Lloret J, Garcia M, Tomás J *et al.* GBP-WAHSN: A group-based protocol for large wireless ad hoc and sensor networks. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 23(3): 461–480 May 2008

GBP-WAHSN: A Group-Based Protocol for Large Wireless Ad Hoc and Sensor Networks

Jaime Lloret, Miguel Garcia, Jesus Tomás, and Fernando Boronat

Department of Communications, Polytechnic University of Valencia, Camino Vera s/n, 46022, Valencia, Spain

E-mail: {jlloret, jtomas, fboronat}@dcom.upv.es; migarpi@posgrado.upv.es

Revised March 11, 2008.

Abstract Grouping nodes gives better performance to the whole network by diminishing the average network delay and avoiding unnecessary message forwarding and additional overhead. Many routing protocols for ad-hoc and sensor networks have been designed but none of them are based on groups. In this paper, we will start defining group-based topologies, and then we will show how some wireless ad hoc sensor networks (WAHSN) routing protocols perform when the nodes are arranged in groups. In our proposal connections between groups are established as a function of the proximity of the nodes and the neighbor's available capacity (based on the node's energy). We describe the architecture proposal, the messages that are needed for the proper operation and its mathematical description. We have also simulated how much time is needed to propagate information between groups. Finally, we will show a comparison with other architectures.

Keywords group-based protocol, group-based architecture, group-based routing algorithm, large networks

1 Introduction

Wireless ad hoc networks (WAHN) are simple networks in which a coordinator is not needed and the numbers of nodes and network topology are not predetermined. A wireless sensor networks (WSN) is a type of WAHN composed of nodes with sensing capability. There are several differences between WSN and WAHN[1]. WSNs usually have a larger number of nodes and are deployed in close proximity to the phenomena under study; the nodes mainly use a broadcast communication paradigm and the network topology can change constantly due, for example, to the fact that the nodes are prone to fail (they have limited power, computational capabilities and memory). Mobile wireless sensor networks (MWSNs) are WSNs with mobile sensors which are randomly deployed in an interesting area for sensing some phenomena. These mobile sensors collaborate with each other to form a sensor network with the capability of reporting sensed phenomena to a data collection point called sink or base station.

A mobile ad hoc network (MANET[2]) is a self-configuring network of mobile nodes connected by wireless technology. This type of network has an arbitrary topology. The network's wireless topology may change rapidly and unpredictably. Independently of the medium access method used[3], in recent years have many routing protocols been developed for these networks[4,5]. The nodes' mobility, the lack of stability of the topology, the lack of a pre-established organization and performing of the wireless communications are the reasons for not using the routing protocols developed for fixed networks.

Depending on the type of the information exchanged by the nodes and on the frequency by which they do it, the routing protocols in ad hoc networks are divided into three types: *proactives*, *reactives* and *hybrids*. The proactive protocols update the routing tables of all the nodes periodically, even though no information is being exchanged. When a topology change occurs, the routing table is updated and the routing protocol finds the best route to forward the information. A periodical control protocol message exchange allows this, but consumes bandwidth and energy. The reactive protocols only maintain routing routes in their tables when a node has to communicate with another node in the network. With these protocols, when a communication starts, as the right route is unknown, a route discovering message is sent. When the response is received, the route is included in the routing tables and the communication is established. The main disadvantage of these protocols is the latency at the beginning of the communications (route discovery time) but they improve the consumption of network and energy resources. Finally, hybrid protocols are a combination of the above two types, taking their advantages. These protocols divide

Regular Paper

ad hoc networks into different zones; consequently near nodes use proactive routing while far nodes use reactive routing.

The aforementioned networks and protocols do not have a predetermined topology, so they could be applied over different types of architectures such as Grids, cluster-based networks, group-based networks and so on.

A key problem in the planning of any kind of network is to design the communication topology. It means deciding how the peers are connected as well as how their messages are exchanged. Topologies can be characterized by several parameters such as the number of nodes in the network, the number of links or connections (hereafter both terms will be used without distinction in this paper) in the network and their bandwidth, the degree of the nodes and the diameter of the topology. On the other hand, communication topology design needs to address several conflicting requirements like, on the one hand, minimizing the overall network diameter, minimizing the convergence time, the infrastructure cost (total number of links), the book-keeping costs (the number of links maintained by each node) and the management cost, and, on the other hand, maximizing load distribution, reliability, efficiency, fault tolerance, the performance of the system, the scalability, and so on. Usually, optimizing on any requirements would be at the cost of others. Designing the optimal topology for a given set of constraints is a difficult problem. Over the years, topology design has received significant interest in many areas. In order to provide real-time infrastructures, reliable, available and efficient networks and QoS-aware distribution services, a topology-aware network is necessary[6,7].

While the physical topology defines how the nodes on a network are physically connected and the physical layout of the devices on the network, the logical topology defines how the nodes on the network communicate (i.e., the way the data passes through the network, with no regard for the physical interconnection between the devices). However, if the logical network is constructed randomly, nearby hosts in the logical network may be far away in the physical network. This may waste too many network resources, and hence degrade data delivery performance significantly.

In this paper, we present a proposal which uses a group-based topology and protocol over WAHSNs in order to improve their performance.

The remainder of the paper is organized as follows. Section 2 describes group-based architectures. Some application environments are presented in Section 3. Section 4 demonstrates that group-based topologies can improve some routing protocols such as Dynamic Source Routing Protocol (DSR), Optimized Link State Routing Protocol (OLSR) and ad hoc on demand distance vector (AODV) routing. The architecture operation and its analytical model are shown in Section 5. Protocol operation is shown in Section 6. Section 7 shows simulations to test our protocol. In Section 8, we compare our proposal with other types of networks. Finally, Section 9 summarizes the results and exposes future research.

2 Group-Based Topologies

The network topology defines how the nodes on a network are physically or logically connected (i.e., the physical layout of the devices on the network). Three types of network topologies can be distinguished:

1) Centralized Networks. In these topologies there could be no direct connection between nodes, and all nodes' messages could be mediated by a mediator, generally known as a central node. This single node acts as a gateway for all the nodes. These topologies have been used for many types of networks[8].

2) Decentralized Networks. Each node is able to connect directly with all other nodes, and messages are sent without intermediation via a central node. All nodes have the same responsibility and functionality in the network. No element in the network is essential for the system operation. A node in a decentralized topology can play three roles: *server*, *client* and *router*. Many types of networks have decentralized topologies, such as pure P2P networks, ad hoc and sensor networks, grids and so on. Many searching algorithms for decentralized networks have been designed[9], all of which perform three basic actions: searching of active nodes, querying for resources or services, and content transferring.

3) Partially Centralized Networks (also known as hybrid networks, layered networks or multi-tier networks). In these networks, there are some nodes with higher roles which form the backbone of the network and are needed to run the system. Nodes with the lower role are called *leaf nodes* and will be placed in the lower logical layer, while nodes with the higher roles could be *supernodes* and will be placed in the higher logical layers. Every supernode or leaf node can have connections with either the other leaf nodes or supernodes. There is a hierarchy where higher layer nodes organize, control or gather data from lower layer nodes. The higher layer nodes are used for forwarding the messages from the lower layer nodes. Layered networks have been used for different types of networks such as satellite networks[10], wireless networks[11] and even models for business processes[12].

Let us suppose we need to divide the network into groups or areas according to the physical implementation of the WAHSN or for scalability purposes. It does not matter which kind of routing protocol is being used inside each group. All architectures shown above fail to solve that problem efficiently, because in the case of centralized architectures, the server will have many wireless connections at the same time, so it will need many resources. There is also a central point of failure and a bottleneck. On the other hand, in the case of fully distributed architectures, it is very difficult to control the system and it needs a long time to process tasks (because of the time needed to reach far nodes), decreasing the performance of the system.

We propose dividing the whole WAHN or wireless sensors and actor networks (WSAN) into several groups, and that when a node receives data for its group, it will propagate the data to the rest of the nodes in its group.

A group is defined as a small number of interdependent nodes with complementary operations that interact in order to share resources or computation time, or to acquire content or data and produce joint results. In a wireless group-based architecture, a group consists of a set of nodes that are close to each other (in terms of geographical location, coverage area or round trip time) and neighboring groups could be connected if a node of a group is close to a node of another group. The main goal in a wireless group-based topology is the network protocol and the group management, that is, the design of an efficient algorithm and a capable protocol is needed to find the nearest (or the best) group to join in when a new node appears in the network. The performance of the network largely depends on the efficiency of the nearby group locating process and on the interaction between the neighbor groups.

We have to distinguish between a groupware architecture and a group-based architecture. In a groupware architecture all nodes collaborate towards the correct operation and the success of the network purpose, while in a group-based architecture the whole network is broken down into groups and each group can perform different operations or can have different routing protocols.

Some important issues must be taken into account in a wireless group-based architecture regardless of the protocol inside the group as follows.

1) How to build neighboring groups.

2) A protocol to exchange messages between neighboring groups.

We can distinguish two types of group-based topologies: planar group-based topologies and layered group-based topologies. In planar group-based topologies all nodes perform the same roles and there is only one layer. However, in some work there is a directory server or a rendezvous point (RP) for content distribution coordination. Nodes from layered group-based topologies could have several roles (2 roles at least). Depending on which type of role they are playing, they will belong to a specific layer. All nodes in the same layer will have the same role. There will be connections between nodes from the same layer and from different layers, but these layers must be adjacent. We have included hierarchical architectures in this group, because the hierarchies could be considered as layers. There are several differences between both the group-based topologies. While layered group-based topologies grow in a structured form, organized by upper layers, planar group-based topologies grow in an unstructured form, without any organization. On the one hand, in layered group-based topologies any node can know exactly where each group is and how to reach it; on the other hand, planar group-based topologies, because the groups join the network as they appear, and every time there is a connection between the nodes from different groups, the message should travel through many unknown groups in the path. Delays between groups in layered group-based topologies could be lower because connections between groups can be established taking this parameter into account. In planar group-based topologies, connections between groups are established by the group's position, their geographical situation or their appearance in the network. Layered networks involve some complexity because nodes could have several types of roles and fault tolerance must be designed for each layer. Planar networks are simpler because all nodes have the same role. In order to be more scalable, layered group-based topologies must add more layers to its logical topology, while planar group-based topologies could grow without any limitation, just the number of hops of the message.

Group-based networks provide some benefits for the whole network, such as the following.

- Spread the work efficiently to the network in groups, giving more flexibly, and lower delays.
- Content availability will increase because it could be replicated in other groups.
- Anyone could search and download data from every group using only one service.
- Fault tolerance. Other groups could carry out tasks from a failed one.
- Scalability. A new node can join any group and a new group could be added easily.
- Network measurements could be taken from any

group.

There are some works in the literature where nodes are divided into groups and connections are established between nodes from different groups, but all of them have been developed to solve specific issues[13−16], but none of them for MANET networks.

The Rhubarb system[13] organizes nodes in a virtual network, allowing connections across firewalls/NAT (Network Address Translation), and efficient broadcasting. Nodes can be active, if they establish connections, or passive, if they do not do it. The Rhubarb system has only one coordinator per group and coordinators could be grouped hierarchically. It uses a proxy coordinator, an active node outside the network, and all nodes inside the network make a permanent TCP connection with the proxy coordinator, which, if broken, can be renewed by the firewall or NAT. When a node from outside the network wishes to communicate with an inner node, it sends a connection request to the proxy coordinator, which forwards the request to the inner node.

A Peer-to-Peer Based Multimedia Distribution Service was presented in [14]. Xiang *et al.* proposed a topology-aware overlay in which nearby hosts or peers self-organize into application groups. End hosts within the same group have similar network conditions and can easily collaborate with each other to achieve Quality of Service (QoS) awareness. When a node wants to communicate with a node from another group, the information is routed through several groups until it reaches its destination.

There are some hierarchical architectures where nodes are structured hierarchically and parts of the tree form groups, such as the ones in references [15, 16]. In some cases, some nodes have connections with nodes from other groups although they are in different layers of the tree, but in all cases, the information has to be routed through the hierarchy.

There are many cluster-based hierarchical architectures[17]. In a cluster-based architecture the mobile nodes are divided into virtual groups. Each cluster has adjacencies with the other clusters. All the clusters have the same rules. A cluster can be made up of a Cluster Head node, Cluster Gateways and Cluster Members[18,19]. The Cluster Head node is the parent node of the cluster, which manages and checks the status of the links in the cluster, and routes the information to the right clusters. The rest of the nodes in a cluster are all leaf nodes. In this kind of network, the Cluster Head nodes have a total control over the cluster and the size of the cluster is usually about 1 or 2 hops from the Cluster Head node. The cluster gateways have links to other clusters and route the information to those clusters. On the other hand, a cluster member is a node without any inter-cluster links. Finally, we want to emphasize that the cluster-based networks are a subset of the group-based networks, because every cluster could be considered as a group. But a group-based network is capable of having any type of topology inside the group, not only clusters. However, both types of networks have been created for solving the scalability problems of the WAHSN.

We can also find in the literature a routing protocol based on zones. It is the Zone Routing Protocol (ZRP)[20,21]. Each node proactively maintains routing information for a local neighborhood (routing zone), while reactively acquiring routes to destinations beyond the routing zone. ZRP and our proposal have several common features, e.g., they could be applied over any type of routing protocol, they scale well and the information is sent to border nodes in order to reach destinations outside their zones. The main difference between them is that in ZRP each node maintains a zone and the nodes in that zone have different nodes in their zone while in our proposal all the nodes that form a group have the same nodes in their group.

On the other hand, we will not consider other work of group systems such as the following. The community-based mobility model for ad hoc network research presented in [22], because although the network is organized in groups, and nodes can move from one host to another, there is not any connection between border nodes from different groups. The landmark hierarchy presented in [23], because although there is a node with a higher role which has connections with the nodes from the other groups, its leaf nodes do not. Another example similar to the last one is the BGP routing protocol architecture[24]. Finally, we will not consider moving groups such as Landmark Routing Protocol (LANMAR[25]), where the set of nodes move as a group, so the group can enlarge or diminish with the motion of the members.

3 Application Environment

Group-based networks can be used when there is a need to setup a network where groups could appear and join the network at anytime or when the network has to be split into smaller zones to support a large number of nodes, that is, in any system where the devices are grouped and there must be connections between groups.

The following list gives several group-based WAHSN application areas.

1) Let us suppose a job where all human resources need to be split into groups to achieve a purpose (such as fire fighter squads for putting out the fire). Now, let

us suppose that all the people involved in that activity need a device that has to be connected with other devices in the same group to receive information from the members within the group, and closer groups have to be connected to coordinate their efforts. Currently coordination between groups is done through a wireless connection to the command center or using satellite communications. But, some times neither of those solutions can be used because a free obstacle line of sight is needed, because there are too many wall looses or because more gain or power is needed to reach the destination.

2) For battle field communication, it is especially useful for inter-squad communication to collaborate when an objective is targeted by position detectors.

3) Groups could also be established because of geographical locations or unevenness. It happens in rural and agricultural environments. A group-based topology in this kind of environment could be useful to detect plagues or fire and to propagate an alarm to neighbor lands. It will provide easier management and control for detecting fires and plagues as well as for allowing scalability.

4) Health monitoring[26]. A patient might need to be monitored in several locations while he is doing his activity. Every room or place could have a group of sensors (and even each group with different type of topology inside) and neighbor groups must be communicated to keep track of the patients.

5) It could be used in any kind of system in which an event or alarm is based on what is happening in a specific zone, but conditioned to the events that are happening in neighbor zones. One example is a group-based system that measures the environmental impact on a place. It could be better measured if the measurements are taken from different groups of sensors, but those groups of sensors have to be connected in order to estimate the whole environmental impact.

6) Group-based virtual games. There are many games where the players are grouped virtually in order to perform a specific task. Interactions between groups in virtual reality should be given by interactions between players from different groups to exchange their knowledge.

In the following section we will show that group-based topologies give better performance to the whole wireless ad hoc and sensor network.

4 Group-Based WAHSN Topologies Performance

This section compares the performance of 3 common MANET protocols and shows which one is the best when they are using group-based topologies.

4.1 Test Bench

First, we present the test-bench used for all the evaluated protocols. The number of nodes and the coverage area of the network have been varied. We have simulated 4 scenarios for each protocol: the first one with fixed nodes; the second one with mobile nodes and failures; the third one with grouped nodes; and, the fourth one with grouped mobile nodes and failures. We have simulated each scenario for 100 and 250 nodes to observe the system scalability. It has been obtained using the version Modeler of OPNET simulator[27].

Instead of a standard structure we have chosen a random topology. The nodes can move randomly during the simulation. The physical topology does not follow any known pattern. The obtained data do not depend on the initial topology of the nodes nor on their movement pattern, because all of it has been fortuitous.

In order to take measurements from the mobile nodes simulation, we have forced failures in the networks with the consequent recovering processes. It allows us to observe the network behavior, against physical topology changes and node failures. Failures and recoveries usually happen in these kinds of networks, so, we are going to study how a network-level protocol works when those events occur.

We have created 6 groups for the 100 nodes topology, covering approximately, a circular area with a 150 meter radius each group. There are approximately 16 or 17 nodes in each group. The number of nodes in each group varies because of the node's random mobility. A node can change a group anytime. For the 250 nodes topology, we have created 12 groups, with 15 or 16 nodes per group approximately, covering a circular area with a 150 meter radius each group.

The ad-hoc nodes of the topologies have a 40MHz processor, a 512KB memory card, a radio channel of 1Mbps and their working frequency is 2.4GHz. Their maximum coverage radius is 50 meters. This is a conservative value because most of the nodes in ad-hoc network have larger coverage radius, but we preferred to have lower transmitting power for the ad-hoc devices to enlarge their lifetime.

The traffic load used in the simulations is MANET traffic generated by OPNET. We inject this traffic 100 seconds after the beginning. The traffic follows a Poisson distribution (for the arrivals) with a mean time between arrivals of 30 seconds. The packet size follows an exponential distribution with a mean value of 1024 bits. The injected traffic has a random destination address, obtaining a simulation independent of the traffic direction. We have simulated both scenarios for DSR, AODV and OLSR protocols. The results obtained are shown in the following subsections.

4.2 Average Delay at Application Layer

Figs.1 and 2 show the average delay of the DSR protocol in fixed and mobile topologies at the application layer. In Fig.1 we observe that group-based topologies have an average delay close to 0.005 seconds regardless of the number of nodes in the network. In the regular network the delay has a value of 0.02 seconds for 100-node topology and of 0.03 seconds for the 250-node topology when the network converges. In the case of the 100-node topology there is an improvement of 75%, and it is better in the 250-node topology (an 83% improvement). The topologies with mobility and errors (Fig.2) show that the average delays at the application layer are higher in the group-based topologies until the network converges. We observe that group-based topologies present worse behavior up to 1300 seconds. Then, the delay decreases. There is an improvement of around 5%.

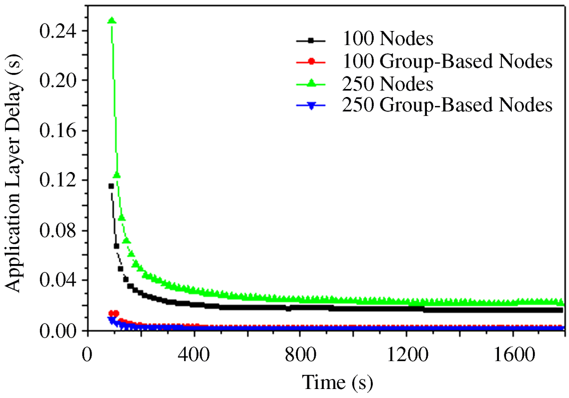


Fig.1. DSR average delay at the application layer in fixed topologies.

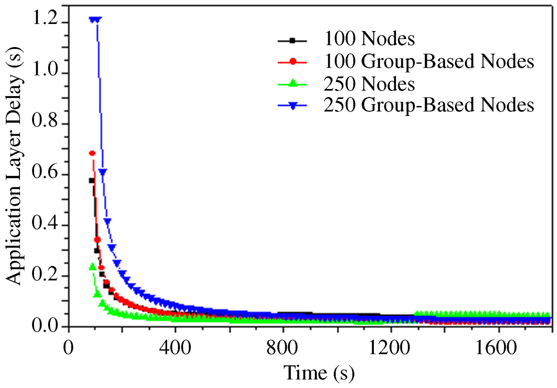


Fig.2. DSR average delay at the application layer in mobile topologies.

The average delay at the application layer in the AODV protocol can be seen in Figs.3 and 4. When we are talking about fixed topologies (Fig.3), both of 100-node and 250-node, give an average delay higher than 0.5 seconds when the network converges, but there are some peaks higher than 2.5 seconds. On the other hand, group-based topologies have a similar delay which is around 0.15 seconds. Group-based topologies improve the delay at the application layer by 70%. When the topology with mobile nodes is used, the simulation shown in Fig.4 is obtained. In the case of 250 nodes, there is a delay of 1 second when the network has converged. The case of 100 nodes gives an average delay around 0.75 seconds. When there are group-based topologies, the delay decreases to 0.25 seconds in both cases. There is an improvement of 75% for the 250-node topology and 67% for the 100-node topology.

In Fig.5, the delay at the application layer for the OLSR protocol using fixed topologies is shown. In the case of 250 nodes we have obtained a delay of around

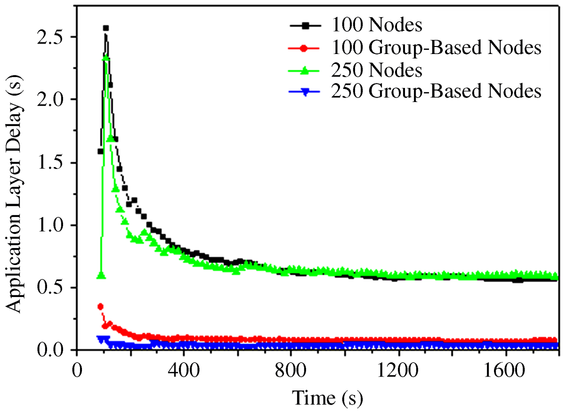


Fig.3. AODV average delay at the application layer in fixed topologies.

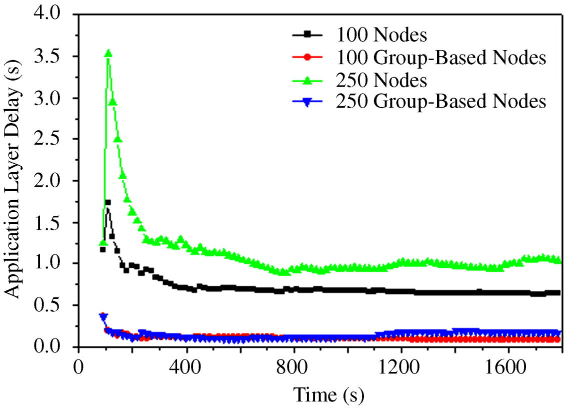


Fig.4. AODV average delay at the application layer in mobile topologies.

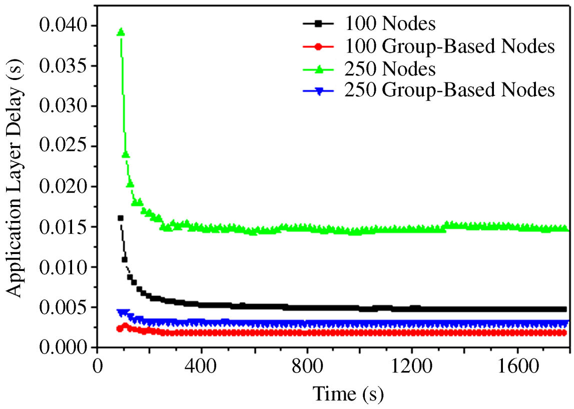


Fig.5. OLSR average delay at the application layer in fixed topologies.

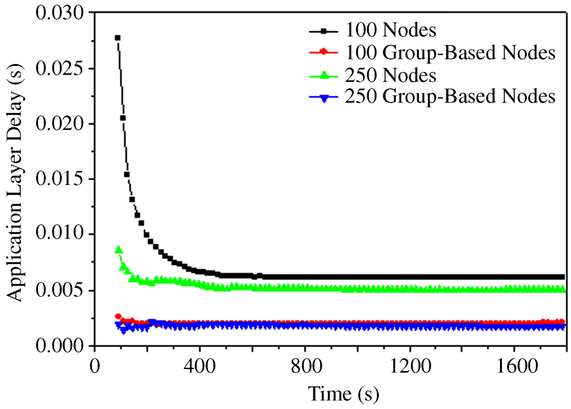


Fig.6. OLSR average delay at the application layer in mobile topologies.

0.015 seconds, and the delay has changed to 0.0035 seconds in the case of 250-node group-based topology (there is a 76% improvement). In the case of 100 nodes, the delay has decreased from 0.005 seconds in the regular topology to 0.002 seconds in the group-based topology, so there is a 60% improvement. When there is mobility, errors and failures in the network for the OLSR protocol (see Fig.6), we observe that the 100-node regular topology has a delay at the application layer of 0.007 seconds when the network has converged, but there is a delay of 0.0025 seconds for the 100-node group-based topology (a 64% improvement). In the case of 250 nodes the improvement is around 60%. We have obtained a delay of 0.005 seconds in the regular topology versus 0.002 seconds in the group-based topology.

4.3 Routing Traffic Received

We have compared the routing traffic received in the DSR protocol (Figs.7 and 8). Fig.7 shows that the traffic is quite stable because it is a fixed network without errors or failures. The traffic received in the 250-node topology is around 500Kbits/s, but when we group the nodes, this traffic decreases to 200Kbits/s (a 60% improvement). The value obtained in a 100-node topology (250Kbits/s) is also improved when we group the nodes (100Kbits/s), therefore there is a 60% improvement. In Fig.8 we observe a similar behavior. In this case we conclude that when there are errors and failures in the 250-node topology the traffic fluctuates and is less stable (we can observe it in the intervals from 600 to 800 seconds and around 1200 seconds). We also observe that the instability is much lower in group-based topologies. 100-node topology has a mean value around 175Kbits/s, while 100-node group-based topology has a mean value around 95Kbits/s, so there is an improvement of 46%. On the other hand, 250-node topology has a mean value around 400Kbits/s, while 250-node group-based topology has a mean value around 180Kbits/s, so there is an improvement of 55%.

Then, the routing traffic received for the AODV in each simulated topology can be seen in Figs.9 and 10.

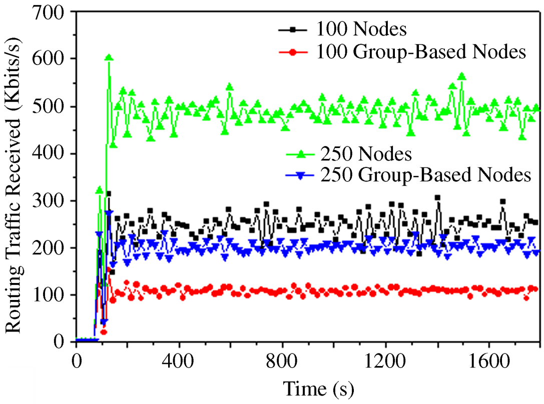


Fig.7. DSR routing traffic received in fixed topologies.

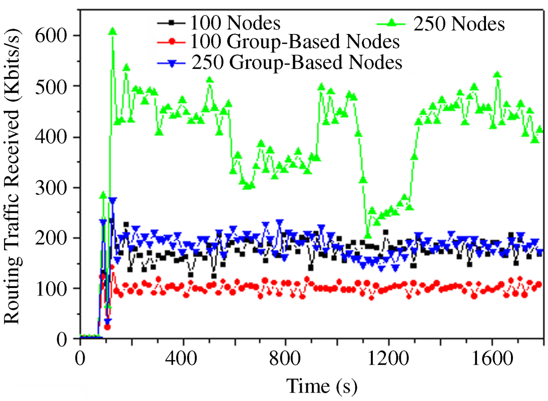


Fig.8. DSR routing traffic received in mobile topologies.

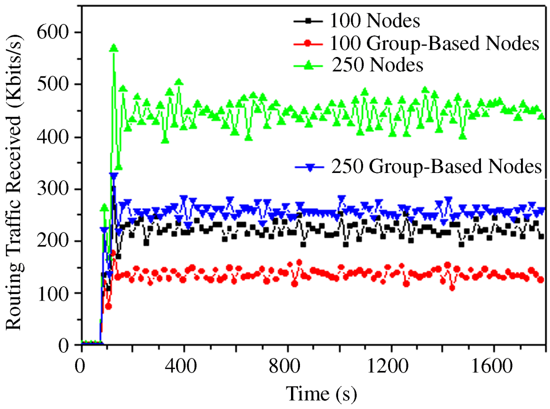


Fig.9. AODV routing traffic received in fixed topologies.

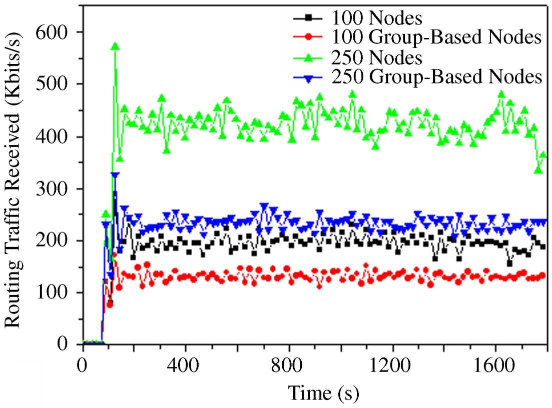


Fig.10. AODV routing traffic received in mobile topologies.

We observe that the routing traffic received is independent of the mobility of the nodes. In Fig.9 we can see that the routing traffic goes from 440Kbits/s for 250-node case to 250Kbits/s when there are groups of nodes (a 43% improvement). In the 100-node topology, it goes from 230Kbits/s to 140Kbits/s in the group-based topology case (a 39% improvement). When there are mobility, errors and failures (see Fig.10), in the 250-node topology the values go from 440Kbits/s to 250Kbits/s in the group-based topology (a 43% improvement). We obtained 200Kbits/s in the regular 100-node topology and 135Kbits/s for the group-based one (a 32% improvement).

Finally, we have studied the behavior of the OLSR protocol analyzing the mean routing traffic received (Figs.11 and 12). In Fig.11, we see that the routing traffic received in the 100-node fixed topology is around 180Kbits/s, while in group-based topology it has decreased to 70Kbits/s, so there is a 61% improvement. In the 250-node topology case, we appreciate that this traffic was approximately 300Kbits/s, but there are values lower than 150Kbits/s in the group-based topology, so there is a 50% improvement. Fig.12 shows the results of a network with mobility and errors and failures. We have observed some fluctuations due to the failures and errors in the network, in both 100-node and 250-node topologies. Those fluctuations are minimized when we use group-based topologies. Improvements of 61% and 50% are obtained in 100-node and 250-node topologies, respectively.

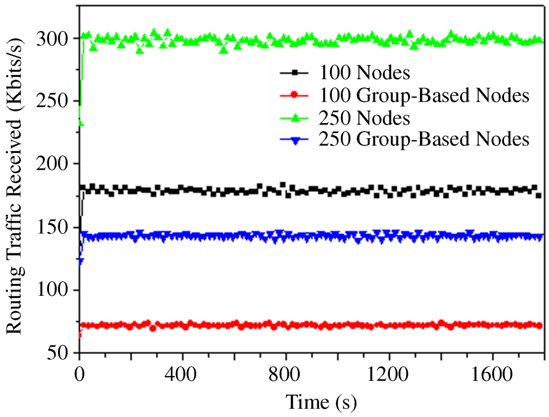


Fig.11. OLSR routing traffic received in fixed topologies.

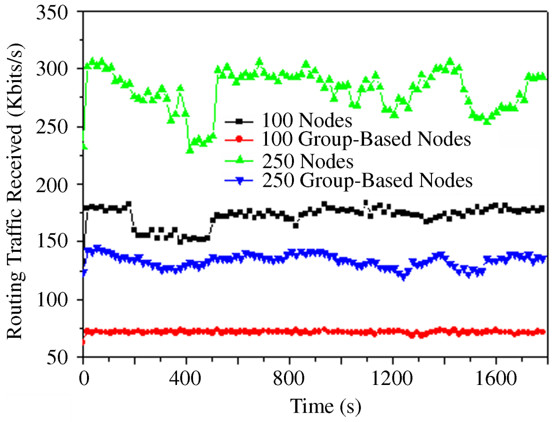


Fig. 12. OLSR routing traffic received in mobile topologies.

4.4 Throughput

When we study the network throughput (Figs.13 and 14), we observe that group-based topologies give a much lower value than the one obtained in regular topologies. For the 100-node topology (Fig.13), the throughput varies from 225Kbits/s to 100Kbits/s in the group-based topology (a 56% improvement). In the 250-node topology we obtain 460Kbits/s of throughput for the regular topology and 190Kbits/s of throughput for the group-based one (a 59% improvement). Moreover, when we compare Figs.13 and 14, we can conclude that the throughput in group-based topologies has a very low variation regarding a fixed or mobile scenario. The obtained improvement is quite important. We can see in Fig.14 that, after 1200 seconds, the obtained throughput in 250-node topology is similar to the obtained throughput in the 100-node topology.

Fig.15 shows the throughput for fixed topologies. The 100-node scenario gives a 200Kbits/s mean value, but a value of 120Kbits/s is obtained for the group-based scenario (a 40% improvement). In the 250-node case, we obtain mean values of 425Kbits/s for the fixed scenario and of 225Kbits/s for the group-based scenario (a 47% improvement). Fig.16 shows the results for mobile topologies with errors and failures. The improvement obtained by grouping nodes decreases in the 100-node case (37%), but it does not vary in the 250-node cases.

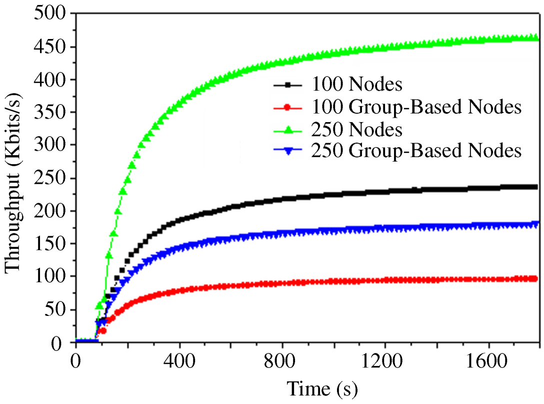


Fig.13. DSR mean throughput in fixed topologies.

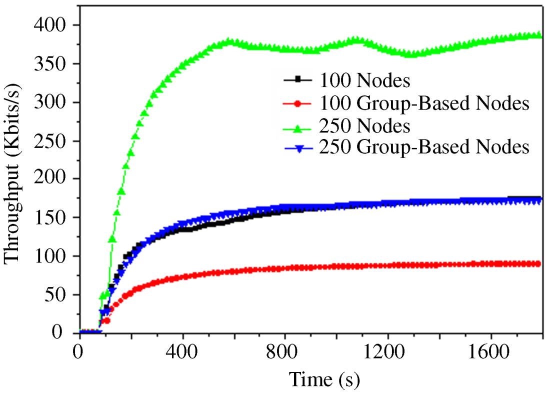


Fig.14. DSR mean throughput in mobile topologies.

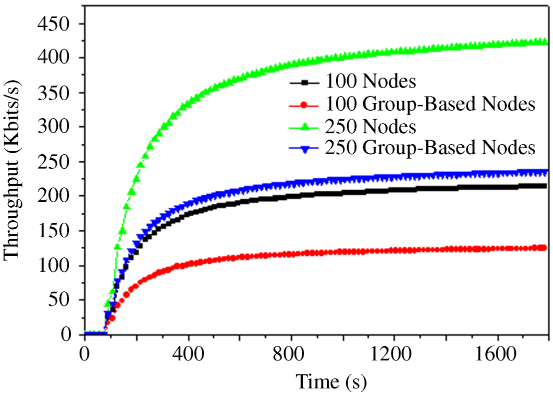


Fig.15. AODV mean throughput in fixed topologies.

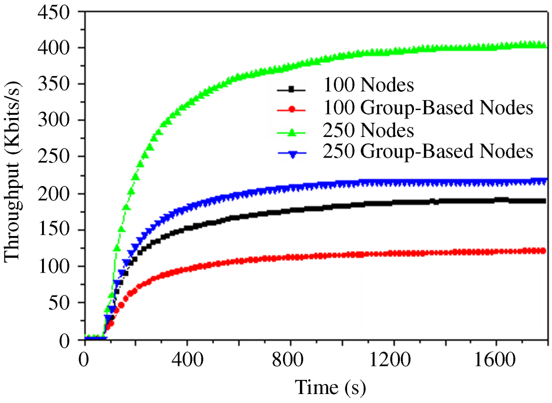


Fig.16. AODV mean throughput in mobile topologies.

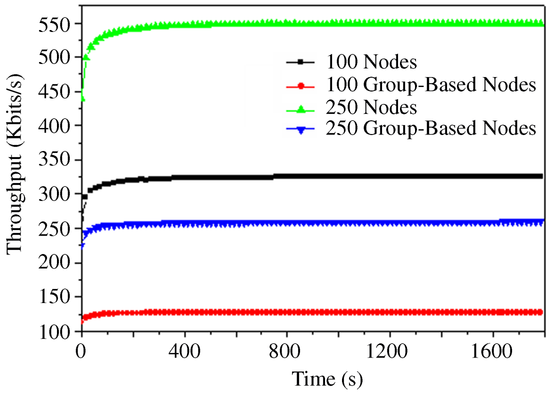


Fig.17. OLSR mean throughput in fixed topologies.

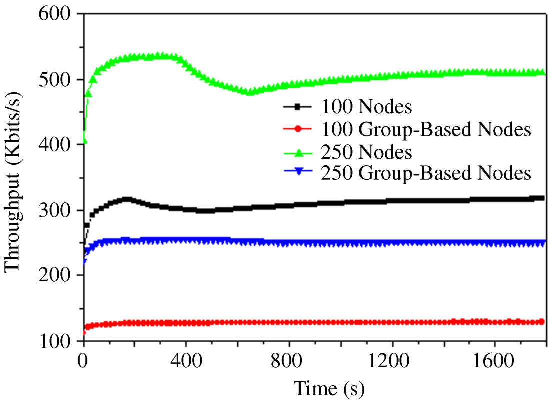


Fig.18. OLSR mean throughput in mobile topologies.

Finally, the mean throughput measured in fixed topologies can be observed in Fig.17. In scenarios with 250 nodes we obtained a mean throughput of 550Kbits/s and 250Kbits/s (group-based, with a 54% improvement). In 100-node regular topology the throughput is 325Kbits/s and 125Kbits/s (group-based, with a 61% improvement). When we consider mobility, errors and failures (Fig.18) the throughput is not so stable as in above case but, we can observe that the improvements are quite similar. In the case of 250 nodes we obtain a 52% improvement in the group-based scenario; in the case of 100 nodes the improvement reaches the 60%.

4.5 Group-Based Topologies Comparison

In order to make the comparison of DSR, AODV and OLSR using group-based topologies, we have used the same test bench used previously. This comparison will show us which mobile and ad-hoc routing protocol performs better using group-based topologies.

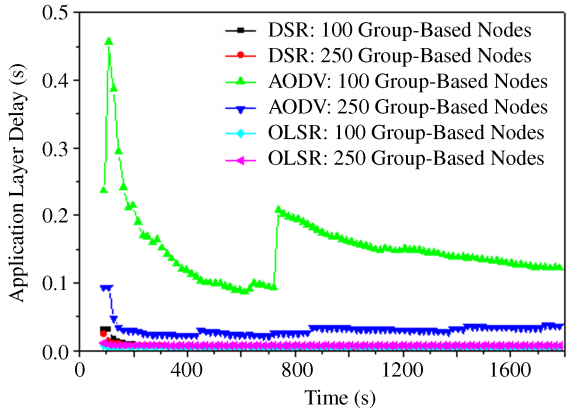


Fig.19. Comparison of the average delay at application layer in fixed topologies.

Fig.19 shows the average delay at application layer in fixed group-based topologies. The most instable protocol with higher delay in 100-node and 250-node topologies is AODV protocol. It has peaks with more than 0.45 seconds and it is stabilized around 1700 seconds with a mean value of 0.15 seconds. DSR and OLSR are the ones with lowest delay. Fig.20 shows the average delay at application layer in mobile group-based topologies. DSR protocol is the one that has the worst delay until the network converges. Then, when the network is stabilized, the worst is AODV protocol which has delays between 0.1 and 0.15 seconds. OLSR protocol gives the lowest delays.

The routing traffic received in fixed and mobile group-based topologies is shown in Figs.21 and 22, respectively. In fixed group-based topologies (see Fig.21) AODV protocol is the one that gives higher routing traffic received (around 250Kbits/s in 250-node topology and 135Kbits/s in 100-node topology). OLSR protocol is the most stable and the one with lower routing traffic received (145Kbits/s in 250-node topology and 70Kbits/s in 100-node topology). When the mobile group-based topologies are analyzed (Fig.22), AODV protocol is the one that has the worst behaviour and OLSR is the most stable and the one that has lower routing traffic sent. DSR protocol is the most instable.

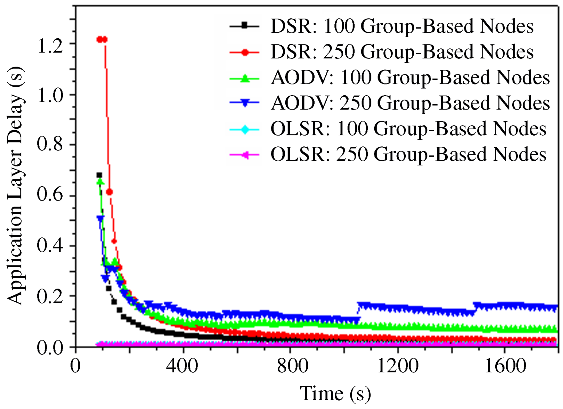


Fig.20. Comparison of the average delay at application layer in mobile topologies.

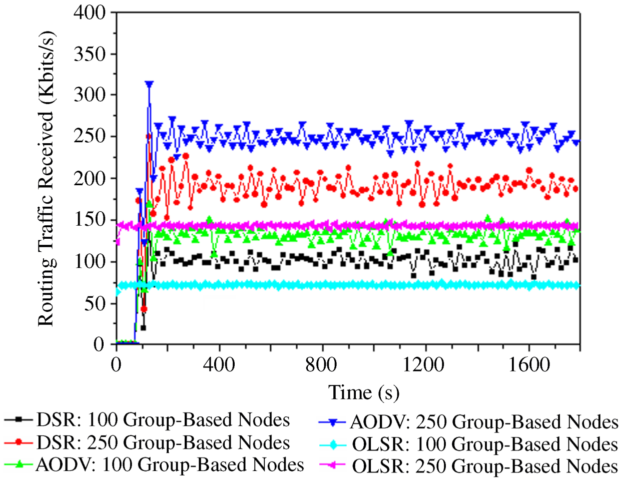


Fig.21. Comparison of routing traffic received in fixed topologies.

The average throughput consumed in the fixed group-based topologies is compared in Fig.23. The protocol that consumes the lowest throughput is the DSR protocol (90Kbits/s in the 100-node topology and 170Kbits/s in the 250-node topology). The protocol with the most stable throughput consumed is the OLSR

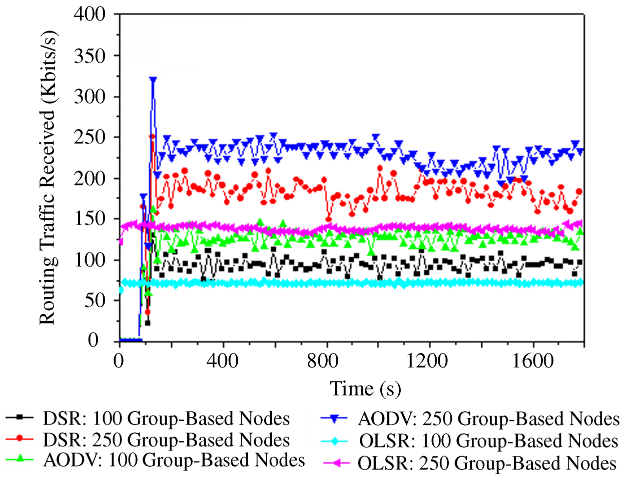


Fig.22. Comparison of routing traffic received in mobile topologies.

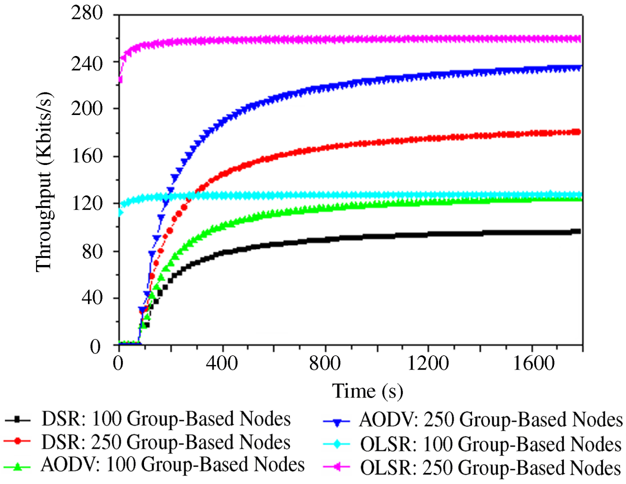


Fig.23. Comparison of average throughputs consumed in fixed topologies.

protocol. When the network converges, both AODV and OLSR protocols have the same average throughput in the 100-node topology, but the OLSR protocol has the lowest convergence time.

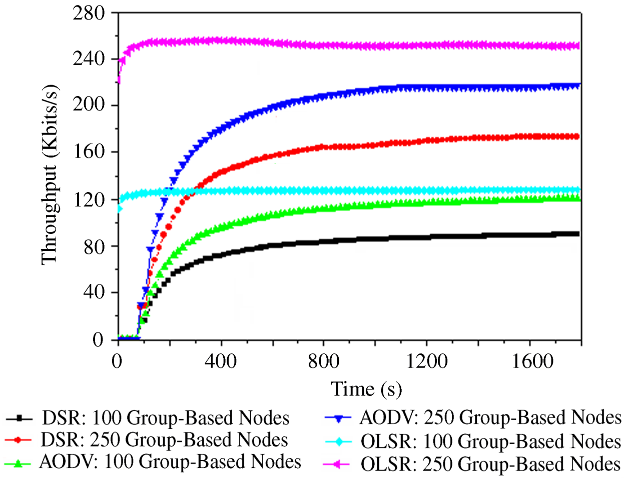


Fig.24. Comparison of average throughputs consumed in mobile topologies.

In case of having a group-based topology with mobility, errors and failures (see Fig.24), the results are very similar to the previous ones. The protocol that consumes lower throughput is DSR. AODV protocol consumes lower throughput while the network is converging, but this throughput becomes very similar to the one given by OLSR protocol when the network converges. OLSR protocol is still the most stable.

4.6 Analyzed Protocols Summary

In this subsection we show the benefits of using a group-based topology in ad-hoc networks, and we show several examples in which they can be used. We have simulated DSR, AODV and OLSR protocols with and without groups and the results show that group-based topologies give better performance.

In Table 1 we can see a summary where there is percentage improvement when group-based topologies are used.

Table 1. Percentage of Improvement When Group-Based Topologies Are Used

	Fixed Topology	Fixed Topology	Mobile Topology	Mobile Topology
	(100 Nodes)	(250 Nodes)	(100 Nodes)	(250 Nodes)
DSR Average Delay at the Application Layer	75%	83%	5%	5%
DSR Routing Traffic Received	60%	60%	46%	55%
DSR Mean Throughput	56%	59%	48%	55%
AODV Average Delay at the Application Layer	70%	70%	67%	75%
AODV Routing Traffic Received	39%	43%	32%	43%
AODV Mean Throughput	40%	47%	37%	47%
OLSR Average Delay at the Application Layer	60%	76%	64%	60%
OLSR Routing Traffic Received	61%	50%	61%	50%
OLSR Mean Throughput	54%	61%	52%	60%

Table 2. Comparison of Mobile and Ad-Hoc Routing Protocols in Group-Based Topologies

	Best in Fixed	Best in Mobile	Worst in Fixed	Worst in Mobile
Delay at MAC Layer	OLSR	OLSR	DSR	AODV
Throughput Consumed	DSR	DSR	AODV & OLSR	AODV & OLSR
MANET Traffic	AODV	DSR	OLSR	OLSR
Routing Traffic Sent	OLSR	OLSR	AODV	AODV
Routing Traffic Received	OLSR	OLSR	AODV	AODV
Delay at Application Layer	DSR & OLSR	OLSR	AODV	AODV
Average Number of Hops in a Path	AODV	DSR	AODV	DSR
Route Request Sent	DSR	AODV	DSR	AODV

In this study we have made other measures. Table 2 shows the best and worst protocols for every one of the parameters analyzed.

The best improvement percentage, when group-based topologies were used, came from the DSR protocol when the average delay at the application layer was simulated. On the other hand, in the same case for mobile topologies, DSR protocol gave the worst percentage of improvement.

We observed it has more percentage of improvement in fixed topologies when there are more nodes in the topology, but when there is a mobile topology, the improvement is higher in the topology with lower number of nodes. We have also observed that when a routing protocol is the best one in a fixed group-based topology, it continues being the best one in the mobile group-based topology. On the other hand, we observed that a routing protocol, which is the best (or worst) in a group-based fixed topology, could not be the best (or worst) in the mobile topology. The routing protocol that appeared as the best one was OLSR and the one that appeared as the worst was AODV.

5 Architecture Description

5.1 Architecture Operation

We propose an architecture of nodes and a protocol based on the creation of groups of nodes where nodes have the same functionality in the network. Every group has a central node that limits the zone where the node from the same group will be placed, but its functionality is the same as the rest of the nodes. Every node has a *nodeID* that is unique in its group. The first node in the network acquires a group identifier (*groupID*) that is given manually, using GPS (Global Positioning System), or using a wireless location system or through other means[28]. New joining nodes will know their group identifier from their new neighbors. Border nodes are, physically, the edge nodes of the group. When there is an event in a node, this event is sent to all the nodes in its group in order to take appropriate actions. All nodes in a group know all the information about their group. Border nodes have connections with other border nodes from neighbor groups and are used for sending information to other groups or receiving information from other groups and distributing it inside. Because a fast routing protocol is needed, we have chosen SPF (Shortest Path First) routing algorithm[29] to route information, but it can be changed by the other routing protocols depending on the network's characteristics. When the information is for a node of the same group it is routed using the *nodeID*. Every node runs SPF algorithm locally and selects the best path to a destination based on a metric. But, when the information has to be sent to other groups, the information is routed directly to the closest border node to the destination group using the *groupID*. When a node from a destination group receives the information, it routes it to all nodes in its group using Reverse Path Forwarding Algorithm[30]. Links between border nodes from different groups are established primarily as a function of their positions, but, in the case of multiple possibilities, neighbors are selected as a function of their capacity λ which will be explained in the following section. In order to establish the boundaries of the group, we can consider two choices: (i) limiting the diameter of the group to a maximum number of hops (e.g., 30 hops, as the maximum number of hops for a tracer of a route), and (ii) establishing the boundaries of the area that is to be covered. Fig.25 shows the proposed architecture topology.

5.2 Analytical Model and Neighbor Selection

Every node has 3 parameters (*nodeID*, *groupID* and λ) that characterize the node. Let λ parameter be the node capacity that depends on the node's upstream and downstream bandwidth (in Kbps), its number of available links (*Available_Con*) and its maximum number of links (*Max_Con*), its percentage of available load and its energy consumption. It is used for determining the best node to connect with. The higher the λ parameter,

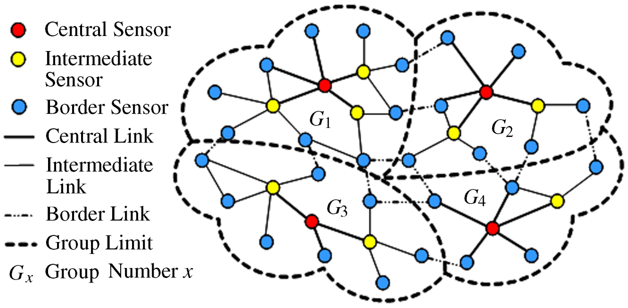


Fig.25. Proposed architecture topology.

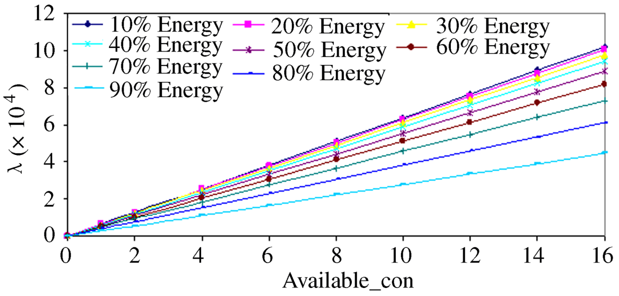


Fig.26. λ parameter values with number of links variation.

the better node to connect with. λ equation is shown in (1)

$$\lambda = \frac{(BW_{\text{up}} + BW_{\text{down}}) \cdot \mathit{Available\_Con} \cdot L + K_2}{\mathit{Max\_Con}} \cdot \sqrt{1 - \frac{E^2}{K_1}}, \tag{1}$$

L is the available load and E is the energy consumption. Their values vary from 0 to 100. $E = 0$ indicates it is fully charged, so λ parameter is 0 and $E = 100$ indicates it is fully discharged.

K_1 defines the minimum value of energy remaining in a node to be suitable for being selected as a neighbor. K_2 gives different λ values from 0 in the case of $L = 0$ or $\mathit{Available\_Con} = 0$. We have considered $K_2 = 100$, to get λ into desired values. Fig.26 shows λ parameter values at the time when the maximum number of links for a node is 16, for a bandwidth value of 2Mbps, as a function of its available number of links for different available energy values of the node. Node's load is fixed to 50%. Fig.27 shows λ parameter values when the maximum number of links of the node is 16 as a function of the node energy available for different bandwidth values. Node's load is fixed to 80% and all nodes have 6 available number of links ($\mathit{Available\_con} = 6$). It shows that as the Energy is being consumed, λ parameter is lower, but when it gets the 80% of consumption, the λ parameter decreases drastically, so the node is more likely to be chosen as a neighbour, in case of more energy available. Fig.27 also shows that a node with higher bandwidth is preferred.

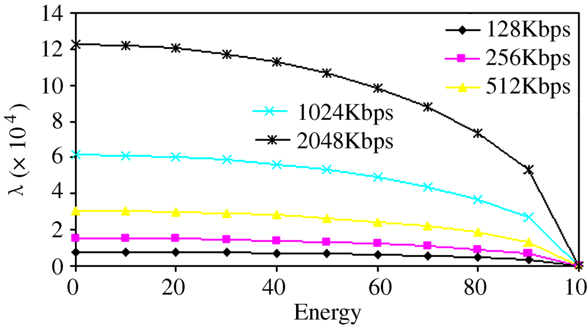


Fig.27. λ values as a function of the Energy of the node.

We have defined the cost of the i-th node as the inverse of the i-th node parameter multiplied by T (the delay of its reply in ms). The cost is shown in (2)

$$C = \frac{T \cdot K_3}{\lambda}. \tag{2}$$

$K_3 = 10^3$ gives $C \geqslant 1$. The metric for each route is based on the hops to a destination (r) and on the cost of the nodes (C_i) in the route as shown in (3)

$$\mathit{metric} = \sum_{i=1}^{r} C_i. \tag{3}$$

The metric gives the best path to reach a node.

Let $G = (V, \lambda, E)$ be a network of nodes, where V is the set of nodes, λ is the set of their capacities ($\lambda(i)$ is the capacity of the i-th node and $\lambda(i) \neq 0$ $\forall i$-th node) and E is the set of links between nodes. Let k be a finite number of disjoint subsets of V, so $V = \cup V_k$, and there is no node in two or more subsets ($\cap V_k = 0$), and let $n = |V|$ (the number of nodes in V), the equation given for n is shown in (4)

$$n = \sum_{i=1}^{k} |V_k|. \tag{4}$$

Every V_k has a central node, several intermediate nodes and several border nodes as shown in (5)

$$n = 1 + n_{\text{intermediate}} + n_{\text{border}}. \tag{5}$$

Now we can describe the whole network as the sum of all these nodes from all groups as shown in (6)

$$\begin{aligned} n &= \sum_{i=1}^{k} |(n_{\text{central}} + n_{\text{intermediate}} + n_{\text{border}})_k| \\ &= k + \sum_{i=1}^{k} (|n_{\text{intermediate}}|)_k + \sum_{i=1}^{k} (|n_{\text{border}}|)_k. \end{aligned} \tag{6}$$

On the other hand, the number of links in the whole network $m = |E|$ depends on the number of groups (k), on the number of links in each group (k_m) and on the number of links between border nodes. (7) gives m value for a physical topology.

$$m = \sum_{i=1}^{k} \left(k_l + \frac{1}{2}k_b\right) \tag{7}$$

where k_l is the number of links inside the group k and k_b is the number of external links of the group k.

6 Protocol Operation and Messages

This section describes the designed messages and how the designed protocol operates.

6.1 Group Creation and Maintenance

Let a new node join the network (it could be the first). It sends a hello message (called *helloGroup*) in order to join a group. If there is no response from any node for 3 seconds, the node considers itself as a central node of a group in the network, and it will take the value *groupID* = 1 and *nodeID* = 1. When the node receives *helloGroup ACK* messages from several candidate neighbors, first it puts a timestamp on their reply and chooses the best nodes to have a link with (this election is taken based on the λ parameter which comes in the *helloGroup ACK* message). The timestamp will be used to calculate C parameter. Responses received after 3 seconds will be discarded. In case of receiving replies from nodes of different groups, it will choose the group whose replies have the highest average λ parameter, so it will take into account replies only from that group. Then, the node will send an *okGroup* message to the selected neighbors, and the neighbors will reply with the *okGroup ACK* message with the assigned *nodeID* and indicates the link has been established. Nodes will send *keepalive* messages periodically to their neighbors. If a node does not receive a *keepalive* message from a neighbor before the dead time, it will remove this entry from its database and will start the group update process. As the *groupID* is in the *helloGroup ACK* message, the new node will know which group has joined. Finally, the neighbor node will send a *newNode* message to the central node, to run the algorithm for changing the central node if needed.

Links between border nodes from different groups are established as a function of their replying delay and the λ parameter of the replying nodes, but it could be changed by an algorithm using node's position or choosing the neighbor with the shortest distance (in number of hops) to the central node. If we base our proposal on the λ parameter, we will distribute the load of the network between groups, but if we base our proposal on a node's position or choose the neighbor with the shortest distance to the central node we will balance the number of nodes in the groups.

When a new node joins the group, the central node of the group could be changed. The procedure designed for changing the central node is as follows. We define the group diameter (d_{group}) as the smallest number of hops, between the two most remote nodes in the group (in our case, $d_{\text{group}} \leqslant 30$).

When there is a change of the central node of a group, all the nodes in the group must be alerted. In order to update all nodes in the group, the new central node will send a *changeCentral* message to indicate the new central node and the distance from it to the node processing this control packet. This update is distributed using the Recursive Proportional-Feedback (RPF) algorithm. Once the links between neighbors are established, every node sends *keepalive* messages periodically to its neighbors. Figs.28 and 29 show the procedure when the central node changes and when it does not. It is also shown in Fig.30.

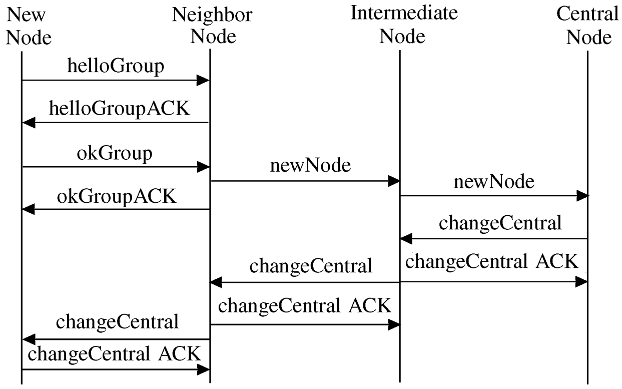


Fig.28. Messages when central node changes.

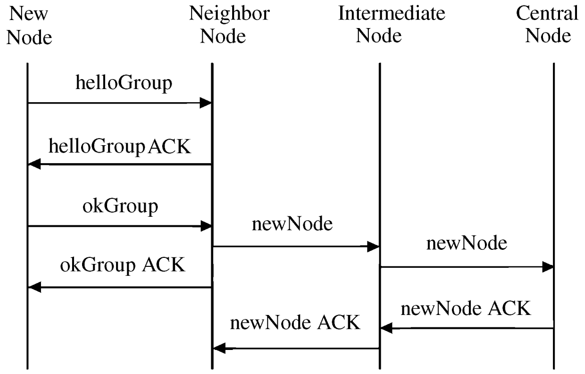


Fig.29. Messages when it does not change.

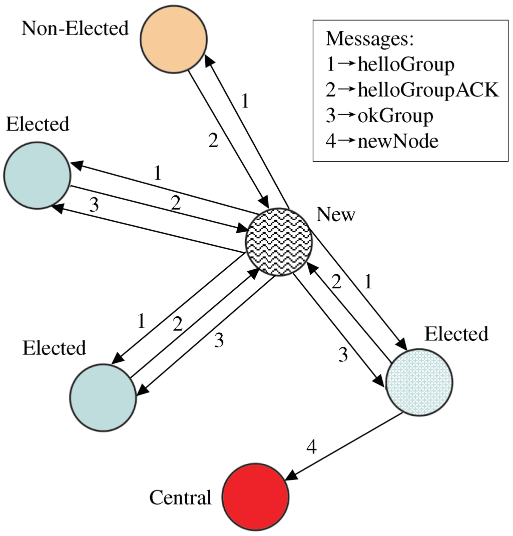


Fig.30. Message exchange when a new node joins the group.

We have proposed two choices to establish the boundaries of the group.

1) When the boundaries of the group are the same as the area that is to be covered, border nodes are known using GPS.

2) When the boundary of the group is limited by the diameter of the group, the maximum number of hops from the central node must be known. Every time a new node joins a group, it receives the *newNode ACK* message with the number of hops to the central node. When it achieves the maximum number of hops, the node is marked as a border node, and it will inform new joining nodes that they must create a new group.

6.2 Leavings and Fault Tolerance

When a node leaves the group, it will send *nodeDisconnect* message to its neighbor nodes. They must reply with a *nodeDisconnect ACK* message and send to the central node the *nodeDisconnect* message. The central node distributes the update information using RPF algorithm. If the neighbor node does not have links with other neighbors, it must start a new connection process sending a *helloGroup* message. If the leaving node is the central node, it assigns the central node role to the best candidate. This decision is taken using the value of the diameter of the group. In case of a draw, it will choose the older one in the group. Then, it sends a *changeCentral* message to the group to inform them and leaves the group. When a node fails down, its neighbor nodes will know the failure because of the absence of its *keepalive* messages. The procedure is the same as when the node leaves the network voluntarily. The central node calculates which is the best candidate, and the neighbor node will be informed by periodical *keepalive-Central* messages. New central node will distribute the update.

7 Simulations

Let T_i be the time needed by two nodes to communicate with each other, and RTT (Round Trip Time) be the mean value of the round trip time between both nodes. So, T_i can be calculated using the (8)

$$T_i = \frac{RTT_i}{2}. \tag{8}$$

The time needed to communicate a source node with a destination node in a different group is calculated using the expression given for $T_{\text{max\_intergroup}}$ in (9)

$$T_{\text{max\_intergroup}} = t_{\text{source\_border}} + \sum_{i=1}^{n} t_{\text{max\_intragroup\_}i} + \sum_{i=1}^{n+1} t_{\text{border\_}i\text{-border\_}i+1}, \tag{9}$$

n is the number of intermediate groups, $t_{\text{source\_border}}$ is the time needed to arrive from the source node to the border node in the same group, $t_{\text{max\_intragroup\_}i}$ is the time required to go through the i-th group, and $t_{\text{border\_}i\text{-border\_}i+1}$ is the time needed to transmit the information from the border node of a group to the border node of another group connected to the previous one.

We define t_p as the average propagation time for all the message transmissions between two nodes in the architecture. Its expression is shown in (10)

$$t_p = \frac{\sum_{i=1}^{m} T_i}{m}, \tag{10}$$

m represents the number of nodes involved in the path minus one. Taking into account t_p, the time needed to transmit information from the source node to the border node of the same group ($T_{\text{source\_border}}$) is defined in (11)

$$T_{\text{source\_border}} = d_{\text{source\_border}} \cdot t_p, \tag{11}$$

$d_{\text{source\_border}}$ are the number of hops needed to arrive form the source node to the border node of the same group. The maximum time to cross through a group ($T_{\text{max\_intragroup\_}i}$) is defined by the expression shown in (12)

$$T_{\text{max\_intragroup}} = d_i \cdot t_p, \tag{12}$$

i indicates the group and the d_i is the number of hops in the group. On the other hand, the number of hops for j groups is shown in (13)

$$d_i = \sum_{j=1}^{d_j} d_j. \tag{13}$$

Replacing equations in (10), (11), (12) and (13) in (9), we obtain (14)

$$T_{\text{max\_intergroup}} = \left(d_{\text{source\_border}} + \sum_{i=1}^{n} d_i + n + 1\right) \cdot t_p. \tag{14}$$

In Fig.31, we see how the interconnection time evolves between nodes of different groups.

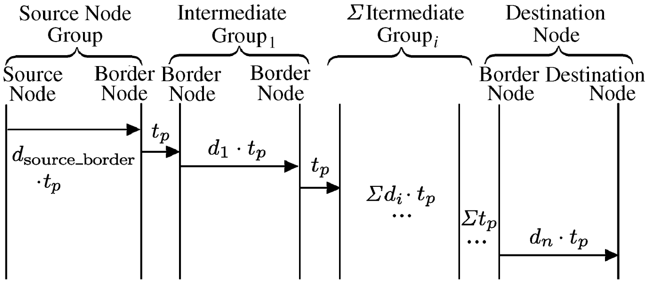


Fig.31. Connection time between nodes of different groups.

In the following subsections we are going to use (14) in order to model our proposal.

7.1 Connection Time Variation as a Function of the Number of Hops to the Border Node When All the Groups Have the Same Number of Hops

In order to do this simulation, we use a constant value for the number of intermediate groups and we varied the number of hops between the source node and the border node of its group. Then, we can observe what happens when the number of hops of the intermediate groups increases.

We have chosen the number of intermediate groups as 4. Considering that all the intermediate groups have the same number of hops, it means $d_1 = d_2 = d_3 = d_4 = d$, and introducing these values in (6) we obtain (15)

$$T_{\text{max\_intergroup}} = (d_{\text{source\_border}} + 4 \cdot d + 5) \cdot t_p. \tag{15}$$

When we give higher values to $d_{\text{source\_border}}$ for each value of d, the maximum inter group time ($T_{\text{max\_intergroup}}$) increases lineally.

7.2 Connection Time Variation When the Number of Hops to Cross the Groups Varies

This subsection studies what happens when we maintain the distance between the source node and the border node of the source group constant and we vary the number of hops of the intermediate groups and for different number of groups. We fix the parameter $d_{\text{source\_border}}$ to a value of 10. Using (14), (16) is obtained.

$$T_{\text{max\_intergroup}} = \left(11 + \sum_{i=1}^{n} d_i + n\right) \cdot t_p. \tag{16}$$

Now, we can vary d_i to observe the time needed to achieve its destination. Results are shown in Fig.32. We can deduce that the number of groups in a network does not affect the connection time to a large extent when the mean number of hops to go through the groups is small. Nevertheless, when the mean diameter of the groups is big, increasing the number of intermediate groups implies a large increase in the connection time. So, we can state that the mean diameter of the groups becomes more relevant in the calculation of the final connection time ($T_{\text{max\_intergroup}}$) for bigger networks.

In Fig.33, we can observe how the connection time varies according to the number of groups for different numbers of hops. We have chosen $d_{\text{source\_border}} = 20$, and we have varied the number of groups that will be crossed for different mean diameters of the groups, instead of varying the mean diameter of the groups.

7.3 Connection Time Variation for Different Number of Groups and Different Distances Between Source and Border Nodes in the Same Group

In this subsection we analyze how the maximum inter group time varies when we maintain the mean diameter of the group as a constant value and vary the number of groups for different distances between the source and the border nodes of the same group. To perform this experiment, we have chosen 20 as the mean diameter of the groups. (17) shows the connection time depends on the distance between the source and the border nodes in the same group and on the amount of groups in the network.

$$T_{\text{max\_intergroup}} = (d_{\text{source\_border}} + 21 \cdot n + 1) \cdot t_p. \tag{17}$$

Fig.34 shows the behavior of the $T_{\text{max\_intergroup}}$ as a function of n for several $d_{\text{source\_border}}$ values. The maximum inter group time (t_p) increases when the number of intermediate groups increases. This has happened in all the analyzed cases. Nevertheless, as we can see, there is not a big difference in the final time when we have a large or short distance between the source and the border node ($d_{\text{source\_border}}$). It means that the number of hops between the source and the border node ($d_{\text{source\_border}}$) is more relevant for having better $T_{\text{max\_intergroup}}$ that the number of groups when there are few groups. This is an important subject to take into account when designing node networks.

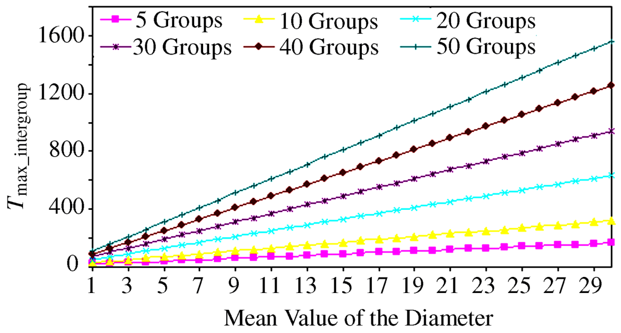


Fig.32. $T_{\text{max\_intergroup}}$ variation according to the mean diameter of the groups.

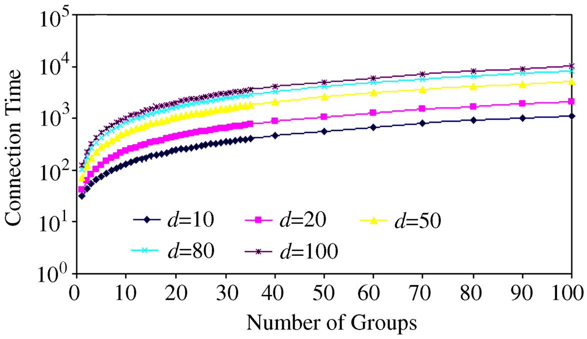


Fig.33. Connection time variation for different diameters.

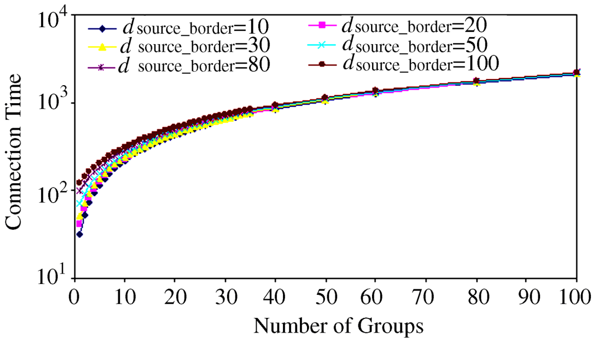


Fig.34. Connection time variation according to the number of hops to the border nodes.

7.4 Connection Time for Getting a Destination Group According to the Diameters of the Groups

In this subsection, we show the results of several simulations that give us an objective point of view about how to design a group-based node network to obtain a short connection time between two nodes belonging to different groups. We have simulated the time needed by a message sent by a node in a group until it arrives at another node of another group. Then, we observed the variation of the number of hops and the variation of the time needed to reach the destination group.

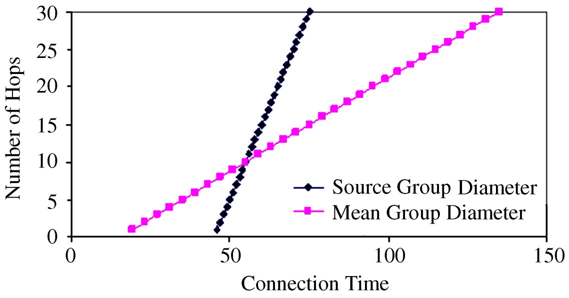


Fig.35. Connection time to reach the destination group according to the number of hops.

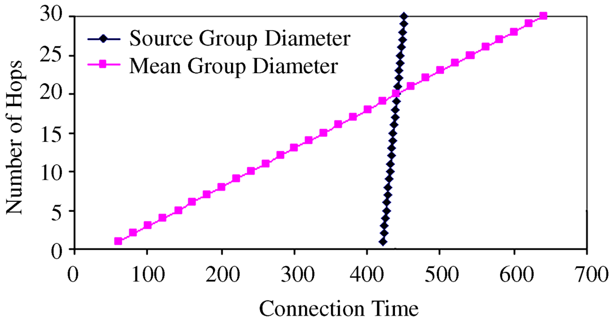


Fig.36. Connection time to reach the destination group according to the number of hops.

In Fig.35 we see the connection time of the two groups in a network with 4 groups. In order to obtain the series of the source group, we have fixed a value of 10 hops for the mean diameter of the groups and the diameter of the source group has varied between 1 and 30 hops (we have considered that groups have a maximum diameter of 30 hops). To obtain the series of the mean diameter of the group, we have fixed a value of 10 hops for the diameter of the source group and the mean diameter of the groups varies between 1 and 30 hops. As we can see, the connection time between 2 nodes increases more when the mean diameter of the intermediate groups increases. Moreover, the interconnection time between the two nodes is not so significant when the diameter of the source group increases.

In Fig.36, we have simulated the connection time between two nodes of a network with 20 groups. In order to obtain the series of the source group, a mean diameter of the groups of 20 hops has been fixed and the diameter of the source group has been varied between 1 and 30 hops. To obtain the series of the mean diameter of the group, a diameter of the source group of 20 hops has been fixed and the mean diameter of the intermediate groups varies between 1 and 30 hops.

In Figs.35 and 36, we can observe that the delay (connection time) increases when the mean diameter of the groups increases, but that increase is less significant when the number of hops from the source node to the border node of the same group increases, as we expected. Note that when we want to design a group-based network with many groups, the best solution is to increase the mean diameter of the intermediate groups instead of increasing the diameter of the source group. When a network with few groups is needed, the interconnection time varies less when we increase the number of hops in the source group.

8 Network Comparison

This section shows the comparison of our proposal with other planar group-based networks. The first one is the proposal of Xiang *et al.* (a locality-aware overlay network based on groups[31] is proposed, which has been used for Peer-to-Peer Based Multimedia Distribution Service[14]). The second one is the cluster-based network.

Table 3 shows the comparison. Our proposal stands out because of its higher efficiency in the neighbor selection system (we have added the capacity parameter), lower management cost, high fault tolerance and very high scalability.

9 Conclusions

A group-based architecture provides some benefits for the whole network. It provides fault tolerance because other groups could carry out tasks from a failed group and it is very scalable because a new group could be added to the system easily. On the other hand, a group-based network can significantly decrease the communication cost between end-hosts by ensuring that a message reaches its destination with little overheads and highly efficient forwarding. Grouping nodes increases the productivity and the performance of the network with low overheads and low extra network traffic.

In this paper we have proposed a group-based architecture where links between groups can be established by physical proximity plus the neighbor node capacity. Its operation, maintenance and fault tolerance have been detailed. Messages designed to work properly have been shown. All simulations show its viability and how it could be designed to improve its performance. Finally we have compared it with another group-based logical architecture to show their differences.

Table 3. Planar Group-Based Topologies Comparison

	Locality-Aware Overlay Network (Z. Xiang *et al.*)	Cluster Based Topologies	Our Group-Based Proposal
Need of a Rendezvous Point	Yes	No	No
Nodes with Higher Role	No	Yes	No
Type of Topology	Logical (but it could be implemented in physical)	Physical and Logical	Physical (but it could be implemented in logical)
Neighbor Selection	Proximity in the Underlying Network (IP)	Physical Proximity	Physical Proximity + Capacity
Which Group to Join In	Based on Rendezvous Point Decision + Boot Nodes	Proximity	Based on Neighbor Discovery (time to reply or closest)
Management Cost	Medium (because of the rendezvous point)	Medium (because of cluster head)	Low
Fault Tolerance	Very Low (because Rendezvous Point or boot nodes failure)	Low (because cluster head failure)	Very Much
Scalability	Very Much (depending on the RP)	Medium	Very Much
Availability	Low (when boot nodes from head a group are not available, the group is not available)	Low (when a cluster head is not available, the group is not available)	Very High (when a sensor finds a neighbor it joins the network)

The architecture proposed can be used for specific cases or environments, such as the ones which require the set up of a network where groups appear and join the network or by networks that are wanted to be split into smaller zones to support a large number of sensors. There are many application areas for this proposal such as rural and agricultural environments or even for military purposes. Now, we are programming the protocol for a specific wireless sensor device to test it over a real environment.

References

[1] Akyildiz I F, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. *IEEE Communications Magazine*, 2002, 40: 102–114.

[2] Frodigh M, Johansson P, Larsson P. Wireless ad hoc networking. The art of networking without a network. *Ericsson Review,* 2000, (4): 248–263.

[3] Kumar S, Raghavan V S, Deng J. Medium access control protocols for ad hoc wireless networks: A survey. *Ad Hoc Networks,* May 2006, 4(3): 326–358.

[4] Royer E M, Toh C K. A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Communications,* April 1999, 6(2): 46–55.

[5] Rajaraman R. Topology control and routing in ad hoc networks: A survey. *ACM SIGACT News,* June 2002, 33(2): 60–73.

[6] Ratnasamy S, Handley M, Karp R, Shenker S. Topologically-aware overlay construction and server selection. In *Proc. InfoCom*, New York, USA, June 2002, pp.1190–1199.

[7] Lv Q, Ratnasamy S, Shenker S. Can heterogeneity make Gnutella scalable? In *Proc. the First International Workshop on Peer-to-Peer Systems*, MIT, Cambridge, MA, USA, March 7∼8, 2002, pp.94–103.

[8] Woolston K, Albin S. The design of centralized networks with reliability and availability constraints. *Computers and Operations Research,* May 1988, 15(3): 207–217.

[9] Liu-Sheng Huang, Hong-Li Xu, Yang Wang, Jun-Min Wu, Hong Li. Coverage and exposure paths in wireless sensor networks. *Journal of Computer Science and Technology,* July 2006, 21(4): 490–495.

[10] Jaeook Lee, Sun Kang. Satellite over satellite (SOS) network: A novel architecture for satellite network. In *Proc. IEEE Infocom 2000,* Tel Aviv, Israel, March 26∼30, 2000, pp.315–351.

[11] Ganz A, Krishna C M, Tang D, Haas Z J. On optimal design of multitier wireless cellular systems. *Communications Magazine, IEEE,* February 1997, 35(2): 88–93.

[12] Chong-Yi Yuan, Wen Zhao, Shi-Kun Zhang, Yu Huang. A three-layer model for business processes — Process logic, case semantics and workflow management. *Journal of Computer Science and Technology,* May 2006, 22(3): 410–425.

[13] Wierzbicki A, Strzelecki R, Swierczewski D, Znojek M. Rhubarb: A tool for developing scalable and secure peer-to-peer applications. In *Proc. Second IEEE International Conference on Peer-to-Peer Computing,* Linköping, Sweden, 5∼7 September 2002, pp.144–151.

[14] Xiang Z, Zhang Q, Zhu W, Zhang Z, Zhang Y. Peer-to-peer based multimedia distribution service. *IEEE Transactions on Multimedia,* April 2004, 6(2): 343–355.

[15] Hongjun L, Luo L P, Zhifeng Z. A structured hierarchical P2P model based on a rigorous binary tree code algorithm. *Future Generation Computer Systems,* February 2007, 23(2): 201–208.

[16] Thallner B, Moser H. Topology control for fault-tolerant communication in highly dynamic wireless networks. In *Proc. the 3rd International Workshop on Intelligent Solutions in Embedded Systems*, Hamburg University of Technology, Hamburg, Germany, May 20, 2005, pp.89–100.

[17] Yu J Y, Chong P H J. A survey of clustering schemes for mobile ad hoc networks. *IEEE Communications Surveys & Tutorials,* 2005, 7(1): 32–48.

[18] Jiang M, Li J, Tay Y C. Cluster based routing protocol (CBRP). Internet-draft, draft-ietf-manet-cbrp-spec-01.txt, National University of Singapore, August 14, 1999.

[19] Chiang C C, Wu H K, Liu W, Gerla M. Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel. In *Proc. the IEEE SICON'97*, National University of Singapore, Kent Ridge, Singapore, April 14∼17, 1997, pp.197–211.

[20] Zygmunt J Hass, Marc R Pearlman, Prince Samar. The zone routing protocol (ZRP) for ad hoc networks. IETF, Internet Draft, draft-ietf-manet-zone-zrp-04.txt, July 2002.

[21] Haas Z J, Pearlman M R. The Zone Routing Protocol: A Hybrid Framework for Routing in Ad Hoc Networks. Ad Hoc Networks, Perkins C E (ed.), Reading, MA: Addison-Wesley, 2000.

[22] Mirco Musolesi, Cecilia Mascolo. A community based mobility model for ad hoc network research. In *Proc. Second International Workshop on Multi-Hop Ad Hoc Networks: From Theory to Reality, REALMAN 2006*, Florence, Italy, May 26, 2006, pp.31–38.

[23] Tsuchiya P F. The landmark hierarchy: A new hierarchy for routing in very large networks. *Computer Communication Review,* August 1988, 18(4): 35–42.

[24] Rekhter T, Li T. A border gateway protocol 4 (BGP-4). RFC 1771, March 1995.

[25] Pei G, Gerla M, Hong X. LANMAR: Landmark routing for large scale wireless ad hoc networks with group mobility. In *Proc. IEEE/ACM MobiHOC*, Boston, MA, USA, August 2000, pp.11–18. .

[26] Srdjan Krco. Health care sensor networks — Architecture and protocols. *Ad Hoc & Sensor Wireless Networks,* 2005, 1(1/2): 1–25.

[27] OPNET Modeler website. http://www.opnet.com/solutions/network_rd/modeler.html.

[28] P Gober, A Ziviani, P Todorova *et al.* Topology control and localization in wireless ad hoc and sensor networks. *Ad Hoc & Sensor Wireless Networks,* Oct. 2005, 1(4): 301–321.

[29] McQuillan J M, Richer I, Rosen E C. The new routing algorithm for the ARPANET. *IEEE Transactions on Communications,* May 1980, 28(5): 711–719.

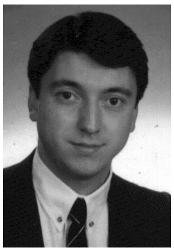
[30] Dalal Y K, Metcalfe R M. Reverse path forwarding of broadcast packets. *Communications of the ACM,* December 1978, 21(12): 1040–1048.

[31] Zhang X, Zhang Q, Zhang Z, Song G, Zhu W. A construction of locality-aware overlay network: mOverlay and its performance. *IEEE Journal on Selected Areas in Communications,* January 2004, 22(1): 18–28.

Jaime Lloret received his M.Sc. degree in physics in 1997 from University of Valencia and a postgraduate Master in corporative networks and systems integration in 1999. He received his M.Sc. degree in electronic engineering in 2003 from University of Valencia and his Ph.D. degree in telecommunication engineering from the Polytechnic University of Valencia in 2006. He obtained the first place given by the Spanish Agency for Quality Assessment and Accreditation for the Campus of Excellence in the New Technologies and Applied Sciences area and he was awarded the prize of the best doctoral student in the telecommunications area in 2006 according to the Social Council of the Polytechnic University of Valencia. He is a Cisco Certified Network Professional Instructor. He worked as a network designer and administrator in several companies. He has been editor of several conference proceedings and associated editor and guest editor of several international journals. Dr. Lloret has been involved in more than 40 program committees of international conferences till 2008. He was the chairman of SENSORCOMM 2007 and UBICOMM 2008.

Miguel Garcia received the M.Sc. degree in telecommunication engineering in 2007 from Polythecnic University of Valencia in Spain. He is currently a Ph.D. candidate in the Department of Communications of the Polythecnic University of Valencia. His major research interest includes sensor, ad-hoc and P2P networks, and grid computing. He has been technical committee member in several conferences. He is a CCNA Cisco instructor and an IEEE student member.

Jesus Tomás graduated in computer science in 1993 from Polytechnic University of Valencia. He finished his dissertation in 2004. From 1993 he is a lecturer at Polytechnic University of Valencia. He is member of the Pattern Recognition and Human Language Technology Group, the "Instituto Tecnológico de Informática". His main research focus is on speech recognition and machine translation. In these areas, he has been involved in a number of projects with public and private budgets.



Fernando Boronat was born in Gandia, Spain and went to the Polytechnic University of Valencia (UPV) in Spain, where he obtained, in 1993, his M.Sc. degree in telecommunications engineering. From 1994 he worked for a couple of years for Telecommunication Companies. In 1996 he moved back to the UPV, where he is a lecturer in the Communications Department at the Escuela Politécnica Superior de Gandia. He obtained his Ph.D. degree in 2004 and his topics of interest are communication networks, multimedia systems and multimedia synchronization protocols. He is a member of IEEE since 1993 and is involved in several TPCs of national and international conferences.