LNCS 4785

Alexander Clemm
Lisandro Zambenedetti Granville
Rolf Stadler (Eds.)

# Managing Virtualization of Networks and Services

18th IFIP/IEEE International Workshop
on Distributed Systems: Operations and Management, DSOM 200
San José, CA, USA, October 2007, Proceedings

ifip

Springer

Alexander Clemm
Lisandro Zambenedetti Granville
Rolf Stadler (Eds.)

# Managing Virtualization of Networks and Services

18th IFIP/IEEE International Workshop
on Distributed Systems: Operations and Management, DSOM 2007
San José, CA, USA, October 29-31, 2007
Proceedings

Springer

Volume Editors

Alexander Clemm
Cisco Systems
170 West Tasman Drive (SJC23/2)
San Jose, CA 95134-1706, USA
E-mail: alex@cisco.com

Lisandro Zambenedetti Granville
Federal University of Rio Grande do Sul (UFRGS)
Instituto de Informática Av. Bento Gonçalves
9500 - Bloco IV - Agronomia 91501-970 - Porto Alegre, RS Brazil
E-mail: granville@inf.ufrgs.br

Rolf Stadler
School of Electrical Engineering
KTH Royal Institute of Technology
KTH/EE/S3, Osquldas väg 10
SE-100 44 Stockholm, Sweden
E-mail: stadler@ee.kth.se

Library of Congress Control Number: 2007936689

CR Subject Classification (1998): C.2.4, C.2, D.1.3, D.4.4, K.6, K.4.4

LNCS Sublibrary: SL 5 – Computer Communication Networks
and Telecommunications

ISSN 0302-9743
ISBN-10 3-540-75693-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-75693-4 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12175086 06/3180 5 4 3 2 1 0

# Lecture Notes in Computer Science 4785

*Commenced Publication in 1973*
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

# Lecture Notes in Computer Science

## Sublibrary 5: Computer Communication Networks and Telecommunications

For information about Vols. 1–4427
please contact your bookseller or Springer

Vol. 4785: A. Clemm, L.Z. Granville, R. Stadler (Eds.), Managing Virtualization of Networks and Services. XIII, 269 pages. 2007.

Vol. 4773: S. Ata, C.S. Hong (Eds.), Managing Next Generation Networks and Services. XIX, 619 pages. 2007.

Vol. 4745: E. Gaudin, E. Najm, R. Reed (Eds.), SDL 2007: Design for Dependable Systems. XII, 289 pages. 2007.

Vol. 4725: D. Hutchison, R.H. Katz (Eds.), Self-Organizing Systems. XI, 295 pages. 2007.

Vol. 4712: Y. Koucheryavy, J. Harju, A. Sayenko (Eds.), Next Generation Teletraffic and Wired/Wireless Advanced Networking. XV, 482 pages. 2007.

Vol. 4686: E. Kranakis, J. Opatrny (Eds.), Ad-Hoc, Mobile, and Wireless Networks. X, 285 pages. 2007.

Vol. 4685: D.J. Veit, J. Altmann (Eds.), Grid Economics and Business Models. XII, 201 pages. 2007.

Vol. 4581: A. Petrenko, M. Veanes, J. Tretmans, W. Grieskamp (Eds.), Testing of Software and Communicating Systems. XII, 379 pages. 2007.

Vol. 4572: F. Stajano, C. Meadows, S. Capkun, T. Moore (Eds.), Security and Privacy in Ad-hoc and Sensor Networks. X, 247 pages. 2007.

Vol. 4549: J. Aspnes, C. Scheideler, A. Arora, S. Madden (Eds.), Distributed Computing in Sensor Systems. XIII, 417 pages. 2007.

Vol. 4543: A.K. Bandara, M. Burgess (Eds.), Inter-Domain Management. XII, 237 pages. 2007.

Vol. 4534: I. Tomkos, F. Neri, J. Solé Pareta, X. Masip Bruin, S. Sánchez Lopez (Eds.), Optical Network Design and Modeling. XI, 460 pages. 2007.

Vol. 4517: F. Boavida, E. Monteiro, S. Mascolo, Y. Koucheryavy (Eds.), Wired/Wireless Internet Communications. XIV, 382 pages. 2007.

Vol. 4516: L. Mason, T. Drwiega, J. Yan (Eds.), Managing Traffic Performance in Converged Networks. XXIII, 1191 pages. 2007.

Vol. 4503: E. Airoldi, D.M. Blei, S.E. Fienberg, A. Goldenberg, E.P. Xing, A.X. Zheng (Eds.), Statistical Network Analysis: Models, Issues, and New Directions. VIII, 197 pages. 2007.

Vol. 4479: I.F. Akyildiz, R. Sivakumar, E. Ekici, J.C.d. Oliveira, J. McNair (Eds.), NETWORKING 2007. Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet. XXVII, 1252 pages. 2007.

Vol. 4465: T. Chahed, B. Tuffin (Eds.), Network Control and Optimization. XIII, 305 pages. 2007.

Vol. 4427: S. Uhlig, K. Papagiannaki, O. Bonaventure (Eds.), Passive and Active Network Measurement. XI, 274 pages. 2007.

Vol. 4396: J. García-Vidal, L. Cerdà-Alabern (Eds.), Wireless Systems and Mobility in Next Generation Internet. IX, 271 pages. 2007.

Vol. 4373: K.G. Langendoen, T. Voigt (Eds.), Wireless Sensor Networks. XIII, 358 pages. 2007.

Vol. 4357: L. Buttyán, V.D. Gligor, D. Westhoff (Eds.), Security and Privacy in Ad-Hoc and Sensor Networks. X, 193 pages. 2006.

Vol. 4347: J. López (Ed.), Critical Information Infrastructures Security. X, 286 pages. 2006.

Vol. 4325: J. Cao, I. Stojmenovic, X. Jia, S.K. Das (Eds.), Mobile Ad-hoc and Sensor Networks. XIX, 887 pages. 2006.

Vol. 4320: R. Gotzhein, R. Reed (Eds.), System Analysis and Modeling: Language Profiles. X, 229 pages. 2006.

Vol. 4311: K. Cho, P. Jacquet (Eds.), Technologies for Advanced Heterogeneous Networks II. XI, 253 pages. 2006.

Vol. 4272: P. Havinga, M. Lijding, N. Meratnia, M. Wegdam (Eds.), Smart Sensing and Context. XI, 267 pages. 2006.

Vol. 4269: R. State, S. van der Meer, D. O'Sullivan, T. Pfeifer (Eds.), Large Scale Management of Distributed Systems. XIII, 282 pages. 2006.

Vol. 4268: G. Parr, D. Malone, M. Ó Foghlú (Eds.), Autonomic Principles of IP Operations and Management. XIII, 237 pages. 2006.

Vol. 4267: A. Helmy, B. Jennings, L. Murphy, T. Pfeifer (Eds.), Autonomic Management of Mobile Multimedia Services. XIII, 257 pages. 2006.

Vol. 4240: S.E. Nikoletseas, J.D.P. Rolim (Eds.), Algorithmic Aspects of Wireless Sensor Networks. X, 217 pages. 2006.

Vol. 4238: Y.-T. Kim, M. Takano (Eds.), Management of Convergence Networks and Services. XVIII, 605 pages. 2006.

Vol. 4235: T. Erlebach (Ed.), Combinatorial and Algorithmic Aspects of Networking. VIII, 135 pages. 2006.

Vol. 4217: P. Cuenca, L. Orozco-Barbosa (Eds.), Personal Wireless Communications. XV, 532 pages. 2006.

Vol. 4195: D. Gaiti, G. Pujolle, E.S. Al-Shaer, K.L. Calvert, S. Dobson, G. Leduc, O. Martikainen (Eds.), Autonomic Networking. IX, 316 pages. 2006.

Vol. 4124: H. de Meer, J.P.G. Sterbenz (Eds.), Self-Organizing Systems. XIV, 261 pages. 2006.

Vol. 4104: T. Kunz, S.S. Ravi (Eds.), Ad-Hoc, Mobile, and Wireless Networks. XII, 474 pages. 2006.

Vol. 4074: M. Burmester, A. Yasinsac (Eds.), Secure Mobile Ad-hoc Networks and Sensors. X, 193 pages. 2006.

Vol. 4033: B. Stiller, P. Reichl, B. Tuffin (Eds.), Performability Has its Price. X, 103 pages. 2006.

Vol. 4026: P.B. Gibbons, T. Abdelzaher, J. Aspnes, R. Rao (Eds.), Distributed Computing in Sensor Systems. XIV, 566 pages. 2006.

Vol. 4003: Y. Koucheryavy, J. Harju, V.B. Iversen (Eds.), Next Generation Teletraffic and Wired/Wireless Advanced Networking. XVI, 582 pages. 2006.

Vol. 3996: A. Keller, J.-P. Martin-Flatin (Eds.), Self-Managed Networks, Systems, and Services. X, 185 pages. 2006.

Vol. 3976: F. Boavida, T. Plagemann, B. Stiller, C. Westphal, E. Monteiro (Eds.), NETWORKING 2006. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems. XXVI, 1276 pages. 2006.

Vol. 3970: T. Braun, G. Carle, S. Fahmy, Y. Koucheryavy (Eds.), Wired/Wireless Internet Communications. XIV, 350 pages. 2006.

Vol. 3964: M.Ü. Uyar, A.Y. Duale, M.A. Fecko (Eds.), Testing of Communicating Systems. XI, 373 pages. 2006.

Vol. 3961: I. Chong, K. Kawahara (Eds.), Information Networking. XV, 998 pages. 2006.

Vol. 3912: G.J. Minden, K.L. Calvert, M. Solarski, M. Yamamoto (Eds.), Active Networks. VIII, 217 pages. 2007.

Vol. 3883: M. Cesana, L. Fratta (Eds.), Wireless Systems and Network Architectures in Next Generation Internet. IX, 281 pages. 2006.

Vol. 3868: K. Römer, H. Karl, F. Mattern (Eds.), Wireless Sensor Networks. XI, 342 pages. 2006.

Vol. 3854: I. Stavrakakis, M. Smirnov (Eds.), Autonomic Communication. XIII, 303 pages. 2006.

Vol. 3813: R. Molva, G. Tsudik, D. Westhoff (Eds.), Security and Privacy in Ad-hoc and Sensor Networks. VIII, 219 pages. 2005.

Vol. 3462: R. Boutaba, K.C. Almeroth, R. Puigjaner, S. Shen, J.P. Black (Eds.), NETWORKING 2005. XXX, 1483 pages. 2005.

# Preface

This volume of the Lecture Notes in Computer Science series contains all papers accepted for presentation at the *18$^{th}$ IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM 2007)*, which was held in the heart of Silicon Valley, San Jose, California, USA, on October 29–31, 2007.

DSOM 2007 was the 18th event in a series of annual workshops. It followed in the footsteps of previous successful meetings, the most recent of which were held in Dublin, Ireland (DSOM 2006), Barcelona, Spain (DSOM 2005), Davis, California, USA (DSOM 2004), Heidelberg, Germany (DSOM 2003), and Montreal, Canada (DSOM 2002). The goal of the DSOM workshops is to bring together researchers from industry and academia working in the areas of networks, systems, and service management, to discuss recent advances and foster future growth. In contrast to the larger management conferences, such as IM (Integrated Network Management) and NOMS (Network Operations and Management Symposium), DSOM workshops have a single-track program in order to stimulate more intense interaction among participants.

The theme of DSOM 2007 was "*Managing Virtualization of Networks and Services*". Virtualization, in which the properties of a service are decoupled from its physical realization over networking and IT infrastructure, is capturing the imagination of industry and the research community alike. Questions need to be addressed such as: what is different about virtualization in 2007 compared with virtualization in the mainframe era, which advances in network control and self-management may advance virtualization technologies, which new problems will we incur when managing virtualized networks and services, and in which ways may management itself benefit from virtualization. At the same time, DSOM 2007 continued its tradition of giving a platform to papers that address general topics related to the management of distributed systems. As a result, DSOM 2007 included sessions on decentralized and peer-to-peer management, fault detection and diagnosis, performance tuning and dimensioning, problem detection and mitigation, operations and tools, service accounting and auditing, and Web services and management as well as a session with short papers.

Like the previous two DSOM workshops, DSOM 2007 was co-located with several related events as part of the Third International Week on Management of Networks and Services (MANWEEK 2007). The other events were the 10$^{th}$ IFIP/IEEE International Conference on Management of Multimedia and Mobile Networks and Services (MMNS 2007), the 7$^{th}$ IEEE International Workshop on IP Operations and Management (IPOM 2007), the 2$^{nd}$ IEEE International Workshop on Modeling Autonomic Communications Environments (MACE 2007), and the 1$^{st}$ IEEE/IFIP International Workshop on End-to-End Virtualization and Grid Management (EVGM 2007). Co-locating those events provided the opportunity for an exchange of ideas between research communities that work on related topics, allowing participants to forge links and exploit synergies.

DSOM 2007 attracted a total of 54 paper submissions by authors from 21 different countries. Each paper received at least three, and in most cases four, reviews by experts in the field. The authors were invited to write a rebuttal to the reviews. The final paper selection was based on the reviews, the authors' feedback, and (in some cases) online discussions among Technical Program Committee members. A total of 20 submissions were finally accepted into the program as full papers, 5 as short papers.

DSOM 2007 owes its success in large part to a dedicated community of researchers from academia and industry, which has formed over many years. First and foremost, we want to thank the authors of the submitted papers – without them, there would be no program. We also want to thank the members of the Technical Program Committee and the additional reviewers for their constructive and detailed reviews. A big "thank you" goes to Tom Pfeifer, our publications chair, who played a big part in creating these proceedings. Finally, we want to thank our patrons, Cisco Systems and France Telecom, whose financial support was essential to making DSOM 2007 a great event.

October 2007

Alexander Clemm
Lisandro Zambenedetti Granville
Rolf Stadler

# DSOM 2007 Organization

### Program Committee Co-chairs

| | |
|---|---|
| Alexander Clemm | Cisco, USA |
| Lisandro Zambenedetti Granville | Federal University of Rio Grande do Sul, Brazil |
| Rolf Stadler | Royal Institute of Technology (KTH), Sweden |

### Publication Chair

| | |
|---|---|
| Tom Pfeifer | Waterford Institute of Technology, Ireland |

### Publicity Chair

| | |
|---|---|
| Sumit Naiksatam | Cisco, USA |

### Treasurers

| | |
|---|---|
| Raouf Boutaba | University of Waterloo, Canada |
| Brendan Jennings | Waterford Institute of Technology, Ireland |

### Website and Registration Co-chairs

| | |
|---|---|
| Edgar Magana | UPC/Cisco, USA |
| Sven van der Meer | Waterford Institute of Technology, Ireland |

### Submission Chair

| | |
|---|---|
| Lisandro Zambenedetti Granville | Federal University of Rio Grande do Sul, Brazil |

### Manweek 2007 General Co-chairs

| | |
|---|---|
| Alexander Clemm | Cisco, USA |
| Silvia Figueira | Santa Clara University, USA |
| Masum Z. Hasan | Cisco, USA |

### Manweek 2007 Advisors

| | |
|---|---|
| Raouf Boutaba | University of Waterloo, Canada |
| Brendan Jennings | Waterford Institute of Technology, Ireland |
| Sven van der Meer | Waterford Institute of Technology, Ireland |

### DSOM 2007 Technical Program Committee

| | |
|---|---|
| Ehab Al-Shaer | DePaul University, USA |
| Javier Baliosian | University of the Republic, Uruguay |
| Claudio Bartolini | HP Laboratories, USA |
| Raouf Boutaba | University of Waterloo, Canada |
| Nevil Brownlee | University of Auckland, New Zealand |
| Marcus Brunner | NEC Europe Ltd., Germany |
| Mark Burgess | University College Oslo, Norway |
| Thierry Coupaye | France Telecom R&D, France |
| Yixin Diao | IBM Research, USA |
| Petre Dini | Cisco Systems, USA |
| Metin Feridun | IBM Research, USA |
| Olivier Festor | LORIA - INRIA, France |
| Alex Galis | University College London, UK |
| Luciano Paschoal Gaspary | Federal University of Rio Grande do Sul, Brazil |
| Kurt Geihs | University of Kassel, Germany |
| Yacine Ghamri-Doudane | LRSM - INSIIE, France |
| Masum Hasan | Cisco Systems, USA |
| Heinz-Gerd Hegering | Leibniz Supercomputing Center, Germany |
| Joseph Hellerstein | Microsoft, USA |
| James Hong | POSTECH, Korea |
| Cynthia Hood | Illinois Institute of Technology, USA |
| Brendan Jennings | Waterford Institute of Technology, Ireland |
| Alexander Keller | IBM Global Technology Services, USA |
| Yoshiaki Kiriha | NEC, Japan |
| David Lewis | Trinity College Dublin, Ireland |
| Hong Li | Intel, USA |
| Antonio Liotta | University of Essex, UK |
| Jorge López de Vergara | Universidad Autónoma de Madrid, Spain |
| Emil Lupu | Imperial College London, UK |
| Hanan Lutfiyya | University of Western Ontario, Canada |
| Jean-Philippe Martin-Flatin | NetExpert, Switzerland |
| Saverio Niccolini | NEC Europe Ltd., Germany |
| Jose Marcos Nogueira | Federal University of Minas Gerais, Brazil |
| Declan O'Sullivan | Trinity College Dublin, Ireland |
| George Pavlou | University of Surrey, UK |
| Aiko Pras | University of Twente, The Netherlands |
| Juergen Quittek | NEC Europe Ltd., Germany |
| Ammar Rayes | Cisco Systems, USA |
| Danny Raz | Technion, Israel |
| Gabi Dreo Rodosek | University of Federal Armed Forces Munich, Germany |
| Akhil Sahai | HP Laboratories, USA |
| Jürgen Schönwälder | Jacobs University Bremen, Germany |
| Joan Serrat | Universitat Politècnica de Catalunya, Spain |
| Adarsh Sethi | University of Delaware, USA |
| Radu State | LORIA - INRIA, France |

| | |
|---|---|
| Burkhard Stiller | University of Zurich and ETH Zurich, Switzerland |
| John Strassner | Motorola Labs, USA |
| Sven van der Meer | Waterford Institute of Technology, Ireland |
| John Vicente | Intel Corporation, USA |
| Vincent Wade | Trinity College Dublin, Ireland |
| Felix Wu | University of California at Davis, USA |
| Geoffrey Xie | Naval Postgraduate School, USA |
| Makoto Yoshida | The University of Tokyo, Japan |
| Xiaoyun Zhu | HP Laboratories, USA |

**DSOM 2007 Additional Paper Reviewers**

| | |
|---|---|
| Florence Agboma | University of Essex, UK |
| Khalid AlBadawi | DePaul University, USA |
| Mina Amin | University of Surrey, UK |
| Kamal Bhattacharya | IBM Research, USA |
| Steffen Bleul | University of Kassel, Germany |
| Pieter-Tjerk de Boer | University of Twente, The Netherlands |
| Aimilios Chourmouziadis | University of Surrey, UK |
| Alan Davy | Waterford Institute of Technology, Ireland |
| Steven Davy | Waterford Institute of Technology, Ireland |
| Walter M. Fuertes | Universidad Autónoma de Madrid, Spain |
| Tom Gardos | Intel Corporation, USA |
| Stylianos Georgoulas | University of Surrey, UK |
| José Alberto Hernández | Universidad Autónoma de Madrid, Spain |
| Mohammad Ullah Khan | University of Kassel, Germany |
| Ling Lin | University of Essex, UK |
| Xue Liu | HP Laboratories, USA |
| Henrik Lundqvist | NEC Europe Ltd., Germany |
| Maitreya Natu | University of Delaware, USA |
| Pradeep Padala | University of Michigan, USA |
| Roland Reichle | University of Kassel, Germany |
| Anna Sperotto | University of Twente, The Netherlands |
| Martin Stiemerling | NEC Europe Ltd., Germany |
| Yongning Tang | DePaul University, USA |
| Michael Wagner | University of Kassel, Germany |
| Zhikui Wang | HP Laboratories, USA |
| Yi Zhu | University of Essex, UK |

# Table of Contents

## Session 1: Decentralized and Peer-to-Peer Management

## Session 2: Fault Detection and Diagnosis

## Session 3: Performance Tuning and Dimensioning

## Session 4: Problem Detection and Mitigation

## Session 5: Operations and Tools

## Session 6: Short Papers

## Session 7: Service Accounting and Auditing

## Session 8: Web Services and Management

# Botnets for Scalable Management

Jérôme François, Radu State, and Olivier Festor

MADYNES - INRIA Lorraine, CNRS, Nancy-Université, France
{jerome.francois,radu.state,olivier.festor}@loria.fr

**Abstract.** With an increasing number of devices that must be managed, the scalability of network and service management is a real challenge. A similar challenge seems to be solved by botnets which are the major security threats in today's Internet where a botmaster can control several thousands of computers around the world. This is done although many hindernesses like firewalls, intrusion detection systems and other deployed security appliances to protect current networks. From a technical point of view, such an efficiency can be a benefit for network and service management. This paper describes a new management middleware based on botnets, evaluates its performances and shows its potential impact based on a parametric analytical model.

## 1 Introduction

Network and service management is an important component to assure the well functioning of a network. It is divided into five domains: fault management, configuration, accounting tasks, performance and security monitoring. However network management planes face several problems to be scalable. Authors of malware (bots, worms) already faced these challenges and some of their achievements are very surprising. There are cases, where one botmaster can control up to 400 000 bots [1]. It is thus natural to investigate if it is possible to use a botnet to perform management operations on a large scale infrastructure. This approach is somehow a time travel, since long time ago, among the first IRC (Internet Relay Chat) [2] bots, Eggdrop [3] was created not for hackers but for helping administrator of IRC networks. The main contribution of this paper is to propose a management plane based on a botnet model, evaluate its performance and show its feasibility. Our paper is structured as follows. In section 2, we introduce the malware communication system and its possible adaption for managing networks. In section 3, the mathematical model and the associated metrics are explained in details. The next section 4 highlights our first experimental results. Related works are presented in section 5. Finally, we conclude the paper and outline future works.

## 2 Malware-Based Management Architecture

### 2.1 Classical Management Architecture and Challenges

Network management solutions show their limits today due to several reasons. First of all, there are more and more hosts to be managed and the management

A. Clemm, L.Z. Granville, and R. Stadler (Eds.): DSOM 2007, LNCS 4785, pp. 1–12, 2007.

domains have no well delimited boundaries. The management domain is split on several sites and a lot of tasks are usually delegated to other companies which need to access to the network. Moreover, a management operation could be performed on different locations in different countries and has to pass through a lot of active equipments like firewalls or network address translators (not only under the responsibility of the company). For a comprehensive overview, please refer to [4]. The main challenges that we address are related to scalability.

### 2.2 Internet Worm and Malware Communication Paradigms

A worm primary goal is to infect multiple machines without being detected or countered. To reach this goal, the worm can exploit security holes and there are various ways to improve the infection rate. In [5], some existing mechanisms are listed. Malware contain generally malicious payload. The most dangerous malware are stealthy and are able to retrieve private information (password, credit card number...) or to get the control of a system in order to use it as a proxy for future malicious activities (spamming, distributed denial of service attacks, beginning a worm infection, password cracking...).

This kind of malware is based on a control mechanism as in figure 1. Once the bot software is installed on a computer, the bot connects itself to the botnet. This technique is able to bypass most of firewalls and network address translators related problems, since outgoing connections are used. If a firewall blocks outgoing traffic too, it should allow some traffic like web traffic. Thus the IRC server can use different ports to bypass this kind of firewalls.

### 2.3 Malware Based Management Framework

We consider that malware communication scheme can be a reliable middleware solution for network and service management [4]. Firstly, the exchange of commands is simple and multiple operations are possible. Moreover, the decentralized communication topology of these networks allows to manage many bots. In [1] some statistics about botnets show that controlling 400 000 bots is possible contrary to the current management framework. In [6], the authors model and evaluate distributed management approaches and the main result is that a botnet management architecture is scalable.

IRC is one communication channel used to control a botnet as in the figure 1. A user wanting to chat connects to a server and chooses a chat channel. Many users can be connected simultaneously to the same channel due to the architecture of an IRC network. In fact, several servers are interconnected and share the different channels conceptually equivalent to a multicast group. Thus all the participants are not connected to the same server and this decentralized architecture avoids server overloading. The quantity of messages is well adapted because they are often sent to the channel. The servers form a spanning tree. In a botnet, the master is connected to one server and sends the orders on a channel, the bots are connected to any servers in the network and get the orders through the chat channel. The responses can be sent to the master in the same way also.

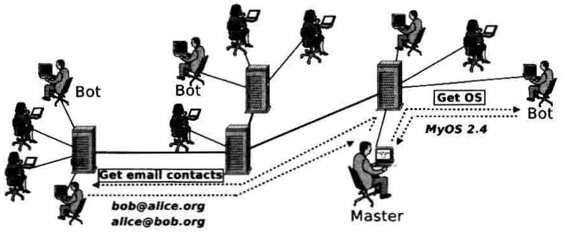

**Fig. 1.** An IRC botnet

These previous facts are the motivation to build a management system based on an IRC botnet where an administrator requests management operations through an IRC network. However an administrator need a proof of the real efficiency and benefits of this system before deploying it. In this study, our goal is to model IRC botnet and evaluate this approach from a network management point of view by asking several questions like:

- what is the probability to reach 80% of the hosts ?
- how many servers I need to deploy ?
- how should the servers be connected ?
- how much time is needed to reach 75% of hosts ?
- what is the server load ?

Since this new management framework is based on botnet, deploying some IRC servers is needed which is not necessary with a typical centralized management solution. In all cases, the devices to be managed have to execute a specific software: an agent for a typical solution or a modfied IRC client in our case.

## 3 An IRC Botnet Mathematical Model

Although IRC based botnets proved their efficiency in practice, little is known related to their analytical performance. The tree of servers is the main component of an IRC architecture. Thus our model is based on interconnected nodes (the servers) within a tree. We assume two kinds of failure. The first is due to the overloading of a server. The second introduces the risk to be attacked. In this case, a node or a server can be discovered by an attacker and we consider that once one node is discovered, all the system is unreliable because the attacker is able to use this server to compromise and command all the servers and bots.

The bots connected on the servers are not yet considered. The branching factor parameter $m$ is the maximum number of adjacent links for every nodes in the network. The number of adjacent links has to be between 1 and m and the probability function is equiprobable.

The overloading factor $\alpha(m)$ models the fact that the more a server can have connections with others, the more possible the server can be crashed due to needed operations to maintain the connectivity and synchronize the messages