Overlay Networks: Overview, Applications and Challenges

Jaime Galán-Jiménez[†] *and Alfonso Gazo-Cervero*[†]

[†]*Department of Computing and Telematics System Engineering,*
Polytechnic School of Cáceres, University of Extremadura, Cáceres, 10003 Spain

Summary
In recent years, overlay networks have rapidly evolved and emerged as a promising platform to deploy new applications and services in the Internet, becoming widely used for content delivery and file sharing services. This is because they provide effective and reliable services by creating a virtual topology on top of existing networks. However, new network environments and network services require new management strategies which can cope with resource constraints, scalability, dependability, context awareness, security, mobility, and other issues. This paper presents a survey on several different research topics of applicability of overlay networks. As a conclusion, it is predictable that new requirements of applications and technology improvements will stimulate the evolution of overlay networks; some of these approaches are discussed as well.

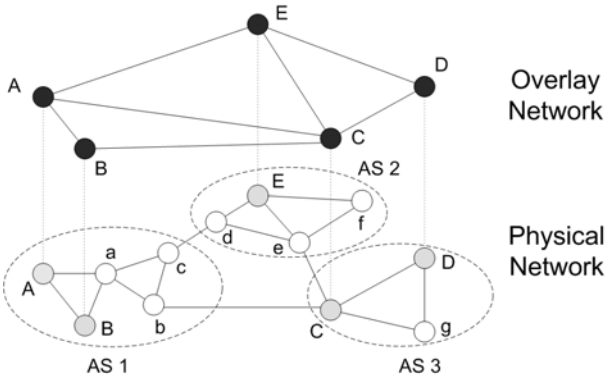
Key words:
Overlay Multicast, Overlay topologies, Content Distribution, P2P, VPN.

1. Introduction

A number of application layer overlay designs have been proposed to address issues like ensuring performance and availability of Internet routing, enabling multicasting, providing Quality of Service (QoS) guarantees, protecting from denial of service attacks, and content distribution and file sharing services [1].
It is well known that flooding-based systems do not scale well due to the bandwidth and processing requirements they impose on the network. In addition, they provide no guarantees as to lookup times or content accessibility. Overlay networks can help in addressing these issues because they have a network semantics layer above the basic transport protocol level (Fig. 1). This organizes the network topology according the nodes' content, implementing a distributed hash table abstraction that provides load balancing, query forwarding and bounded lookup times [2].
In an overlay topology, node behavior can be either cooperative or selfish. In the cooperative mode of operation, each node creates overlay links to send its traffic demands to allow other nodes to route their traffic demands over them. In the selfish mode of operation, nodes create overlay links in the network to maximize their own benefits. Thus, an overlay network has the following properties:

- To be built on top of one or more existing networks.
- To add an additional layer of indirection/virtualization.
- To change properties in one or more areas of underlying networks.
- To be possible to change an existing network layer.

Large scale distributed applications can take advantages of promising characteristics of overlay networks, such as resilience in the event of node failures, adaptation of extended structures and applications and ease of deployment in setting up overlay networks and services.
There are several issues currently studied regarding overlay networks research topic. Table 1 shows a classification of them and their corresponding references in the text. First column represents the issue studied and the second one the number of those references related to it.



Link overlay	Physical path
A-B	A-B
A-C	A-**a**-b-C
A-E	A-**a**-c-d-E
B-C	B-**a**-b-C
C-D	C-D
C-E	C-**e**-E
D-E	D-C-**e**-E

Fig. 1 Example of an Overlay Network.

Manuscript received December 5, 2010.
Manuscript revised December 20, 2010.

Table 1: Classification and related work of current issues in Overlay Networks

Issue	References
Management of Peer-to-Peer networks	[3-7]
Management of Virtual Private Networks	[8-11]
Overlay multicast	[12-39]
Overlay service topology design	[40-60]
Content distribution on overlay networks	[61]
Overlay-based failure detection and recovery	[62-68]
Overlay protocols in ad-hoc networks	[69-76]
Overlay networks and Pocket Switched Networks	[77, 78]

The rest of this paper is organized as follows. An extensive description of Peer-to-peer networks is addressed in Section 2; Section 3 explains Virtual Private Networks; and Section 4 offers a comparison between them. In Section 5, the issue of overlay multicast is considered, while the problem of the overlay service topology design is raised in Section 6. Section 7 addresses the topic of massive content distribution on overlay networks; and other overlay network challenges are reviewed in Section 8. Finally, conclusions and future work are provided in Section 9.

2. Peer-to-peer Networks

Peer-to-peer (P2P) networks and Virtual Private Networks (VPNs) are two typical overlay networks in constructing large scale distributed applications over large networks.
Peer-to-peer networks run on top of the Internet. Peer-to-peer networks are distributed systems where the software running on each node provides equivalent functions. A definition of P2P networking is a set of technologies that enable the direct exchange of services or data between computers. Implicit in this definition are the fundamental principles that peers are equals. P2P systems emphasize sharing among these equals. A pure peer-to-peer system runs without any centralized control or hierarchical organization. A hybrid system uses some centralized or hierarchical resources. Peers can represent clients, servers, routers, or even networks [3].

2.1 Goal in P2P Networks

In an opposite approach from the client/server model, it is expected for all clients in Peer-to-peer networks to provide resources, including bandwidth, storage space, and computing power. Thus, as nodes arrive and make new requests, the total capacity of the system also increases. This is not different from the client-server architecture, where a fixed set of servers involves that adding more clients generally means that they perceive a decrease in the global performance.

The distributed nature of P2P networks also increases robustness in case of failures by replicating data over multiple peers. In addition, in pure peer-to-peer systems, peers can find data without relying on a centralized index server. In the latter case, there is no single point of failure in the system.

2.2 Classification in P2P Networks

Peer-to-peer networks can be classified according to their uses:

- File sharing.
- VoIP.
- Instant messaging and streaming media (audio, video).
- Online social networks.

However, there is another classification of peer-to-peer networks according to their degree of centralization:

- Peers act as equals, merging the roles of clients and server.
- There is no central server managing the network.
- There is no central router.

2.3 Architectures of P2P Networks

Every peer-to-peer network uses one of the following three types of architectural formats. These formats may include peers and servers:
Centralized Architecture: Central servers respond to peers requests. In this architecture, the peer-to-peer application executing on the peer systems establishes a persistent connection to the central server. The centralized architecture provides excellent performance for search requests and is popular in smaller networks where the community controls user access. However, it is expected that centralized architectures do not scale adequately to large networks and suffer from severe weakness with the central server. Hackers and malicious attacks can easily disable peer-to-peer networks built on the centralized architecture by attacking and disabling the central server.
De-centralized Architecture ("true" P2P Networks): Multiple peers respond to requests from other peers on the network. The de-centralized architecture uses a distributed computing model in which each peer is an equal within the network and this kind of architecture does not contain a central server. There are two advantages over the centralized approach: First, this architecture scales to large networks of peers. Second, malicious attackers cannot easily disable the de-centralized approach due to the distributed control. However, the disadvantage to de-centralized networks is the significantly longer time required to perform search operations.
Hybrid Architecture: This type of architecture combines both the centralized and decentralized approaches into a sole system. This hybrid architecture introduces the

concept of SuperNode (also commonly known as UltraPeer), with similar functions to the central server of the Centralized Architecture. In this architecture, SuperNodes are geographically dispersed to create a larger network. The peer-to-peer application executing on the peer systems establishes a persistent connection to one or more SuperNodes and transmits a directory listing of the items available for sharing on the peer system. The hybrid architecture scales to large networks of peers. As with the de-centralized approach, the hybrid network cannot be easily disabled due to the distributed and dynamic nature of the SuperNodes.

2.4 Management of P2P Networks

For peer-to-peer networks, the management considers three different issues: traffic management, scalability management and security management.
Traffic management: Critical applications must not be affected by non-priority applications. Because of this, approaches like providing flexible bandwidth limits, bandwidth borrowing, and traffic queuing should be considered.
Self-Organization in Peer-to-peer: Peer-to-peer systems have to provide services like routing, searching for and accessing of resources. An open question is how much can self-organization emerge as an essential feature for improving the quality of the services. Requirements for self-organization in peer-to-peer networks [4] include issues like feedback, reduction of complexity, randomness, self-organized criticality and emergence.
Security Management: There are important issues related to security in overlay networks, like file sharing where extensive security requirements must be satisfied (e.g., enterprise content sharing and distributed computing) [5], [6]. Likewise, many peer-to-peer networks are under constant attacks such as:

- Different types of attacks like denial of service attacks (attacks that may make the network run very slowly or break completely), spamming (sending unsolicited information across the network) or identity attacks (tracking down the users of the network).
- Most attacks can be controlled from design and through the use of encryption.
- The “Byzantine Generals Problem” [7].

3. Virtual Private Networks

A Virtual Private Network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits over shared or public communication networks (e.g., the Internet) as opposed to their conduction across a single private network.

The link-layer protocols of the virtual network are said to be tunneled through the larger network. One common application is secure communications through the Internet. Although a VPN does not need to have explicit security features, such as authentication or content encryption, they can be used to separate the traffic of different user communities over an underlying network with strong security features [8], [9].

3.1 Tunneling and Benefits of VPNs

A VPN may have best-effort performance, or may have a defined service level agreement (SLA) between the VPN customer and the VPN service provider.
VPNs are deployed with privacy through the use of a tunneling protocol and security procedures. Tunneling has two forms:

- Remote-access: User-to-LAN connection.
- Site-to-site: An organization can connect multiple fixed sites over a public network.

Creating a VPN benefits an organization as in:

- Extended geographical communication.
- Reduced operational cost.
- Enhanced organizational management.
- Enhanced network management with simplified local area networks.
- Improved productivity and globalization.

3.2 Management of VPNs

Management of VPNs faces some challenges in security management, service management, data management and even tunnel management [10], [11] to maintain fast, secure and reliable communications. These challenges include:
Security Management: VPNs remain susceptible to security issues when they try to connect between two private networks using a public resource. The challenge in making a practical VPN, therefore, is finding the best security for it:

- User authentication mechanisms before VPN connection.
- Some ISPs offer managed VPN service for business customers who want the security and convenience of a VPN but not to administer it.
- Trusted Delivery Networks (Actual Private Networks, APNs). L2TP, L2F, PPTP.
- Security Mechanisms.
- Secure VPN protocols:
    - IPsec.
    - SSL/TLS.
    - OpenVPN.
    - L2TPv3.
- VPN Quarantine.
- Security on Mobile VPNs (HIP).

Service Management: VPN management simplifies the task of defining, distributing, enforcing and deploying VPN policies to keep all remote sites synchronized with the latest security policies.
Data Management: VPN management supports access to back-end databases for highly efficient and reliable data storage and retrieval.
Tunnel Management: It can be thought in terms of what type of tunneling protocols will be used.

4. Comparison between P2P Networks and VPNs

Peer-to-peer networks and VPNs have some common characteristics, such as ease to reconstruct the communications states, dynamic deployment for scalability and use of the services of communications layers beneath them. However, they have some differences in their design, applications and management:
Purpose: Data sharing and communications between peers (P2P) versus extension of enterprise networks (intranet) over public networks (VPN).
C*ommunication style:* communication between peers with equal roles (P2P) versus addition of a node to an extended intranet (VPN) with different roles, similar than client/server model.
Communication technology: Application layer overlay network on top of the native or physical network topology (contents exchanged directly over the IP network) in P2P versus the use of tunneling protocols (they can be designed over layer 1, 2 and 3) in VPN.
Scalability: Performance of the system not sensitive to scaled networks (P2P) versus architectures not fully distributed (impact on system performance if they grow up, VPN).
Management: Traffic management, search strategies and dynamic structure management (P2P) versus security management and tunnel management (VPN).

5. Overlay Multicast

Many applications (e.g., audio and video streaming, multi-party games) rely on some support for data multicast, where clients interested in a given data stream can join a corresponding multicast group.
Although IP multicast approaches can be considered to be solutions for various new emerging services which require active participation from many users, they do not work well in the current Internet which is based on unicast communications [12]. Various alternative methods are being developed to overcome this limitation of the current Internet. One such method is overlay multicast. These networks are typically composed of one or more propagation trees or a single mesh. In these structures, nodes are computers and edges are overlay links formed by the establishment of peering relationships between the nodes. Overlay multicast networks can be characterized by a set of measures and properties, an important element of which is the diffusion pattern. Peer selection in these systems is based on classic measures like end-to-end delay and outgoing bandwidth. In mesh-based systems, where nodes pull the data from their neighbors, peer selection is primarily based on the availability of content on nodes.
Most overlay multicast uses bi-directional TCP connections between the end-systems. Although TCP guarantees an abutted sequence for reception and reliable transmission, TCP does not satisfy all properties of the overlay multicast. This is why there are some research work around the overlay multicast topic.
In [13], authors propose to combine two mechanisms by deploying a protocol stack and design a two-layered architecture for media streaming in overlay networks. The first layer is a generic and customizable protocol which is able to construct and maintain different types of meshes. The second layer is responsible for data propagation to the nodes in the mesh by constructing an optimized diffusion tree. The goal of this modular approach is to address some inherent problems in tree-based overlay streaming solutions, in particular the vulnerability of the diffusion tree against failures and its poor resource utilization. This architecture is lightweight in terms of bandwidth usage and maintains an acceptable average reception rate.
Allani et al. [14] take a probabilistic approach by considering the probability of node failure and message loss and using retransmission to compensate for the failures. In the realm of tree-based systems, Overcast [15], NICE [16] and ESM [17], mostly focus on multimedia streaming. Some systems have also proposed building multiple trees. Some examples are CoopNet [18], Splitstream [19] and ChunkySpread [20]. Generally, these systems use Multiple Description Coding (MDC). Nevertheless, it is crucial to design an efficient network-aware overlay network to enable multicast service to adjust under the dynamic underlying network conditions and node churn in a scalable manner. In [21], Keong Lua et al. propose an accurate and scalable Internet subspace geometry to embed the nodes onto a geometric plane by measuring delay latencies between some nodes and assign geometric coordinates to all nodes in such a way that the geometric distances between node coordinates closely approximate their delay latencies.
Related work shows a scalable application-level multicast [22], [23] built on Pastry [24] and a source-specific, application-level multicast scheme that is built on top of Tapestry known as Bayeux [25]. CAN-Multicast [26] is built on top of Content Addressable Network (CAN), by creating a separate CAN overlay for each multicast group,

and then perform flooding of multicast messages to all nodes.

It is known that overlay routing enhances both reliability and performance of IP networks [27]. This is because it can bypass network congestion and transient outages by forwarding traffic through one or more intermediate overlay nodes. Therefore, there are many researchers working on the design of algorithms for multicast applications in overlay networks. In [27], Pompili et al. propose two different multicast algorithms to achieve traffic balancing on the overlay network so as to avoid traffic congestion and fluctuation on the underlay network, which cause low performance.

There are many works related to the construction of multicast algorithms in overlay networks [19], [23], [28], [29], although neither of these algorithms have addressed QoS requirements of multicast groups. Overlay multicast network infrastructures have been proposed as feasible solutions to support scalable inter-domain multicast services for real-time applications [30], [31] (utilization of MSNs: multicast service nodes). QUEST (a QoS assUred composEable Service infrastructure) provide both QoS assurances under multiple QoS constraints, and load balancing in service overlay networks [32].

In [33], the authors consider overlay multicast in the scenarios where any participant node is a potential data source. Existing multicast algorithms for single-source always require a long time to deliver messages or have high maintenance overhead when multiple data sources are allowed. However, there are other algorithms that are designed for multi-source scenarios, but they consume too much network resources and have a long convergence time because of proximity ignorance. In this way, they propose an algorithm called FPCast, which leverages node heterogeneity and proximity information at the same time.

The introduction of a reliable data delivery scheme for relay-based overlay multicast is tackled in [34]. The proposed method is based on the architecture for n-plex multicast service which realizes simultaneous communications between multiple senders and multiple receivers [35], [36]. Jeon et al. [37] raise the multicast tree reconstruction procedure required when a non-leaf node fails or leaves. They propose a proactive approach to solve the aforementioned defect of overlay multicast scheme by using a resource reservation of some nodes in the tree construction procedure. A route maintenance approach makes it possible to shorten recovery time from parent node's abrupt failure. Otherwise, Yu et al. propose in [38] a novel overlay multicast protocol named Fuzzy priority based Overlay Multicast (FOM), which adopts a fuzzy mechanism to accurately calculate the priority by taking all the properties of nodes into consideration, like delay and available bandwidth to build multicast trees. When the available bandwidth is insufficient to build a multicast tree, a priority based filtering mechanism is implemented to rebuild it. Finally, the aforementioned described requirements make multicast routing an important and difficult challenge in the Internet and even more so in ad hoc networks. In fact, mainly due to the dynamic nature of the routes, multicast protocols developed for wired networks cannot operate in the harsher wireless environment. The work published by Rodolakis et al. [39] studies the benefits of multicast routing in the performance of wireless ad hoc networks: if a node wishes to communicate with n distinct destinations, multicast can reduce the overall network load by a factor O(sqrt(n)) in comparison of unicast. Hence, the aggregate multicast capacity of wireless ad hoc networks is O(sqrt(n)) larger than the unicast capacity when the group size n is small compared to the total number of nodes in the network. They use and evaluate the multicast protocol called Multicast Overlay Spanning Trees (MOST) for wireless mesh networks through simulations (ns-2) and tests in real network environments.

6. Overlay Service Topologies

Overlay topology design has been one of the most challenging research areas over the past few years. Several studies have appeared in the literature with the purpose of providing optimal routing and topology design in different contexts, such as wired backbone networks [40–43], wireless networks [44], [45] and recently Service Overlay Networks [46–55].

Service Overlay Networks (SONs) have emerged as one of the most promising architectures envisioned to provide end-to-end QoS guarantees in the Internet. They create a virtual topology on top of the Internet and provide end-to-end QoS guarantees with no support from the underlying network. A distinguishing characteristic of SONs is that the overlay links can be overlapped at the physical layer even though they are completely disjointed at the overlay layer. The SON establishes bilateral service level agreements with the individual underlying ISPs for hosting overlay nodes and purchasing the bandwidth needed for serving its users. An adaptive topology design framework for SONs is presented in [46] to ensure inter-domain QoS, and a set of heuristics is proposed to solve the least-cost topology design problem. The problem is, however, formulated considering full coverage of all traffic demands and assuming that overlay node locations are given. Moreover, no bounds on link capacities are included and the user assignment is not optimized.

The joint end-system assignment and routing problem is investigated in [47] to determine the minimum cost overlay network. Another set of heuristics for SONs design is proposed in [48]: these algorithms aim to construct an overlay topology maintaining the connectivity between overlay nodes under various IP-layer path failure

scenarios. To increase the performance of the network in case of a link failure, the Resilient Overlay Networks (RON) approach was proposed [54]. RON routes packets based on minimizing routing cost function [48]. The problem of dynamic overlay network reconfiguration is addressed in [50], where the main goal is to find the optimal reconfiguration policies that can both accommodate time-varying communication requirements and minimize the total overlay network cost. The optimization of the resources utilized by an SON is a fundamental issue for an overlay operator owing to the costs involved and the need to satisfy user requirements. Careful decisions are necessary to provide enough capacity to overlay links, to route traffic, to assign users to access nodes and to deploy overlay nodes.

Two mathematical programming models are proposed for user assignments in [55], traffic routing optimization and dimensioning of the capacity reserved on overlay links in SONs. The first model minimizes the SON installation cost while providing full access to all users. The second model maximizes the SON profit by selecting which users to serve, based on the expected gain, and taking into consideration budget constraints of the SON operator. Authors conclude that the overlay topology design techniques proposed in previous works [48–55] are less general than their SON design models since they consider at least one of the following special cases:

(i) The number and location of overlay nodes are pre-determined.
(ii) The routing is fixed and known.
(iii) There are no capacity constraints on overlay links.
(iv) Full coverage of all network users is provided without consideration of the SON profit maximization issue.

Researchers have noticed that among the most interesting open problems in overlay network design is topology creation such as node location and link setup. The creation of virtual networks has been proposed for various network technologies, like optical networks or virtual topologies in the wavelength domain created on top of optical networks (Lightnet). Youssef et al. [56] try to find the optimal overlay network topology considering both transport and overlay link creation costs. They address the challenge of overlay topology design by considering which overlay topology best minimizes cost function, taking into account overlay link creation cost and routing cost. Bimodal traffic demands are considered, which simulate a high level of variation in the traffic demands between the network nodes. Finally, guidelines for the selection of the best heuristic as a function of the cost parameters are also provided. In [57], the topology design problem of a SON is addressed from a performance point of view. Since the analytical solution of the problem is too computationally complex, authors compare the performance of some well-known topologies and propose a new traffic demand aware overlay topology called K-shortest-path-tree (KSPT). This is accomplished by varying the number of overlay nodes and the IP network size. When considering different topologies, it is necessary to understand how they affect the overlay routing performance and how to efficiently build overlay topologies connecting all the overlay nodes. Some work has focused on the selection of the best overlay links (e.g. [47]), but other issues, such as binding end systems to overlay access nodes, positioning the overlay nodes [49], [58] or choosing the right number of overlay nodes, have also been faced. In these studies, the overlay topology is usually represented as a graph and the topology design problem is expressed as an optimization problem. The general approach relies on the use of heuristic algorithms that allow finding a near-optimal solution.

Most works [46], [47], [49], [50], [59] analyze the topology design problem from a monetary cost point of view with the aim to minimize the cost for the deployment of the SON. Only a few works [48], [60] deal with the SON topology design problem from a network performance perspective. In [60], authors aim at finding the overlay topology minimizing a cost function which takes into account the overlay link creation cost and the routing cost. They also highlight how the traffic demand affects the creation of new overlay links. In [48], instead, authors compare several existing and some new overlay topologies in terms of resilience.

7. Content Distribution on Overlay Networks

Massive content distribution on overlay networks stresses both the server and the network resources because of large volumes of data to be transmitted, relatively high bandwidth requirement, and many concurrent clients. While the server limitations can be overcome by replicating the data in more nodes, the network limitations is a different challenge. Network limitations bear difficulty in determining the cause and location of congestion and in provisioning extra resources accordingly. Several pieces of work present schemes for massive content distribution. For example, Chul Han et al. [61] try to assign the clients to appropriate servers, so that the network load is reduced and also well balanced, and the network resource consumption is low. This scheme allows scaling to very large systems because the algorithms are efficient and do not require network measurements nor topology or routing information. They partition the clients into disjoint subsets according to the degree of interference criterion. This degree reflects network resource usage and the interference among the concurrent connections. However, this problem is NP-complete but authors present heuristic algorithms for them.

8. Other Overlay Network Challenges

Up to this point, application-layer overlay networks have been proposed as an alternative method to overcome IP-layer path anomalies and provide users with improved routing services. Running on the application layer, overlay networks usually rely on probing mechanisms for IP-path performance monitoring and failure detection. Their service performance is jointly determined by their topology, parameters of probing mechanism and failure restoration methods.

Several works have addressed these issues by defining metrics to evaluate the performance of overlay networks in terms of failure detection and recovery, network stability and overhead. In [62], the authors model the overlay-based failure detection and recovery process and through extensive simulations investigate how different IP-layer path failure characteristics and overlay topologies, detection and restoration parameters affect service performance of overlay networks. They examine the tradeoffs among different overlay performance metrics and the optimal performance conditions, which can help to understand overlay-based failure. Zhuang et al. [63] investigate the tradeoffs of different overlay/P2P node failure detection algorithms in terms of overhead, packet loss ratio and failure detection ratio. The same topic is also discussed in [64], in which the authors focus on analytical models and propose a self-tuning method.

Some work has been done on setting up optimal hello message intervals in OSPF network environment. Goyal et al. [65] investigate the impact of topologies and network congestion on optimal HelloInterval for OSPF network through simulation. Basu et al. [66] perform experimental study of the stability of OSPF in terms of convergence time, routing load and number of routing flaps. In [67], authors use analytical methods to study the effects of traffic overload on OSPF and BGP by quantifying the stability and robustness properties. Qiu et al. [68] studied the vertical interaction between selfish overlay network and lower-layer traffic engineering mechanisms. In addition, application-layer overlay protocols have been considered for enhancing delivery services in mobile ad-hoc networks. In [69], it is shown that overlay networks can provide forward and backward secrecy for application data in an ad-hoc network. Authors present a key management and encryption scheme, called neighborhood key method, where each node shares a secret with authenticated neighbors in the ad-hoc network. Through indoor and outdoor measurement experiments they evaluate the effectiveness of the neighborhood key method and the performance of application-layer ad-hoc networks. Furthermore, several studies recently applied application-layer overlay protocol solutions in a mobile ad-hoc context to run ad-hoc routing protocols at the application layer [70], [71] or to realize a multicast service in ad-hoc networks [72], [73], [74], [75].

To end this work, many authors indicate that a management system that controls and adapts overlay networks behavior is needed. This will meet not only specific demands of users but also those of the network and service providers. Al-Oqily et al. [76] present an approach to the issue of automating overlay network management, but in contrast to existing management approaches which require static a priori policy configurations, policies are created dynamically. A policy layer consists of a set of policy enforcement points and policy decision points. This is used to capture the goals of the users, services and networks into network-level objectives.

The behavior of the overlay network is adapted to the changing conditions in its environment. The creation, adaptation, and termination of overlays are achieved through policies, which are generated and enforced from the context information of the user, the network and the service provider. This approach provides users and applications with more flexibility to dynamically change their QoS requirements.

9. Conclusion

Requirements in network management and control have been amended by emerging network and computing models. As an example, overlay networks is one emerging network application, but the new network environments and network services require new management strategies which can cope with resource constraints, scalability, dependability, context awareness, security, and mobility. Thus, the management of overlay networks should import self-management and intelligent strategies to deal with the complex management tasks. The management issues which are discussed in this paper will probably be supplemented by new approaches. It is predictable that new requirements of expanded applications will stimulate the evolution of overlay networks, technology improvement and related management in overlay networks. In addition, there have been studied other different issues related to overlay networks in this paper, like the specific management of P2P networks, VPNs and a comparison between them, the challenges of overlay multicast and the problem of the overlay service topology design.

Likewise, the topic of massive content distribution on overlay networks has been addressed as well as the overlay-based failure detection and recovery process and the issue of automating overlay network management. Furthermore, some application-layer overlay protocols have been considered for enhancing delivery services in mobile ad-hoc networks.

Future research could focus on dynamic multicast groups on overlay networks and on the dynamic interactions between overlay and underlay networks. Another interesting direction for future work consists in enhancing protocol MOST studied in [39] with quality of service mechanisms and providing measurement studies of the protocol performance.

Considering the problem of overlay topology design, future work could also focus on studying the overlay topology creation and adaptation in case of unknown traffic demands. A hybrid network with a mix of selfish and cooperative nodes is an additional interesting scenario. Heterogeneous values of the overlay cost coefficient could be proposed for each node in the network, and its effect on the overlay topology creation could be studied. Otherwise, there can be an interesting joint between overlay networks and Pocket Switched Networks [77], [78] which could be studied in depth to make solid proposals.

References

[1] N.M. Mosharaf Kabir Chowdhury and R. Boutaba, (2009). "Network Virtualization: State of the Art and Research Challenges". IEEE *Communications Magazine*, Vol. 47, Issue 7, pp20-26.

[2] D. Doval and D. O'Mahony, (2003). "Overlay Networks: A Scalable Alternative for P2P". IEEE *Internet Computing*, Vol. 7, No. 4, pp79-82.

[3] M. Hofmann and L.R. Beaumont, (2005). "Content networking: architecture, protocols, and practice". Morgan Kaufmann, ISBN: 1558608346.

[4] H. De Meer and C. Koppen, (2005). "Self-Organization in Peer-to-Peer Systems". R. Steinmetz and K. Wehrle (Eds.): *P2P Systems and Applications*, LNCS 3485, pp247-266.

[5] L. Paschoal Gaspary, M.P. Barcellos, A. Detsch and R.S. Antunes, (2007). "Flexible security in peer-to-peer applications: Enabling new opportunities beyond file sharing". *Computer Networks*, Vol. 51, Issue 17, pp4797-4815.

[6] R. Boutaba and A. Marshalla, (2006). "Management in peer-to-peer systems: Trust, reputation and security". *Computer Networks*, Vol. 50, Issue 4, pp469-471.

[7] L. Lamport, R. Shostak and M. Pease, (1982). "The Byzantine Generals Problem". ACM *Transactions on Programming Languages and Systems*, Vol. 4, No. 3, pp382-401.

[8] RFC 2764, (2000). "A Framework for IP Based Virtual Private Networks", http://www.ietf.org/rfc/rfc2764.txt.

[9] RFC 3809, (2004). "Generic Requirements for Provider Provisioned Virtual Private Networks (PPVPN)", http://www.ietf.org/rfc/rfc3809.txt.

[10] K.H. Cheung and J. Misic, (2002). "On virtual private networks security design issues". *Computer Networks*, Vol. 38, Issue 2, pp165-179.

[11] C. Xenakis, C. Ntantogian and I. Stavrakakis, (2008). "A network-assisted mobile VPN for securing users data in UMTS". *Computer Communications*, Vol. 31, Issue 14, pp3315-3327.

[12] S.E. Deering, (1988). "Multicast routing in internetworks and extended LANs". *Symposium proceedings on Communications architectures and protocols*, pp55-64, August 1988, Stanford, California, USA.

[13] A. Malekpour, F. Pedone, M. Allani and B. Garbinato, (2009). "Streamline: An Architecture for Overlay Multicast". *Eight IEEE International Symposium on Network Computing and Applications*, pp44-51, August 2009, Los Alamitos, CA, USA.

[14] M. Allani, B. Garbinato, F. Pedone and M. Stamenkovic, (2007). "A gambling approach to scalable resource-aware streaming". In *Proc. SRDS '07*, pp288–300, August 2007, Washington DC, USA.

[15] J. Jannotti, D.K. Gifford, K.L. Johnson, F.M. Kaashoek and J.W. O'Toole, (2000). "Overcast: Reliable multicasting with an overlay network". In *Proc. Usenix OSDI Symposium 2000*, pp197–212, October 2000, San Diego, CA, USA.

[16] S. Banerjee, B. Bhattacharjee and C. Kommareddy, (2002). "Scalable application layer multicast". In *Proceedings of the ACM SIGCOMM 2002*, pp205–217, August 2002, Pittsburgh, PA, USA.

[17] Y.H. Chu, A. Ganjam, T.S. Eugene Ng, S.G. Rao, K. Sripanidkulchai, J. Zhan and H. Zhang, (2004). "Early experience with an internet broadcast system based on overlay multicast". In *Proc. USENIX Annual Technical Conference 2004*, pp12–12. August 2004, Boston, MA, USA.

[18] V.N. Padmanabhan, H.J. Wang, P.A. Chou and K. Sripanidkulchai, (2002). "Distributing streaming media content using cooperative networking". In *Proc. NOSSDAV '02*, pp177–186, August 2002, New York, NY, USA.

[19] M. Castro, P. Druschel, A.M. Kermarrec, A. Nandi, A. Rowstron and A. Singh, (2003). "Splitstream: high-bandwidth multicast in cooperative environments". ". In *Proceedings of ACM Symposium on Operating Systems Principles (SOSP)*, pp298-313, October 2003, Bolton Landing, NY, USA.

[20] V. Venkataraman, P. Francis and J. Cal, (2006). "Chunkyspread: Multi-tree unstructured peer-to-peer multicast". *In Proc. IPTPS '06*, pp1-6, August 2006, Santa Barbara, CA, USA.

[21] E.K. Lua, X. Zhou, J. Crowcroft and P. Van Mieghem, (2008). "Scalable multicasting with network-aware geometric overlay". *Computer Communications*. Vol. 31, Issue 3, pp464-488.

[22] M. Castro, M.B. Jones, A.-M. Kermarrec, A. Rowstron, M. Theimer, H. Wang and A. Wolman, (2003). "An evaluation of scalable application-level multicast built using peer-to-peer overlays". In *Proceedings of the IEEE INFOCOM 2003*, Vol. 2, pp1510-1520, March 2003, San Francisco, CA, USA.

[23] M. Castro, P. Druschel, A.-M. Kermarrec and A. Rowstron, (2002). "Scribe: a large-scale and decentralized application-level multicast infrastructure". IEEE *Journal on Selected Areas in Communication (JSAC)*, Vol. 20, Issue 8, pp1489-1499.

[24] P. Druschel and A. Rowstron, (2001). "Pastry: scalable distributed object location and routing for large-scale peer to peer systems". In *Proceedings of the 18th IFIP/ACM Middleware*, pp329-350, November 2001, Heidelberg, Germany.

[25] S.Q. Zhuang, B.Y. Zhao, A.D. Joseph, R.H. Katz and J.D.Kubiatowicz, (2001). "Bayeux: an architecture for scalable and faulttolerant wide-area data dissemination". In *ACM NOSSDAV*, pp11–20, June 2001, Port Jefferson, NY, USA.

[26] S. Ratnasamy, M. Handley, R.M. Karp and S. Shenker, (2001). "Application level multicast using content-addressable networks". In *Proceedings of the Third International COST264 Workshop on Networked Group Communication*, pp14–29, November 2001, London, UK.

[27] D. Pompili, C. Scoglio, L. Lopez, (2008). "Multicast algorithms in service overlay networks". *Computer Communications*. Vol. 31, Issue 3, pp489-505.

[28] D. Kostic, A. Rodriguez, J. Albrecht and A. Vahdat, (2003). "Bullet: High Bandwidth Data Dissemination Using an Overlay Mesh". In *Proceedings of ACM Symposium on Operating Systems Principles (SOSP)*, pp282-297, October 2003, Bolton Landing, NY, USA.

[29] V. Pai, K. Kumar, K. Tamilmani, V. Sambamurthy and A. Mohr, (2005). "Chainsaw: eliminating trees from overlay multicast". In *Proceedings of International Workshop on Peer-to-Peer Systems (IPTPS)*, pp127-140, February 2005, Ithaca, NY, USA.

[30] S.Y. Shi and J.S. Turner, (2002). "Routing in Overlay Multicast Networks". In *Proceedings of the IEEE INFOCOM 2002*, Vol. 3, pp1200-1208, June 2002, New York, NY, USA.

[31] L. Lao, J.-H. Cui and M. Gerla, (2005). "TOMA: a viable solution for largescale multicast service support". In *Proceedings of IFIP International Conference of Networking*, pp906-917, May 2005, Waterloo, Ontario, Canada.

[32] X. Gu, K. Nahrstedt, R. Chang and C. Ward, (2003). "QoS-assured service composition in managed service overlay networks". In *Proceedings IEEE International Conference on Distributed Computing Systems (ICDCS)*, pp194-201, May 2003, Providence, Rhode Island, USA.

[33] Z. Li, Z. Zhu, G. Xie and Z. Li, (2009). "Fast and proximity-aware multi-source overlay multicast under heterogeneous environment". *Computer Communications*. Vol. 32, Issue 2, pp257-267.

[34] S.-H. Kim, C.-K. Lee and S.-G. Kang, (2009). "Reliable data delivery for relay-based overlay multicast". In *Proceedings of the 11th international conference on Advanced Communication Technology*, Vol. 1, pp782-785, June 2009, Gangwon-Do, South Korea.

[35] J. Park, J.M. Lee and S.-G Kang, (2007). "Design and Implementation of Overlay Multicast Protocol for many-to-many Multicast services", In *ICACT 2007*, pp2144-2147, February 2007, Gangwon-Do, South Korea.

[36] C.-K. Lee, S.-H. Kim and S.-G. Kang, (2008). "A study of n-ton overlay multicast with static core domain for service stability improvement", In *CEIC 2008*, pp1-6, April 2008, Lake Las Vegas, NV, USA.

[37] J.-H. Jeon, S.-C. Son and J.-S. Nam, (2008). "Overlay multicast tree recovery scheme using a proactive approach". *Computer Communications*. Vol. 31, Issue 14, pp3163-3168.

[38] J. Yu, L. Chen and G.-C. Chen, (2008). "Fuzzy priority based overlay multicast". *Computer Communications*. Vol. 31, Issue 10, pp1919-1933.

[39] G. Rodolakis, A. Laouiti, P. Jacques and A.M. Naimi, (2008). "Multicast overlay spanning trees in ad hoc networks: Capacity bounds, protocol design and performance evaluation". *Computer Communications*. Vol. 31, Issue 7, pp1400-1412.

[40] R.R. Boorstyn and H. Frank, (1977). "Large-scale network topological optimization", IEEE *Transactions on Communications*. Vol. 25, Issue 1, pp29–47.

[41] M. Pioro and D. Medhi, (2004). "Routing Flow, and Capacity, Design in Communication and Computer Networks", Morgan Kaufman Publishers.

[42] S. Ratnasamy, M. Handley, R. Karp and S. Shenker, (2002). "Topologically-aware overlay construction and server selection". In *Proceedings of the IEEE INFOCOM 2002*, Vol. 3, pp1190-1199, June 2002, New York, NY, USA.

[43] A. Kershenbaum, P. Kermani and G. A. Grover, (1991). "MENTOR: an algorithm for mesh network topological optimization and routing". IEEE *Transactions on Communications*. Vol. 39, Issue 4, pp503-513.

[44] A. Hills, (2001). "Large-scale wireless LAN design". IEEE *Communications Magazine*. Vol. 39, Issue 11, pp98–107.

[45] E. Amaldi, A. Capone, M. Cesana and F. Malucelli, (2007). "Optimization models for the radio planning of wireless mesh networks". In *Proceedings of the Networking 2007*, pp287-298, May 2007, Atlanta, GA, USA.

[46] H.T. Tran and T. Ziegler, (2007). "A design framework towards the profitable operation of service overlay networks". *Computer Networks*. Vol. 51, Issue 1, pp94–113.

[47] S.L. Vieira and J. Liebeherr, (2004). "Topology design for service overlay networks with bandwidth guarantees". In *Proceedings of the 12th IEEE International Workshop on Quality of Service (IWQoS)*, pp211-220, June 2004, Montreal, Canada.

[48] Z. Li and P. Mohapatra, (2007). "On investigating overlay service topologies". *Computer Networks*, Vol. 51, Issue 1, pp54–68.

[49] J. Han, D. Waston and F. Jahanian, (2005). "Topology aware overlay networks". In *Proceedings of the IEEE INFOCOM 2005*, pp2554-2565, March 2005, Miami, FL, USA.

[50] J. Fan and M.H. Ammar, (2006). "Dynamic topology configuration in service overlay networks: a study of reconfiguration policies". In *Proceedings of the IEEE INFOCOM 2006*, pp1-12, April 2006, Barcelona, Spain.

[51] S. Shi and J. Turner, (2002). "Placing servers in overlay networks". In *Proceedings of the International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, pp1-8, July 2002, San Diego, CA, USA.

[52] B.D. Vleeschauwer, F.D. Turck, B. Dhoedt and P. Demeester, (2004). "On the construction of QoS enabled overlay networks". In *Proceedings of the Fifth International Workshop on Quality of Future Internet Services (QofIS04)*, pp164-173, October 2004, Barcelona, Spain.

[53] S. Roy, H. Pucha, Z. Zhang, Y.C. Hu and L. Qiu, (2007). "Overlay node placement: analysis, algorithms and impact on applications" In *Proceedings of the 27th International Conference on Distributed Computing Systems*, pp53-53, June 2007, Toronto, Canada.

[54] D. Andersen, H. Balakrishnan, M. Kaashoek and R. Morris, (2001). "Resilient overlay networks". In *Symposium on*

Operating Systems Principles, pp131-145, October 2001, Banff, Alberta, Canada.
[55] A. Capone, J. Elias and F. Martignon, (2009). "Routing and resource optimization in service overlay networks". *Computer Networks*, Vol. 53, Issue 2, pp180-190.
[56] M. Youssef, C. Scoglio, (2009). "On graph-based characteristics of optimal overlay topologies". *Computer Networks*, Vol. 53, Issue 7, pp913-925.
[57] D. Adami, C. Callegari, S. Giordano, G. Nencioni and M. Pagano, (2009). "Design and performance evaluation of service overlay networks topologies". In *Proceedings of the 12th international conference on Symposium on Performance Evaluation of Computer & Telecommunication Systems*, pp296-303, July 2009, Istanbul, Turkey.
[58] A. Capone, J. Elias and F. Martignon, (2008). "Optimal design of service overlay networks". In *Proceedings of the Fourth International Workshop on QoS in Multiservice IP Networks*, pp1-7, February 2008, Venice, Italy.
[59] L. Zhou and A. Sen, (2007). "Topology design of service overlay network with a generalized cost model". In *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM) 2007*, pp75–80, November 2007, Washington DC, USA.
[60] M. Kamel, C. Scoglio and T. Easton, (2007). "Optimal topology design for overlay networks". *Lectures Notes in Computer Science, Springer*, Vol. 4479/2007, pp714–725.
[61] S.C. Han and Y. Xia, (2009). "Network load-aware content distribution in overlay networks". *Computer Communications*, Vol. 32, Issue 1, pp51-61.
[62] Z. Li, L. Yuan, P. Mohapatra and C.-N. Chuah, (2007). "On the analysis of overlay failure detection and recovery". *Computer Networks*, Vol.51, Issue 13, pp3828-3843.
[63] S.Q. Zhuang, D. Geels, I. Stoica and R.H. Katz, (2005). "On failure detection algorithms in overlay networks". In *Proceedings of the IEEE INFOCOM 2005*, pp2112–2123, March 2005, Miami, FL, USA.
[64] R. Mahajan, M. Castro and A. Rowstron, (2003). "Controlling the cost of reliability in peer-to-peer overlays". In *Proc. International Workshop on Peer-to-Peer Systems*, pp21–32, February 2003, Berkeley, CA, USA.
[65] M. Goyal, K.K. Ramakrishnan and W. Feng, (2003). "Achieving master failure detection in OSPF networks" In *Proc. International Conference on Communications*, pp296–300, May 2003, Anchorage, AK, USA.
[66] A. Basu and J.G. Riecke, (2002). "Stability issues in OSPF routing". In *Proceedings of the ACM SIGCOMM 2002*, pp225–236, August 2002, Pittsburgh, PA, USA.
[67] A. Shaikh, L. Kalampoukas, R. Dube and A. Varma, (2000). "Routing stability in congested networks: Experimentation and analysis". In *Proceedings of the ACM SIGCOMM 2000*, pp163–174, August 2000, Stockholm, Sweden.
[68] L. Qiu, Y.R. Yang, Y. Zhang and S. Shenker, (2003). "On selfish routing in internet-like environments". In *Proceedings of the ACM SIGCOMM 2003*, pp151–162, August 2003, Karlsruhe, Germany.
[69] J. Liebeherr and G. Dong, (2007). "An overlay approach to data security in ad-hoc networks". *Ad Hoc Networks*, Vol. 5, Issue 7, pp1055-1072.
[70] Y.C. Hu, S.M. Das and H. Pucha, (2003). "Exploiting the synergy between peer-to-peer and mobile ad hoc networks". In *Proceedings of 9th Workshop on Hot Topics in Operating Systems (HotOS IX)*, pp37-42, May 2003, Lihue, Hawaii, USA.
[71] R. Shollmeier, I. Gruber and M. Finkenzeller, (2002). "Routing in mobile adhoc and peer-to-peer networks: A comparison". In *Proceedings of International Workshop on Peer-to-Peer Computing*, pp172-186, May 2002, Pisa, Italy.
[72] K. Chen and K. Nahrstedt, (2005). "Effective location-guided overlay multicast in mobile ad hoc networks". *International Journal of Wireless and Mobile Computing, Special Issue on Group Communications in Ad Hoc Networks*, Vol. 3, pp1-15.
[73] M. Ge, S.V. Krishnamurthy and M. Faloutsos, (2004). "Overlay multicasting for ad hoc networks". In *Proc. of Third Mediteranean Ad Hoc Networking Workshop (Med-Hoc-Net)*, pp1-12, June 2004, Bordum, Turkey.
[74] C. Gui and P. Mohapatra, (2003). "Efficient overlay multicast for mobile ad hoc networks". In *Proc. of IEEE Wireless Communications and Networking Conference (WCNC)*, Vol. 2, pp1118–1123, March 2003, New Orleans, USA.
[75] L. Xiao, A. Patil, Y. Liu, L.M. Ni and A.H. Esfahanian, (2004). "Prioritized overlay multicast in mobile ad hoc environments". IEEE *Computer*, Vol. 37, Issue 2, pp67–74.
[76] I. Al-Oqily and A. Karmouch, (2009). "Towards automating overlay network management". *Journal of Network and Computer Applications*, Vol. 32, Issue 2, pp461-473.
[77] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass and J. Scott, (2005). "Pocket switched networks: Real-world mobility and its consequences for opportunistic forwarding". *Technical Report UCAM-CL-TR-617*, University of Cambridge, Computer Laboratory, February 2005.
[78] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft and C. Diot, (2005). "Pocket switched networks and human mobility in conference environments". In *Proceedings of the ACM SIGCOMM workshop on Delay-tolerant networking 2005*, pp244-251, August 2005, Philadelphia, USA.

Jaime Galán-Jiménez received his Engineering degree in Computer Science Engineering at the University of Extremadura (Spain) in 2007, where he is currently working in the Computing Systems and Telematics Engineering Department. In 2009, he received a PhD grant from the Regional Government of Extremadura to conduct his research. His main research topics are overlay networks, delay-tolerant networks, energy efficient networks and interferences in wireless technologies.

Alfonso Gazo-Cervero received his PhD in computer science and communications from the University of Extremadura. He is currently the main researcher of the Advanced and Applied Communications Engineering Research Group (GITACA) of the University of Extremadura, where he also holds an assistant professor position. His research interests are mainly related to capacity planning, routing protocols, overlay networks and energy efficient networks.