. The design

Consider the usual scenario where a server, responsible for service delivery inside a MANET locality, i.e., the local PAN consisting of all the nodes in direct network visibility, suddenly and transparently leaves the locality during the service session. In this situation, the clients in the locality have to reorganize to reach the server independently of its movement, and to continue service session seamlessly. Depending on service implementation, the clients could either look for another equivalent server (if the provided service is stateless or the session state is maintained at the client side and exchanged at the server re-connection), or search for exactly the same server instance that left the locality (if the service is stateful and the state is exclusively stored at the server side).

When a server leaves a locality, the provided services would become immediately unavailable for all currently served clients. When the servers possibly move, the model tries to exploits client/server location visibility to reorganize the locality via the dynamic election of a proxy agent.

The proxy takes care of searching servers by need, of forwarding client requests, and of performing multihop routing it permits to organize solutions for client/server rebinding and service reestablishment that are scalable and mobility-transparent.

Once the proxy finds the server, the proxy starts forwarding service requests/responses from/to interested clients. In other words, all service messages are automatically and transparently sent through the proxy, acting as a bridge between the clients and the server.

The introduction of a support proxy in a MANET locality, where we cannot assume the availability of any static infrastructure, is possible only if the proxy is conceived as a totally dynamic role, assigned to one of the local clients in a completely distributed and decentralized way.

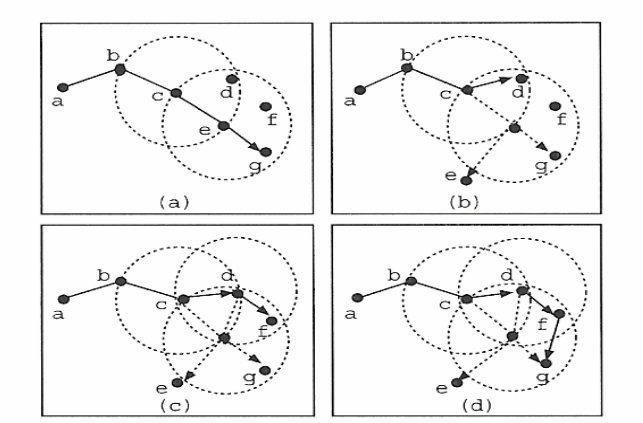

Fig.7. File transferring through the proxies

At this figure a client can download a file directly from the local server (a) and continue the file downloading transparently via the locally elected proxies (b, c, d).

We use a detailed simulation model based on *ns-2* [22].In this model we have one server, 3 proxies and at least 5 clients.

7. Experimental Analysis

We use the file transfer protocol to measure the performance of our model. The protocol provides file downloading from a dynamically discovered service component available in a MANET locality, even if the server moves during file transfer.

The communications take place between clients and their local proxies and between proxies with the retrieved server. As depicted in figure 7, file transfer replies run along the reverse path.

In this way, the proxy supports the multi-hop routing of service packets: the proxy acquires routing information during the server discovery phase and adds this routing data to the service packet header.

At first, we measured how long it takes for a client to complete the transfer of various file capacity (i.e. 10, 20, 30, 40 and 50 MB file, approximately) first directly from a server that does not move during service provisioning and secondary via proxy when server leaves the MANET locality during the downloading and reconnects via proxy when entered in a new locality (figure 1a) using the AODV routing protocol. In the first configuration the time a client requires to find the information about the server leaving was assumed to be 1 second (1 sec).

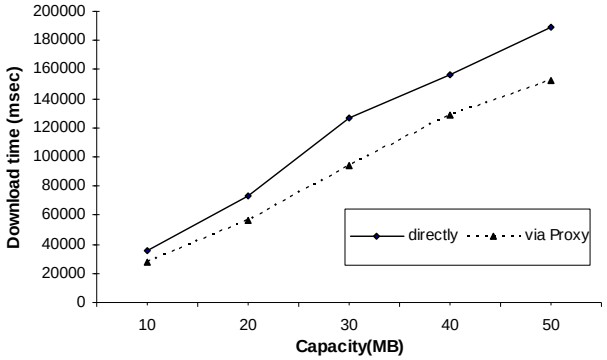

Figure1a. Downloading either directly from server or via proxy using the AODV routing protocol, when (1 sec) is needed by clients to find the server leaving

Figure 2a depicts the performance results when the time a client needs to find the information about the server leaving through the proxy service was assumed to be 5 seconds (5 sec). According to this figure the gain (reduce) for the download time is considerable again and greater in comparison with previous co nfiguration setup.

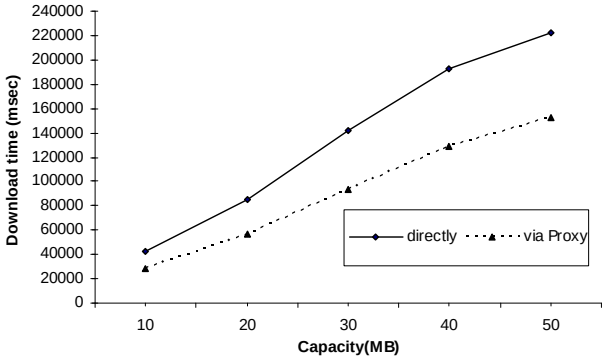

Figure2a. . Downloading either directly from server or via proxy using the AODV routing protocol, when (5 sec) is needed by clients to find the server leaving

Subsequently, at figure 3a the corresponding measurements were evaluated, at the case, where a client needs 20 seconds (20 sec) to find the server through the proxy service. It is worth mentioning the grammatical fall of downloading time for all sizes of file transferring.

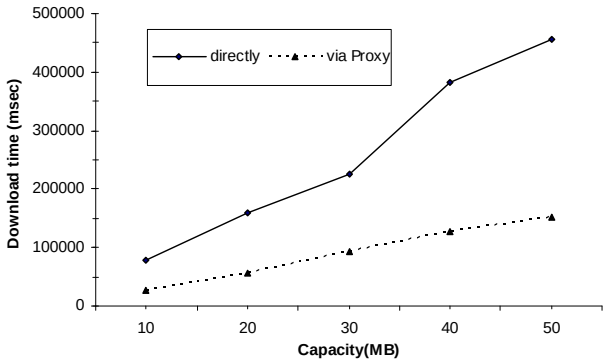

Figure3a. . Downloading either directly from server or via proxy using the AODV routing protocol, when (20 sec) is needed by clients to find the server leaving

At this point (figure 4a), we can observe a comparative view of all obtained performance measurements, when the required time for finding the server is 1sec, 5 sec, and 20 sec respectively.

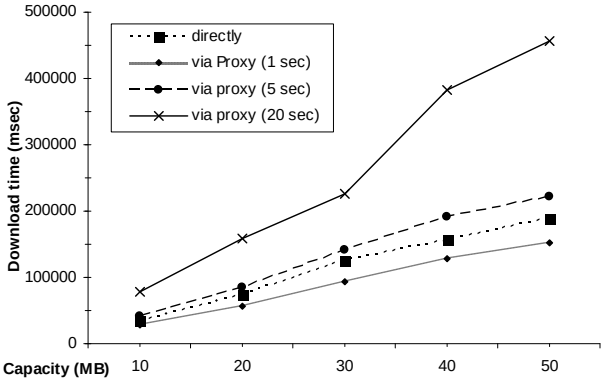

Figure4a. Summary results for AODV routing protocol

Similarly, the following figures (1b…4b) represent the corresponding measurements for the second routing protocol DSR, using the same configuration parameters at both configuration setups: directly and via proxy.

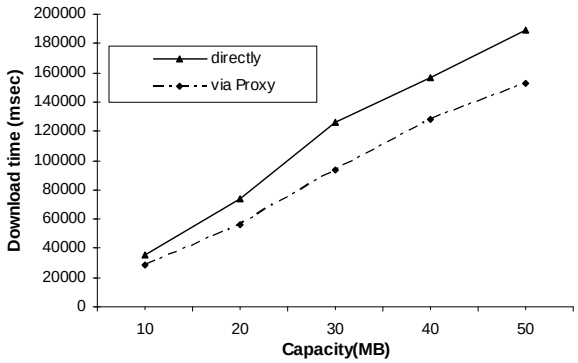

Figure1b. Downloading either directly from server or via proxy using the DSR routing protocol, under 1 sec detection time

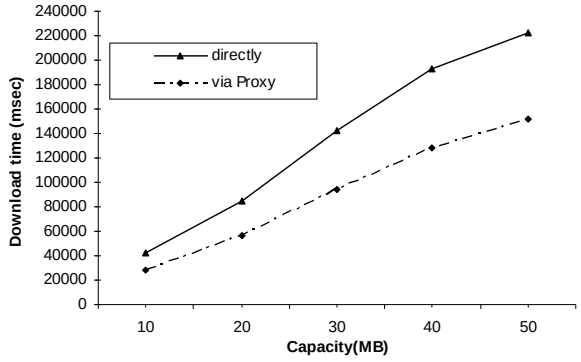

Figure2b. Downloading either directly from server or via proxy using the DSR routing protocol, under 5 sec detection time

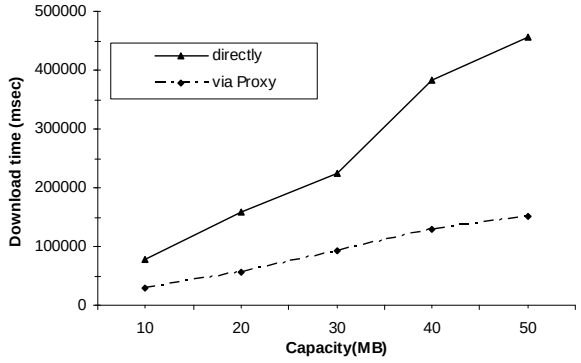

Figure3b. Downloading either directly from server or via proxy using the DSR routing protocol, under 1 sec detection time

According to these figures, it is clear again that the gain for the downloading time is more considerable as the time a proxy needs to detect the server increase, because the clients are closer to the corresponding proxy servers.

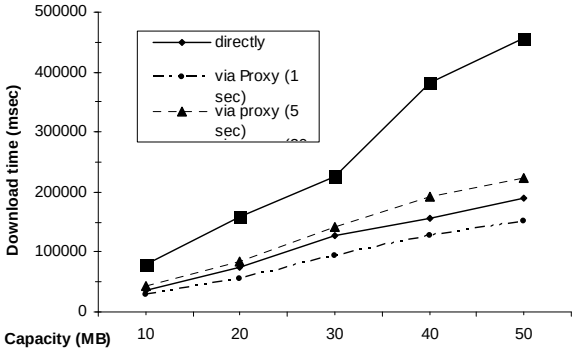

Figure4b. Summary results for DSR routing protocol

Finally, we summarized the measurements obtained for both routing protocols (AODV and DSR) through the next figures, in order to depict their comparative performance evaluation.

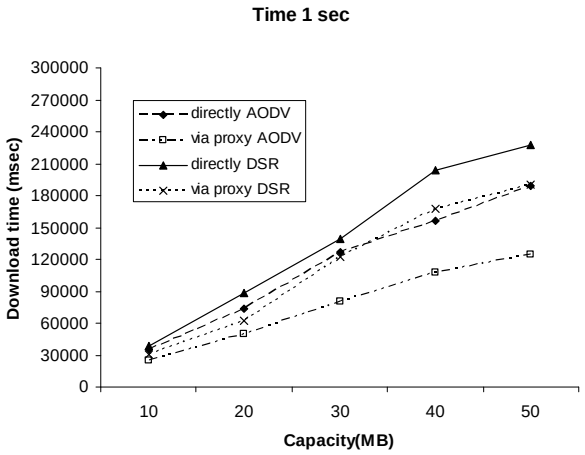

Figure1c. Summarized AODV and DSR (1 sec)

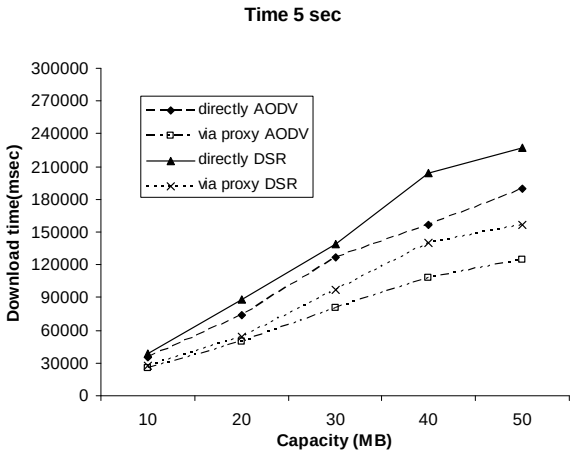

Figure2c. Summarized AODV and DSR (5 sec)

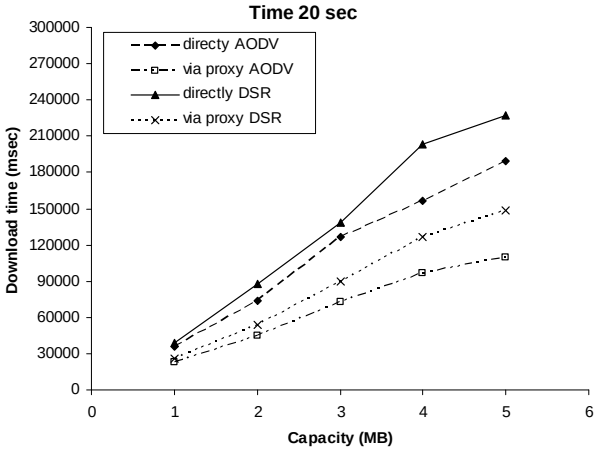

Figure3c. Summarized AODV and DSR (20 sec)

All above comparative curves at figures (1c, 2c, and 3c) show that the performance of AODV protocol is better than DSR at all configuration setups. Nevertheless, the gain for downloading time is greater for the DSR protocol under the use of proxy service.

8. Conclusions

In this work, we have compared performance characteristics of two widely used protocols for ad-hoc network routing, namely DSR and AODV in a Client-Proxy-Server service model.

We have compared performance of DSR and AODV, two prominent on-demand routing protocols for ad hoc networks. DSR and AODV both use on-demand route discovery, but with different routing mechanics. In particular, DSR uses source routing and route caches and does not depend on any periodic or timer-based activities. DSR exploits caching aggressively and maintains multiple routes per destination. AODV, on the other hand, uses routing tables, one route per destination, and destination sequence numbers, a mechanism to prevent loops and to determine freshness of routes.

The general observation is that AODV outperforms DSR in more stressful situations, (e.g., more capacity, higher time).

While we expected similar –or comparable- results for both protocols, having in mind that they both perform routing activities “on-demand” rather than proactively, considerable differences have been identified. The differences can be attributed to the different mechanisms employed by the two protocols to implement their routing activities. Summarizing our results, we can conclude that AODV behaves better than DSR, when server leaves the MANET locality during the downloading and reconnects via proxy when entered in a new locality and the transfer file capacity increases within the ad-hoc network.

When any of these parameters (capacity or time) increases, AODV appears to have a performance better than DSR; in fact, the more these parameters increase, the clearer the AODV advantage over DSR becomes.

References:

[1] P. Bellavista, A. Corradi, R. Montanari, C. Stefanelli, “Dynamic binding in mobile applications: a middleware approach”, *IEEE Internet Computing*, Vol. 7, No. 2, pages 34-42, Mar.-Apr. 2003.

[2] J. Macker, S. Corson, “Mobile Ad-hoc Networks (MANET)”, http://www.ietf.org/html.charters/manet-charter.html, 1997.

[3] IETF MANET Working Group, http://www.ietf.org/html.charters/manetcharter.html.

[4] L. Clare, G. Pottie, J. Agre, "Self-organizing distributed sensor networks", SPIE Conf. Unattended Ground Sensor Technologies and Applications, pp.229-237, 1999.

[5] Bluetooth SIG Inc. *Bluetooth*, http://www.bluetooth.com

[6] IEEE 802.11b Working Group, “Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: higher speed physical layer (PHY) extension in the 2.4 GHz band”, http://grouper.ieee.org/groups/802/11/, 1999.

[7] Cisco Systems. OSPF, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ospf.htm. 2004.

[8] Cisco Systems. RIP, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rip.html. 2004.

[9] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," *ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications*, pp. 234-244, Aug. 1994.

[10] C. C. Chiang, H. K. Wu, W. Liu, and M. Gerla, "Routing in Clustered Multihop Mobile Wireless Networks with Fading Channel," *IEEE Singapore International Conference on Networks*, pp. 197-211, Apr. 1997.

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

[12] D. B. Johnson and D. A. Maltz. *Dynamic Source Routing in Ad Hoc Wireless Networks in Mobile Computing*, Kluwer Publishing Company, 1996.

[13] C. E. Perkins and E. M. Belding-Royer, "Ad-hoc On Demand Distance Vector Routing," *2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90-100, Feb. 1999.

[14] D.B. Johnson and D.A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," in Mobile Computing, edited by T. Imielinski and H. Korth, chapter 5, pp.153-181, Kluwer Academic Publishers, 1996

[15] M.R. Pearlman and Z.J. Haas, "Determining the Optimal Configuration for the Zone Routing Protocol," *IEEE Journal on Selected Areas in Communications, Special Issue on Wireless Ad Hoc Networks*, vol.17, no.8, pp.1395-1414, August 1999

[16] Per Johansson, Tony Larsson, Nicklas Hedman, and Bartosz Mielczarek. Routing protocols for mobile ad-hoc networks - a comparative

performance analysis. In *Proceedings of the 5th International Conference on Mobile Computing and Networking (ACM MOBICOM'99)*, pages 195. 206, August 1999.

[17] D. Johnson and D. Maltz. Dynamic source routing in ad hoc wireless networks. In T. Imielinski and H. Korth, editors, *Mobile computing*, chapter 5. Kluwer Academic, 1996.

[18] J. Macker and S. Corson. Mobile ad hoc networks (MANET). http: //www.ietf.org/ html.charters/manet-charter.html, 1997. IETF Working Group Charter.

[19] David Maltz, Josh Broch, Jorjeta Jetcheva, and David Johnson. The effects of on-demand behavior in routing protocols for multi-hop wireless ad hoc networks. *IEEE Journal on Selected Areas in Communication*, 1999.

[20] Charles Perkins and Elizabeth Royer. Ad hoc on-demand distance vector routing. In *Proceedings of the 2nd IEEEWorkshop on Mobile Computing Systems and Applications*, pages 90.100, Feb 1999.

[21] Charles Perkins, Elizabeth Royer, and Samir Das. Ad hoc on demand distance vector (AODV) routing. http:// www.ietf.org/ internet-drafts/ draft-ietf-manet-aodv-03.txt, June 1999. IETF Internet.

[22] Kevin Fall and Kannan Varadhan (Eds.). *ns* notes and documentation, 1999. available from http://www-mash.cs.berkeley.edu/ns/