Computer Communications 31 (2008) 3438–3450

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Improving networks using group-based topologies

Jaime Lloret [*], Carlos Palau, Fernando Boronat, Jesus Tomas

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

ARTICLE INFO

Article history:
Received 25 November 2007
Received in revised form 27 May 2008
Accepted 27 May 2008
Available online 6 June 2008

Keywords:
Group-based topologies
Group-based networks
Improving performance

ABSTRACT

Communication network topology design needs to address several conflicting requirements, such as minimizing the overall network diameter, minimizing the infrastructure cost, minimizing management cost, maximizing load distribution and so on. Centralized, decentralized, and partially centralized networks have their respective benefits as well as several drawbacks. It is known that grouping nodes gives better performance to the group and to the whole system, thereby avoiding unnecessary message forwarding and additional overheads. This paper proposes a survey of group-based topologies. It shows their main issues and in which real environments they could be used. The improvement of the networks by using these kinds of topologies will also be discussed. We have split group-based topologies into two classes, planar and layered group-based topologies, and we will discuss existing group-based systems in both types. Highlighting one of the main aims of the paper, their comparison, benefits and drawbacks are presented. Finally, authors will describe two group-based topologies designed by them, one for planar group-based topologies and another for layered group-based topologies, and they will be compared with different previous works. We consider this work as a starting point for researchers on new group-based topologies.

1. Introduction

A central problem in the planning of any kind of network is to design the communication topology, how peers are connected as well as how their messages are passed. Topologies can be characterized by several parameters such as the number of nodes in the network, the number of links or connections (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 minimizing such things as the overall network diameter, the convergence time, the infrastructure cost (total number of links), book-keeping costs (number of links maintained by each) and management cost while maximizing items such as load distribution, reliability, efficiency and fault tolerance, the performance of the system, the scalability, and so on.

Usually, optimizing on any requirement 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. On the other hand, in order to provide real-time infrastructures, reliable, available and efficient networks and QoS-aware multimedia distribution services, a topology-aware network is necessary [1,2].

While the physical topology defines how the nodes on a network are physically connected, the physical layout of the devices on the network, the logical topology defines how the nodes on the network communicate, i.e. the way that the data passes through the network, with each other without regard to the physical interconnection of 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 much of the network resources, and hence degrade data delivery performance significantly. Regardless of the case we are talking about, three kinds of networks can be distinguished:

- Centralized networks
- Decentralized networks
- Partially centralized networks

All of them will be described and compared in the following section.

As far as we know, there is not any survey of group-based topologies in existence, so we hope this paper could be a good starting point for researchers on group-based topologies. On the other hand, this paper will show the main issues and benefits of group-based topologies.

The rest of the paper is structured as follows. Different kinds of known networks are listed in Section 2. Section 3 explains what a group-based architecture is and gives some examples where it could be applied. Some mathematical considerations, when

[*] Corresponding author. Tel.: +34 609549043.
E-mail address: jlloret@dcom.upv.es (J. Lloret).

0140-3664/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2008.05.030

group-based topologies are used in the network, are shown in Section 4. Several works in the literature related with group based topologies are described in Section 5. Section 6 presents two group-based architectures developed by the same authors of this paper. The comparison of all group-based topologies shown in this paper is given in Section 7. Finally, Section 8 gives the conclusions.

2. Networks classification

Networks can be classified taking into account different parameters such as the proximity of the devices, the structure, transmission techniques and so on. But, in this paper, they will be classified by using the grade of centralization of the topology because one of the main goals of our research is to balance the load and to avoid points of failure. Taking it into account, the following main types can be observed:

1. Centralized Networks (also called server-based systems in logical networks). They are topologies in which there could be no direct connection between nodes and all nodes' messages could be mediated by a mediator generally known as a central device. It acts as a gateway for all nodes. In logical topologies the central server is to be consulted (e.g. for services, resources, nodes information and so on) keeping track of active services, nodes and indexes of shared contents. Normally, messages are passed via the server, participating in content transfer actions, but sometimes messages are sent directly between edge nodes. One of the main drawbacks in centralized networks is that the central device will have too many logical connections with other nodes at the same time, so it will need too many resources (in the case of a physical topology, it should have many interfaces), so it could be a bottleneck. On the other hand, they are not fault tolerant because there is a central point of failure (routing computations are only located in one place or, in case of a server, there is a single index repository). They lack of scalability. Finally, when there is a new link (or service), the central device must be updated (sometimes this update can not be done without stopping the system, so the owner of the topology could lose money). Otherwise, a centralized network has several benefits such as the easy of overall control, because by controlling the central device, the administrator controls the network. On the other hand, a centralized topology has the smallest diameter, so there are faster transmissions between all nodes, providing faster transfers and searches. Centralized topologies have been used for many types of networks [3], such as teleprocessing networks [4] and multimedia networks [5].
2. In decentralized networks, every node is able to establish connections directly with all other nodes in the network and messages are sent without intermediation via a central device. All nodes have the same responsibility and functionality in the network. No element in the network is essential for the system operation. A node can play three roles: as a server, as a client, and as a router. Many searching algorithms for decentralized networks have been designed. All of them perform three basic actions: searching of active nodes, querying for resources or services, and transferring content. The search could be done using a list of known nodes, sending a multicast or broadcasting message to the network or to specific nodes chosen based on a mathematical algorithm. Decentralized networks provide several main benefits such as providing multiple connections between nodes, removing single points of failures and improving the connectivity and reliability of a centralized network. On the other hand, load is distributed between nodes and they provide redundancy and adaptability, while they are very scalable. But, they suffer from several main drawbacks. On the one hand, there is an increase in overall network traffic and route processing and, because the diameter of the network is usually big, too much time to obtain results from searches and to transmit data to the whole network is needed. And, on the other hand, the level of routing complexity is increased considerably, and it is difficult to control the network. There are many decentralized topology networks such as pure P2P networks, ad-hoc and sensor networks, grids and so on. Examples given of decentralized networks in P2P networks are Freenet [6], CAN [7], Chord [8], Pastry [9] and Tapestry [10].
3. In partially centralized networks (also known as hybrid networks, layered networks or multi-tier networks) there are some nodes with higher roles which form the backbone of the network and are needed to run the system. Nodes with a lower role are called leaf nodes and will be placed in the lower logical layer, while nodes with higher roles could be servers or supernodes and will be placed in the higher logical layers. Every supernode or leaf node can have connections with either leaf nodes or supernodes. There is a kind of hierarchy where higher layer nodes organize, control or gather data from lower layer nodes. Higher layer nodes are used to forward messages from lower layer nodes. Partially centralized networks can be broken into two subclasses: the first subclass is similar to a centralized network, but instead of a single server, there is a farm of servers that form the higher layer. In this subclass, a node sends its request to a server that is transmitted to the other servers to perform node's request. Each server maintains the indexes of the local nodes, services or resources and, in some cases, the indexes from neighbour servers. The server indexes are not static and can change according to the nodes, services or resources in the network. The second subclass has supernodes that offer some level of centralization. Nodes with a higher bandwidth and process capacity will be considered automatically as supernodes. They act as a representation of their leaf nodes and form the higher layer. They can work in conjunction with other supernodes and perform searches sent by their leaf nodes using a flow control algorithm for sending queries and replies. They can have a diagram of priorities for discarding some messages. In both subclasses, the data transfer can be made directly between the edge nodes, without central servers or supernodes mediating of this transfer, or through the path given by servers or supernodes. Partially centralized networks have many benefits. They improve the connectivity and reliability of a centralized network, and they provide adaptability, redundancy and fault tolerance. Partially centralized networks perform faster searches than decentralized networks. On the other hand, they give higher functionality, better coverage, and better reliability than single-tier networks. The total system cost is lower in a multi-tier than in a single tier. A multi-tier network reduces the network traffic and provides higher performance than single-tier networks while it is scalable. Otherwise, partially decentralized networks have several main drawbacks such as supernodes must have enough bandwidth and process capacity to support their role operation. They are more complex than centralized networks, but less than decentralized networks. There are communication delays and there could be inadequate tracking of the data transmitted. Searches in large networks will not provide results from the whole network because of the network overload (messages have a maximum TTL). Examples given of partially centralized networks are superpeer P2P networks and Content Delivery Networks. FastTrack [11], Gnutella 2 [12] and eDonkey [13] are P2P partially centralized networks. Layered networks have been used for different kinds of networks such as cache server networks [14], satellite networks [15] and wireless networks [16].

Table 1 summarizes their main network features.

All these networks have their advantages and disadvantages and each of them performs better than the other ones according to the environment where it is being implemented or according to a desirable parameter.

3. Application environment

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. First, we have to distinguish between a groupware architecture, where all nodes collaborate towards the correct operation and the success of the purpose of the network, and a group-based architecture, where the whole network is broken down into groups and each group could perform different operations. In a group-based architecture, a logical group consists of a set of nodes that perform the same protocol sharing services, resources or files, i.e. the information is completely shared among all the nodes within the same group regardless of their physical location, but in the case of a physical group-based architecture, nodes are close (in terms of geographical location or round trip time) to each other. The main goal in a group-based topology is the network protocol and the group management, that is, the design of an efficient algorithm for a new node to find its nearest (or the best) group to join in. Then, three important issues must be designed:

- How to build neighbouring groups. Neighbouring groups are those groups that are close to a group, so their boundaries are in touch.
- A protocol to exchange messages between neighbouring groups.
- A protocol to route information through the groups if needed.

The performance of the network highly depends on the efficiency of the nearby group locating process and on the interaction between neighbouring groups.

The application areas for our proposal could be any system where the devices are grouped and there must be connections between groups. These connections have to be established between the devices that are placed in the boundaries of the groups. Examples given are the following:

1. Let us suppose a job where it is necessary to split all human resources into groups to achieve a purpose (such as firefighter squads for putting out the fire). Now, let us suppose that all 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. Actually, coordination between groups is done through a wireless connection to the command center or using communications satellite. But, sometimes none of those solutions can be used because a line of sight free of obstacles is needed, or because there are too much wall looses or because more gain or power to reach the destination is needed.
2. 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 neighbouring areas. It will give an easier management and control for detecting fires and plagues while it will allow scalability.
3. It could be used in any kind of system whose event or alarm is based on what is happening in a specific zone, but conditioned to the events that are happening in neighbouring zones. One example is a group-based system to measure the environmental impact of a place. It could be better measured if measurements are taken from the animals, the plants and from the trees in that place. Each kind of measurement could be taken from different groups of sensors, but those groups of sensors have to be connected in order to estimate the whole environmental impact.
4. Another example is group-based games. There are many games where the players are grouped virtually in order to perform a specific task. Interactions between groups should be given by interactions between players from different groups to exchange their knowledge.

Finally, the authors of this paper have implemented group-based networks for multimedia groups [17], for content delivery networks [18] and for scaling grids [19].

Some group-based architectures have been used in wireless sensor networks. 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). A survey of cluster algorithms for wireless sensor networks is shown in reference [20].

We can also find the implementation of group-based networks schemes over P2P networks in reference [21]. Although, in this case, the authors make this survey from point of view of the search system.

4. Group-based considerations

This section describes a group-based topology analytically and analyzes several types of network topologies taking into account that they are used in a group-based system.

Table 1
Networks features summary

	Centralized	Decentralized	Partially centralized
Overall network diameter	Very small	Very big	Big
Convergence time	Very little	Very much	Quite much
Infrastructure cost (total number of links)	Low	High	Very high
Book-keeping costs (number of links maintained per each node)	Very high (central node)	Low	High
Management cost	Low	Low	High
Load	Very much	Very little	Only in higher layer nodes
Efficiency	Low	Low	High
Fault tolerance	Very low	Very much	Quite much
Scalability	Very low	Very much	Quite much
Performance of the system	Low	High	Very high
Availability	Low	Very high	High
Reliability	Low	High	Very high
Total execution time of jobs	Very little	Very much	Quite much
Complexity	Very low	Quite high	Very high

Let a network of nodes be $G = (V, E)$, where V is the set of nodes and E is the set of connections between nodes. Let k be a finite number of disjoint subsets of V, so $V = U(V_k)$ and there is no node in two or more subsets $(\cap V_k = 0)$. Let us suppose $N = |V|$ (the number of nodes of V) and k the number of subsets of V. Eq. (1) gives the number of nodes.

$$N = \sum_{i=1}^{k} |V_k| \tag{1}$$

On the other hand, the number of connections for each V_k (we call it E_k) will depend on number of nodes of V_k and on the degree of its border nodes.

The following subsections show the analytical model of a group-based network from the border nodes point of view and from the number of connections in the network point of view.

4.1. From the border nodes point of view

Any topology can be considered to be formed by a central node, no one, one or several core nodes and one or several border nodes. Expression (2) shows the classes of nodes that from a group.

$$n = 1 + n_{\text{core}} + n_{\text{border}} \geqslant 2 \tag{2}$$

Now, the whole network can be described as the sum of all these nodes from all groups as it is shown in Eq. (3).

$$\begin{aligned} n &= \sum_{i=1}^{k} |(n_{\text{central}} + n_{\text{core}} + n_{\text{border}})_k| \\ &= k + \sum_{i=1}^{k} (|n_{\text{core}}|)_k + \sum_{i=1}^{k} (|n_{\text{border}}|)_k \end{aligned} \tag{3}$$

Next, several types of topologies are going to be analyzed as a function of the number of core and border nodes in the group. Our consideration will leave out the full mesh, ring and torus topologies, and structured topologies such as CAN and Chord, because all nodes can be considered border nodes, so there are not a central node and core nodes.

The best topology is one central node with all other nodes as border nodes like a star topology, but the main drawback is that its scalability is very poor, because the central node has a connection with every border node, and there is no fault-tolerance, because if the central node fails, there is not any other core node to replace it, so the topology fails.

4.1.1. Tree topology

Tree topologies have a node acting as a trunk and from this node several branches stem out. Two kinds of tree topologies can be considered: N-ary trees (every node has the same number of leaf nodes, binary, ternary and so on) and backbone trees, where there is a trunk and there are nodes that branch from it. In both cases the information flows hierarchically. We are going to study the first case only. The backbone tree is similar to the case of partially centralised P2P Networks with superpeers, so it will be discussed later. In a tree topology, the number of nodes n is given by expression (4).

$$n = \sum_{i=0}^{k} M^i \tag{4}$$

where $M = 2$ in a binary tree, $M = 3$ in a ternary tree and so on, and k is the number of levels of the tree. The number of links is $n - 1$ and the diameter of the network is $2k - 2$. Supposing balanced trees, where all branches have the same number of levels, the number of core nodes can be seen in Table 2. *Grade* is the number of leaf nodes for each node. Using expression (2), the number of border nodes can be calculated as a function of the number of core nodes (see Table 2). Tree topologies have been implemented in several types of networks such as the one shown in [22].

4.1.2. Grid topology

Let us consider 2-dimensional grid and 3-dimensional grids. To make the mathematical development easy, in a 2D grid a square matrix with equal sides will be used, where $l = m$ for $n \geqslant 3$ and in a 3D grid a cube matrix where $l = m = p$ for $n \geqslant 3$ will be used. In both cases, when $n = 3$, there is one central node, but there is not any core node. The number of nodes in a 2D grid is l^2 (where $l = 3, 4, \ldots$). The number of neighbours of a core node is 4, the border node has 3 neighbours and the vertex node has 2 neighbours. We have observed that the number of border nodes in a 2D grid topology follows the expression given in Table 2. Using expression (2), the number of border nodes related with the number of core nodes is obtained as is shown in Table 2. 2D grid topologies have been implemented in several works such as the one shown in [23].

The number of nodes in a 3D grid is l^3 $(l = 3, 4, \ldots)$. The number of neighbours of a core or central node is 6, border nodes have 5 neighbours and the vertex nodes have 4 neighbours. The number of border nodes in a 3D grid topology can be measured by the expression in Table 2. Using expression (2), the number of border nodes as a function of the number of core nodes is obtained as is given in Table 2.

4.1.3. Power law topology

In [24], M. Faloutsos et al. showed that the nodes of a distribution network can be modelled using mathematical laws. They state that power law fits real measurements with correlation coefficients of 96%. Power law states that the grade of a v-node (d_v) is proportional to its range (r_v) to the power of a constant called R, where R varies depending on it is applied. Applying Lemma 1, from paper [24], the grade of a node is given by expression (5).

$$d_v = \frac{1}{n^R} \cdot r_v^R \tag{5}$$

where n is the number of nodes in the network. From the power law appears the Zipf's law. It states that some nodes have many links, while many nodes have one or two links. Zipf's law has been proposed to model Internet and several P2P filesharing networks. Zipf's

Table 2
Expressions for each topology

Topology	Border nodes vs all nodes	Border nodes vs core nodes
Tree	$n_{\text{border}} = \frac{(\text{grade}-1)\cdot(n-1)}{\text{grade}}$	$n_{\text{border}} = (\text{grade} - 1) \cdot n_{\text{core}} + \text{grade}$
2D grid	$n_{\text{border}} = 4 \cdot (\sqrt{n} - 1)$	$n_{\text{border}} = 4 \cdot (1 + \sqrt{n_{\text{core}} + 1})$
3D grid	$n_{\text{border}} = 6 \cdot \sqrt[3]{n^2} - 12 \cdot \sqrt[3]{n} + 8$	$n_{\text{border}} = 6 \cdot \sqrt[3]{(n_{\text{core}} + 1)^2} + 12 \cdot \sqrt[3]{(n_{\text{core}} + 1)} + 8$
Power law	$n = \frac{(n_{\text{border}})^{\frac{\alpha+1}{\alpha}}}{(n_{\text{border}})^{1/\alpha}+1}$	$n_{\text{border}} = \frac{(n_{\text{border}}+n_{\text{core}}+1)^{\alpha}}{(n_{\text{core}}+1)^{\alpha}}$
Logarithmic	$2 \cdot n_{\text{border}} \leqslant n \leqslant (n_{\text{core}} + 1) \cdot (1 + \ln(n_{\text{core}} + 1))$	$(n_{\text{core}} + 1) \leqslant n_{\text{border}} \leqslant (n_{\text{core}} + 1) \cdot \ln(n_{\text{core}} + 1)$
Partially cent. P2P networks	$n_{\text{border}} = \begin{cases} \frac{n}{2} & \text{broker model} \\ \frac{96\cdot(n-2)}{97} & \text{superpeer} \end{cases}$	$n_{\text{border}} = \begin{cases} n_{\text{core}} + 1 & \text{broker model} \\ 96 \cdot (n_{\text{core}} - 1) & \text{superpeer} \end{cases}$

function states that the range of r nodes follows the proportionality shown in expression (6).

$$f(r) = C \cdot r^{-\alpha} \tag{6}$$

where α varies depending on how the nodes are distributed. It is also known as the Zipf coefficient. C is a constant that varies depending on the kind of network. Taking into account expressions (5) and (6), it is assumed that $R = -\alpha$, so the relationship between border nodes and core nodes is given by the expression shown in Table 2. Taking expression (2) into account, the number of border nodes related with the total number of nodes in the topology can be obtained as is shown in Table 2. As Internet topology has varied over the years, because of the growth of the number of computers connected to it, α value has varied from 0.74 to 3 in last measurements, as B.A. Huberman et al. showed in [25].

4.1.4. Logarithmic law topology

Logarithmic law was introduced by György Hermann in [26]. This law proposes that the border nodes, or the nodes with higher roles in the network, are responsible for the stability of the network. It also proposes that the border nodes are responsible for the security of the network because they are the ones that communicate with exterior nodes. The relationship between the number of border nodes and the core nodes can be seen in Table 2. It also shows the limits of the number of nodes in the network.

4.1.5. Partially decentralized P2P topology

In [27], a three-layered architecture for partially centralized P2P networks was proposed. We measured the number of brokers or superpeers (depending on the kind of network), that were inside the architecture on behalf of all brokers or superpeers in the whole network. We obtained that the number of border nodes could be equal to the number of core nodes plus one for the broker model. But, for the superpeer model, because some superpeer networks have a TTL of 7, and assuming an average of 24 neighbour superpeers every hop, our measurements show that one supernode in the distribution layer every 96 supernodes were needed. It could be applied to the proposal presented in this paper if we suppose that the core nodes plus the central one are the distribution layer nodes of that paper and the border nodes are the nodes in the access layer. The relationship between core and border nodes and between border and all nodes are different according to the type of P2P network is shown in Table 2.

4.1.6. Topologies comparison

This section compares the number of border nodes versus the number of core nodes and the number of border nodes versus the number of nodes in the group for all classes of topologies shown. In both cases partially centralized P2P networks with brokers model has the same law than the minimum values of the logarithmic model.

Fig. 1 shows the number of border nodes in the group as a function of the number of core nodes for all topologies previously analyzed. We have used numerical methods to obtain Zipf's law graph. As shown in the figure, when a group with few border nodes is needed, if there are less than 24 core nodes, the best election is the minimum value of the logarithmic law, but when there are more than 24 core nodes the best option is 2D grid. The most desirable is to have many border nodes in order to have many connections with nodes from other groups, so there will be higher probability to contact with more neighbouring groups. It can be checked that for less than 770 core nodes the best topology is the partially centralized P2P networks with superpeer model, but when the number of core nodes is equal or higher that 770, the best topology is Zipf's law with $R = -2.45$. Fig. 2 shows the number of border nodes in the group as a function of the number of nodes in the group. We have used numerical methods to know the number of border nodes as a function of the number of nodes in the group for the logarithmic model and for Zipf's law model. It can be seen that when many border nodes are needed versus the number of nodes in the group, for less than 40 nodes the best election is 3D grid, but for 40 nodes or more, the best election is the partially centralized network with superpeers model. Despite of it is not the most desirable in our case, when it is needed few border nodes versus the number of nodes in the group, for less than 110 nodes the best topology is the ternary tree, but for more than 110 nodes the best topology is 2D grid.

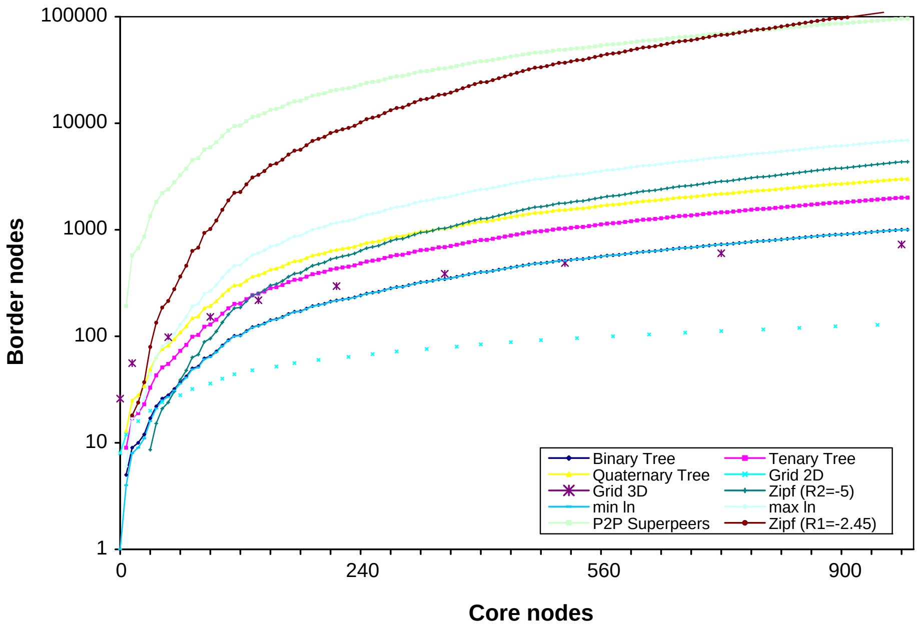


Fig. 1. Number of border nodes vs the number of core nodes.

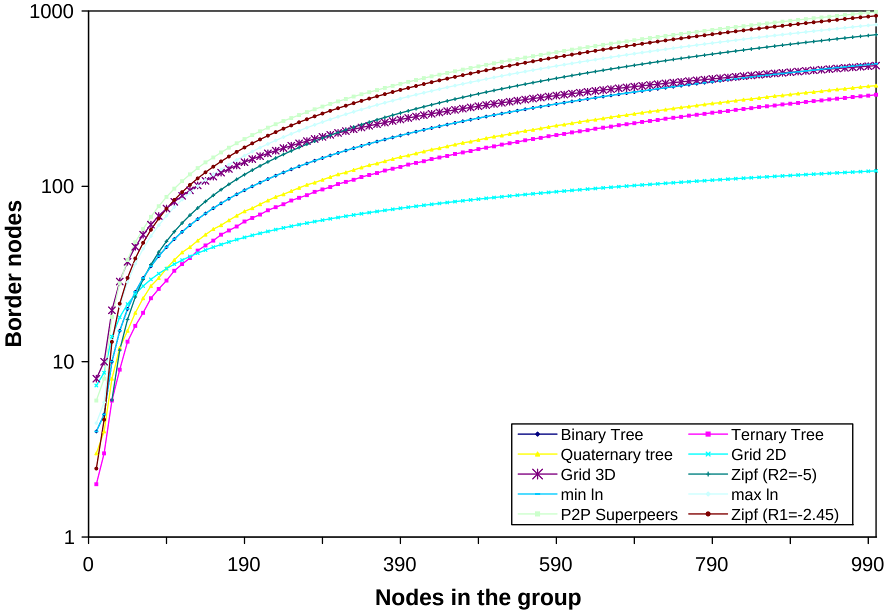


Fig. 2. Number of border nodes vs. the number of nodes.

4.2. From the connections between groups point of view

The number of links in the whole network $m = |E|$ depends on the number of groups (k), on the number of links inside each group (k_l) and on the number links between border nodes. The main issue in a group-based topology is the number of connections between groups. When the group-based topology is used in a logical network, any group can have connections with any other group (even with all groups), while a physical group-based topology, a group can just have connections with physical neighboring groups. Expression (7) gives m value when there is a physical topology of k groups.

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

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. Fig. 3 shows the number of links in the whole topology as a function of the number of groups in the network. Two cases have been considered; in the first case there is a physical topology, where each border node has just one connection with its closest neighbouring group, and in the second case, there is a logical topology where all border nodes of each group have a connection with one border node from each group. We have fixed a value of 100 internal links for all groups and all groups have 25 border nodes.

5. Existing solutions

There are several works in the literature where nodes are divided into groups and connections are established between nodes

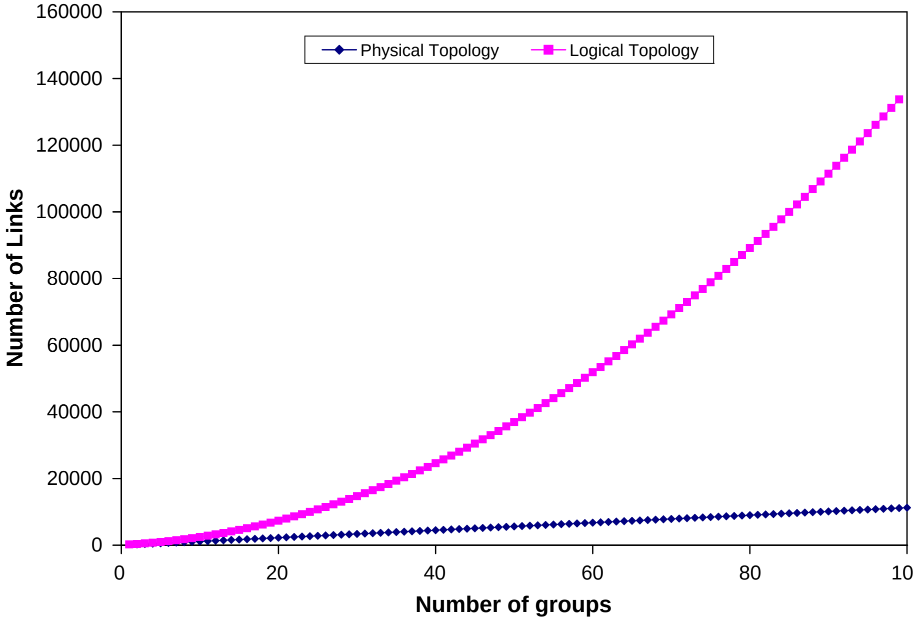


Fig. 3. Number of links as a function of the number of groups.

from different groups, but all of them have been developed to solve specific issues such as distribution service in multimedia networks, group-based games over NAT/Firewalls, and so on. Two classes of group-based topologies can be distinguished: planar group-based topologies and layered group-based topologies. Although some authors consider when a network is broken into groups, it is a two-layer network, where the top level consists of groups, and of a bottom level consists of nodes within one group, we will consider them just a single layer.

5.1. Planar group-based topologies

They are group based topologies where all nodes perform the same roles, and in case of several roles, nodes with higher roles are not directly connected forming a higher layer. There is just one layer. However, in some works there is a directory server or a rendezvous point (RP) for content distribution coordination.

One of the best known systems with groups is the multicast technique. It was created for delivering information to a group of destinations simultaneously [28]. There are many implementations of the multicast distribution strategy such as [29,30]. But many of them can not be considered as a group-based system because there are no connections between multicast groups. Each group works alone without exchanging any information with other groups.

Reliable multicast transport protocol (RMTP), presented by Sanjoy Paul et al. in [31], is a multicast implementation that organizes nodes in groups and there are connections between groups. RMTP is based on a hierarchical structure (multicast tree) in which receivers are grouped into local regions based on their proximity in the network. In each region there is a special receiver called a designated receiver (DR) which is responsible for sending acknowledgments periodically and for retransmitting lost packets to the corresponding receivers. RMTP provides sequenced, lossless delivery of bulk data from one sender to a group of receivers.

Z. Xiang et al. proposed a locality-aware overlay network based on groups [32], and later, they presented a peer-to-peer based multimedia distribution service [33] based on this proposal. They proposed a topology-aware overlay in which nearby nodes in the underlying network, which are very close to each other, self-organize into application groups. Generally, nodes under the same gateway to the Internet or within the same subnetwork will naturally belong to one group. Each peer contributes its local storage and I/O capacity to support multimedia distribution service to other peers. End nodes within the same group have similar network conditions and can easily collaborate with each other to achieve QoS awareness.

When a new node arrives, it uses a locating method to join a nearest group or form its own group according to the group criterion. In order to find a nearby group for a new joining node, they designed an algorithm based on distance measurement using a global server cache, called the rendezvous point (RP), in the network. All new hosts know where the RP is, so they contact the RP to fetch cached nodes. These nodes, called boot nodes, are selected by the RP randomly. Boot nodes will guide the new node to the nearest group measuring the distance from it to the new node and it will be compared with a predefined value to find the closest group. This information is sent by all boot nodes to the new node and it selects groups sequentially from a candidate list. The distance between group members are limited to a certain value to eliminate the transmission delay between group members. Each group maintains a local node cache, which consists of nodes in the same group responsible for communications with nodes in other groups. The group also maintains information about its neighbour groups, such as distance, nodes in their neighbour groups' node cache. The first host in the host cache, called the leader, is responsible for updating information of its host cache and of its neighbouring groups. The second host in the host cache will stand up and take over the leader's responsibilities in case of the leader failure.

The described locating scheme guaranties that a new node can find its nearby groups within O(log N) steps, where N is the number of hosts in the overlay network. In order to achieve the load balance and avoid hot spots, the neighbours of a group are used to act as the dynamic landmarks for new host in the overlay forming process.

When a node in this architecture wants to communicate with a node from other group, the information is routed through several groups until it arrives at the destination. When a request for a given content arrives, if the requested content is within the same group, the content will be delivered to the requestor directly. If not in the same group, a flooding search algorithm is carried out at group level. Once the content is found, it is first sent to the requesting group through the shortest path at the group level. After the content arrives at the requesting group, it will be sent to the node that requests the content.

5.2. Layered group-based topologies

Nodes from layered group-based topologies could have several roles (2 roles at least). Depending on which type of role they are running, they will become to a specific layer. All nodes in a 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. Hierarchical architectures are located in this group because their hierarchies could be considered as layers.

The global Internet is a collection of over 16,000 administratively independent networks (called Autonomous Systems, or ASs) that participate in global routing of IP traffic. An AS may be a corporation, an Internet service provider, or a government entity.

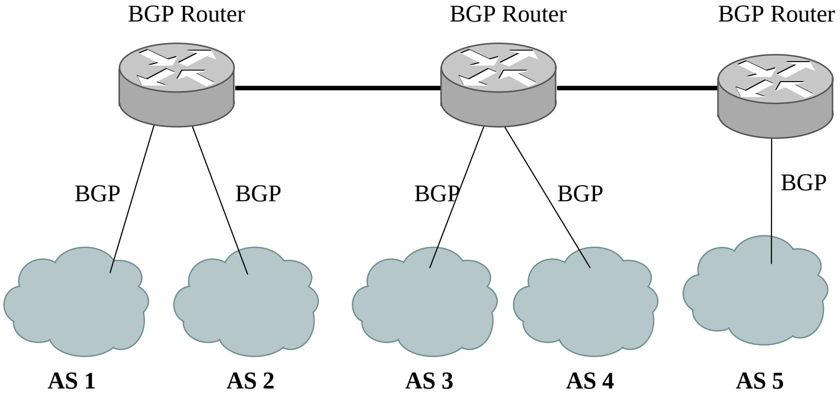


Fig. 4. BGP routers topology.

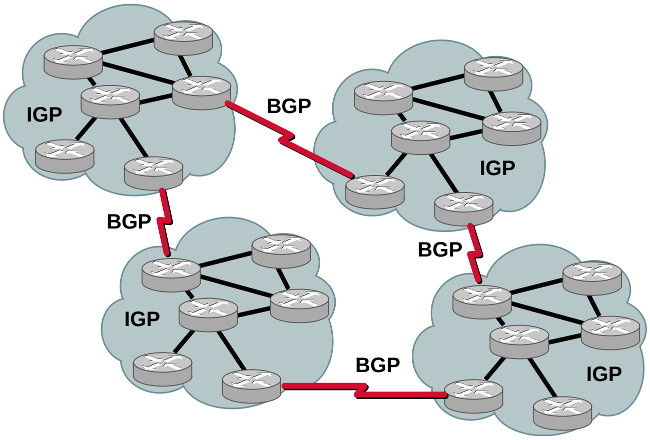


Fig. 5. BGP topology that joins IGPs.

The ASs operate under service agreements governing how the traffic should be sent from one AS to another. Every enterprise, that is an Autonomous System, owns a number of border routers that are connected to its own internal network on the inside, and to border routers of neighbouring ASs on the outside. BGP (border gateway protocol) [34] is a distributed software protocol, defined in the Internet standards, that is running on the AS's border routers. BGP is currently the core routing protocol of the Internet. BGP works by maintaining a table of IP networks or 'prefixes' which designates network reachability among autonomous systems (AS). It exchanges routing information between gateway routers (see Fig. 4).

Very large private IP networks can also make use of BGP. An example would be the joining of a number of large networks running an interior gateway protocol (IGP) such as RIP, OSPF or IS–IS where the interior gateway protocol could not scale to size. Another reason to use BGP would be multi-homing a network for better redundancy either to a multiple access points from a single ISP.

Considering the network that is running the interior gateway protocol as a group, and connections between routers running BGP as the connections between groups, there is a topology which joins groups. So, thinking on a group-based topology, routers running the IGP will be in the lower layer and BGP routers will be in the higher layer. An example of a BGP joining IGPs is shown in Fig. 5.

When information is sent from an AS to another AS, it is routed to the BGP router that will forward it to the BGP router from the other AS, and it will forward to the destination. Taking into account this process, all traffic will go through the hierarchy when data is transmitted between networks.

There are other architectures based on superpeer models such as FastTrack [35] and Gnutella 2 [36] networks. Each super-peer in these networks creates a group of leaf nodes as it is shown in Fig. 6.

Superpeers perform query processing on behalf of their leaf nodes. A study made by B.T. Loo et al. [37] reveals that superpeers in the FastTrack network support up to 30 of leaf nodes and up to 32 neighbour supeerpeers. On the other hand, the specifications given for Gnutella 2 state that the number of neighbour superpeers should be up to 6 superpeers while the number of leaf nodes for a superpeer should be a maximum of 75. All these values are given by their designers and they are limited by the desktop P2P application. When a leaf node sends the query to its superpeer that floods it to its superpeer neighbours up to a limited number of hops (it use to be a TTL of 7). The main drawback of this architecture is that all information has to be routed through the superpeer logical network. Data is transmitted between nodes directly. On the other hand, superpeers should have much process capacity when there are many leaf nodes and they process many requests.

Wierzbicki et al. presented Rhubarb [38] in 2002. It organizes nodes in a virtual network, allowing connections across firewalls/NAT and efficient broadcasting. The nodes can be active, if they establish connections to support the system, or passive, if they do not. All active nodes know which nodes are active and which ones not. Rhubarb cannot work without active nodes. Nodes inform the coordinator of their group periodically about their state. Rhubarb system has only one coordinator per group and coordinators could be grouped into groups in a hierarchy. A new node in a group must contact the group coordinator which gives the addresses of the nodes in the group and a list of other possible coordinators. Groups are limited to 100 nodes. A new group is created when the number of nodes exceeds this value and the group elects a new coordinator. The system 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 is renewed if it is broken by the firewall or NAT. When a node from outside the network wishes to communicate with a node that is inside, it sends a connection request to the proxy coordinator, who forwards the request to the node inside the network. Rhubarb has a three-level group hierarchy. It may be sufficient to support a million nodes, but when there are several millions of nodes in the network it might not be enough, so it suffers from scalability problems. On the other hand, all nodes need to know the IPs of the proxy coordinator nodes to establish connections with nodes from other virtual networks.

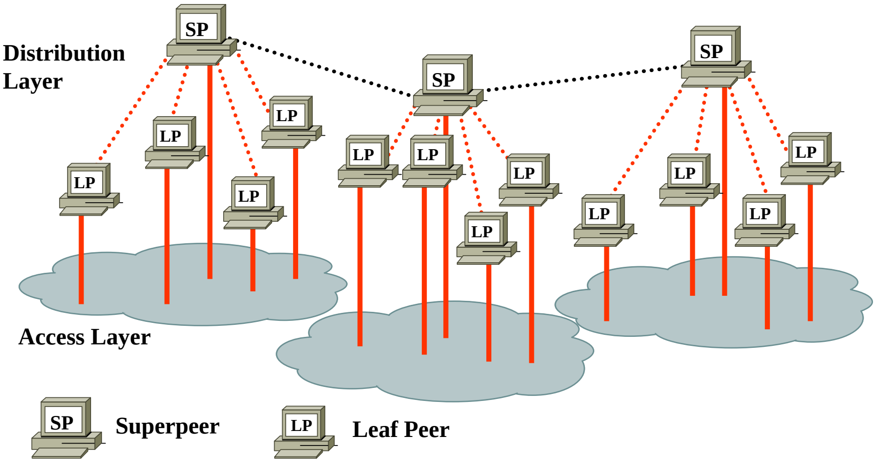


Fig. 6. Superpeer model topology.

There are some hierarchical architectures where nodes are structured hierarchically and parts of the tree are aggregated into groups such as the one presented by Liu Hongjun et al. in [39] and the one presented by B. Thallner et al. in [40]. In some cases, 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 to achieve nodes from other groups.

Their main drawback is that all layers of the hierarchy could be overloaded in case of having many data to be transferred. On the other hand, in the case of many groups, the hierarchical structure could become unstructured because there could be many connection establishments between nodes from different groups placed on different layers of the hierarchy.

6. Proposals for improvement

This section shows two group-based systems designed by the same authors of this paper one for each class of group-based topology.

6.1. Planar group-based topology

In [41,42], we proposed a structure of nodes based on the creation of groups of wireless sensors with the same functionality in the network. There is a central sensor that limits the zone where the sensors from the same group will be placed, but its functionality is the same as the rest of the sensors. A sensor knows in which group it is because it is given manually, by GPS, using a wireless location system or through other means. Border sensors are the physically (or logically) edge routers of the group.

When there is an event in one sensor, this event is sent to all sensors in its group. All nodes in a group know all the information of their group. Border sensors are those sensors in the border of the group, and they have connections with border sensors from other groups as it is shown in Fig. 7.

Border sensors are used to send or receive information from other groups and distribute it within the groups. When a sensor has to send some information to its group and to neighbouring groups, the information is forwarded using reverse path forwarding (RPF) algorithm (each group has one RPF database), but when the information has to be sent to other groups only, the information is routed directly to the border sensor closest to that group. When the sensor from the neighbour group receives that information, it routes it to all nodes in its group.

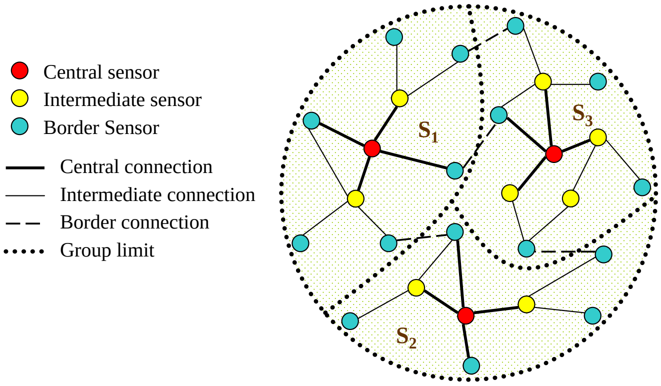


Fig. 8. Logical view of the proposed architecture.

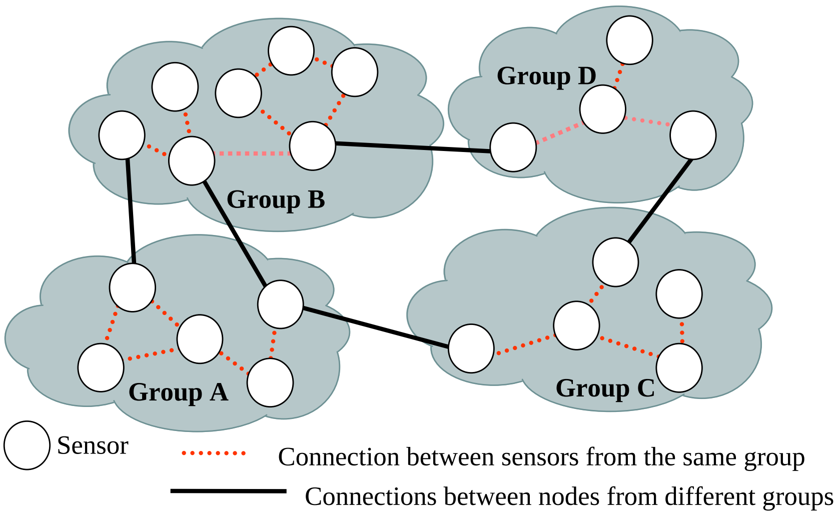
Because the system is based on groups, the information is forwarded very quickly to other groups (the information is routed through the shortest path to the border area sensor). Connections between border sensors from different groups are established primarily as a function of the RTT, but in the case of multiple possibilities, neighbours are selected as a function of their capacity λ. The capacity λ combines several parameters such as bandwidth, load, energy, available number of connections and the maximum number of connections of the sensor. It is given by expression (8).

$$\lambda = \frac{(BW_{\mathrm{up}} + BW_{\mathrm{down}}) \cdot \mathrm{Available\_Con} \cdot L + K_2}{\mathrm{Max\_Con}} \cdot \sqrt{1 - \frac{E^2}{K_1}} \tag{8}$$

where $0 \leqslant \mathrm{Available\_Con}\ \mathrm{Max\_Con}$. L is the available load and E is the energy consumption. L and E values vary from 0 to 100, according to the state of the sensor. An energy consumption of 0 indicates it is fully charged and when it has a value of 100, indicates it is fully discharged. K_1 defines the minimum value of energy remaining in a sensor to be suitable for being selected as a neighbour. K_3 gives λ values different from 0 in case of $L = 0$ or $\mathrm{Available\_Con} = 0$. The root is out of the division because when the sensor is fully discharged, λ parameter has to be 0.

Fig. 8 shows a logical view of the proposed architecture.

The application areas for this proposal could be rural and agricultural environments to detect plagues and to propagate it to neighbouring areas, or for military purposes to propagate information between neighbouring squads.



Group A
Group B
Group C
Group D
Sensor
Connection between sensors from the same group
Connections between nodes from different groups

Fig. 7. Topology example.

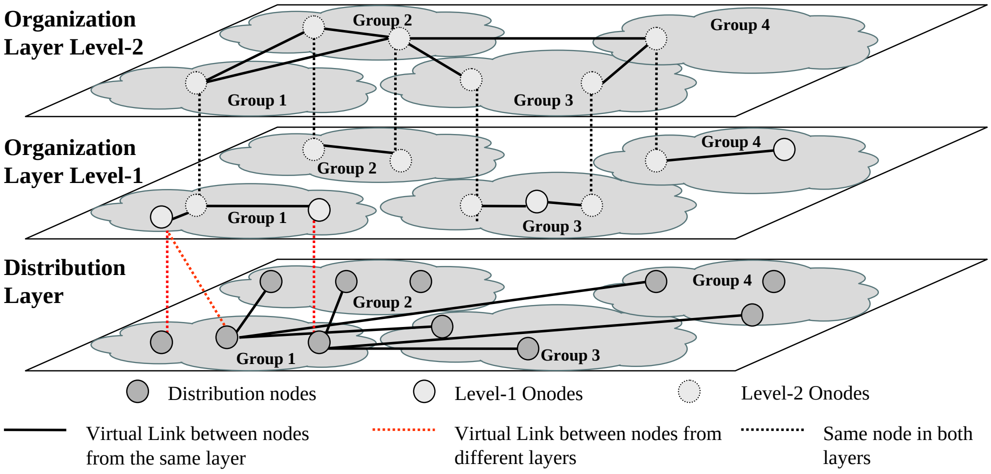


Fig. 9. Architecture layers.

6.2. Layered group-based topology

In [17,27,43], we presented a layered group-based architecture to interconnect nodes from different groups. They assume that every node in the same group use the same application layer protocol (or data-link layer protocol) and use it to interact with any other node within their group sharing services, resources or files. When a node looks for some information, first it will try to get it from its group. In case of no result, the search is sent to other networks using the proposed protocol. If it is found, the information can be downloaded. Once the node has the information, it will act as a cache for its network, sharing this information.

There are three types of node roles (a node could run all them simultaneously):

- Dnodes: they have connections with Dnodes from other groups. They are used to send searches and data transfers between groups.
- Level-1 Onodes: they organize Dnodes into zones to have a scalable architecture.
- Level-2 Onodes: they have connections with Level-2 Onodes from other groups. Level-2 Onodes are used to organize connections between Dnodes from different groups.

Fig. 9 shows the architecture layers. Onodes maintain and manage the architecture. Every new Onode must authenticate with other Onodes from its group and/or from others groups (when they are Level-2 Onodes). When a new node joins the proposed architecture, it starts with its upstream and downstream bandwidths, its maximum number of supported connections from other nodes (Max_con), its maximum % of CPU load used for joining the architecture by the desktop application (Max_load) and what kind of content or data shared are in its group. All nodes have a unique node identifier (*nodeID*), first node in the group will be Dnode, level-1 Onode and level-2 Onode, it will have *nodeID* = 0 × 01 and a group identifier (*groupID*) that could be chosen manually. Then, it will assign *nodeIDs* sequentially to new nodes in its group. All groups have a unique *groupID* and all nodes in the same group have the same *groupID*.

δ parameter is the node suitable parameter. It depends on node's bandwidth and in the time it has belonged to the architecture. It is used to know which node is the best node to promote and have a higher role. The age is defined in a non-linear form because first nodes are more important than the last ones, in terms of stability. Nodes with higher bandwidth and older are preferred for promotion so they will have higher δ. Eq. (9) defines δ.

$$\delta = (BW_{\text{up}} + BW_{\text{down}}) \cdot K_1 + (32 - \text{age}) \cdot K_2 \tag{9}$$

where $\text{age} = \log_2(\text{nodeID})$, so age varies from 0 to 32. The age is defined in a logarithmic form instead of a linear form, because it gives higher granularity in low nodeID values. Nodes with high bandwidth and relatively new ones could have higher δ values.

Table 3
Planar group-based topologies comparison

	Locality-aware overlay network	Reliable multicast transport protocol (RMTP)	Group-based architecture for WSN
Need of a Rendezvous point	Yes	Yes	No
Kind of topology	Logical, but it could be implemented in physical	Logical	Physical, but it could be implemented in logical
Neighbour selection	Proximity in the underlying network (IP)	Proximity in the underlying network (IP)	Physical proximity + neighbour node capacity
Which group to join in	Based on rendezvous point decision + boot nodes	Proximity in the underlying network (IP)	Based on neighbour discovery (time to reply, closest neighbour or capacity)
Is there a leader responsible for updating information	Yes	Yes	No (the central node is only to know group boundaries)
Convergence time	Very little	Very little	Very much
Management cost	Medium because of the rendezvous point	Medium because of the rendezvous point	Low
Fault tolerance	Very low (because of rendezvous point or boot nodes failure)	Very low (because of rendezvous point or boot nodes failure)	Very much
Availability	Low (when boot nodes from a group are not available the group is not available)	High	Very high (when a node finds a neighbour it joins the network)

Every new Dnode in the logical network will authenticate with a level-1 Onode in its network. In order to have a scalable network, when there are β Dnodes, the Dnode with higher δ will start level-1 Onode role and it will create a new zone. When there are α level-1 Onodes, the level-1 Onode with higher δ will become a level-2 Onode. α and β values depend on the number of nodes in the network and their data traffic.

Using our explanations given in [27], our estimation gives β values between 64 and 96 and one level-2 Onode every 50 level-1 Onodes ($\alpha = 50$) is enough to maintain and manage level-1 Onodes' network (our measurements give that it supports thousands of millions of nodes).

λ parameter is the node's capacity. It depends on the node's bandwidth (in Kbps), its number of available connections (Available_Con), its maximum number of connections (Max_Con) and its % of available load. It is used to determine the best node to have connections with. λ parameter is defined by Eq. (10).

$$\lambda = \frac{\mathrm{int}\left[\frac{(BW_{\mathrm{up}}+BW_{\mathrm{down}})}{256}+1\right]\cdot \mathrm{Available\_Con}\cdot(100-\mathrm{load})+K_3}{\mathrm{Max\_Con}} \tag{10}$$

where $0 \leqslant$ Available_Con Max_Con. *Load* varies from 0 to 100. A *load* of 100% indicates the node is overloaded. K_3 gives λ values different from 0 in case of a load of 100% or Available_Con = 0. We have considered $K_3 = 10^3$ to get λ into desired values.

Dnodes have connections with Dnodes from other groups based on the λ parameter.

Virtual-link cost is based on node's capacity. The more the node's capacity, the lower its cost. Eq. (11) defines virtual-link cost.

$$C = \frac{K_4}{\lambda} \tag{11}$$

With $K_4 = 10^3$, higher values than 1 are given for λ in equation 10.

The metric is based on the number of hops to a given destination and the link cost of those nodes involved in the path. The metric is used by the SPF algorithm to obtain the best path to reach a node. Eq. (12) shows the metric to a j destination.

$$\mathrm{Metric}(j) = \sum_{i=1}^{n} C_i \tag{12}$$

where C_{i} is the ith node virtual-link cost and n is the number of hops to a j destination.

SPF (shortest path first) routing algorithm has been chosen to route information between Onodes. It is fast and allows sending fast searches to find Dnodes adjacencies, but it can be changed for other routing protocol depending on the networks' characteristics. Both layers of Onodes use SPF algorithm. Level-l Onodes route information within the network using *nodeID* values. Level-2 Onodes route information between networks. *groupID* is used to route information in this layer. Every node runs SPF algorithm locally and selects the best path to a destination based on the metric. Level-1 Onodes only add level-2 Onodes in their network entries and level-2 Onodes add all level-1 Onodes in its network, so they know how to reach all level-1 Onodes in their network. SPF routes are calculated using the virtual-link cost.

Once the connections between different groups are established, content delivery could be done between groups without using organization layer nodes because they are used only for organizational purposes. This architecture has been adapted for CDNs [18] and for grids [19].

7. Analysis

Several differences exist between planar and layered group-based topologies. While layered group-based topologies grow

Table 4
Layered group-based topologies comparison

	BGP	Fast Track and Gnutella 2	Rhubarb	Hierarchical architectures	Layered group-based architecture
Overall network diameter	Very big	Very big	Big	Big	Very low
Convergence time	Very much	Very much	Quite much	Quite much	Very little
All network nodes are reachable	Yes	No	Yes	Yes	Yes
Infrastructure cost (total number of links)	Medium	Medium	High	High	Very high
Book-keeping costs (number of links maintained per each node)	Medium	Medium	Medium	Medium	High
Management cost	High	Low	Low	Medium	Low
Load	Only in higher layer nodes	Only in higher layer nodes	Only in higher layer nodes	Only in higher layer nodes	Only in higher layer nodes
Efficiency	Low	Low	High	Medium	High
Fault tolerance	Very low (but there could be multihomed)	Medium	Quite much	Medium	Quite much
Performance of the system	Low	High	Very high	High	Very high
Availability	Low (but there could be multihomed)	Quite high	Quite High	High	Very high
Complexity	Low	Low	High	High	Quite High

structurally organized by upper layers, planar group-based topologies grow unstructured without any organization. In layered group-based topologies anyone can know where each group is exactly and how to reach it; otherwise planar group-based topologies because of groups join the network as they appear, every time a node wants to reach another group, the message should travel through many unknown groups. Delays between groups in layered group-based topologies could be lower because connections between groups can be established taking into account this parameter, otherwise, in planar group-based topologies, connections between groups are established by the groups' positions, their geographical situation or because of their appearance in the network. Layered networks address several complexities such as different types of roles, promotion procedure or fault-tolerance implementation. On the other hand, planar networks are more simple because all nodes have the same role (although in some cases nodes could be the ones which delimitate the coverage area, and in other cases there are some nodes that support others to join the group). In order to be more scalable, layered group-based topologies must add more layers to their logical topology, while planar group-based topologies could grow without any limitation, just the number of hops of the message.

Table 3 shows the planar group-based topologies comparison. Table 4 shows the layered group-based topologies comparison.

Both group-based architectures presented by us have higher availability, more performance and lower management cost (because its self-organization) than the others.

8. Conclusions

Group-based topologies allow interaction between working groups and, by spreading work to the network, give the capability to operate more flexibly, efficiently and less time consuming without the delays and information congestion of a strict workflow system.

Although several group-based systems have been proposed for different research topics, to the extent of our knowledge there is not any previous study related with group-based topologies in any type of network.

This paper has shown several types of network topologies for group-based topologies from the border nodes point of view. Connections between groups point of view has been also discussed. We have distinguished two classes of group-based topologies: planar group-based topologies and layered group-based topologies. Layered topologies use the higher layer to organize nodes in zones and help to establish connections between nodes from lower layers. In planar group-based topologies, it is difficult to establish group boundaries. All group-based architectures presented in this paper are able to self-organize connections between nodes from different groups based on some predefined parameters.

This work has shown that a group-based architecture provides some benefits for the whole network:

- Spreads the work to the network in groups giving more flexible, efficient and lower delays.
- Content availability will be increased because it can be replicated to other groups.
- Desktop applications can search and download from every group using only one open service.
- It provides fault tolerance because other groups can carry out tasks from a failed group.
- It is scalable because a new group can be added to the system easily.
- Network measurements can be taken from any group.

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 small overhead and highly efficient forwarding. So, grouping nodes increases the productivity and the performance of the network with low overhead and low extra network traffic. Therefore, good scalability can be achieved in group-based architectures.

We have compared two group-based topologies designed and developed by the authors. The benefits of these proposals have been shown in Section 7. In planar group-based topologies, our proposal does not need a Rendezvous Point and the neighbour selection is based in some parameters that allow balancing the load of the network. It could be implemented in physical and logical topologies. It has lower management cost than the others and it has a great deal of fault tolerance and high availability. On the other hand, in layered group-based topologies, our proposal provides low network diameter providing lower convergence time. With a consequent low management cost and high efficiency and performance. And also provides an increasing fault tolerance and availability compared with the other studied mechanisms.

One of the main drawbacks of group-based topologies is that their protocol is quite complex. The protocol must have two working environments, one used inside the group and another between the groups. On the other hand, it could be even more complex if we take into consideration a group-based network in which each group is formed by different topological structure. The complexity involves several issues such as the protocol design, analytical simulation, network management and control and so on.

Group-based networks have many application areas. They could be used when it is necessary to setup a network where groups appear and join the network or by networks that need to be split into smaller zones to support a large number of nodes.

This paper has demonstrated that group based topologies improve systems in existence and starts new research lines by encouraging researchers to consider group-based topologies for their future designs.

References

[1] S. Ratnasamy, M. Handley, R. Karp, S. Shenker, Topologically-aware overlay construction and server selection, in: Proc. InfoCom, 2002, pp. 1190–1199.

[2] Q. Lv, S. Ratnasamy, S. Shenker, Can heterogeneity make Gnutella scalable?, in: Proc. First Int. Workshop on peer-to-peer systems (IPTPS), 2002, pp. 94–103.

[3] K. Woolston, S. Albin, The design of centralized networks with reliability and availability constraints, Comp. Oper. Res. 15 (1988) 207–217.

[4] Aaron Kershenbaum, Robert R. Boorstyn, Centralized teleprocessing network design, Networks 13 (2) (1983) 279–293.

[5] S. Shirmohammadi, J.C. Olivera, N.D. Georganas, Applet-based telecollaboration: a network-centric approach, IEEE Multimedia Magazine 5 (2) (1998).

[6] I. Clarke et al., Freenet: a distributed anonymous information storage and retrieval system, in: ICSI Workshop on Design Issues in Anonymity and Unobservability, Int'l Computer Science Inst., 2000.

[7] S. Ratnasamy, P. Francis, M. Handley, R. Karp, S. Shenker, A Scalable Content-addressable Network, ACM Sigcomm, 2001.

[8] I. Stoica, R. Morris, D. Karger, F. Kaashoek, H. Balakrishnan, Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications, ACM Sigcomm, 2001.

[9] A. Rowstron, P. Druschel, Pastry: scalable, distributed object location and routing for large-scale peer-to-peer systems, in: IFIP/ACM International Conference on Distributed Systems Platforms (Middleware), Heidelberg, Germany, November 2001, pp. 329–350.

[10] B. Zhou, D.A. Joseph, J. Kubiatowicz, Tapestry: a fault tolerant wide area network infrastructure, UC Berkeley Technical Report UCB/CSD-01-1141.

[11] J. Liang, R. Kumar, K.W. Ross, The fasttrack overlay: a measurement study, Computer Networks 50 (6) (2006) 842–858.

[12] Y. Chawathe, S. Ratnasamy, L. Breslau, N. Lanham, S. Shenker, Making gnutella-like networks scalable, in: ACM SIGCOMM, 2003, pp. 407–418.

[13] O. Heckmann, A. Bock, The eDonkey 2000 protocol, Technical Report KOM-TR-08-2002, Multim. Communications Lab, Darmstadt University of Technology, December 2002.

[14] Y.W. Park, K.H. Baek, K.D. Chung, Reducing network traffic using two-layered cache servers for continuous media data on the Internet. in: Proceedings of the 24th Annual International Computer Software and Applications Conference, 25–27 October 2000, pp: 389–394.

[15] J. Lee, S. Kang, Satellite over satellite (SOS) network: a novel architecture for satellite network, in: IEEE Infocom 2000, March 2000.

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

[17] J. Lloret, Juan R. Diaz, Jose M. Jimenez, F. Boronat, An Architecture to Connect Disjoint Multimedia Networks Based on node's Capacity, Lecture Notes in Computer Science. Springer-Verlag Berlin Heidelberg, 4261/2006, November 2006, pp. 890–899.

[18] J. Lloret, C. Palau, M. Esteve, Structuring Connections Between Content Delivery Servers Groups, Future Generation Computer Systems, Elsevier Editorial, 2007.

[19] J. Lloret, M. Garcia, F. Boronat, J. Tomas, Group-based Self-organization Grid Architecture, Lecture Notes in Computer Science, Springer-Verlag, Berlin Heidelberg, 2007.

[20] A.A. Abbasia, M. Younisb, A survey on clustering algorithms for wireless sensor networks, Computer Communications 30 (14–15) (2007) 2826–2841.

[21] C. Gkantsidis, M. Mihail, A. Saberi, Hybrid search schemes for unstructured peer-to-peer networks, in: Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'05), Miami, Fla, USA, vol. 3, March 2005, pp. 1526–1537.

[22] J. Beutel, M. Dyer, M. Hinz, L. Meier, M. Ringwald. Next-generation prototyping of node networks, in: Proceedings of the 2nd International Conference on Embedded Networked Node Systems, 2004, pp. 291–292.

[23] R. Stoleru, A. John, Stankovic, Probability grid: a location estimation scheme for wireless sensor networks, sensor and ad hoc communications and networks, 2004, in: IEEE SECON 2004, 4–7 October 2004, pp. 430–438.

[24] G. Siganos, M. Faloutsos, P. Faloutsos, C. Faloutsos, Power laws and the AS-level internet topology, IEEE/ACM Transactions on Networking 11 (4) (2003).

[25] B.A. Huberman, L.A. Adamic, Growth dynamics of the World-Wide Web, Nature 40 (1999) 450–457.

[26] G. Hermann, Mathematical investigations in network properties, in: Proceedings IEEE Intelligent Engineering Systems, 2005. INES'05, September 16–19, 2005, pp. 79–82.

[27] J. Lloret, F. Boronat, C. Palau, M. Esteve, Two levels SPF-based system to interconnect partially decentralized P2P file sharing networks, in: International Conference on Autonomic and Autonomous Systems International Conference on Networking and Services Joint ICAS'05 and ICNS'05, Papeete, Tahiti (French Polynesia), October 23–28, 2005.

[28] D. Meyer, Administratively Scoped IP Multicast, RFC 2365, July 1998.

[29] M. Castro, P. Druschel, A.-M. Kermarrec, A. Rowstron, Scribe: a large-scale and decentralized application-level multicast infrastructure, IEEE J. Select. Areas Commun. 20 (8) (2002).

[30] S. Ito, H. Sogawa, H. Saito, Y. Tobe, A propagation of virtual space information using a peer-to-peer architecture for massively multiplayer online games. in: Proceedings of the 26th IEEE International Conference on Distributed Computing Systems Workshops, Lisbon (Portugal), July 2006.

[31] S. Paul, Krishan K. Sabnani, John C.-H. Lin, S. Bhattacharyya, Reliable multicast transport protocol (RMTP), IEEE J. Select. Areas Commun. 15 (3) (1997).

[32] X. Zhang, Q. Zhang, Z. Zhang, G. Song, W. Zhu, A construction of locality-aware overlay network: mOverlay and its performance, in: IEEE J. Select. Areas Commun., Special Issue on Recent Advances in Service Overlay Networks, vol. 22, January 2004, pp. 18–28.

[33] Z. Xiang, Q. Zhang, W. Zhu, Z. Zhang, Y. Zhang, Peer-to-peer based multimedia distribution service, IEEE Trans. Multimedia 6 (2) (2004).

[34] Y. Rekhter, A border gateway protocol 4 (BGP-4), RFC 1771, March 1995.

[35] N. Leibowitz, M. Ripeanu, A. Wierzbicki, Deconstructing the Kazaa Network, in: 3rd IEEE Workshop on Internet Applications (WIAPP'03), June 2003.

[36] T. Klingberg, R. Manfredi, Gnutella 0.6 draft, june 2002. Available from: <http://rfc-gnutella.sourceforge.net/src/rfc-0_6-draft.html>.

[37] B.T. Loo, R. Huebsch, I. Stoica, J. Hellerstein, The case for a hybrid P2P search infrastructure, in: Proc. 3rd International Workshop on Peer-to-peer Systems, February 2004.

[38] A. Wierzbicki, R. Strzelecki, D. Swierczewski, M. Znojek, Rhubarb: a tool for developing scalable and secure peer-to-peer applications, in: Second IEEE International Conference on Peer-to-peer Computing (P2P2002), Linöping, Sweden, 2002.

[39] L. Hongjun, L.P. Luo, Z. Zhifeng, A structured hierarchical P2P model based on a rigorous binary tree code algorithm, Future Generation Comput. Syst. 23 (2) (2007) 201–208.

[40] B. Thallner, H. Moser, Topology control for fault-tolerant communication in highly dynamic wireless networks, in: Proceedings of the Third International Workshop on Intelligent Solutions in Embedded Systems, May 2005.

[41] J. Lloret, M. Garcia, J. Tomas, A group-based architecture for wireless sensor networks, in: International Conference on Networking and Services (ICNS'07), Athens (Greece), June 2007.

[42] M. Garcia, D. Bri, F. Boronat, J. Lloret, A new neighbor selection strategy for group-based wireless sensor networks, in: The Fourth International Conference on Networking and Services (ICNS 2008), Gosier, Guadeloupe, March 2008.

[43] J. Lloret, Juan R. Diaz, F. Boronat, Jose M. Jiménez, A fault-tolerant P2P-based protocol for logical networks interconnection, in: International Conference on Networking and Services (ICNS'06), Silicon Valley, USA, July 2006.