e-Business and Telecommunication Networks

e-Business and Telecommunication Networks

edited by

João Ascenso

ISEL,
Lisbon, Portugal

Luminita Vasiu

University of Westminster,
London, UK

Carlos Belo

IST/IT,
Lisbon, Portugal

and

Mónica Saramago

INSTICC,
Setúbal, Portugal

Springer

A C.I.P. Catalogue record for this book is available from the Library of Congress.

ISBN-10 1-4020-4760-6 (HB)
ISBN-13 978-1-4020-4760-2 (HB)
ISBN-10 1-4020-4761-4 (e-book)
ISBN-13 978-1-4020-4761-9 (e-book)

Published by Springer,
P.O. Box 17, 3300 AA Dordrecht, The Netherlands.

www.springer.com

Printed on acid-free paper

Printed in the Netherlands

TABLE OF CONTENTS

INVITED SPEAKERS

PART 1 – GLOBAL COMMUNICATION INFORMATION SYSTEMS AND SERVICES

PART 2 – SECURITY AND RELIABILITY IN INFORMATION SYSTEMS AND NETWORKS

PART 3 – WIRELESS COMMUNICATION SYSTEMS AND NETWORKS

PART 4 – MULTIMEDIA SIGNAL PROCESSING

PREFACE

This book contains the best papers of the First International Conference on E-business and Telecommunication Networks (ICETE 2004), held in Setúbal (Portugal) and organized by INSTICC (*Institute for Systems and Technologies of Information, Communication and Control*) in collaboration with the School of Business of the Polytechnic Institute of Setúbal, who hosted the event.

This conference represents a major initiative to increase the technical exchanges among professionals, who work on the e-Business and Telecommunication Networks fields, and who are deploying new services and technologies into the lives of ordinary consumers. The major goal of this conference is to bring together researchers and developers from academia and industry working in areas related to e-business, with a special focus on Telecommunication Networks. This year, four simultaneous tracks were held, covering different aspects, including: "*Global Communication Information Systems and Services*", "*Security and Reliability in Information Systems and Networks*", "*Wireless Communication Systems and Networks*" and "*Multimedia Signal Processing*". The sections of this book reflect the conference tracks.

ICETE 2004 received 202 paper submissions from 43 different countries, from all continents. 110 papers were published and orally presented as full papers, i.e. completed work, and 44 papers were accepted for poster presentation. The full paper acceptance ratio confirms our confidence that ICETE 2004 has achieved a high quality standard that we will strive to keep and enhance in order to ensure the success of the next year ICETE edition.

Additionally, the ICETE conference included a number of invited talks, including keynote lectures and technical tutorials. These special presentations made by internationally recognized experts have definitely increased the overall quality of the Conference and provided a deeper understanding of the Telecommunication Networks field. Their contributions have been included in a special section of this book.

The program for this conference required the dedicated effort of many people. Firstly, we must thank the authors, whose research and development efforts are recorded here. Secondly, we thank the members of the program committee and the additional reviewers for their diligence and expert reviewing. Thirdly, we thank the invited speakers for their invaluable contribution and for taking the time to synthesise and prepare their talks. Finally, we thank the workshop chairs whose collaboration with ICETE was much appreciated.

João Ascenso
School of Technology of Setúbal, IPS,
Setúbal, Portugal

Luminita Vasiu
Middlesex University, WITRC, London,
U.K.

Joaquim Filipe
School of Technology of Setúbal and
INSTICC, Setúbal, Portugal

Carlos Belo
Institute of Telecommunications and IST,
Lisbon, Portugal

CONFERENCE COMMITTEE

Conference Chair
Joaquim Filipe, Escola Superior de Tecnologia de Setúbal, Portugal

Programme co-Chairs
Carlos Belo, Instituto de Telecomunicações, Portugal
Luminita Vasiu, Middlesex University, U.K.

Program Committee Chair
João Ascenso, Escola Superior de Tecnologia de Setúbal, Portugal

Secretariat
Mónica Saramago, INSTICC, Portugal

Programme Committee:
Acharya, A. (USA)
Ahmed, K. (THAILAND)
Al-Sharhan, S. (KUWAIT)
Ansari, N. (USA)
Asatani, K. (JAPAN)
Assuncão, P. (PORTUGAL)
Barn, B. (UK)
Bedford, A. (AUSTRALIA)
Bella, G. (ITALY)
Benzekri, A. (FRANCE)
Boavida, F. (PORTUGAL)
Bonyuet, D. (USA)
Boutaba, R. (CANADA)
Broadfoot, P. (UK)
Cappellini, V. (ITALY)
Cheng, T. (SINGAPORE)
Cheung, K. (CHINA)
Choras, R. (POLAND)
Clarke, R. (UK)
Cohen, R. (ISRAEL)
Comley, R. (UK)
Constantinides, T. (UK)
Correia, M. (PORTUGAL)
Correia, P. (PORTUGAL)
Devetsikiotis, M. (USA)
Elmirghani, J. (UK)
Fang, Y. (USA)
Faria, S. (PORTUGAL)
Figueiredo, M. (PORTUGAL)
Gaspary, L. (BRAZIL)
Georghiades, C. (USA)
Giannakis, G. (GREECE)
Goldszmidt, G. (USA)
Goulart, C. (BRAZIL)
Granai, L. (SWITZERLAND)
Granville, L. (BRAZIL)
Greaves, D. (UK)
Gritzalis, S. (GREECE)
Kang, C. (KOREA)
Hamdi, M. (CHINA)
Hanzo, L. (UK)
Harris, R. (AUSTRALIA)
Helal, S. (USA)
Hoang, N. (SINGAPORE)
Hong, D. (KOREA)
Hu, J. (AUSTRALIA)
Huston, G. (AUSTRALIA)
Isaías, P. (PORTUGAL)
Jagodic, M. (SLOVENIA)
Jahankhani, H. (UK)
Jain, A. (INDIA)
Jefferies, N. (UK)
Júnior, E. (BRAZIL)
Kahlil, I. (AUSTRALIA)

Karmouch, A. (CANADA)
Kihl, M. (SWEDEN)
Kollias, S. (GREECE)
Kos, M. (CROATIA)
Kunt, M. (SWITZERLAND)
Kuo, G. S. (TAIWAN)
Landfeldt, B. (AUSTRALIA)
Lee, M. (AUSTRIA)
Lewis, L. (USA)
Liu, K. (UK)
Lloyd-Smith, B. (AUSTRALIA)
Lorna, U. (UK)
Loureiro, A. (BRAZIL)
Lu, S. (USA)
Magedanz, T. (GERMANY)
Magli, E. (ITALY)
Mahmoud, Q. (CANADA)
Makki, K. (USA)
Malek, M. (USA)
Malumbres, M. (SPAIN)
Man, H. (USA)
Marshall, A. (UK)
Marshall, I. (UK)
Mascolo, S. (ITALY)
Matsuura, K. (JAPAN)
McGrath, S. (IRELAND)
Merabti, M. (UK)
Mirmehdi, M. (UK)
Morikawa, H. (JAPAN)
Navarro, A. (PORTUGAL)
Nordholm, S. (AUSTRALIA)
Obaidat, M. (USA)
Ohtsuki, T. (JAPAN)
Osadciw, L. (EUA)
Pach, A. (POLAND)
Perkis, A. (NORWAY)
Petrizzelli, M. (VENEZUELA)
Pigneur, Y. (SWITZERLAND)
Pinnes, E. (USA)
Pitsillides, A. (CYPRUS)
Plagemann, T. (NORWAY)
Podvalny, S. (RUSSIA)
Preston, D. (UK)
Queluz, P. (PORTUGAL)
Ramadass, S. (MALAYSIA)
Raychaudhuri, D. (USA)
Regazzoni, C. (ITALY)
Reichl, P. (AUSTRIA)
Reis, L. (PORTUGAL)
Rodrigues, A. (PORTUGAL)
Rosales, C. (MEXICO)
Roth, J. (GERMANY)
Roztocki, N. (USA)
Sanadidi, M. (USA)
Schulze, B. (BRAZIL)
Sericola, B. (FRANCE)
Skarbek, W. (POLAND)
Specialski, E. (BRAZIL)
Steinmetz, R. (GERMANY)
Suda, T. (USA)
Sun, L. (UK)
Sure, Y. (GERMANY)
Tarouco, L. (BRAZIL)
Tirri, H. (FINLAND)
Toh, C. K. (USA)
Ultes-Nitsche, U. (SWITZERLAND)
Valadas, R. (PORTUGAL)
Vidal, A. (SPAIN)
Waldron, J. (IRELAND)
Weghorn, H. (GERMANY)
Weigel, R. (GERMANY)
Wilde, E. (SWITZERLAND)
Wilson, S. (USA)
Wu, G. (USA)
Wu, W. X. (UK)
Yasinsac, A. (EUA)
Yeo, B. (SINGAPORE)
Yin, Q. (SINGAPORE)
Youn, H. (KOREA)
Yu, W. (USA)
Yuan, S. (TAIWAN)
Zhang, J. (USA)

Invited Speakers

Luminita Vasiu, Middlesex University, U.K.
Manu Malek, Institute if Technology, USA
Henry Tirri, Nokia Research Fellow/Nokia Research Center, Finland
Nirwan Ansari, New Jersey Institute of Technology, USA
Mohamed Atiquzzam, Uiversity of Oklahoma, USA

Invited Speakers

DATA MINING TECHNIQUES FOR SECURITY OF WEB SERVICES

Manu Malek and Fotios Harmantzis
Steven Institute of Technology, Castle Point on the Hudson, Hoboken, NJ 07030, USA
Email: {mmalek, fharmant}@stevens.edu

Keywords: Security services, Security attack, Denial of service, Intrusion detection, Security safeguards.

Abstract: The Internet, while being increasingly used to provide services efficiently, poses a unique set of security issues due to its openness and ubiquity. We highlight the importance of security in web services and describe how data mining techniques can offer help. The anatomy of a specific security attack is described. We then survey some security intrusions detection techniques based on data mining and point out their shortcomings. Then we provide some novel data mining techniques to detect such attacks, and describe some safeguard against these attacks.

1 INTRODUCTION

Cyberspace is used extensively for commerce. For years banks and other financial organizations have conducted transactions over the Internet using various geographically dispersed computer systems. Businesses that accept transactions via the Internet can gain a competitive edge by reaching a worldwide customer base at relatively low cost. But the Internet poses a unique set of security issues due to its openness and ubiquity. Indeed, security is recognized as a critical issue in Information Technology today. Customers will submit information via the Web/ Internet only if they are confident that their private information, such as credit card numbers, is secure. Therefore, today's Web/Internet-based services must include solutions that provide security as a primary component in their design and deployment.

Web services generally refer to web-based applications that make it possible for enterprises to do transactions on the web and for users to share documents and information with each other over the Web. The standard that makes it possible to describe the communications in some structured way is Web Services Definition Language (WSDL). WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information (http://www.w3.org/TR/wsdl).

But openness and integration have their price. Without adequate security protections and effective security management, these features can be used to attack the availability and integrity of information systems and the networks connecting to them. Here we highlight a few typical ways an attacker may gain illegal access to an information system, or to make it unavailable to legitimate users. We identify the profiles or signatures for the sequence of actions an attacker may perform to perpetrate such attacks. We use data mining techniques to discover such attack profiles to detect the attacks.

Data mining refers to a technique to intelligently and automatically assist humans in analyzing the large volumes of data to identify valid, novel, and potentially useful patterns in data. It offers great promise in helping organizations uncover patterns hidden in their data that can be used to predict the behavior of customers, so that they can better plan products and processes. Data mining takes advantage of advances in the fields of artificial intelligence (AI) and statistics. Both disciplines help in pattern recognition and classification. Other disciplines used in data mining include rule-based and case-based reasoning, fuzzy logic, and neural networks. The techniques used in data mining include rule induction, clustering, projection, and visualization (e.g., see (Berry, M. and L. Gordon, 1997) for details).

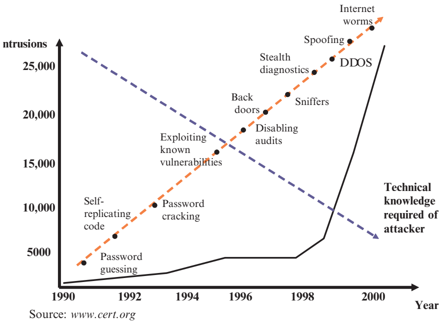
J. Ascenso et al. (eds.), e-Business and Telecommunication Networks, 3–10.

This paper provides a glimpse at the cyberspace security situation, and offers some techniques to manage the security of web services. The paper describes some security attacks, and provides some techniques to detect and defend against them. In Section 2, we present some statistics related to security attacks to highlight the urgency of the issue. Some typical security vulnerabilities and attacks are discussed in Section 3. In Section 4, we provide a survey of data mining applications in intrusion detection and point out their shortcomings. We then define attack signatures and outline how to use them in conjunction with data mining techniques for efficient intrusion detection. Section 5 summarizes the paper.

2 BACKGROUND

Based on data provided by CERT/CC, the number of incidents and vulnerabilities for cyber attacks have increased exponentially during the period 1998 to 2002 (CERT/CC). Figure 1 shows that intrusions were relatively few in the early1990s, but there has been a major increase since 2000. About 25,000 intrusions were reported in the Year 2000 (CERT/CC). Keep in mind that not all enterprises that suffer security breaches report them. The line moving upward in this figure shows various types of threats, starting with very simple ones in the early '90s, like password guessing. The sophistication of attacks increased with self-replicating codes, such as viruses, then password cracking (where the cryptographic password is broken), and on to the more sophisticated threats shown. Against this rising sophistication in threats, we have easy availability of hacking tools: hackers no longer have to be experts in computer science or security; they could use available tools. For example, a tool such as nmap (www.insecure.org/nmap/nmap-fingerprinting-aticle.html) can be used to find all the open ports, a first stage in an attack. This combination of decreasing knowledge required of the attackers and the increasing sophistication of the attacks is giving rise to major security concerns.

According to the Federal Computer Incidence Response Center (FedCIRC), the incident handling entity for the federal government, 130,000 government sites totaling more than one million hosts were attacked in 1998 (NIST ITL Bulletin, 1999). Also, a 1999 survey conducted by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) revealed that 57% of organizations cited their Internet connections as a frequent point of attack, 30% detected actual network intrusion, and 26% reported theft of proprietary information (CSI, 2002). A similar survey in 2002, showed that 90% of the 507 participating organizations detected computer security breaches within the past 12 months, 74% cited their Internet connections as a frequent point of attack, but only 34% reported security intrusions to law enforcement agencies. These numbers must be considered observing that they relate to only known attacks and vulnerabilities. However, they do indicate the magnitude of the problem.



Source: *www.cert.org*

Figure 1: Security vulnerabilities and threats.

A key to preventing security attacks is to understand and identify vulnerabilities, and to take corrective action. A threat to computing systems or communication network is a potential violation of security unauthorized, illegitimate, malicious or fraudulent purposes. An attack is the implementation of a threat using the system vulnerabilities. Vulnerability is a weakness in the security system that might be exploited to launch an attack. Finally, a control is a protective measure – an action, device, procedure, or technique – that reduces vulnerabilities.

Table 1 sows the top 10 security vulnerabilities as reported periodically by The SANS Institute (The SANS Institute, 2003). The reasons for the existence of these vulnerabilities include: buggy software design and development, system administrators being too busy to install security patches in a timely manner, and inadequate policies and procedures. Another factor is that due to the ubiquity of the Internet, vulnerabilities are quickly and widely published.

Table 1: Top 10 security vulnerabilities (The SANS Institute, 2003).

Vulnerabilities of Windows Systems	***Vulnerabilities of Unix Systems***
1. Internet Information Services (IIS) *2. Microsoft Data Access Components (MDAC)– Remote Data Services* *3. Microsoft SQL Server* *4. NETBIOS – Unprotected Windows Networking Shares* *5. Anonymous Logon – Null Sessions* *6. LAN Manager Authentication – Weak LM Hashing* *7. General Windows Authentication – Accounts with No Passwords or Weak Passwords* *8. Internet Explorer* *9. Remote Registry Access* *10. Windows Scripting Host*	*1. Remote Procedure Calls (RPC)* *2. Apache Web Server* *3. Secure Shell (SSH)* *4. Simple Network Management Protocol (SNMP)* *5. File Transfer Protocol (FTP)* *6. R-Services – Trust Relationships* *7. Line Printer Daemon (LPD)* *8. Sendmail* *9. BIND/DNS* *10. General Unix Authentication – Accounts with No Passwords or Weak Passwords*

The motive of attackers could be anything from pure joy of hacking to financial benefit. The attackers are either highly technically capable, or they sometimes breaks into the network by trial and error. Disgruntled employees have more access rights to enterprise computer networks compared to outside attackers. According to the CSI/FBI 2002 Survey (CSI, 2002), 60% of attacks in the US were inside attacks (attacks that originated inside the institutions) and 40% were outside attacks.

3 SOME TYPICAL SECURITY ATTACKS

As mentioned, a security attack occurs when an attacker takes advantage of one or more security vulnerabilities. To improve security, one needs to minimize security vulnerabilities. In this section we present some typical security attacks, point out the vulnerabilities abused to perpetrate the attacks. Some safeguards against these attacks will be described in the next section. An attack that we deal with specifically in this section and in Section 4 is the HTTP GET attack.

3.1 Denial-of-Service Attack

In a Denial-of-Service (DoS) attack, the attacker attempts to use up all the victim system's resources like memory or bandwidth. When the attack is successful, legitimate users can no longer access the resources and the services offered by the server will be shut down. According to the 2002 CSI/FBI survey (CSI, 2002), 40% of all attacks are DoS attacks.

An attack can be directed at an operating system or at the network. The attacker may send specially crafted packets that crash remote software/services running on the victim server. It will be successful if the network is unable to distinguish between legitimate traffic and malicious or bogus traffic. Some common DoS attacks follow.

ICMP Flooding and Smurf Attack

These are both ICMP-based attacks. Flooding with ICMP packets slows down the victim server so that it can no longer respond quickly enough for the services to work properly. If packets are sent with forged IP addresses, the victim server not only has to allocate system resources to receive, but to reply to packets to addresses which do not exist. The Smurf attack uses a similar idea: the attacking machine sends Echo requests with broadcast IP addresses, thus not only the victim server but the attached network will be flooded by a large amount of ICMP traffic.

SYN Flooding

SYN flooding exploits the weakness of the TCP Three-way Handshake (Comer, D., 2000). In a normal TCP connection request, the source sends a SYN (synchronization) packet to the destination to initiate the connection; then waits for a SYN ACK (synchronization acknowledged) packet from the destination. The connection is established when the destination receives a FIN ACK (finishing acknowledged) packet from the source. In the SYN flooding attack, the attacker sends a large number of SYN packets, often from bogus IP addresses, to the victim server, which adds the entry to the connection queue and replies with SYN ACKs. As the source addresses are incorrect or non-existent, FIN ACKs will never be received by the victim server, so the last part of the Three-way Handshake never completes and the connection queue of the victim server fills up.

Badly-formed Packets

In this type of attack, the attacker sends badly-formed IP packets, e.g., packets that consist of invalid fragments, protocol, packet size, or header values, to the victim server. Once the destination TCP stack receives such invalid packets, the operating system must allocate resources to handle them. If the operating system cannot handle the misbehavior, it will crash. An example of this is the Ping-of-Death attack (www.insecure.org/sploits/ping-o-death.html) which causes buffer overflow in the operating system. In this attack, the attacker sends a larger than standard ICMP (Internet Control Message Protocol) packet, such as a ping, in fragments to the target server. Since the allowed maximum size of such a packet is 65,535 bytes, the server allows a corresponding buffer space to collect the fragments. A clever attacker may create a ping with many fragments destined to a target server. The server receives the fragments and starts to reassemble them. When reassembled, the buffer will overflow, leading to program termination, overwriting other data or executable code, kernel dump, etc. More than 50% of attacks on servers are due to buffer overflow (CERT/CC).

Distributed Denial of Service Attack

With the speed and power of computing resources today, an attacker may not be able to simply use one computer to craft a DoS attack. In the Distributed Denial of Service (DDoS) attack, many computers may be hijacked by the attacker as agents (zombies) to simultaneously flood a victim system's resources. A typical way to recruit zombie computers is for the perpetrator to send viruses to multiple computers, or to break into computer systems and load them with DDoS programs. Each infected system then finds other vulnerable systems and loads them with the programs, etc. The perpetrator uses the first system that was overtaken to instruct all the other compromised systems to launch the attack simultaneously.

3.2 HTTP GET Attack

For many web applications, a client should be able to send information to the server. HTML 2.0 and later versions support the Form element within an HTML document to allow data to be sent to web servers (www.w3c.org). One of the attributes of Form is Method which indicates how data is submitted to the web server. Valid choices for the Method attribute are GET and POST. In METHOD = GET the values inputted by the user are concatenated with the URL, separated by a special character (usually ?) fields are separated by &; space is represented by + For example, the following URL: http://www.gadgets,com?customer **= John + Doe** & address = **101 + Main + Street** & cardno = **1234567890** & cc =; **visacard** indicates that the customer's name and address with the customer's credit card number are to be sent to the web server at www.gadgets.com A savvy user (attacker) may be able to use this feature to get access to proprietary information if appropriate security mechanisms are not in place. The following scenario, adopted from Ref. (McClure, S. et al., 2003), is an HTTP GET attack on a typical web server which has some vulnerabilities.

The server http://www.acme.com runs Apache 1.3.12 on a Linux operating system. Firewalls prevent all but HTTP traffic via ports 80 (HTTP default port) and 443 (SSL port). Perl CGI scripts are used for the online store. A visitor to this site first begins browsing through the www.acme.com site, viewing the site's main page and a few images on it. The visitor notices that for the last selection (viewing the picture of a sunset), the URL in the browser window shows: http://www.acme.com/index.cgi?page=sunset.html. Following this pattern, the visitor (now attacker) issues a request for index.cg by typing the following URL: http://www.acme.com/index.cgi?page=index.cgi

Now, if the program does not validate the parameters passed to the index.cgi script, the filename passed as a parameter from the URL is captured by the CGI script, appended to the absolute path, and causes to open the index.cgi script as requested. Consequently, the browser display shows the source code of the index.cgi script!

At this point the attacker realizes that this technique can be further exploited to retrieve arbitrary files from the server. So the attacker may send the following request through the browser: http://www.acme.com/index.cgi?page=/../../etc/passwd

If permissions are not set properly on the /etc/passwd file, its contents will be displayed by the browser, providing the attacker with user's password information. The attacker could now execute arbitrary commands on the server, for example, by sending http://www.acme.com/index.cgi?page=|ls+-la/%0aid%0awhich+xterm| (% plus the hex characer

0a indicates line feed) requesting ls –al (to show a file list of the server's root directory) id (the effective user id of the process running index.cgi) which xterm (path to the xterm binary code, to gain interactive shell access to the server and the attacker could gain full interactive shell-level access to the web server.

Note again that the vulnerabilities: the program does not validate the parameters passed to the index.cgi script, and permissions are not set properly on the /etc/passwd file.

4 DATA MINING TECHNIQUES FOR INTRUSION DETECTION

In this section we review server logs, introduce attack signatures, and present our main contribution: how security attack signatures are used in conjunction with data mining to detect security intrusions. More specifically, we first describe the relevance and importance of the different log files that are available; we then define specific patterns in the log files for an attack (the individual log records as well as their sequence/order) as the attack signature; and use data mining to search and find such patters for attack detection. The efficiency and speed of the overall process can even lead to attack prediction capabilities.

4.1 Logs

Every visit to a Web site by a user creates a record of what happens during that session in the server's log. A busy site may generate thousands of log entries per hour, compiled in various log files. A log file entry contains items like the IP address of the computer requesting the Web page, the date and time of the request, the name and the size of the file requested. Logs vary by the type of server and the file format. Following are some typical logs and what they record:

- Access Log records every transaction between server and browsers (date, time, domain name or IP address, size of transaction, …).
- Referrer Log records the visitor's path to the site (the initial URL from which the visitor came).
- Agent Log records the type and version of the browser.

For secure systems, the standard logs and directories may not be sufficient and one must employ additional logging tools, e.g., information about which computer is connecting to which services on the system. There are many programs under the heading of IP loggers available for this purpose, e.g., EnviroMon (http://www.interwld.com/pico/subs/pico_Environ_IP_Logging.htm) and ippl http://packages.debian.org/unstable/net/ippl.html).

4.2 Mining Logs

The data available in log files can be "mined" to gain useful information. Data mining offers promise in uncovering hidden patterns in the data that can be used to predict the behavior of (malicious) users. Using data mining in intrusion detection is a relatively new concept. In (Lee, W. and Stolfo, S. J., 1998), the authors outline a data mining framework for constructing intrusion detection models. The central idea is to utilize auditing programs to extract an extensive set of features that describe each network connection or host session, and apply data mining to learn rules that capture the behavior of intrusions and normal activities. Detection models for new intrusions are incorporated into an Intrusion Detection Systems (IDS) through a meta-learning (or co-operative) learning process. The strength of this approach is in classification, meta-learning, and association rules.

In (Almgren, M. et al., 2000), the authors present an intrusion detection tool aimed at protecting servers. However, their method does not effectively handle all matches of the signature (e.g., of the 404 type: document not found). Attacks that have no matching signature and are sent by a previously unknown host may be missed.

Ref. (Forrest, S. et al., 1996 represents a first attempt to analyze sequences of system calls issued by a process for intrusion detection. The authors introduce a method based on sequences of Unix system calls at the process level for anomaly detection resulting in intrusion detection. They address sendmail, lpr, and ftpd processes and obtain some good results in terms of false-positives. Ref. (Hofmeyr, S.A., 1998) also uses sequences of system calls for intrusion detection. The authors choose to monitor behaviour at the level of privileged processes. Their proposed approach of detecting irregularities in the behavior of privileged programs is to regard the program as a black-box, which, when it runs, emits some observable behavior. Privileged processes are trusted to access only relevant system resources, but in cases where there is a programming error in the code that the privileged process is running, or if the privileged process is incorrectly configured, an ordinary user may be able to gain super-user privileges by exploiting the problem in the process. The system-call method, however, is specific to processes and cannot detect generic intrusion attempts, e.g., race condition attacks, session hijacking(when one user masquerades as another), and cases in which a user violates policy without using privileged processes.

Artificial intelligence techniques have also been applied to help in decision making for intrusion detection. In (Frank, J., 1994), the author presents a survey of such methods and provides an example of using feature selection to improve the classification of network connections. In (Liu, Z. et al., 2002), the authors present a comparison of some neural-network-based method and offer some "classifiers" for anomaly detection in Unix processes. All the techniques based on artificial intelligence, however, suffer from lack of scalability: they work only for small size networks and data sizes.

4.3 Attack Signatures

We use attack signatures in combination with data mining to not only detect, but predict attacks. An attack signature encapsulates the way an attacker would navigate through the resources and the actions the attacker would take. For example, in a denial-of-service attack, the attacker may send a large number of almost simultaneous TCP connect requests from one or more IP addresses without responding to server acknowledgements.

To illustrate a specific attack signature, let us look at the log lines stored by the web server in the HTTP GET attack example described in the previous section. The log line in the Access Log corresponding to the visitor's (attacker's) first attempt is

A. 10.0.1.21 – [31/Oct/2001:03:02:47] "GET/HTTP/1.0" 200 3008 where 10.0.1.21 is the visitor's IP address, followed by date and time of visit, the Method and the Protocol used. The number 200 indicates the "normal" code, and 3008 indicates the byte size of the file retrieved. The following log line corresponds to the visitor's selection of the sunset picture:

B. 10.0.1.21 – [31/Oct/2001:03:03:18] "GET/sunset.jpg HTTP/1.0" 200 36580 and the following log line corresponds to the visitor's first attempt at surveillance of the site (issuing a request for index.cgi):

C. 10.0.1.21 – [31/Oct/2001:03:05:31] "GET/index.cgi?page= index.cgi HTTP/1.0" 200 358 The following log lines correspond to the visitor (by now, attacker) attempting to open supposedly secure files:

D. 10.0.1.21 – [31/Oct/2001:03:06:21] "GET/index.cgi?page=/../../etc/passwd HTTP/1.0" 200 723

E. 10.0.1.21 – [31/Oct/2001:03:07:01] "GET/ index.cgi?page=|ls+-la+/%0aid%0awhich+xterm|HTTP/1.0" 200 1228

This pattern of log lines from the same source IP address can be recognized as a signature of an HTTP GET attack. In the above example, the sequence of log lines A-B-C-D-E, A-C-D-E, B-C-D-E, or C-D-E constitutes the signature of this HTTP GET attack. Even some individual log lines from a source IP address could provide tell-tale signs of an impending HTTP GET attack. For example, the existence of a "pipe" (i.e.,) in the URL, as in log line E above, would indicate that the user is possibly trying to execute operating system commands.

In our research, we try to establish signatures for various types of attacks. Note the importance of good comprehensive attack signatures in detecting attacks. Incomplete signatures result in false-positive or false-negative detection. Another point is the use of data mining to detect attack signatures. One can imagine the tremendous amount of data collected by web services, resulting in multi-tera-byte databases. With such large amounts of data to analyze, data mining could become quite computationally expensive. Therefore, efficiency becomes a major issue. Currently, we are continuing our efforts to identify ways data should be efficiently analyzed in order to provide accurate and effective results.

In our research, we use the Rule Induction Kit (RIK) and Enterprise Data-Miner (EDM) tools (http://www.data-miner.com) to detect and mine attack signatures. The RIK package discovers highly compact decision rules from data, while the EDM software kits implement the data-mining techniques presented in (Weiss, S. and Indurkhya, N., 1997) and includes programs for (a) data preparation (b) data reduction or sampling, and (c) prediction. Our selection of this tool package was based on criteria related to efficiency (speed, especially when it comes to large amounts of data, as is the case with log files), and portability (multiple platforms), as well as extensibility (where the user can compose new methods with the existing building blocks).

Based on this software platform, we are able to create a sophisticated data mining methodology for efficient intrusion detection.

4.4 Security Safeguards

Safeguards are applied to reduce security risk to an acceptable/desirable level. They may be Proactive to prevent security incidents, or Reactive, to protect information when an incidence is detected. In either case, they must be cost effective, difficult to bypass, and with minimal impact on operations. Examples of safeguards are: avoidance (keeping security incidents from occurring, e.g., by removing vulnerabilities), limiting access (e.g., by reducing the number of entry points where attacks may originate), transference (shifting risk to someone else, e.g., via insurance or outsourcing), and mitigation (minimizing the impact of an incidence, e.g., by reducing its scope or improving detection).

One of the major safeguards is to detect and reduce/remove vulnerabilities. The main reasons for existing vulnerabilities are buggy software design and development, or system administration problems. Existence of bugs in software are due to

- programming for security not being generally taught,
- good software engineering processes not being universal, as well as
- existence of legacy code.

The system administration problems are due to inadequate policies and procedures, or the system administrators being too busy with many machines to administer, too many platforms and applications to support, and too many updates and patches to apply.

For the attack examples given in the previous section, we can offer some rather simple safeguards. For attacks that are based on making multiple requests and ignoring the server acknowledgments, such as ICMP Flood and Smurf Attack, and SYN Flooding, one could employ a timer: if the response does not arrive within a reasonable time, the request could be dropped and the resources freed. For attacks that are based on buffer overflow, one could use operating systems written in "safe" languages that perform range checking (like Java). The HTTP GET attack could be prevented by making sure that programs validate the parameters passed to them, and that file permissions are set properly.

5 CONCLUSIONS

We have first set the stage emphasizing the magnitude of the security problem, raising awareness and focusing on the impact of security. We have detailed two attacks: Denial of Service and the HTTP GET attack, and defined the signature of the latter. The application of data mining techniques for detecting attacks was described. The novelty of our approach is in determining the relevance/importance of different log records, defining intelligent signatures, and using efficient data mining techniques. Preliminary results have been encouraging.

There is significant work still to be done, e.g., improving the effectiveness of attack signatures, developing distributed algorithms for detection/ prediction, and improving the efficiency of pattern searching. We are currently working on these issues.

REFERENCES

http://www.w3.org/TR/wsdl

Michael J. A. Berry and Gordon Linoff, Data Mining Techniques, Wiley Computer Publishing, 1997

Computer Emergency Response Team/Coordination Center (CERT/CC) at Carnegie Mellon University's Software Engineering Institute, http://www.cert.org/

www.insecure.org/nmap/nmap-fingerprinting-article.html

NIST ITL Bulletin, "Computer attacks: what they are and how to defend against them," May 1999.

CSI, "2002 CSI/FBI Computer Crime and Security Survey," http://www.gocsi.com/.

The SANS Institute (http://www.sans.org/top20/), May 2003

Douglas Comer, Internetworking with TCP/IP Vol. 1: Principles, Protocols, and Architecture (4th Edition), Prentice Hall, 2000

www.insecure.org/sploits/ping-o-death.html

www.w3c.org?

S. McClure, S. Shah, and S. Shah, Web Hacking: Attacks and Defenses, Addison Wesley, 2003

http://www.interwld.com/pico/subs/pico_Environ_IP_Logging.htm

http://packages.debian.org/unstable/net/ippl.html

W. Lee and S. J. Stolfo, "Data Mining Approaches for Intrusion Detection," Usenix Security Symposium, San Antonio, Texas, July 1998

Jeremy Frank, “Artificial Intelligence and Intrusion Detection: Current and Future Directions,” June 1994 (http://citeseer.nj.nec.com/frank94artificial.html)

Zhen Liu, German Florez, and Susan Bridges, “A Comparison of Input Representation in Neural Networks: A Case Study in Intrusion Detection,” Proc. International Joint Conference on Neural Networks, May 12-17, 2002, Honolulu, Hawaii. http://www.data-miner.com

S. Weiss and N. Indurkhya, Predictive Data Mining: A Practical Guide, Morgan Kaufmann, 1997.

Magnus Almgren, Herve Deba, and Marc Dacier, “A Lightweight Tool for Detecting Web Server Attacks,” http://www.ce.chalmers.se/~almgren/Publications/almgren-ndss00.pdf

S. Forrest, S. A. Hofmeyr, A. Somayaji, and T. A. Longstaff, “A Sense of Self for Unix Processes,” Proc. 1996 IEEE Symp. Security and Privacy, Los Alamitos, CA, pp. 120-128, 1996

S. A. Hofmeyr, A. Somayaji, and S. Forrest, “Intrusion Detection using Sequences of System Calls,” Journal of Computer Security Vol. 6, pp. 151-180, 1998.

TOWARDS AN ALTERNATIVE WAY OF VERIFYING PROXY OBJECTS IN JINI

Nikolaos Papamichail and Luminita Vasiu
School of Computer Science, Middlesex University, London, UK
Email: n.papamichail@mdx.ac.uk, l.vasiu@mdx.ac.uk

Keywords: Jini Security, Proxy Trust Verification.

Abstract: Jini networking technology represents an exciting paradigm in distributed systems. Its elegant approach in computer networking possesses immense advantages, but also generates security problems. Extensive research has been undertaken and existing security methodologies have been applied to provide a safe execution environment. However the unique nature of Jini has made it hard for traditional security mechanisms to be applied effectively. Part of the problem lies within the downloaded code and in the lack of centralised control. Current solutions are based on assumptions; therefore they are inadequate for enforcing the security requirements of the system. The goal of our research is to increase the security of the Jini model without altering its initial characteristics. We present our preliminary research efforts in providing an alternative, fault tolerant security architecture that uses a trusted local verifier in order to evaluate and certify the correctness of remote calls.

1 INTRODUCTION

Jini networking technology (Sun Microsystems Inc.2003a; http://www.jini.org/) presents an exciting paradigm in distributed computing. Based on the Java programming language, it allows the development of spontaneous networked systems. Users and applications are able to dynamically locate one another and form on-the-fly communities. Unlike traditional systems that rely on a fixed protocol and central administration, Jini requires no further human intervention once being set up. It employs strong fault-tolerance mechanisms that do not attempt to eliminate or hide the fact that network failures may happen. On the contrary it provides a programming model and an infrastructure that allow developers to recognise and isolate any faults that might occur.

When Jini was made publicly available, no security has been taken into consideration. The Java language alone was not adequate to cope with the security required in a distributed setting. Although some solutions have been proposed, Jini lacked a generic security model that could be applied to counter any threats that might arise. The Davis project (http://davis.jini.org/) presents such a security model that has been recently incorporated into the latest Jini release. The security model is based on well known and proven techniques to enforce the basic requirements for network security. However, some of the mechanisms that Jini employs are unique in distributed computing. Additionally, neither any real world applications that make use of the model nor a formal evaluation of it have appeared yet. Thus any assumptions about the correctness of the design and the degree of security provided might prove to be mistaken. The purpose of our research is to examine the security model employed by Jini technology for any potential security faults and propose appropriate modifications. In this paper we focus in the algorithm responsible for verifying trust in Jini proxy objects.

The rest of the paper is organised as follows. Section 2 presents an overview of the Jini programming model and infrastructure, particularly the components that constitute a Jini system and other mechanisms relevant to Jini operation. Section 3 presents some security problems related to proxy objects, Lookup Services and Jini Services while Section 4 presents an overview of the current Jini security model, the Davis Project, and a critical approach to its proxy verification algorithm. Section 5 presents an outline of two proposed solutions to the issues related with proxy object verification and the advantages that they may possess. Section 6 presents related work and some concluding thoughts are drawn in Section 7.

J. Ascenso et al. (eds.), e-Business and Telecommunication Networks, 11–18.

2 BACKGROUND

Jini (Sun Microsystems Inc., 2003a; http://www.jini.org/) is a distributed system based in Java that allows the establishment of spontaneous network communities or federations. To make that possible, Jini provides the following:

An infrastructure that enables devices, human users and applications to dynamically discover one another without any prior knowledge of their location or of the network's topology and form dynamic distributed systems. The infrastructure is composed of a set of components based on Jini's programming model. Parts of the infrastructure are the discovery join and lookup protocols and the Lookup Service (Sun Microsystems Inc., 2003a). A programming model that is used by the infrastructure as well as by services. Besides service construction, the programming model provides interfaces for performing leasing as well as event and transaction handling.

Services that are employed inside a federation and provide some functionality. Services exploit the underlying infrastructure and are implemented using the programming model.

2.1 Services

Every entity that participates in a Jini system and provides some functionality is perceived as a service. No separation is made regarding the type or the characteristics of the service. A service could be either a hardware device, a piece of software or a human user. Jini provides the means for services to form interconnected systems, and each one separately to offer its resources to interested parties or clients. The separation between a service and a client, however, is sometimes blurred, as sometimes a Jini service may act both as a service and a client.

A word process application, for example, is perceived as a service by any human user that writes a document, although the same application acts as a client whenever it uses a device such as a printer. The latter is again a Jini service, thus for the infrastructure the word application is now its client.

2.2 Proxy Objects

In order for services to participate in a Jini system they must create an object that provides the code by which they can be exploited by potential clients, the proxy object. The proxy object contains the knowledge of the service's location and the protocol that the service implements. It also exposes an interface that defines the functions that can be invoked. A client is able to make use of a service only after the correspondent service's proxy object is downloaded to the client's local space. By invoking functions defined in the proxy interface, clients are able to contact and control services. Clients need only to be aware of the interface that the proxy implements and not of any details of the proxy implementation.

2.3 Lookup Service

The Lookup Service (LUS) is a special kind of service that is part of the Jini infrastructure. It provides a mechanism for services to participate in a Jini system and for clients to find and employ these services. The Lookup Service may be perceived as a directory that lists all the available services at any given time inside a Jini community. Rather than listing String based entries that point back to the location of a service, the Lookup Service stores proxy objects registered by Jini services.

2.4 Discovery Join and Lookup

Relevant to the use of Lookup services are three protocols called discovery, join and lookup (Sun Microsystems Inc. 2003a). Discovery is the process where an entity, whether it would be a service or a client, is trying to obtain references to a lookup service. After a reference has been successfully obtained, the entity might register a proxy object with the Lookup service (join), or search the Lookup Service for a specific type of service (lookup). The discovery protocol provides the way for clients and services to find available Lookup Services in the network, and for Lookup Services to announce their presence.

3 JINI SECURITY ISSUES

Typically security is concerned with ensuring the properties of confidentiality, integrity, authentication and non-repudiation (Menezes et al., 1996):

- Confidentiality ensures that information remains unseen by unauthorised entities
- Integrity addresses the unauthorised alteration of data
- Authentication is the verification of identity of entities and data
- Non-repudiation prevents an entity from denying previous commitments or actions

These properties are generic and apply to a wide variety of systems. Inside Jini, no prior knowledge of the network's infrastructure is assumed. For that reason, Jini is not only bound to security problems related to distributed systems, but also to any additional issues that the spontaneity of the environment invokes. The following components present different security requirements and they will be examined separately.

3.1 Proxy Object Issues

Nothing should be able to alter the state of the proxy object, either by intention or by fault. That means that the integrity of the proxy object must be ensured (Hasselmeyer et al., 2000a). Since the proxy object is downloaded from an unknown location in the network, neither the source nor the intentions of the proxy object can be verified. Therefore, even the act of downloading the proxy of a service is considered by itself a security risk. Moreover, the proxy is responsible for performing the communication between the client, and the service that the proxy represents. Therefore the integrity and confidentiality of the communication has to be preserved, since the communication link might be intercepted, altered, or simulated by someone with malicious intentions. The privacy and anonymity of the client may be abused, because the client can not be ensured that the proxy does indeed provide the functionality it claims (Hasselmeyer et al., 2000a). On the other hand it has to be verified that any data that needs to be supplied to the proxy object, for the interaction with the service to take place, reaches the appropriate service (JAAS).

3.2 Lookup Service Issues

The Lookup Service lacks any mechanism for authenticating services (Schoch et al., 2001). That means every service can discover the Lookup Service and register its proxy. Malicious proxies may register and pretend they provide some functionality, while they don't. Moreover, every client can search the Lookup Service and find which services are provided. Some services may require only registered users to access them. Therefore access control mechanisms need to be imposed. Additionally, clients might encounter unfairness while searching the Lookup Service for available services (Hasselmeyer et al., 2000a). There is no way a client of a service can be assured that he received the best available service from the Lookup Service. The fact that every service can register and even re-register with the Lookup Service can lead to "man-in-the-middle" attacks (Schoch et al., 2001). A malicious service just has to re-register its proxy with the same service ID as the original one. Every time a client tries to access the required service, the Lookup Service may provide him with the new, malicious proxy. The client is unaware of the change, as the new proxy looks like it implements the same interface as the original one.

3.3 Service Interaction issues

In order for an interaction between two services to take place, the service acting as a client must first locate the provider of the desired service, via the process of discovery, and then download its corresponding proxy object. However, in a spontaneous environment like Jini, hundreds of services may be present at the same time and many of them may provide the same functionality. No standard names or address for recognising individual services exist, besides a unique service ID that is assigned by the Lookup Service. However, it is dependent upon the provider of each service to decide whether or not the assigned ID will be stored and used in any future transactions. Therefore clients have to be able to authenticate the services they access (Eronen et al., 2000). Similarly, the service provider has to be able to authenticate clients that try to use its resources and call its provided functions.

Another aspect in the service interaction is different access levels (Kagal et al., 2001). An obvious solution to this problem is the integration of access control lists. Every user could be identified by a unique username and password that would grant him or deny certain permissions. However, new problems arise, like the distribution of the appropriate keys and the way that the permissions are to be decided.

4 THE DAVIS PROJECT

The Davis project (http://davis.jini.org/) is an effort led by Sun Microsystems' project team responsible for the development of Jini. The purpose is to satisfy the basic Jini requirements for security, by providing a security programming model that would be tightly integrated with the original Jini programming model and infrastructure. Part of the requirements (Scheifler, 2002) has been to avoid changing any existing application code by defining security measures at deployment time. Also to extend the security mechanisms provided by the Java programming language, such as the Java Authentication and Authorisation Service (JAAS).

The Davis project has been integrated with the original release of Jini networking technology (Jini specifications archive – v 2.0) resulting in the release of the Jini starter kit version 2 (Sun Microsystems Inc., 2003a).

4.1 Constraints

In order to support a broad variety of applications and requirements, the security model dictates that both service providers and their clients should specify the type of security they require before any interaction between them takes place. Decisions upon the type of the desirable security are expressed by a set of constraints that have the form of Java objects. Any service that wishes to incorporate security in its current implementation has to implement a proxy object that implements a well-known interface (Sun Microsystems Inc., 2003b). The interface defines a method for clients and services to set constraints to the proxy object. If the proxy implements that interface, all the imposed constraints apply to every single call through any method defined by the proxy. The basic constraints are the equivalent of Boolean constants that allow decisions upon the type of security required to be specified in proxy objects. Typically service providers specify the constraints during the proxy creation, while clients set the constraints after the proxy object has been downloaded. Constraints specify only what type of security is expected but not how this is implemented.

The security model dictates that constraints imposed by services and clients are combined to a single set of constraints. If any of them contradict with each other then no calls are performed. It is possible, however, that alternative constraints are defined. This provides an elegant way for all parties participating in a Jini interaction to have direct control over the security imposed.

4.2 Object Integrity

There are two mechanisms that the current security model employs to provide integrity for the code of proxy objects. Both assume that the http protocol is used. The first mechanism is http over SSL (https) (Rescorla, 2000), the standard protocol for providing web site security in terms of server authentication, confidentiality and integrity. The other is a custom defined protocol called HTTPMD (Scheifler, 2002; Sun Microsystems Inc., 2003b) The proxy object consists of code which is downloaded by clients, and data which is downloaded from the service. Therefore to ensure total integrity these mechanisms have to apply to both the location where the proxy object is downloaded from and the location of the object's codebase. Along with integrity, the https protocol provides confidentiality and encryption, resulting in additional overhead when these are not required. In these cases the HTTPMD protocol is used. The location of objects, including their code, is specified by a normal http URL. Attached to it is a cryptographic checksum of the contents of the code, a message digest (Rivest, 1992). By computing the checksum of the downloaded data and code and comparing it with the attached message digest, clients are ensured that integrity has been preserved, since any modification in the contents would result in a different message digest.

4.3 Proxy Trust Algorithm

In terms of deciding whether a client trusts a proxy object downloaded by an unknown source, the current model (http://davis.jini.org/) employs the procedure described below. It is assumed that the client has already downloaded a proxy object from somewhere but it can not yet trust neither the proxy object not its correspondent service. Initially the client performs an object graph analysis of the proxy object. By checking recursively all the classes that the object is composed of it can be determined whether these classes are local or not. If the classes are local, in perspective to the client, then the proxy object is considered trusted. This is accepted on the basis that all local code is considered trustworthy. In the case where the proxy object is not fully constructed of local classes, the following components take part in the proxy trust verification algorithm:

1. Proxy object
This is the object that implements the server's functionality. It is downloaded by the client, traditionally from the Lookup Service and it contains the knowledge of how to communicate back with the server. All remote calls to the server are passing through this object and this is the object that needs to be verified.

2. A 'bootstrap' proxy
If the object graph analysis proves that the classes used for the construction of the proxy object are not local relatively to the client, the client uses the initial proxy object to request another object called the 'bootstrap' proxy. The bootstrap proxy should be only consisted of local classes (relevant to the client). The purpose is that clients can trust an object that only uses local code to run. The 'bootstrap' proxy is also used to authenticate the server to the client, as well as to provide him with the verifier described next.

3. A proxy Verifier
The Verifier is an object sent to the client by the

server, using the 'bootstrap' proxy. It checks the downloaded proxy object in order to verify whether the server trusts the initial proxy object or not.

A client obtains a proxy object from the network using Jini discovery and lookup mechanisms. The client examines whether the proxy object is using local code (relative to the client). Since this is normally not the case the client has to verify whether the proxy object can be trusted. The way that this is performed by the current security model is illustrated in Figure 1.

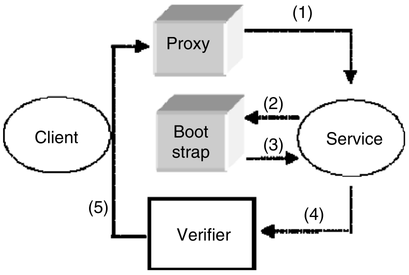


Figure 1: The proxy trust authentication employed by the current security model.

In order to verify that the proxy originates from a legitimate service, the client has to contact the same service and ask the service whether the proxy should be trusted. Since there is no way to directly contact the service, the client places a call through the proxy it can not yet trust, asking for a 'bootstrap' proxy (1). The bootstrap proxy has to use only local classes, relative to the client, in order to be considered trustworthy. After the bootstrap proxy is downloaded to the client's local address space (2), and the locality of the classes that compose the bootstrap object is verified, the client performs a call through it (3). Part of the call is to request from the service to authenticate. After the service has authenticated successfully, it passes a verifier object to the client (4). Finally the verifier is used to verify the legitimacy of the initial proxy object (5).

4.4 Critical Review of the Proxy Trust Algorithm

A number of potential problems might arise from the verification algorithm described above. The first is that clients have to rely on an object downloaded from an unknown source (the proxy object) to obtain the bootstrap proxy. In order for the latter to occur, clients have to place a remote call through an untrusted object. Since the functionality that the proxy object implements is unknown, clients may unintentionally execute an operation that presents a security risk in case the proxy is a malicious object. The second problem is that the service provider has to have some knowledge of the type of classes that are local to the user. If the bootstrap proxy is not consisted entirely by local classes, relevant to the client, the client would not utilize it to obtain the verifier.

A third type of problem is related to the way and type of checks that the verifier performs to the proxy object. There is no standardised set of tests that could be performed, since these are left for the service providers to implement. The method suggested is that the verifier carries the code of the proxy object. By checking the equality of the code that the verifier carries with the code of the proxy object, it is possible for a service to identify the correctness of the proxy object. However, there is no way to ensure whether the checks performed are adequate or if any checks are performed at all.

Therefore a 'lazy' verifier that just confirms the correctness of proxies without performing any checks might incorrectly identify a malicious object as a legitimate one.

Finally faults might occur if a service provider updates the implementation of the proxy object without updating the implementation of the verifier too. In that case legitimate proxy objects would not be able to be identified correctly, since the equality check would fail. Therefore the service provider might unintentionally cause a denial of service attack not initiated by a malicious client, but by himself.

5 AN ALTERNATIVE WAY OF VERIFYING PROXY TRUST

Instead of relying on the untrusted proxy object downloaded from an unknown source to obtain a proxy verifier, clients might be able to protect themselves from malicious proxy objects by using their own local verifier. The verifier is generated locally by clients before any participation in a Jini federation takes place. In order to create the verifier, clients specify their security requirements such as authentication, confidentiality and integrity. These requirements are injected to the verifier and might vary for different scenarios. Specification of the security requirements is similar to the concept of constraints specified by the current Jini security model (http://davis.jini.org/). This permits the specification of application independent security requirements and allows better interoperability with the current security model. The difference is that the client requirements are not injected into a downloaded proxy, but into the locally generated verifier.

The notion of a locally generated verifier is central to all of the proposed solutions. The operations that the verifier performs, however, are different in every variation of the algorithm. The entities employed in all the solutions proposed here case are the following:

- Client: The entity that wishes to use a service. Clients need to be protected from any potential hazards.
- Proxy object: Typically the object that is downloaded by clients and used to access services. Presents the major source of incoming threats.
- Local Verifier: An entity generated by clients before any interaction with downloaded objects takes place. Used to either verify proxy objects or isolate clients from them.
- Service: The entity that lies somewhere in the network and provides some functionality. Services supply proxy objects and should be considered untrusted.

In every proposed solution it is assumed that a service has already discovered an available Lookup Service and registered its proxy object. The client is ready to perform discovery and lookup in order to obtain a proxy object from the same Lookup Service.

5.1 Proxy Verification Based on a Local Generated Verifier

In order to verify that the downloaded proxy object can be trusted, the following process is performed:

1. Before any discovery process takes place, the client generates a local verifier

2. Client's security requirements are injected to the verifier by the client

3. The client performs discovery of the Lookup Service and downloads a service proxy object

4. Before any interaction with the proxy takes place, the proxy object is passed to the verifier

5. The verifier performs a series of security checks according to the client requirements and makes a decision on behalf of the client about the trustworthiness of the proxy object

6. In case the verifier has decided that the security requirements are satisfied, the client interacts with the service through the proxy object as defined by Jini programming model.

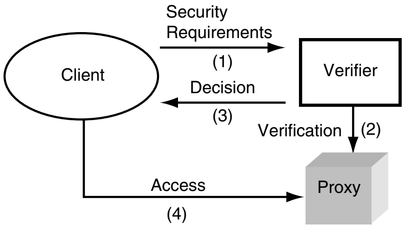


Figure 2: Proxy trust verification by a local verifier.

The described process is illustrated in Figure 2 Initially the client generates the verifier and specifies the security requirements (1). The verifier performs a series of tests to verify trust in the proxy object (2). The result of the verification procedure is expressed as a decision and the client gets notified (3). If proxy has been considered to be trustworthy, the client is allowed to contact the proxy object (4) and access the related service. Comparing this solution with the default proxy verification algorithm, in both algorithms the client is responsible for specifying the type of security required. However, the entity that is responsible for enforcing these requirements is not an untrusted proxy object anymore, but a locally generated verifier. The type of checks performed and the way these are carried out is much more transparent from the client's point of view. Moreover, clients do not have to rely on a verifier object downloaded from a service since the process of such object verifying the initial proxy object is not clear to the client.

Therefore the problem of a service generated verifier that performs no actual check to the proxy object, resulting in the verification of a faulty proxy, is eliminated.

Service providers also do not need to worry about having to provide a bootstrap proxy and a verifier. The only entity that services need to expose is the default proxy object. Absence of a bootstrap proxy eliminates the need for services to implement an object based on the assumption that it would consist of classes that the client already has. Moreover, the current algorithm dictates that every time the implementation of a proxy object changes the verifier object has to change as well, since proxy verification is based on equality checking. Finally by eliminating the need for services to produce two additional objects (the bootstrap proxy and the verifier), administration burden is removed from the service provider.

5.2 Restricting Proxy Object in a Controlled Environment

1. Before any discovery process takes place, the client generates a local verifier
2. Client injects to the verifier the security requirements and the maximum amount of local resources permitted for use by proxy objects
3. The client performs discovery of the Lookup Service and downloads a service proxy object
4. The verifier provides a controlled environment for the proxy object to run. Besides performing security checks to the proxy object, the verifier ensures that the proxy does not use more resources than specified. All requests to and from the proxy object pass through the verifier.

Figure 3 illustrates the followed process. The client generates a local verifier and assigns the security requirements as well as any resources that proxy objects are permitted to use (1). After the proxy object has been downloaded, it is passed to the verifier. The verifier performs similar type of security checks as in proposed solution 1, and additionally provides a controlled environment where proxy objects run. Any client requests and any responses from the proxy object pass through the verifier (2). The same is true for any communication held between the proxy object and its corresponding service.

The advantages of this solution are similar to those of the solution proposed in Section 5.1. The need for service providers to produce additional objects besides the default proxy object is eliminated and so are the assumptions relevant to the locality of classes in the bootstrap proxy and the checks

performed by the service's verifier. Moreover, by restricting execution of the proxy object into a set of finite resources, a protected environment safeguarded by the verifier is created. Verification does not occur only once, but the verifier is monitoring the proxy object continuously. Therefore any potential hazards that might take place during the execution of the proxy are more likely to be identified and get dealt with.

6 RELATED WORK

In (Eronen et al., 2000) certificates are used to establish trust between services and users. Secure interaction is assumed, by allowing users and services to interact only if they carry the appropriate credentials, supplied by a security library. However, these credentials must be assigned to every service of the Jini community before any interaction could be realised. That reduces the spontaneity that Jini provides, and requires prior knowledge of the services' properties to exist, in order for the appropriate permissions to be assigned correctly. Trust establishment is also the purpose of (Hasselmeyer et al., 2000a). Trust establishment is attempted between the Lookup Service, the service provider and the client. The authors propose an extension to the Jini architecture with a certification authority, which provides certifications for the authentication of components. Capability managers are responsible for administering the rights for each user. In that way, different access levels for each client can be easily implemented. Their solution, however, assumes that one central certification authority exists, in order for the appropriate certificates and capabilities to be distributed to every Jini component that exists in the system. Thus, a prior knowledge of every service's characteristics should exist something that is not usually the case in Jini. Moreover, the existence of a centralised authority is opposed to the decentralised nature of the Jini technology. The integration of authorisation and authentication techniques in Jini is also examined in (Schoch et al., 2001). The authors try to achieve that without introducing any additional components, besides the facilities that Jini and Java already provide. They try to prevent man-in-the-middle attacks, by signing the proxy object with a digital signature. This allows the clients to authenticate the source of the provided service, although it still can not be verified how the service users the provided by the service data.

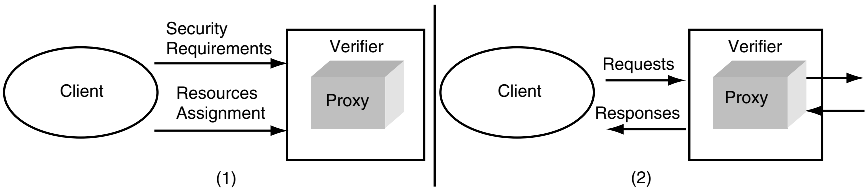


Figure 3: Verifier creation and interaction with the proxy object.

7 CONCLUSION

We presented some security problems related with Jini and how they are countered by the current Jini security model. Our focus is placed in the proxy trust verification algorithm since we believe that an alternative way of verifying proxy object trust might encounter some of the existing problems. We presented our initial ideas in providing an alternative way of ensuring that hostile proxy objects would not impose any risk to clients of the system. We sketched two different approaches in solving the problem. Both involve the concept of a local generated verifier that either verify a downloaded proxy object or impose restrictions to that object's functionality. We also pointed out the advantages of these solutions. Future work includes further rectifying the presented concepts and come up with a viable solution that would integrate with the existing model. Also implement a working prototype and test it in a real world environment.

REFERENCES

Eronen, P., Lehtinen, J., Zitting, J., and Nikander, P., 2000. Extending Jini with Decentralized Trust Management. In Short Paper Proceedings of the 3rd IEEE Conference on Open Architectures and Network Programming (OPENARCH 2000), pages 25-29. Tel Aviv, Israel.

Hasselmeyer, P., Kehr, R., and Voß M. 2000a.Trade-offs in a Secure Jini Service Architecture. In 3rd IFIP/GI International Conference on Trends towards a Universal Service Market (USM 2000), Munich, Germany. Springer Verlag, ISBN 3-540-41024-4, pp. 190-201.

Java Authentication and Authorisation Service (JAAS) http://java.sun.com/products/jaas/ [Accessed 10 Feb. 2004]

Jini specifications archive – v 2.0 http://java.sun.com /products/jini/1_2index.html [Accessed 10 Feb. 2004]

Kagal, L., Finin T. and Peng, Y. 2001. A Delegation Based Model for Distributed Trust. In Proceedings of the IJCAI-01 Workshop on Autonomy, Delegation, and Control: Interacting with Autonomous Agents, pp 73-80, Seattle.

Menezes, A., van Oorschot, P., and Vanstone S. 1996. Handbook of Applied Cryptography. CRC Press. ISBN: 0849385237

Rescorla, E. 2000. HTTP Over TLS, the IETF Network Working Group http://www.ietf.org/rfc/rfc2818.txt [Accessed 09 Feb. 2004]

Rivest, R. 1992. RFC 1321 - The MD5 Message-Digest Algorithm, the IETF Network Working Group, http://www.ietf.org/rfc/rfc1321.txt [Accessed 09 Feb. 2004]

Scheifler, Bob 2002. Comprehensive Network Security for Jini Network Technology Java One Conference Presentation, San Francisco, March 2002 http://servlet.java.sun.com/javaone/sf2002/conf/sessions/display-1171.en.jsp [Accessed 15 Dec. 2003]

Schoch, T., Krone, O., and Federrath, H. 2001. Making Jini Secure. In Proc. 4th International Conference on Electronic Commerce Research, pp. 276-286.

Sun Microsystems Inc. 2003a. Jini architecture specification. http://www..sun.com/software/jini/specs /jini2_0.pdf [Accessed 15 Dec. 2003]

Sun Microsystems Inc. 2003b. Jini architecture specification. http://wwws.sun.com/software/jini/specs /jini2_0.pdf [Accessed 15 Dec. 2003]

http://www.jini.org/ [Accessed 11 Feb. 2004] The Davis project http://davis.jini.org/ [Accessed 11 Feb. 2004

AN EXPERIMENTAL PERFORMANCE ANALYSIS STUDY OF LOSS RATE AND JITTER CHARACTERISTICS IN WIRELESS NETWORKS

M. S. Obaidat[1] and Yulian Wang[2]
[1]*Monmouth University, NJ, USA and* [2]*Tampere University of Technology, Tampere, Finland*
Corresponding Author: Prof. M. S. Obaidat, Department of Computer Science,
Monmouth University, W. Long Brach, NJ07764, USA
E-mail: Obaidat@monmouth.edu

Keywords: Wireless networks, Jitter, loss rate, mobile IP, performance evaluation, bit error rate (BER), Quality of Service (QoS), Diffserv, resource reservation, performance evaluation.

Abstract: Among the challenges in wireless networks is the high bit error rate, which is due mainly to atmospheric noise, physical obstructions found in the signal's path, multipath propagation, interference from other systems and terminal mobility. This high bit error rate makes it difficult to offer guaranteed services over the wireless link. In this paper, we present an experimental analysis study on the loss rate of wireless systems using six different scenarios. We also present an experimental study of jitter for UDP traffic over wireless Mobile IP networks. It is found that in order to provide different Quality of Service, QoS, to downstream traffic flows and control network's loss rate and jitter, it is not enough to have only DiffServ flow control mechanisms. A protocol for wireless link resource reservation and cooperation by senders is also needed. We identify the relationship of jitter, loss rate and class allocation's effect using Class Based Queueing (CBQ) and the packet sending rates in the wireless networks. It is found that loss rate and jitter can be controlled with DiffServ flow control mechanism, but it requires that the total traffic rate should be within the limit of the wireless link capacity. Various tests have been conducted under different settings and operating conditions.

1 INTRODUCTION

1.1 Study of Loss Rate

There are fundamental differences between wireless and wired LANs, which pose difficulties in the design of such systems and protocols (Nicopolitidis, P. et al., 2003), (Nicopolitidis, P. et al., 2002). (The wireless medium is characterized by high bit error rates (BERs) that can be ten times than that for wired LANs. Moreover, errors in wireless LANs occur in bursts, whereas in traditional wired systems errors appear randomly. Among the challenges in wireless networks are: (a) wireless medium unreliability, (b) spectrum use, (c) power management, (d) security, (e) routing, and (f) interfacing with wired networks. The phenomena causing reception errors in wireless systems are: (a) free space path loss, (b) Doppler shift due to station mobility, and (c) multipath propagation due to mechanisms such as reflection, diffraction, and scattering. Such mechanisms cause the signals to travel over many different paths (Nicopolitidis, P. et al., 2003), (Green, D. and Obaidat, M. S., 2003). Mobile IP protocol is an extension of the Internet protocol intended to support mobility in the Internet across all kinds of networks, both fixed (wire-line) and wireless types. When employed with wireless access networks, it can be used to create truly mobile networks. In practice, it enables people to access the Internet continuously with their laptop computers and other portable IP-capable devices while moving around an area covered by wireless LANs.

Mobile IP was developed in response to the increasing use of mobile computers in order to enable them to maintain Internet connection during their movement from one access point to the other. The term mobile here implies that the user is connected to one or more application across the Internet and the access point changes dynamically.

J. Ascenso et al. (eds.), e-Business and Telecommunication Networks, 19–29.

Clearly, this is different from when a traveler uses his ISP's account to access the Internet from different locations during his trip (Nicopolitidis, P. et al., 2003), (Papadimitriou, G. et al., 2002). Mobile IP is the modification to the standard IP so that it can allow the client to send and receive datagrams no matter where it is attached to the network. The only main security problem using this mechanism is the redirection attacks, which occur when malicious clients give false information to the home agent in the mobile IP network. The home agent is informed that the client has a new care of address. Thus, all IP datagrams addressed to the actual client are redirected to the malicious client (Nicopolitidis, P. et al., 2003).

These days, wireless networks are accessed freely by Mobile Nodes. However, an accounting and charging system starts to be developed. The idea of charging for network access quickly leads to the question of what kind of Quality of Service (QoS) the customer is paying for and how it is ensured. QoS support is naturally needed for the transfer of multimedia streams. In general, the assumption is that real-time data streams will be carried by wireless Mobile IP networks, which are sometimes called 4th generation wireless networks.

Loss rate is an important performance metric that is used to evaluate QoS over wireless links. It is possible to achieve QoS for Mobile IP over wireless link if we can find the causes that increase loss rate. High losses in wireless networks make it difficult to offer guaranteed services over the wireless link. For TCP connections, high loss rate will introduce extra delay in the data transmission. For UDP connections, it will increase the unreliability of datagram delivery.

The current Internet architecture with its best effort service model is inadequate for applications that need various QoS assurances. Two different models have been proposed for Quality of Service (QoS) in the Internet: the Integrated services (Intserv) and the Differentiated services (Diffserv) models. Intserv provides QoS guarantees to individual streams from end to end, while Diffserv provides QoS assurances to a group of applications. Both of these models have been designed to work for wired networks. Hence, new solutions are needed for providing scalable QoS on wireless Mobile IP networks.

Jitter is considered an important metric that is used to evaluate QoS for real-time streaming traffic. Real-time streaming traffic and multimedia synchronization (Wang, C., et al., 1994) require source clock recovery for smooth playback at the destination (Pocher, H., et al., 1999). The cost of clock recovery depends greatly on the ability of the network to control jitter (Varma, S., 1996), (Wright, D.J., 1996). Thus, jitter control over wireless networks for real time applications has been directly connected to the quality of service, QoS, provided to end users.

The Class Based Queueing algorithm was introduced by Jacobson and Floyd in 1995 (Floyd, S. and Jacobson, V., 1995). It was designed to share limited link resources efficiently by different classes. CBQ is supposed to be used in a router where the links are heavily utilized. It allows traffic flows sharing a data link to be guaranteed some amount of bandwidth whenever congestion happens. In addition, CBQ can be used to give priority over other traffics to packets that require low delay. In this way, the link can be shared by multiple data flows yet still can meet the QoS requirements.

The basic rule of CBQ is that each class is given an average rate or a weight of the total bandwidth. Each class gets different amount of the shared resources. Classes can also be designed in a hierarchical structure. Classes on the same level of hierarchy share the whole resource of the parent class. Packets are sent whenever there are resources available in the class to which the packets belong. However, if there are any unused resources in the parent class, the child classes may borrow them. Priority can be given to each class also. Higher priority traffics can be handled ahead of other lower priority traffics.

We put our emphasis on the downlink traffic jitter control on the wireless link a bit more than uplink traffic. The tests of the downlink behavior are more significant for two reasons. First, most flows requiring QoS are likely to be downstream flows from the Internet to the mobile, such as broadcast audio and video. Second, technical solutions for dividing the downlink capacity such as the CBQ exist and can be deployed incrementally. On the other hand, there are some open problems in the uplink direction.

A testbed system running Dynamics hierarchical Mobile IPv4 and Redhat Linux 6.1 with Class Based Queueing (CBQ) on PCs with 2 Mbps Lucent WaveLAN cards was set up for experiments in a real network environment. A description and analysis of the preliminary results from various experiments are presented in this paper.

The first main goal of this experimental study is to identify the relationship of loss rate and sent packets in both downstream and upstream directions and how Class Based Queuing (CBQ) can be used to provide different services for downstream traffic. We present our test results and give analysis on loss rate of wireless Mobile IP.

The second goal of this study is to identify the relationship between jitter and packet sending rate with and without DifferServ flow control mechanism. We investigate here, the possibility to provide network jitter QoS guarantees with Class Based Queueing (CBQ) link resource sharing method. Our focus area is the wireless link and the Mobile IP Foreign Agent (FA), the bottleneck network and router. Classes based on Class Based Queueing (CBQ) method are designed and implemented for the Foreign Agent.

2 SYSTEM SETUP

In this section, we describe the setup of the test, performance measures, design of CBQ classes, and the tools used for measuring the QoS parameters. We installed a Mobile Ipv4 Home Agent in one PC, Foreign Agent in one laptop PC, and three Mobile Nodes (MNs) in three laptop PCs. Another PC was used as the Correspondent Node (CN). All Mobile Nodes are forced to connect to the FA by using a dynamic tool that comes with dynamic hierarchical Mobile Ipv4 (Mediapoli, 2000), (The Dynamics, 2000). The whole setup is depicted in Figure 1.

The operating system used in all computers was Linux Redhat version 6.1. Two Mbps WaveLAN cards were used for the three Mobile Nodes and Foreign Agent in order to provide wireless connections between the Mobile Nodes and Foreign Agent. The WaveLAN, CBQ, and some other Quality of Service, QoS, support software modules were compiled and loaded to the Linux kernel.

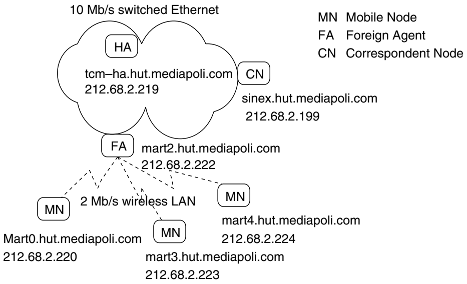


Figure 1: Layout of the test network.

Traffic coming from the CN to MNs went through Foreign Agent. Correspondent Node is connected to Foreign Agent through a high bandwidth Internet connection. Foreign Agent is connected to Mobile Nodes through a wireless connection. In the wired part, the available bandwidth was 10 Mbps. In the wireless part, the available bandwidth was limited to 2 Mbps WaveLAN card. The CBQ was installed in Foreign Agent for downstream traffic. The class design is shown in Figure 2. The bandwidth of the wireless part was divided between two classes. The total bandwidth was set to 1400 kbps. Although the WaveLAN card has a 2 Mbps capacity, the test showed that the total usable bandwidth is 1.4 Mbps. The allocated resource for Class 1 is 100 Kbps with weight 100 Kbps and Class 2 is 1300 Kbps with weight 1300 Kbps. This kind of design of sharing resource is based on the consideration that we can give real time traffic high priority and most of the link resource while give datagram traffic low priority and very little link resource. However, the datagram traffic can use any bandwidth unused by real-time traffic, according to the characteristic of CBQ.

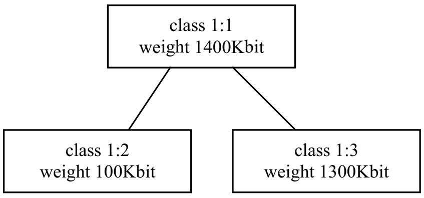


Figure 2: CBQ class design.

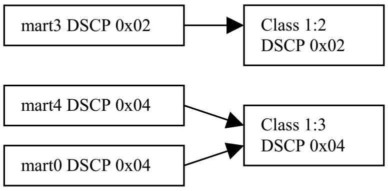


Figure 3: Classifier design.

Packets were marked with different Differentiated Services Code Point (DSCP) values in the IP header before they were sent from the Correspondent Node to Mobile Nodes. In our test system, two DSCP values were used. Thus, all packets were separated into two types; each of which goes through its own class as shown in Figure 3. When these packets come to FA, it will separate them into two classes according to the DSCP values in the IP header of the packets. As shown in Figure 3, DSCP value 0x02 goes to Class 1:2 and 0x04 goes to Class 1:3. The two classes have different bandwidth weights. If the traffic of one class exceeds the bandwidth limit, then the excess packets will be discarded first by CBQ. These two classes can borrow bandwidth from each other if the other has leftover bandwidth. Thus, no bandwidth is wasted.

We installed measurement software called Iperf (Gates, M. and Warshavsky, A., 2000) in the three MNs and CN. Iperf is used to measure the maximum TCP and UDP throughput. It reports bandwidth, jitter (delay variance) and datagram loss. It is a similar tool to ttcp, but it has overcome some of the limitations of ttcp. Iperf can run for a specified time and can print periodic bandwidth, jitter, and loss reports at specified time intervals. In the following experiments, jitter is calculated in average over 1 second.

3 EXPERIMENTS AND RESULTS

This Section describes the experiments performed and measurement results obtained. We have considered six different scenarios; scenario 1 to 6.

3.1 Scenario 1

In this experiment and the next one, we study the relation between loss rate, jitter characteristics and sending rate in the uplink direction of wireless systems. Three MNs (mart0, mart3, and mart4) are sending data to CN. They are forced to connect to the FA mart2. CBQ is not installed because it doesn't affect uplink traffic in the wireless part. Mart0 sends between 0 seconds to 60 seconds. Mart3 sends between 10 seconds to 60 seconds. Mart4 sends between 30 seconds to 50 seconds. Therefore, we can see only one MN sending, two MNs sending at the same time, and three MNs sending at the same time. Three MNs try to send at a rate of 700 Kbps.

The performance results of loss rate are depicted in Figure 4.

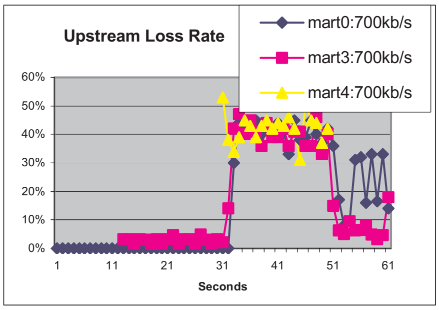


Figure 4: Loss rate chart for scenario 1.

As shown in the figure, we notice that:

1. When only one MN is sending, the total required bandwidth is 700 Kbps which is within the limit of the available bandwidth of the wireless link. The loss rate is about 0.
2. When two MNs are sending at the same time, the total required bandwidth is 1400 Kbps, which is just within the limit of the total available bandwidth. The upstream loss rate for the first stream is almost 0 and for the second stream is about 4%.
3. When three MNs are sending at the same time, the total required bandwidth is 2.1 Mbps, which exceeds the limit of the total available bandwidth. The loss rate for three streams is the same and it is about 42%.

The performance results of Jitter characteristics are depicted in Figure 5.

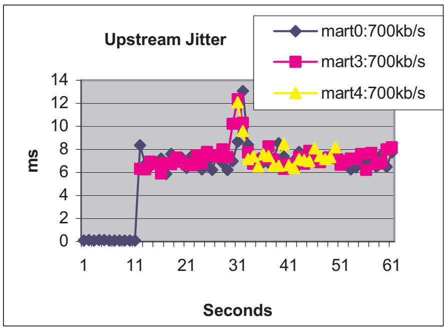


Figure 5: Jitter characteristics for scenario 1.

As shown in the Figure 5, we notice that:

1. Jitter is evenly distributed among different traffic flows.
2. When only one MN is sending, jitter is 0.1ms, which is very small.
3. When two MNs are sending at the same time, jitter is around 7 ms. Jitter is increased from 0.1ms to 7ms when total requested bandwidth increased from 700 Kbps to 1.4 Mbps, which is within the link capacity.
4. When three MNs are sending at the same time, surprisingly the jitter is same as when two MNs are sending. The total requested bandwidth is 2,100 Kbps, which is more than the available bandwidth in the wireless link 1400 Kbps. From our previous related work, we notice that the loss rate is about 42% for all three streams in this situation. This heavy packet loss is mainly caused by data collision and channel contention. We may conclude that whenever we try to observe the jitter characteristic of a stream, we should also consider the packet loss rate as well.

From this experiment, we conclude that jitter characteristic is affected by how many other mobile nodes are sending data at the same time and their sending rate. If the total requested bandwidth is more than the available bandwidth in the link, then we should consider packet loss rates when we analysis the jitter characteristics. In order to mantain the maintain the traffic flow's jitter at a certain level, some controlling methods must be taken.

3.2 Scenario 2

In this experiment, we considered three MNs that try to send at 1.5 Mbps rate. All other settings are the same as in scenario 1. The purpose of the test is to find out how loss rate and jitter characteristic change when MNs send more UDP packets and require more bandwidth resource than the available bandwidth in the wireless link. Figure 6 summarizes the results obtained in this test.

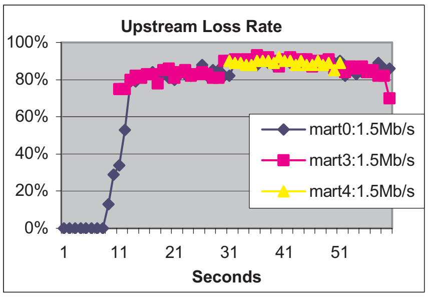


Figure 6: Loss rate chart for scenario 2.

The finding of this experiment can be summarized as follows. When three MNs are sending at the same time, the total required bandwidth is 4.5 Mbps, which is beyond the limit of the total available bandwidth. The loss rate for three streams is same and it is around 90%. We can see that the useful bandwidth is not equal to the available bandwidth 2Mbps in the wireless link. About 90% of bandwidth is wasted due to data collisions. Figure 7 summarizes the results obtained for jitter characteristics in this test.

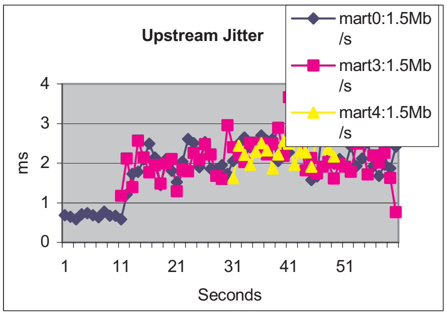


Figure 7: Jitter characteristics for scenario 2.

As shown in the Figure 7, we notice that when two or three MNs are sending at the same time, jitter is around 2.5ms, which is surprisingly small when comparing to the result from scenario 1. From our previous related work, we found that the loss rate is about 90% for all three streams.

We may conclude that whenever we try to observe the jitter characteristic of a stream, we should also consider the packet loss rate. If the packet loss rate is too large, then the jitter characteristic becomes meaningless. There are many studies that have investigated ways to control loss rate and avoid channel contention in the wireless network (Wang, Y. and Obaidat, M. S., 2004), (Kwon, Y. et al., 2003), (Wang, Y. and Obaidat, M. S., 2004).

3.3 Scenario 3

In the following experiments, we study the relation between loss rate, jitter characteristics and sending rate in the downlink direction of wireless Mobile IP system. We also study the impacts of CBQ on the data lose rate in the wireless link.

In this case, we study the downstream bandwidth allocation loss rate and jitter characteristics between three MNs with CBQ method. The CBQ kernel module and the classes shown in Figure 2 and Figure 3 are installed in FA, mart2. Three MNs (mart0, mart3, mart4) are receiving data from CN. The latter sends data to mart3 between 0–90s, to mart4 between 10 and 90s, and to mart0 between 40 and 70s. Mart3 is receiving a stream of 600 Kbps. The packets sent to mart3 are marked with the DSCP value 0x02. Those packets go through Class 1:2. The packets sent to mart0 and mart4 are marked with the DSCP value of 0x04. These packets go through Class 1:3.

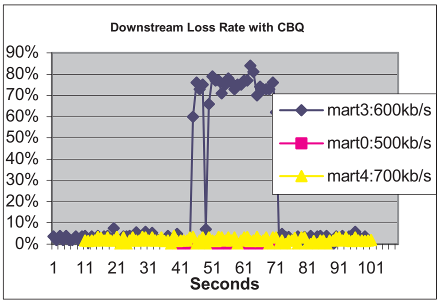


Figure 8: Loss rate chart for scenario 3.

As shown in Figure 8, we can make the following main observations about this experiment:

1. When only one MN is receiving data from the CN, the total required bandwidth is 600 Kbps that is within the limit of the available bandwidth of the wireless link, but beyond the limit of the allocated bandwidth to class 1:2. Since no traffic stream goes in another class, traffic in Class 1:2 can borrow the unused resource in Class 1:3. The loss rate is about 3%.
2. When two MNs are receiving packets and their total requested rate is 1.1Mbps, which is within the available bandwidth, traffic in Class 1:2 can borrow the unused resources in Class 1:3. The loss rate of both streams is around 4%.
3. When three MNs are receiving packets at the same time, the total required bandwidth is 1.8 Mbps, which is beyond the limit of the total available1.4 Mbps bandwidth. The traffic streams toward mart0 and mart4 go through Class 1:3. The total traffic goes through Class 1:3 is 1.2 Mbps that is within the available bandwidth limit. The loss rate for those two streams is the same, which is around 1%.

The stream towards mart3 goes through Class 1:2. The total traffic goes through Class 1:2 is 600 Kbps, which is beyond the limit of the available bandwidth allocated to the class. The loss rate for stream towards mart3 is increased to 79% since it can only borrow 100 Kbps from Class 1:2.

The performance result for jitter characteristics are depicted in Figure 9.

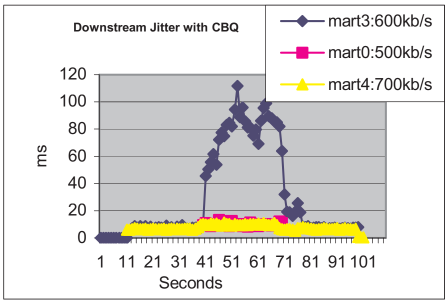


Figure 9: Jitter characteristics for scenario 3.

As shown in Figure 9, we notice that:

1. Jitter characteristics are decided by the allocated resources to each class and the total amount of traffic in the class.
2. When one MN is receiving packets and its requested rate is more than the capacity reserved for its class, but there is enough available bandwidth in the wireless link, the jitter is 0.
3. When two MNs are receiving packets and their total requested bandwidth has been increased to 1300 Kbps that is within the available bandwidth, the jitter increased to 9ms.
4. When three MNs are receiving packets, the jitter for mart4 and mart0 is around 11ms, which has not increased much. Mart4 and mart0 go to the class that has 1300 Kbps capacity, and the total requested bandwidth by them is 1200 Kbps, which is within the class capacity. The jitter for mart3 has been increased from 9ms to 100ms. Mart3 goes to the class that has 100 Kbps capacity and its requested bandwidth is 600 Kbps, which is much more than available bandwidth since now three MNs are receiving at same time. In another class, there is only 100 Kbps unused bandwidth left. Mart3 can borrow this 100 Kbps, but still mart3 cannot get all bandwidth that it needs.

In this experiment, we see that CBQ method can be used to control traffic flow's jitter to a constant level. Mart4 traffic flow's jitter has been controlled at almost constant level. The jitter is not affected by other Mobile Node's sending large amount of data.

3.4 Scenario 4

Contrary to the experiments in scenario 3, experiments in scenario 4 have been performed without CBQ setting. All other settings in this case are the same as in case 3. The purpose of this test is to see the downstream bandwidth allocation between the three MNs without CBQ method. By comparing the results from these two tests, we can analyze the effect of CBQ on the loss rate variations for the traffic towards MNs.

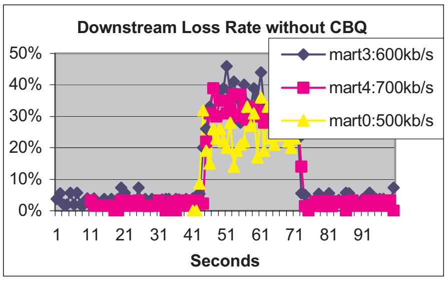


Figure 10: Loss rate chart for scenario 4.

Figure 10 summarizes the results obtained from this experiment. The main findings of this test are: When three MNs are receiving packets at the same time, the total required bandwidth is 1.8Mbps, which is beyond the limit of the total available 1.4 Mbps bandwidth. The loss rate for each of the three traffic streams is almost same, which is around 30%. Here all traffic flows suffer from the insufficient traffic capacity.

The performance result for jitter characteristics are depicted in Figure 11, which summarizes the results obtained from this experiment.

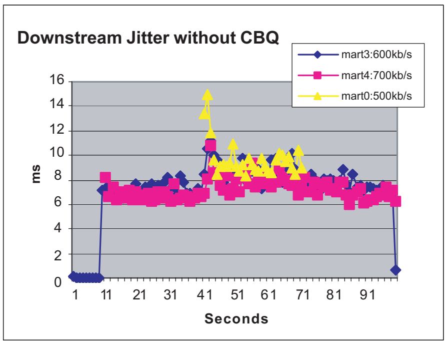


Figure 11: Jitter characteristics for scenario 4.

The main findings of this test are similar to scenario 1 for uplink data. Without CBQ; we cannot see any differentiation of jitter behavior for each traffic flow. All traffic flows jitter are almost same. From our previous work, we found that when three Mobile Nodes are receiving data at same time (the total requested bandwidth is 1800 Kbps), the loss rate was around 40%. In this period, jitter becomes meaningless.

From scenario 3 and 4, we can conclude that CBQ can be used to control jitter to a constant level when the requested bandwidth is within the bandwidth limit of the class. In scenario 5 and 6, we test if CBQ still works if requested bandwidth exceeds the bandwidth limit for the class.

3.5 Scenario 5

In scenarios 5 and 6, all MNs receive large amounts of data that exceed the available bandwidth. Experiments in scenario 5 are performed with CBQ while in scenario 6 without CBQ. The purpose of experiments in this scenario is to see the downstream bandwidth allocation loss rate and jitter characteristic between three MNs under the condition that all MNs receive large volume of data that exceed the available bandwidth in the wireless link. By comparing the results from these two tests, we can analyze the effect of CBQ on the loss rate and jitter characteristic variations for the downlink traffic. The main observations on the results in this scenario are:

1. When one MN, two MNs or three MNs are receiving, the total required bandwidth exceeds the total available bandwidth resource. The loss rate is almost 100% for all of the streams. From the loss rate chart, we can see that the loss rate is in extremely unreliable. Almost all the bandwidth is wasted due to data collisions.

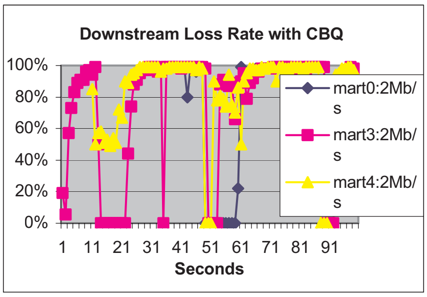


Figure 12: Loss rate chart for scenario 5.

2. We can conclude that CBQ can not ensure the link quality when the total downstream traffic at FA in each class exceeds the total wireless link capacity allocated to each class.

The performance result for jitter characteristics are depicted in Figure 13.

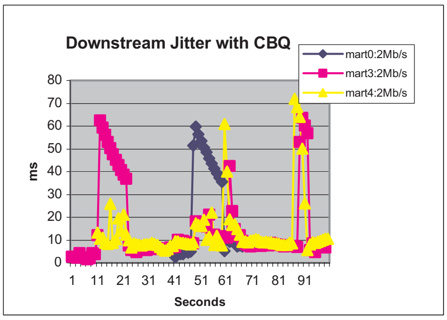


Figure 13: Jitter characteristics for scenario 5.

The main observations on the results in this scenario is that when there are two or three MNs receiving data at the same time, the jitter for each data flow is extremely unstable; it varies between 5 ms to 60 ms. CBQ does not guarantee better jitter characteristics for high priority class. From our previous related work, we noticed that the loss rate is almost 100% for all three streams. The jitter characteristic becomes less important than controlling loss rate in his situation. We conclude that we have to consider loss rate when we analysis jitter characteristics especially in the case when the wireless network resource is in over used condition.

3.6 Scenario 6

Contrary to scenario 5, the test in this scenario has been performed without CBQ setting. All other settings in this test case are same as the test case 5. Figure 14 depicts the downstream loss rate versus time.

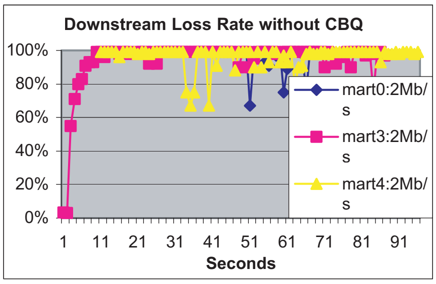


Figure 14: Loss rate chart for scenario 6.

The main observation from the results obtained from this test is that when one MN, two MNs or three MNs are receiving, the total required bandwidth exceeds the total available bandwidth resource. The loss rate is almost 100% for all of the streams.

The performance result for jitter characteristics are depicted in Figure 15.

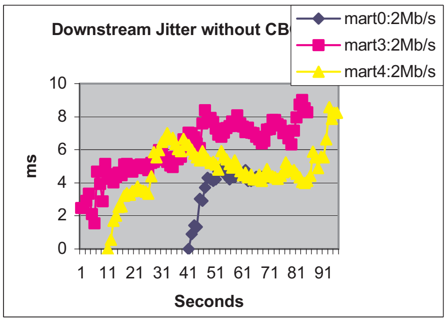


Figure 15: Jitter characteristics for scenario 6.

The result shows that the jitter characteristics become meaningless when all packets almost lost. Again, we conclude here that we have to consider loss rate when we analysis jitter characteristics.

4 DISCUSSIONS

4.1 Loss Rate Analysis

High losses in wireless networks make it more difficult to offer any guaranteed service. The unpredictable losses are mainly due to low quality radio reception and data collisions (Wang, Y. and Obaidat, M. S., 2004), (Claessen, A. et al., 1994). Mobility of Mobile Nodes also increases error rate by approximately 30%. For TCP connections, high loss rate will introduce extra delay in the data transmission. For UDP connections, it will increase the unreliability of datagram delivery. In reference (Xylomenos, G. and Polyzos, G., 1999), the authors point out that some data collisions may sometimes go undetected with WaveLAN so that the error rate visible to higher layers with bidirectional (TCP) traffic increases (Green, D. and Obaidat, M. S., 2003),(Xylomenos, G. and Polyzos, G., 1999), (Nguyen, G. T. et al., 1996).

In wireless LANs with WaveLAN technology, which is used in our testbed, the bandwidth is shared among MNs using CSMA/CA for access control, instead of CDMA/CD. The reason is that it would be expensive to use CDMA/CD because it uses extra bandwidth.

As observed in experiments conducted in scenarios 1 and 2, we found that Wave LAN MAC layer does not divide bandwidth efficiently if the total bandwidth needed by the sending nodes exceeds the link capacity. The loss rate is same for all sending MNs. The bandwidth is divided equally among the sending nodes and there is no technique for allocating different amounts. As mentioned earlier, the unpredictable losses are mainly caused by low quality radio reception and data collisions. The Low radio quality has been improved by enhancing the hardware quality and by technological innovations such as CDMA. Nevertheless, radio transmission is always more prone to errors and link failure than wired networks. Data collisions can be reduced by limiting the total amount of data transmitted by the wireless nodes to the link capacity. There are general two ways to do this: (a) by letting the MN know the total available capacity by broadcasting or by individual signaling, and (b) by letting the MN reserve resources from the nearest FA. The latter keeps accounting of the total available resources. A MN is only allowed to send traffic after it gets confirmation from the FA.

Data collisions can also be avoided by using a token passing protocol that allows only one node to transmit at a time. However, the token-based approach is generally thought to be inefficient. This is due to the fact that in a wireless LAN, token losses are much more likely to happen due to the high bit error rate (losses) of the wireless medium. Moreover, in a token passing network, the token holder needs accurate information about its neighbors and thus of the network topology. Polling, on the other hand, is a more appealing MAC option for a wireless LANs since it offers centralized supervision of the network nodes. However, constant monitoring of all nodes is required, which is not feasible in the harsh fading environment of a wireless LAN (Wang, Y. and Obaidat, M. S., 2004), (Obaidat, M.S., and Green, D., 2003). Hence, we conclude that a protocol is needed for allocating bandwidth to MNs and MNs must themselves limit their send rate.

In reference (Nicopolitidis, P. et al., 2003), the authors propose a self-adaptive neural-based MAC protocol (SANP) for distributed wireless LANs. According to the proposed protocol, the mobile station that is granted permission to transmit is selected via a neural-based algorithm, which is used to train the system in order to adapt to the network traffic pattern. The neural-like training algorithm utilizes a probability distribution vector, which contains the choice probability for each mobile station in the network. The network feedback plays the role of the system tutor. Following the reception of the feedback after a packet transmission, the neural algorithm performs a simple training procedure in order to reach the goal of "learning" the transmission probabilities of the mobile stations. It was proved that the training algorithm asymptotically assigns to each station a portion of the bandwidth proportional to its needs.

As for the downstream transmission, the current Wireless LAN technology is not mature yet to provide good QoS guarantees. This is due to the high loss (high BER), low bandwidth, Doppler shift due to node's mobility, multiple path propagation, and poor bandwidth characteristic in Mobile IP wireless networks. Moreover, losses in wireless networks occur in bursts, which complicate matters further.

We observed from the experiments in scenarios 3 and 4 that CBQ works well when the total downstream traffic at FA does not exceed the total wireless link capacity. That is, while the amount of traffic goes into some classes do not exceed the allocated resources to the classes, the CBQ works well. From our experiments in scenarios 5 and 6, we observe that CBQ fails when the incoming traffic exceeds the total resources available. That is, CBQ, at least in the tested implementation, cannot deal efficiently with excessive traffic.

Resource reservation is required to ensure quality of data routing over the wireless link. Combined with resource reservation, Class-Based Queueing (CBQ) can provide sufficient QoS to downlink traffic for nodes that do not intentionally exceed their reserved capacity.

To sum up, in order to provide different Quality of Service to downstream traffic flows, it is not enough to have only CBQ implemented in FA. A protocol for wireless link resource reservation and cooperation by the senders are also needed. An example of such a protocol is the one we proposed in reference (Nicopolitidis, P. et al., 2003).

4.2 Jitter Characteristics Analysis

Due to the high loss, mobility and low bandwidth characteristics in Mobile IP wireless networks, QoS is especially difficult to achieve in wireless LANs (Obaidat, M.S., and Green, D., 2003), (Nicopolitidis, P. et al., 2002). From the experiments results, we can see network jitter can be controlled though CBQ queuing method for down link traffics, but it requires that the total data rate for the specific class be within the class capacity. For uplink network jitter control, there is no central control point (such as FA) to install any queuing method to control Mobile Nodes' access to the wireless network. From the experiment results, we can see if the total sending rate of all Mobile Nodes exceeds the wireless link capacity, then the packet loss is very large. To control jitter and packet loss rate, first of all, Mobile Nodes must self-limit the sending rate within the wireless link capacity. Secondly, better MAC layer controlling method for channel contention and collision detection must be used or developed.

From scenario 1 and scenario 2 for uplink stream data experiment results, we can see in general that when there is more traffic in the wireless link, the jitter will become higher. If there is no separate flow control mechanism for each MN, then their jitter values for UDP traffic are same. But surprisingly, when the amount of total traffic sending rate is much higher than the link capacity, the jitter for each data flow is not increasing much. The main reason for this is due to the fact that loss rate is very high in this case.

Mobile Nodes self-limit packet sending rate has significant effect on the QoS guarantee of the jitter, packet loss and link capacity usage. Token bucket can be used to control the packet sending rate and burst size, and leaky bucket can be used to shape the traffic. By using both, Mobile Nodes can effectively control their packets' sending. However, more importantly, MAC layer must have advanced collision detect method to control Mobile Nodes contention for the channel. With current IEEE standard 802.11 for wireless LAN, Media Access Control (MAC) layer uses Carrier-sense multiple access/collision avoidance (CSMA/CA) for collision avoidance. Wireless LANs also use channel reservation techniques by exchanging short "request-to-send" (RTS) and "clear-to-send" (CTS) control packets before the data packet is sent (Wang, Y. and Obaidat, M. S., 2004), (IEEE Standards, 1997). Two major factors affecting the throughput performance in the IEEE 802.11 MAC protocol are transmission failure and the idle slots due to backoff at each contention period (Kwon, Y. et al., 2003). This protocol is prone to inefficiencies at heavy loads because of higher waste of bandwidth from collisions and backoffs when traffic increases.

To avoid Mobile Nodes from competing for the wireless link resource and control the total traffic rate within the wireless link capacity, we suggest using capacity reservation method. A simple capacity reservation and cancellation protocol is outlined in (Wang, Y. and Obaidat, M. S., 2004), (Wang, Y. and Obaidat, M. S., 2004). Foreign Agent (FA) will be the central control point to maintain the reservation and monitor the traffics. According to the reservation, each Mobile Node limits its traffic rate. When the total traffic sending rate is within the link capacity, we see from our experiments that jitter can be controlled at a constant level.

We observed from scenarios 3 and 4 that network's jitter can be controlled to different levels by the DiffServ flow control mechanism. With CBQ, jitter can be controlled to a constant level as long as the total traffic rate is within the class capacity. If the traffic exceeds the class capacity, then jitter cannot be guaranteed to be at a certain level. It varies according to the total traffic load of the wireless link.

From these experiments, we see that at least one way we can use to control network's jitter; it is to use CBQ method though designing suitable classes for traffic flows and controlling which class each traffic flow goes to. For example, for important real-time traffic, we can let it go to the class with the high link capacity, while for datagram traffic; we can let it go to the class with low link capacity.

It is worth mentioning that in our experiment, we have used static link capacity reservation by giving different fixed weight to each defined class with CBQ. There are some other ways to dividing link capacity, such as dynamic capacity reservation (Braden, R., et al., 1997) and no capacity reservation (Kilkki, K., 1999). Further research is needed in how to use different link capacity reservation schemes to provide QoS guarantees for wireless Mobile IP networks.

From scenarios 5 and 6 experimental results, we observe that high loss rate of traffic (maximum up to 100%) has made jitter characteristic meaningless. Thus, controlling of the loss rate becomes the first priority. CBQ failed to provide QoS guarantee for the downlink traffics. Thus some better mechanism for controlling wireless network access should be provided.

We can conclude that with current 802.11 MAC layer collision control method, resource reservation is required to assure quality of data routing over the wireless link. With resource reservation, we can make sure that the total traffic that goes through the wireless link is within the resources available. Combined with resource reservation, CBQ can provide sufficient QoS to downlink traffic for nodes that do not intentionally exceed their reserved capacity and jitter can be controlled to a guaranteed level. For uplink traffic, self-limit traffic sending rate together with resource reservation can be used to provide sufficient QoS control, and thus jitter can be controlled to a guaranteed level.

5 CONCLUSIONS

To conclude, loss rate is an essential parameter for providing guaranteed service over wireless links. We observed from the experiments presented in scenarios 1 to 6 that the amount of data sent by Mobile Nodes (MNs) is directly related to the packet loss rate. If MNs send more packets than the wireless link resource capacity, then packet loss rate will increase dramatically. To limit the loss rate, we concluded from the upstream sending and down-stream receiving tests that a protocol for allocating resources for MNs is needed. Moreover, MNs must self limit transmission rate according to the reserved capacity. Clearly, a protocol for wireless link resource reservation is needed. Example of such protocols is our recent work presented in reference (Nicopolitidis, P. et al., 2003). This makes the amount of packets sent and received by MNs not exceed the available wireless link resource limit.

In this paper, we also identify the relationship of network jitter and packet sending rate in the wireless Mobile IP networks. The downlink jitter can be controlled with DiffServ flow control mechanism by using CBQ, but it requires that the total traffic rate be within the limit of the wireless link capacity. We propose the use of resource reservation for the wireless link access for both downstream and upstream directions based on the experimental results. In both directions, a Mobile Node should request a reservation from the Foreign Agent, which must keep track of the reservations and enforce them by dropping excess data. The experience and measured results from these experiments were instrumental in identifying the problem areas and the most viable solutions.

ACKNOWLEDGMENTS

The second author would like to thank Helsinki University of Technology Telecommunication and Multimedia lab for the partial support of this work.

REFERENCES

P. Nicopolitidis, M. S. Obaidat, G. I. Papadimitriou and A. S. Pomportsis, Wireless Networks, John Wiley and Sons Ltd., 2003.

M.S. Obaidat and D. Green, "Simulation of Wireless Networks," in Applied Systems Simulation: Methodologies and Applications (M.S. Obaidat and G.I. Papadimitriou, (Eds.), Kluwer, 2003.

P.Nicopolitidis, G.I. Papadimitriou, A.S. Pomports and M.S. Obaidat,' "Self-Adaptive Polling Protocols for Wireless LANs: A Learning-Automata-Based Approach", Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, pp. 3870-3875, Washington DC, October 2003.

G.I. Papadimitriou, M.S. Obaidat, and A.S. Pomportsis, "On the Use of Learning Automata in the Control of Broadcast Network: A Methodology," IEEE Transaction on Systems, Man and Cybernetics-Part B, Vol. 32, No. 6, pp. 781-790, December 2002.

P. Nicopolitidis, M.S. Obaidat, G.I. Papadimitriou and A.S.Pomportsis, "TRAP: a high performance protocol for wireless local area networks", Computer Communications, Elsevier, Vol. 25, July 2002, pp. 1058-1065.

D. Green and M.S. Obaidat, "Dynamic Waveform-Power Adaptation in Mobile 802.11 Wireless LANs," Proceedings of the 2003 International Symposium on Performance Evaluation of Computer and Telecommunication Systems, SPECTS2003, pp. 116-121, Montréal, Canada, July 2003.

Chang-Jia Wang, Liang-Seng Koh, Chao-Hui Wu, and Ming T. Liu, "A Multimedia Synchronization Protocol for ATM Networks", Proc. Intl. Conf. on Distributed Computing Systems, pp. 476-483, Posman, Poland, Jun 1994.

H. Le Pocher, V.C.M. Leung and D. Gillies, "Explicit Delay/Jitter Bounds for Real-time Traffic over Wireless ATM", Computer Networks, Vol. 31, Vo. 9-10, pp. 1029-1048, May 1999.

S. Varma, "MPEG-2 Over ATM: System Design Issues", Proc.COMPCON'96, pp. 26-31, 1996.

D.J Wright, "Voice over ATM: An Evaluation of Implementation Alternatives", IEEE Communication Magazine, Vol. 34, No. 5, pp.72-80, May 1996.

Sally Floyd and Van Jacobson, "Link-sharing and Resource Management Models for Packet Networks", IEEE/ACM Transactions on Networking, 3:365-386, August 1995.

Mediapoli network, 2000. http://www.mediapoli.com.

The Dynamics - HUT Mobile IP System, Helsinki University of Technology, 2000. http://www.cs.hut.fi/Research/Dynamics/.

Mark Gates and Alex Warshavsky, " Iperf version 1.1.1," February 2000. http://dast.nlanr.net/.

Y. Wang, and M. S. Obaidat "An Experimental Analysis Study of Loss Rate in Wireless Mobile IP Systems," Proc. of Applied Telecommunication Sym-posium, ATS2004, pp. 12-17, April 2004 .

Federico Cali, Marco Conti, and Enrico Gregori, "IEEE 802.11 Protocol: Design and Performance Evaluation of an Adaptive Backoff Mechanism," IEEE JSAC, Vol. 18, no. 9, pp. 1774-1786, September 2000.

Younggoo Kwon, Yuguang Fang and Haniph Latchman, "A Novel MAC Protocol with Fast Collision Resolution for Wireless LANs," Proc. of Infocom, 2003. http://www.ieee-infocom.org/2003/papers/21_03.PDF

A. Claessen, L. Monteban, and H. Moelard, "The AT&T GIS WaveLAN Air Interface and Protocol Stack," Proceedings of the 5th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'94), 1994.

George Xylomenos and George C. Polyzos, "Internet Protocol Performance Over Networks with Wireless Links, "IEEE Network, pp. 55-63, July/August 1999.

G.T. Nguyen, R.H. Katz, B.D. Noble, and M. Satyanarayanan, "A Trace-based Approach for Modeling Wireless Channel Behavior, Proc. Winter Simulation Conference, pp. 597-604, Dec. 1996.

IEEE Standards Department, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE standard 802.11-1997,1997.

22 Robert Braden, Lixia Zhang, Steve Berson, Shai Herzog, and Sugih Jamin, "Resource reservation protocol (RSVP)". RFC 2205, IETF Network Working Group, September 1997.

Kalevi Kilkki, "Differentiated Services for the Internet", Chapter 5.2, pp. 151-155, Macmillan Technical Publishing, 1999.

Y. Wang, and M.S. Obaidat "A Performance Evaluation Study of Jitter Characteristics in Wireless Networks," Proc. of the 2004 Symposium on Performance Evaluation of Computer Systems and Networks, SPECTS2004, pp. 231-237, July 2004.

ON THE SURVIVABILITY OF WDM OPTICAL NETWORKS

Yuanqiu Luo, Pitipatana Sakarindr and Nirwan Ansari
Advanced Networking Laboratory, Department of Electrical and Computer Engineering,
New Jersey Institute of Technology, University Heights, Newark, NJ 07102, USA
Email: yl6@njit.edu, ps6@njit.edu, ansari@njit.edu

Keywords: Wavelength division multiplexing (WDM), Network survivability.

Abstract: At a high speed of a few gigabits per second per wavelength, the *wavelength division multiplexing* (WDM) optical networks offer the capacity of several Terabits per second. More bandwidth in each optical channel means more serious loss each time a failure occurs. Therefore, network survivability is a crucial required provision in WDM optical networks. Survivability is the ability of the network to withstand network failures. Many schemes have been proposed to realize the reliable transmission against network failures. This chapter provides an overview of the survivability issue along with the recently developed solutions in WDM optical networks. We classify these schemes based on their optimization objectives, discuss the schemes in each class, compare their strengths and weaknesses, and present the possible future research issues for survivable WDM optical networks.

1 INTRODUCTION

The explosive growth of data traffic poses important emerging bandwidth requirements on today's networks. The large bandwidth of optical fibres in the order of Terabits per second has made the fibres attractive for high-speed networks. The *wavelength division multiplexing* (WDM) technology is playing a major role in the expansion of our networks by dividing the voluminous bandwidth of a fibre into many wavelengths, with each wavelength offering the capacity of a few gigabits per second. As a result of the high volume traffic carried by WDM optical networks, any node or link failure may have severe consequences and could significantly downgrade the services to the worst extent. This is the reason why network survivability is clearly critical to WDM optical networks.

Survivability refers to the network ability to reconfigure or reestablish the traffic transmission upon any failure. The node failure can be a result of the failure of network components such as wavelength cross-connects (WXCs), wavelength transmitters and receivers. The most common link failure is the fibre cut, which may result from the accidental disruption of cables such as construction works, fires, quakes, or even human errors (Ellinas, 2000). Note that a node failure can be decomposed into failures of the links connected to that node, and multiple link failures can be decoupled into several single link failures; most published research as well as this chapter focuses on the single link failure. Many solutions with a variety of optimization criteria have been proposed recently. WDM network survivability issue can be studied from different perspectives, as summarized in Section 2. Our major focus is to classify the representative survivability solutions into three types based on different optimization objectives, and compare their pros and cons as discussed Sections 3, 4, and 5, respectively. The feasible future research directions are proposed in Section 6, and the conclusions are given in Section 7.

2 SURVIVABILITY PERSPECTIVES

Many paradigms have been explored for the optical network survivability. The recovery schemes can be grouped into several types from different viewpoints. This section briefly describes the WDM network recovery schemes from different perspectives. Their performance comparison is also summarized in Table 1.

J. Ascenso et al. (eds.), e-Business and Telecommunication Networks, 31–40.

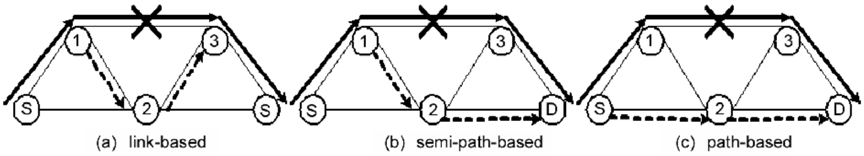


Figure 1: Link-based *vs.* semi-path-based *vs.* path-based recovery schemes.

2.1 Protection *vs.* Restoration

From the viewpoint of resource reservation, existing recovery schemes can be classified as *protection* and *restoration*. In protection schemes, the spare (backup) capacity is reserved during the connection setup and the OXCs and switches are preconfigured. Therefore, the disrupted traffic can be switched to the backup paths (links) as soon as the failure is detected. In restoration schemes, the available spare capacity is allocated to a specific traffic after a failure occurs. While the restoration schemes are more efficient in capacity utilization due to the dynamic sharing of the spare resource, the protection schemes are faster and simpler without additional communications overhead.

2.2 Static Traffic Recovery *vs.* Dynamic Traffic Recovery

Based on the traffic pattern in the network, the recovery schemes can be classified as static and dynamic traffic recovery. In the former, the set of connections is given *a priori*. The recovery schemes configure network equipment and fibre links to minimize the required network resource while providing the recovery against network failures. In the latter, since the traffic changes dynamically, the network configuration should be modified from time to time. To avoid oscillation, a threshold is set to trigger the reconfiguration only when the traffic changes drastically, especially when a network failure occurs. Unlike the static recovery in which the configuration can be done off-line, the dynamic recovery scheme requires fast computation to be done on-line.

2.3 Centralized *vs.* Distributed

From the viewpoint of route computation and fault management mechanisms, there are essentially two paradigms: centralized *vs.* distributed. Centralized recovery schemes depend on the central controller to compute the backup lightpaths and to make the recovery decision based on the up-to-date global network information. Frequent communications between each node and the central controller are required to maintain the accurate link state information. In contrast, distributed recovery schemes make the recovery decision locally. Without the global signalling overhead, the recovery speed is fast. However, each node only has the local information, thus maybe leading to inefficient resource utilization.

2.4 Link-based, Semi-path-based, and Path-based Recovery

Based on the rerouting configuration, the recovery schemes can be grouped as the link, semi-path, and path-based schemes as shown in Figure 1. In the link-based recovery, the single link failure is recovered locally by rerouting traffic around the failed link. Since link recovery is not dependent on specific traffic patterns, it can be preplanned, and therefore fast recovery time can be achieved. In contrast, the failure can be recovered globally by the path recovery. The traffics in the failed link are recovered on an end-to-end basis. All the source-destination nodes of the traffic traversing the failed link reroute the traffic separately and independently. The path recovery scheme requires the involvement of many more nodes and the global network resource information, thus requiring high communications overheads. The semi-path-based scheme is similar to the path-based scheme, except that the disconnected traffic is rerouted from the upstream node of the failed link instead of the source node. Without cranking back to the source node, the semi-path-based scheme has the recovery speed comparable to the link-based scheme.

Table 1: Performance comparison of different recovery perspectives.

Perspective	Type	Recovery Time	Communications Overhead	Resource Utilization Efficiency
Rerouting	Link-based	Fast	Low	High
	Semi-path-based	Medium	Medium	Medium/High
	Path-based	Slow	High	Low
Resource Sharing	Shared	Fast	High	High
	Dedicated	Slow	Low	Low
Fault Management	Centralized	Fast	High	High
	Distributed	Slow	Low	Low
Resource Reservation	Protection	Fast	Low	Low/Medium
	Restoration	Slow/Medium	High	Medium/High
Traffic Pattern	Static-traffic	Fast	Low/Medium	Low/Medium
	Dynamic-traffic	Slow	High	Medium/High

2.5 Shared *vs*. Dedicated Recovery

The recoveries can also be grouped from the viewpoint of resource sharing. In the dedicated recovery scheme, the backup resource is dedicated for a specific primary path (link), and cannot be shared with other backup resource. For shared recovery, several primary paths (links) could share the same backup resource as long as they are disjoint and the failures will not occur simultaneously. Such a sharing results in more efficient resource utilization.

Table 1 summarizes the qualitative performance comparison among different recovery perspectives. In the WDM networks, a particular recovery scheme is essentially a combination of different perspectives. For example, the recovery scheme in reference (Crochat, 1998) is a centralized link protection scheme, and thus it has the properties of fast recovery but with a relatively high communications overhead.

The problem of survivability is basically to optimize the spare network resource in order to realize the reliable functionality against network failures. Therefore, in this chapter, we adopt a new perspective, i.e., the optimization objective, to categorize the survivability schemes into three major classes as design, resource, and traffic optimization recovery schemes. The design optimization recovery is defined as follows: given the network resource and the physical network topology, find the best logical topology that is "immune" from failures, i.e., the logical topology is connected in the event of a single link failure. The resource optimization recovery is defined as follows: given the network topology, find the least network resource required to configure a survivable network against network failures. The resource can be wavelengths, fibres, or wavelength converters. The traffic optimization recovery is defined as follows: given the network topology and specific network resource, find the most guaranteed traffic load or the balanced traffic distribution against failures. Section 3, 4, and 5 will discuss each category one by one. The comparison of strengths and weaknesses among these schemes are summarized in Table 2.

3 DESIGN OPTIMIZATION RECOVERY

We discuss the problems and solutions of the design optimization recovery in this section. Schemes are referred by the authors' names.

The Crochat-Le Boudec scheme (Crochat, 1998) —This scheme optimizes the mapping between the virtual topology and the physical topology to guarantee that each virtual link is independent of others, and no two virtual links share the same physical link. The proposed *disjoint alternate path* (DAP) algorithm maps the virtual topology in such a way that, each virtual link has an alternate virtual path, which shares no physical link with the virtual link itself. In fact, there is a hidden dependency between lightpaths in the virtual topology so that each link is not independent of each other in the physical topology. By deleting the hidden dependencies between primary and backup lightpaths, the DAP algorithm guarantees that when a single link failure occurs, any lightpath can always be recovered by using its predetermined backup lightpath. The complexity is $O(n^4)$, where n is the number of nodes. The studies in (Crochat, 2000) and (Nucci, 2004) extend DAP with the wavelength capacity constraint, and logical topology optimization, respectively. Some of the drawbacks include: first, wavelength converters must be deployed in all nodes; second, the deployed shortest paths may cause an uneven traffic load distribution.

The Modiano-Narula-Tam scheme (Modiano, 2002)—Based on Menger's Theorem, a topology is 2-connected (i.e., redundant) *iff* every cut of the topology has a cut-set size of no less than two, in which a *cut* is a partition of the set of nodes into two subsets. The edges connecting those two subsets in a cut is called a *cut-set*. The number of edges in a cut-set is the *cut-set size*. The authors proposed the necessary condition for network routing survivability, i.e., none of the physical links are shared by all lightpaths in a cut-set so that any single link failure does not cause a cut disconnected. Based on such condition, a set of integer linear programming (ILP) formulations is presented to solve the following problem: given a physical topology G and the corresponding lightpath requirement matrix X, find the logical topology to route the lightpaths such that the lightpaths are survivable in the event of a single link failure. The applied constraints include lightpath connectivity, lightpath survivability, and physical link capacity. The ILP is further relaxed by enforcing single node to reduce the number of lightpath survivability constraints to n, where n is the number of nodes. Such a relaxation works better as the physical topology becomes denser. Built upon this necessary condition, the authors developed the lower bound on the number of links a physical topology must contain to support lightpath survivability (Narula-Tam, 2004).

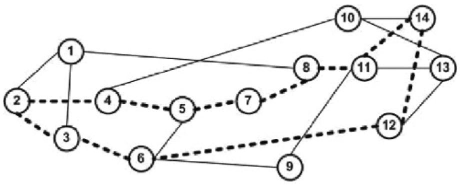


Figure 2: An example of *p-cycle*. Cycle (2, 4, 5, 7, 8, 11, 14, 12, 6, 3, 2) with dotted lines shows an example of the *p-cycle* in the NSFNET.

The Stamatelakis-Grover scheme (Stamatelakis, 2000)—*Stamatelakis* and *Grover* introduced the preconfigured cycles (*p-cycles*) for the survivable network design. *p-cycles* are formed prior to any failure by assigning closed paths in the spare capacity. If a single link in the *p-cycle* fails (called the *on-cycle failure*, e.g., the failure of link (2,4) in Figure 2), the left links in the *p-cycle* form a protection path around that link, exactly working like the rings in SONET. This scheme is particularly effective in mitigating the *straddling* failure (a link which does not belong to the *p-cycle* but its two end nodes that are in the *p-cycle* fails, e.g., the failure of link (5,6) in Figure 2). The *p-cycle* has two restoration paths for a straddling failure. Formed into a closed path, the *p-cycle* provides the recovery speed of rings since each failure only includes the two nodes of the failed link for the recovery operation. By using the spare capacity, the *p-cycle* offers higher capacity utilization since each *p-cycle* contributes to the restoration of more single link failures than a ring. The *p-cycle* approach is in effect a hybrid ring scheme, mixing path restoration for the *straddling* failure with ring recovery for the *on-cycle* failure.

The Medard et al. scheme (Medard, 2002)—The idea of loop-back recovery is realized by assigning two digraphs (directed graphs) for an optical network. The primary digraph is backed up by the secondary digraph. Upon the failure of a link in the primary digraph, the disconnected traffic is carried using the secondary digraph by loop-back. Given an edge-redundant undirected graph $G(N, E)$, this scheme constructs a directed spanning subgraph $B = (N, A)$ and its reversal $R = \underline{B} = (N, \underline{A})$, where each link $a \in A$ in B is reversed to link $\underline{a \in A}$ in R. Since B and R are connected, respectively, there exists a directed path in both of them for each pair of nodes. Each of the two conjugated digraphs, B and R, could provide the primary working paths, with the other offering the backup capacity. When a link fails, the disconnected traffic loops back in the secondary digraph to travel around that link.

The Ellinas et al. scheme (Ellinas, 2000)—*Ellinas et al.* proposed the *protection cycle*s for any link failure in a 2-connected digraph. The scheme sets up a double-cycle ring coverage for network G, so that each edge is covered by two cycles. Each cycle works as a primary or a secondary ring. When a link fails, the *automatic protection switching* (APS) mechanism switches the affected traffic into the secondary cycle. The set of the secondary cycles is referred to as the *protection cycle*. For a planar network, *protection cycle* is created by embedding the graph G in the plane and assigning certain directions for the faces. For a non-planar network, *protection cycle* is created by the heuristic *orientable cycle double cover* (OCDC) algorithm. The OCDC algorithm starts at an arbitrary node by adding outgoing edges that satisfy the double-cycle coverage constraint; all of the edges could be covered twice by two different cycles. The APS mechanism is implemented with the cooperation of protection fibres and protection switches. When a fibre link fails, the failure is detected and the protection switches switch the traffic from the primary fibre to the protection fibre. Since only the end nodes of the failed link are involved in traffic switching, *protection cycles* can be configured distributively to improve the recovery speed.

Summary—The *Crochat-Le Boudec* scheme employs DAP to ensure the network connectivity after a failure occurs. It may yield low performance in large networks due to its high complexity. Unlike the *Crochat-Le Boudec* scheme that uses the Tabu search, the *Modiano-Narula-Tam* scheme formulates the network survivability problem by ILP. It provides the optimal solution for various network topologies. The *p-cycles* in the *Stamatelakis-Grover* scheme are a hybrid approach, which combines path restoration and ring protection. It offers a solution with the ring-like recovery speed and the mesh-like bandwidth efficiency. The *Medard et al*. scheme offers a polynomial time solution based on the generalized loop-back, and is applicable for different network topologies, such as planar, non-planar, and Eulerian networks. On the other hand, the *Ellinas et al*. scheme offers a double cycle cover mechanism, which provides a polynomial time solution for planar networks.

4 RESOURCE OPTIMIZATION RECOVERY

In this section, we discuss the recovery schemes for WDM optical networks that optimize network resource utilization. Such a problem is defined as finding the least network resource assignment against any single link failure for a given network *G*(*N*,E). The schemes are referred by the authors' names.

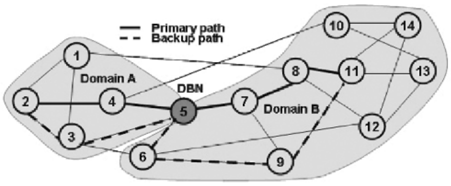


Figure 3: An example of the *Ou et al.* scheme. Lightpath (2, 4, 5, 7, 8, 11) is divided into two primary subpaths (2, 4, 5) and (5, 7, 8, 11) by Domain A and B, respectively. Backup subpath (2, 3, 5) is for primary subpath (2, 4, 5), and backup subpath (5, 6, 9, 11) is for primary subpath (5, 7, 8, 11), respectively.

The Ou et al. scheme (Ou, 2004)—*Ou et al.* proposed to divide an optical network into domains, and a lightpath is thus cut into several subpaths. The shared path protection (SPP) algorithm is then adopted in each domain to provide the least-cost backup subpath for the primary subpath. Two constraints are applied: first, the primary and backup subpaths of an inter-domain lightpath must exit or enter any domain at the same domain-border node (DBN); second, the primary and backup subpaths of an intra-domain lightpath can only use the resource in the same domain. The resource of subpaths is optimized by maximizing backup resource sharing. When a failure occurs, traffic is switched within a domain rather than the entire network, thus contributing to the fast recovery.

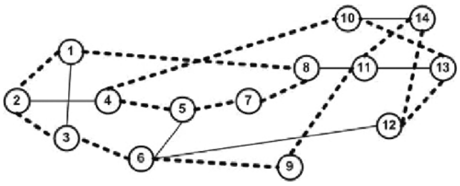


Figure 4: A Hamiltonian cycle with dotted lines in the NSFNET.

The Huang-Copeland scheme (Huang, 2002—A *Hamiltonian cycle* (HC) is a closed path which includes every node in the network exactly once. Figure 4 shows a HC in the NSFNET with dotted lines. Such a cycle is actually the spanning ring of the network. When a single link fails, its two end nodes switch the disconnected traffic to the HC. The network is by design always connected since a single link failure could only reduce the cycle into a spanning tree. Therefore, the HC guarantees the recovery of the network against any single link failure. Since a HC is a spanning ring of the network, it may have a wider recovery coverage than a *p-cycle*. For example, the single link failure of link (10,14) cannot be recovered by using the *p-cycle* in Figure 2. Such a failure can be protected by using the path (10,13,12,14) as shown in Figure 4. In order to cover all links, more than one *p-cycles* are needed while only one HC is enough, and assigning multiple *p-cycles* complicates the network management. The bottleneck for HC is that not every network contains a HC.

The Su-Su scheme (Su, 2001)—The authors proposed the ILP formulations for both off-line and on-line configuration restoration routing. The objective is to maximize the wavelength sharing among the protection paths. The "bucket"-based link metric is applied to measure the path "width", and they indicate the degree of resource sharing among different failures in a link and a path, respectively. The "bucket" is the number of protection wavelengths reserved in link *l* for the failure of link *k*. The wavelengths required being reserved in link *l* for any single link failure equal to the maximum bucket in that link. The "width" of link *l* is proportional to its reserved wavelengths *h*. When *h* = 0, link *l* is called "exhausted" since it does not reserve any wavelength for protection. The "width" of path *p* corresponding to the failure of link *k* is the minimum value of the link width in path *p*.

Maximizing resource sharing is achieved by choosing the widest path among all candidates. This widest path has the largest bucket, and thus the largest number of wavelengths could be shared for protection. The required new resource is minimized by assigning the least hop path as the primary path and the widest path as the protection path.

The Xu et al. scheme (Xu, 2003)—The proposed scheme adopts the shared risk link group (SRLG) information to strengthen the cross-layer protection in WDM networks. It separates an active path (AP) and backup path (BP) into several active segments (ASs) and backup segments (BSs), respectively. The goal is to protect each AS with its corresponding BS rather than to protect the whole AP. Different from the proposal in (Ou, 2004), overlapping links may exist among ASs. Resource sharing among BSs is maximized to achieve high efficiency. The ILP approach is practical for medium-size networks, and the dynamic programming (DP) approach yields the suboptimal results with polynomial time complexity for large networks. Interested readers are referred to (Lei, 2004), (Zang, 2003), and (Qin, 2003) for detailed discussions on cross-layer recovery.

The Ho-Mouftah scheme (Ho, 2004)—The proposed *optimal self-healing loop allocation* (OSHLA) algorithm dynamically selects cycles from a predefined cycle set to cover a given lightpath. Each cycle is assigned a cost based on its sharable capacity. Dijkstra's algorithm is then employed to find the best cycle allocation among different options, aiming to maximize spare capacity sharing. Because the cycle length dominates the computation complexity, proper cycle length limits for typical networks have been further developed from experiments, thus achieving a compromise between efficiency and complexity.

Summary—Generally, this group is developed from the design optimization recovery schemes with the focus on the network resource optimization. The *Ou et al.* scheme maximizes the backup resource sharing within domains. The Hamiltonian cycle scheme saves more resource than the *p-cycles* scheme by aggregating the backup capacity into a spanning ring with the least number of links. The *Su-Su* scheme applies the bucket model and the widest path to ensure that the reserved bandwidth can be maximally shared among multiple link failures as long as they do not occur simultaneously. The *Xu et al.* scheme protects several working segments instead of the whole working path, that results in higher resource sharing than traditional path-based recovery schemes. The *Ho-Mouftah* scheme enhances the SONET self-healing ring by accommodating on-line sharable resource information, and the employment of cycle length limit contributes to its on-line performance.

5 TRAFFIC OPTIMIZATION RECOVERY

The traffic optimization can be divided into two major types: balancing traffic load and maximizing carried traffic load. The two types of traffic optimization problems are closely related. From the point of traffic engineering, the traffic load can be balanced by selecting the link with a light load. By circumventing the heavily loaded links, the traffic blocking probability is reduced, and therefore the overall accepted traffic increases.

The Ruan et al. scheme (Ruan, 2004)—The proposed *routing with load balancing heuristics* (RLBH) algorithm adopts load balancing in restorable path computation. A pair of primary and backup paths is set up for a connection request, and the lighter-loaded links are preferred over the heavier-loaded ones. A *critical index* δ is employed as the threshold to specify the link cost. When the number of free channels over link l is more than δ, the corresponding link cost is set to 1; the link cost is set to ∞ if there are no free channels over link l; otherwise, a constant η ($\eta > 1$) is set as the link cost. When computing the backup path, RLBH prunes the links on the primary path, and prefers the links containing sharable backup channels. The Dijkstra's algorithm is then employed to find the least-cost path pair. RLBH needs the network status information to estimate the number of backup channels in a link, and thereby, *interior gateway protocol* (IGP) has been extended with signalling augment.

The Mohan et al. scheme (Mohan, 2001)—A dependable connection (D-connection), including the primary working and the corresponding back-up lightpath, is established upon a connection request. In order to maximize the number of carried D-connections, network resource multiplexing is employed to share links among lightpaths. Different from other proposals, besides resource sharing among backup lightpaths, this scheme also allows resource sharing among a primary and several backup lightpaths to carry more D-connections. The corresponding assumption is that no single link failure will cause two primary paths to compete for the same backup resource. The computational complexity is O(knw) when the two lightpaths in a D-connection use the same wavelength, and O(k2nw) when they use different wavelengths, where k is the predetermined maximum number of candidate routes for any node pair, n is the number of nodes, and w is the number of wavelengths per fibre.

The Sahasrabuddhe et al. scheme (Sahasrabuddhe, 2002)—The fault management mechanism is proposed to maximize the guaranteed traffic in a network. In the WDM layer, the modified path protection scheme configures a backup lightpath for each primary lightpath. In the IP layer, the modified restoration scheme also pre-configures the network so that the disconnected traffic can be rerouted over the spare capacity. These two schemes aim to maximize the scalar load factor, α. The whole network traffic variation is modeled as αT, where T is the traffic matrix. The larger the load factor, the more guaranteed traffic can be carried by the network. The heuristic algorithm maximizes α by iterating between two steps: step one attempts to free as many wavelengths and lightpaths as possible while maintaining the load in the maximally loaded link; step two attempts to set up as many guaranteed lightpaths among the freed resource as possible while decreasing the load in the maximally loaded link. To improve the efficiency, the shared-path protection is employed to allow resources shared among different backup lightpaths. The WDM layer shared-path protection offers more guaranteed traffic and much faster recovery time than those of the IP layer restoration, which takes longer time for processing link state updates and recomputing routing tables.

The Qiao-Xu scheme (Qiao, 2002)—The distributed partial information management (DPIM) algorithm protects the traffic from the link failure based on a shared path protection approach. It determines a pair of active path (AP) and backup path (BP) for each bandwidth-guaranteed connection to maximize the number of carried connections. The sum of active bandwidth (ABW) and backup bandwidth (BBW) allocated to all connections is called the total bandwidth (TBW). Each candidate link on a new connection distributedly estimates additional BBW, and the path assignment with the least BBW is selected. Besides connection establishment, DPIM takes connection release into consideration. The overhead of link state information distribution increases the accuracy of BBW estimation, thus maximizing the carried traffic load.

Summary—Load balancing is facilitated in the *Ruan et al.* scheme by directing new traffic to the lighter-loaded links, and the performance is determined by the threshold value δ. The *Mohan et al.* scheme maximizes the carried traffic (i.e., D-connections) by sharing spare wavelength channels among different backup lightpaths or among a primary lightpath and several backup lightpaths. The *Sahasrabuddhe et al.* scheme optimizes the guaranteed traffic and the recovery time by maximizing the *load factor*, α, and taking the advantage of the integration of IP restoration and WDM protection. The *Qiao-Xu* scheme maximizes the bandwidth-guaranteed traffic by configuring the shared protection paths based on the distributed information. Unlike the *Su-Su* scheme [8] that every edge node maintains partial and aggregated $O(E^2)$ network information, the *Qiao-Xu* scheme distributes information around the network, and the information maintained by each node is $O(E)$, where E is he number of links.

6 FUTURE DIRECTIONS

Future research of network survivability research should address the following issues.

6.1 Finer Granularity

Most of the design optimization recovery schemes in Section 3, 4, and 5 consider the recovery in the fibre granularity level, in which the traffic carried by a fibre is backed up by another fibre, and the number of available wavelengths is assumed sufficient for the sake of simplicity. All wavelengths in the backup fibre are reserved in advance or reconfigured in real time. Therefore, the wavelength utilization efficiency is significantly deteriorated. Finer granularity, such as wavelength, should be adopted to improve the efficiency. One possible solution could be extending the current schemes by designing the lightpaths in the wavelength-based layered graph (Luo, 2003) instead of the link-based graph.

Since the backup resource assignment is done in the wavelength level instead of the fibre level, less resource will be reserved, and thus more traffic could be carried.

6.2 Complexity Relaxation

The LP formulations are generally used to provide a mathematical formulation of the network survivability. Owing to the large number of constraints and the network size, solving such a set of formulations is time consuming. Thus, most of the schemes can only be implemented off-line, and appropriate heuristic algorithms are desperately needed to simplify the computation. LP relaxation (Krishnaswamy, 2001) and Lagrangian relaxation (Lee, 2004), (Zhang, 2004) could reduce the complexity. LP relaxation converts the LP problem into the ILP problem by quantizing continuous variables into discrete variables (integers). Branch and bound method is implemented into such a relaxed problem to search for the solution. Lagrangian relaxation approach decomposes the larger multiple constraint LP problem into smaller sub-problems. By relaxing wavelength-related constraints through the use of Lagrange multipliers,

Table 2: Strengths and weaknesses of the recovery schemes.

Note: C = Centralized, D = Distributed, L = Link-based, P = Path-based, R = Resource, DE = Design, T = Traffic

Algorithm	Fault Management	Rerouting strategy	Optimization Strategy	Strengths	Weaknesses
Crochat-Le Boudec (Crochat, 1998)	C	L	DE	• Guaranteed link failure recovery	• Unbalanced traffic load • Full-range wavelength converters are required
Modiano-Narula-Tam (Modiano, 2002)	C	L	DE	• Extendable for multiple failures	• Wavelength continuity and wavelength capacity are not taken into consideration
Stamatelakis –Grover (Stamatelakis, 2000)	C	L	DE	• Similar recovery speed to and higher utilization than rings	• More than one p-cycles are required to cover one network
Medard et al. (Medard, 2002)	C	L	DE	• Polynomial time complexity	• Full-range wavelength converters are required
Ellinas et al. (Ellinas, 2000)	D	L	DE	• High recovery speed	• Protection cycles may not be found in non-planar and Eulerian networks
Ou et al. (Ou, 2004)	D	P	R	• Scalable for large networks	• DBN must be capable of wavelength conversion
Huang-Copeland (Huang, 2002)	C	L	R	• Applicable for diverse traffic granularities	• A Hamiltonian cycle may not exist in an arbitrary network
Su-Su (Su, 2001)	D	P	R	• Balanced traffic load	• Needs to distribute information of wavelength availability
Xu et al. (Xu, 2003)	D	L	R	• Polynomial time complexity	• Wavelength continuity may not be satisfied among path segments
Ho-Mouftah (Ho, 2004)	C	P	R	• Variable loop size	• Needs signalling protocol extensions
Ruan et. al (Ruan, 2004)	D	P	T	• Balanced traffic load	• Full-range wavelength converters are required at all nodes
Mohan et al. (Mohan, 2001)	C	P	T	• Sharing resource among a primary and several backup lightpaths	• Low recovery efficiency
Sahasrabuddhe et al. (Sahasrabuddhe, 2002)	D	P	T	• Interoperability of multiple layers	• The IP restoration scheme may not find an optimal solution because of limited transceivers per node
Qiao-Xu (Qiao, 2002)	D	P	T	• Polynomial time complexity	• Needs accurate link state information

the total number of constraints is greatly reduced. The optimal Lagrange multipliers provide the best tradeoff between the recovery coverage and the resource utilization efficiency. Moreover, the relaxation process must ensure that the resulting solutions are also the solutions to the original unrelaxed problem.

6.3 Fault Recovery in Multifibre Networks

The real practice of installing bundles of multiple fibres motivates the research on the fault tolerance problem for multifibre optical networks. In such a network, a link between two nodes contains several fibres; each supports tens of wavelength channels. If the same wavelength on the next hop is not available, traffic can be switched to another fibre, where the same wavelength is unoccupied. An efficient way to analyze the survivability is based on the layered graph. With each edge representing a specific wavelength channel, and each layer representing the connections in one wavelength, the primary and backup lightpaths can be assigned simultaneously and optimized jointly. An important issue for survivable multifibre WDM networks is to determine whether the increased number of fibres trades off favourably with improved survivability. The research in (Luo, 2004) shows that multifibre WDM networks low the traffic blocking probability. Therefore, it is possible to use fewer wavelengths in each fibre with multiple fibres than with a single fibre to carry the same traffic load.

6.4 Multiple Failures Recovery

Most schemes tackle the single link failure in WDM optical networks. Such a single-link failure model assumes that at most one link can fail at any time, and failures do not occur simultaneously. When a link fails, all links that have failed earlier have been repaired (Mohan, 2001). In fact, with the growth of networks, multiple failures are possible. For example, a construction work may cut a buried optical cable, which has a bundle of fibres, thus leading to several link failures. Moreover, the time to repair a cable may be several hours or days. It is possible that another failure occurs during that interval. To recover multiple failures, the network must be configured with redundancy. In order to protect double failures, the graph must be 3-connected (i.e., it takes the removal of at least three links to disconnect the graph) (Choi, 2002), and several backup lightpaths for a primary lightpath have to be predetermined. Careful configuration of network spare resource must be done to ensure that even when multiple links fail, one in the primary working lightpath and another in the primary backup lightpath, the traffic can be continued through the secondary backup lightpath.

7 CONCLUSIONS

Survivability is a crucial network function for the high-speed WDM optical networks. It seeks to recover network failures by means of the efficient use of spare network resource. Based on different optimization criteria, the existing recovery schemes can be divided into three classes: design, resource, and traffic optimization recovery. Design optimization recovery schemes predesign the whole network and reserve the spare resource for the single fibre failure recovery. Since the network traffic matrix is unknown, such predesign is usually done at the fibre-based level. The design in the wavelength-based level should be employed in order to improve efficiency. Resource optimization recovery schemes minimize the resource used for failure recovery by sharing the spare resource among primary or backup lightpaths. Traffic optimization recovery schemes combine the failure recovery and the traffic engineering. In addition to the recovery provisioning, the carried traffic and load balancing among links are considered. The appropriate relaxation methods could simplify the complexity of the above optimization issues. We have summarized the evaluation of various schemes in Table II, and provided directions for future research on survivability of WDM optical networks.

REFERENCES

Choi, H., Subramaniam, S., and Choi, H.-A., 2002. On double-link failure recovery in WDM optical networks. *Proc. INFOCOM'2002*, vol. 2, pp. 808-816, 2002.

Crochat, O., and Le Boudec, J.-Y., 1998. Design protection for WDM optical networks. *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 7, pp. 1158-1165, Sep. 1998.

Crochat, O., Le Boudec, J.-Y., and Gerstel, O., 2000. Protection interoperability for WDM optical networks. *IEEE/ACM Transactions on Networking*, vol. 8, no. 3, pp. 384-395, June 2000.

Ellinas, G., Hailemariam, A., and Stern, T. E., 2000. Protection cycles in mesh WDM networks. *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 10, pp. 1924-1937, Oct. 2000.

Ho, P.H., and Mouftah, H.T., 2004. A novel survivable routing algorithm for shared segment protection in mesh WDM networks with partial wavelength conversion. *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 8, pp. 1548-1560, Oct. 2004.

Huang, H., and Copeland, J., 2002. A series of Hamiltonian cycle-based solutions to provide simple and scalable mesh optical network resilience. *IEEE Communications Magazine*, vol. 40, no. 11, pp. 46-51, Nov. 2002.

Krishnaswamy, R.M., and Sivarajan, K.N., 2001. Algorithms for routing and wavelength assignment based on solutions of LP-relaxations. *IEEE Communications Letters*, vol. 5, no. 10, pp. 435-437, Oct. 2001.

Lee, S.S. W., Yuang, M.C., Tien, P.L., and Lin, S.H., 2004. A Lagrangean relaxation-based approach for routing and wavelength assignment in multigranularity optical WDM networks. *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 9, pp. 1741-1751, Nov. 2004.

Lei, L., Liu, A., and Ji, Y., 2004. A joint resilience scheme with interlayer backup resource sharing in IP over WDM networks. *IEEE Communications Magazine*, vol. 42, no. 1, pp. 78-84, Jan. 2004.

Luo, Y., and Ansari, N., 2003. Performance evaluation of survivable multifibre WDM networks. *Proc. GLOBECOM'2003*, vol. 5, pp. 2524-2528, Dec. 2003.

Luo, Y., and Ansari, N., 2004. A computational model for estimating blocking probabilities of multifibre WDM optical networks. *IEEE Communications Letters*, vol. 8, no. 1, pp. 60-62, 2004.

Medard, M., Barry, R.A., Finn, S.G., He, W., and Lumetta, S.S., 2002. Generalized loop-back recovery in optical mesh networks. *IEEE/ACM Transactions on Networking*, vol. 10, no. 1, pp. 153-164, Feb 2002.

Modiano, E., and Narula-Tam, A., 2002. Survivable lightpath routing: a new approach to the design of WDM-based networks. *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 4, pp. 800-809, May 2002.

Mohan, G., Siva Ram Murthy, C., and Somani, A.K., 2001. Efficient algorithms for routing dependable connections in WDM optical networks. *IEEE/ACM Transactions on Networking*, vol. 9, no. 5, pp. 553-566, Oct. 2001.

Narula-Tam, A., Modiano, E., and Brzezinski, A., 2004. Physical topology design for survivable routing of logical rings in WDM-based networks. *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 8, pp. 1525-1538, Oct. 2004.

Nucci, A., Sansò, B., Crainic, T.G., Leonardi, E., and Marsan, M. A., 2004. On the design of fault-tolerant logical topologies in wavelength-routed packet networks. *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 9, pp. 1884-1894, Nov. 2004.

Ou, C.S., Zang, H., Singhal, N.K., Zhu, K., Sahasrabuddhe, L.H., MacDonald, R.A., and Mukherjee, B., 2004. Subpath protection for scalability and fast recovery in optical WDM mesh networks. *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 9, pp. 1859-1875, Nov. 2004.

Qiao, C., and Xu, D., 2002. Distributed partial information management (DPIM) schemes for survivable networks.1. *Proc. INFOCOM'2002*, vol. 1, pp. 302-311, 2002.

Qin, Y., Mason, L., and Jia, K., 2003. Study on a joint multiple layer restoration scheme for IP over WDM networks. *IEEE Network*, vol. 17, no. 2, pp. 43-48, Mar.-April 2003.

Ruan, L., Luo, H., and Liu, C., 2004. A dynamic routing algorithm with load balancing heuristics for restorable connections in WDM networks. *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 9, pp. 1823-1829, Nov. 2004.

Sahasrabuddhe, L., Ramamurthy, S., and Mukherjee, B., 2002. Fault management in IP-over-WDM networks: WDM protection versus IP restoration. *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 1, pp. 21-33, Jan. 2002.

Stamatelakis, D., and Grover, W.D., 2000. Theoretical underpinnings for the efficiency of restorable networks using preconfigured cycles ("p-cycels"). *IEEE Transactions on Communications*, vol. 48, no. 8, pp. 1262-1265, Aug. 2000.

Su, X., and Su, C.-F., 2001. An online distributed protection algorithm in WDM networks. *Proc. ICC'2001*, vol. 5, pp. 1571-1575, 2001.

Xu, D., Xiong, Y., Qiao, C., and Li , G., 2003. Trap avoidance and protection schemes in networks with shared risk link groups. *Journal of Lightwave Technology*, vol. 21, no. 11, pp. 2683-2693, Nov. 2003.

Zang, H., Ou, C., and Mukherjee, B., 2003. Path-protection routing and wavelength assignment (RWA) in WDM mesh networks under duct-layer constraints. *IEEE/ACM Transactions on Networking*, vol. 11, no. 2, pp. 248-258, April 2003.

Zhang, Y., Yang, O., and Liu, H., 2004. A Lagrangean relaxation and subgradient framework for the routing and wavelength assignment problem in WDM networks," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 9, pp. 1752-1765, Nov. 2004.

SIGMA: A TRANSPORT LAYER MOBILITY MANAGEMENT SCHEME FOR TERRESTRIAL AND SPACE NETWORKS[*]

Shaojian Fu and Mohammed Atiquzzaman
Telecommunications and Networks Research Lab
School of Computer Science, University of Oklahoma,
Norman, OK 73019-6151, USA
Email: {sfu,atiq}@ou.edu

Keywords: Internet Mobility, Mobility Management, Wireless Networks, Handoff management.

Abstract: Mobile IP has been developed to handle mobility of Internet hosts at the network layer. Mobile IP suffers from a number of drawbacks such as requirement of infrastructure change, high handover latency, high packet loss rate, and conflict with network security solutions. In this paper, we describe the architecture of Seamless IP diversity-based Generalized Mobility Architecture (SIGMA) - a new mobility management scheme. SIGMA utilizes IP diversity to achieve seamless handover, and is designed to solve many of the drawbacks of Mobile IP, including requirement for changes in infrastructure. The survivability and security of SIGMA is evaluated and shown that SIGMA has a higher survivability than Mobile IP - thanks to its centralized location management scheme. SIGMA can interoperate with existing network security infrastructures such as Ingress filtering and IPSec fairly easily. We also show the application of SIGMA to manage satellite handovers in space networks.

1 INTRODUCTION

Mobile IP (MIP) (Perkins, 2002; Perkins, 1998) has been designed to handle mobility of Internet hosts at the network layer. It allows a TCP connection to remain alive and receive packets when a Mobile Host (MH) moves from one point of attachment to another Several drawbacks exist when using MIP in a mobile computing environment, the most important ones identified to date are high handover latency, high packet loss rate (Malki, 2003), and requirement for change in Internet infrastructure. Mobile IP is based on the concept of Home Agent (HA) and Foreign Agent (FA) (which requires modification to existing routers in Internet) for routing packets from previous point of attachment to the new one. An MH needs to complete the following four steps before it can receive forwarded data from the previous point of attachment: (i) perform Layer 2 (L2) handover. (ii) discover the new Care of Address (CoA), (iii) register the new CoA with the HA, and (iv) forward packets from the HA to the current CoA. During this period, the MH is unable to send or receive packets through its previous or new point of attachment (Koodli, 2004), giving rise to a large handover latency and high packet loss rate.

MIP is known to have conflict with network security solutions (Perkins, 1998). Base MIP does not cooperate well when the HA is behind a firewall and the MH is outside the firewall, unless firewall transversal solution (Montenegro and Gupta, 1998) is used. Moreover, base MIP has difficulty in the presence of a foreign network which implements ingress filtering, unless reverse tunnelling, where the HA's IP address is used as the exit point of the tunnel, is used to send data from the MH.

1.1 Recent Research on Improving Mobile IP

Many improvements to Mobile IP have been proposed to reduce handover latency and packet loss. IP micromobility protocols like Hierarchical IP (Gustafsson et al., 2001), HAWAII (Ramjee et al., 1999) and Cellular IP (Cambell et al., 1999) use hierarchical foreign agents to reduce the frequency and latency of location updates by handling most of the handovers locally. Low latency Handoffs in Mobile IPv4 (Malki, 2003) uses pre-registrations and post-registrations which are based on utilizing link layer event triggers to reduce handover latency.

[*] The research reported in this paper was funded by NASA Grants NAG3-2528 and NAG3-2922.

J. Ascenso et al. (eds.), e-Business and Telecommunication Networks, 41–52.

Optimized smooth handoff (Perkins and Wang, 1999) not only uses a hierarchical FA structure, but also queues packets at the visited FA buffer and forward packets to MH's new location. To facilitate packet rerouting after handover and reduce packet losses, Jung et.al. (Jung et al., 2002) introduces a location database that maintains the time delay between the MH and the crossover node. Mobile Routing Table (MRT) has been introduced at the home and foreign agents in (Wu et al., 2002), and a packet forwarding scheme similar to (Perkins and Wang, 1999) is also used between FAs to reduce packet losses during handover. A reliable mobile multicast protocol (RMMP), proposed in (Liao et al., 2000), uses multicast to route data packets to adjacent subnets to ensure low packet loss rate during MH roaming. In (Fu and Atiquzzaman, 2003), Fu et al. use SCTP, a new transport layer protocol, to improve the performance of MIP by utilizing SCTP's unlimited SACK Gap Ack Blocks (Fu et al., 2005).

Mobile IPv6 (Johnson et al., 2004) removes the concept of FA to reduce the requirement on infrastructure support (only HA required). Route Optimization is built in as an integral part of Mobile IPv6 to reduce triangular routing encountered in MIPv4 (Johnson et al., 2004). Fast Handovers for Mobile IPv6 (FMIPv6) (Koodli, 2004), aims to reduce handover latency by configuring a new IP address before entering a new subnet. This results in a reduction in the time required to prepare for new data transmission; packet loss rate is thus expected to decrease. Like the Hierarchical IP in MIPv4, Hierarchical MIPv6 mobility management (HMIPv6) (Soliman et al., 2004) also introduces a hierarchy of mobile agents to reduce the registration latency and the possibility of an outdated Collocated CoA (CCOA). FMIPv6 and HMIPv6 can be used together, as suggested in (Soliman et al., 2004), to improve the performance further (in this paper, we refer to this combination as FHMIPv6). The combination of Fast Handover and HMIPv6 allows performance improvement by taking advantage of both hierarchial structure and link layer triggers. However, like FMIPv6, FHMIPv6 also relies heavily on accurate link layer information. MH's high movement speed or irregular movement pattern may reduce the performance gains of these protocols. Even with the above enhancements, Mobile IP still can not completely remove the latency resulting from the four handover steps mentioned earlier, resulting in a high packet loss rate (Hsieh and Seneviratne, 2003).

1.2 Motivation of SIGMA

As the amount of real-time traffic over wireless networks keeps growing, the deficiencies of the network layer based Mobile IP, in terms of latency and packet loss, becomes more obvious. The question that naturally arises is: Can we find an alternative approach to network layer based solution for mobility support? Since most of the applications in the Internet are end-to-end, a transport layer mobility solution would be a natural candidate for an alternative approach. A number of transport layer mobility protocols have been proposed in the context of TCP, for example, MSOCKS (Maltz and Bhagwat, 1998) and connection migration solution (Snoeren and Balakrishnan, 2000). These protocols implement mobility as an end-to-end service without the requirement to change the network layer infrastructures; they, however, do not aim to reduce the high latency and packet loss resulting from handovers. As a result, the handover latency for these schemes is in the scale of seconds.

Traditionally, various *diversity* techniques have been used extensively in wireless communications to combat channel fadings by finding independent communication paths at physical layer. Common diversity techniques include: space (or antenna) diversity, polarization diversity, frequency diversity, time diversity, and code diversity (Rappaport, 1996; Caire et al., 1998). Recently, increasing number of mobile nodes are equipped with multiple interfaces to take advantage of overlay networks (such as WLAN and GPRS) (Holzbock, 2003). The development of Software Radio technology (Glossner et al., 2003) also enables integration of multiple interfaces into a single network interface card. With the support of multiple IP addresses in one mobile host, a new form of diversity: *IP diversity* can be achieved. On the other hand, A new transport protocol proposed by IETF, called Stream Control Transmission Protocol (SCTP), has recently received much attention from the research community (Fu and Atiquzzaman, 2004). In the field of mobile and wireless communications, the performance of SCTP over wireless links (Fu et al., 2002), satellite networks (Fu et al., 2003; Atiquzzaman and Ivancic, 2003), and mobile ad-hoc networks (Ye et al., 2002) is being studied. Multihoming is a built-in feature of SCTP, which can be very useful in supporting IP diversity in mobile computing environments. Mobility protocols should be able to utilize these new hardware/software advances to improve handover performance.

The *objective* of this paper is to describe the architecture, survivability, and security of a new scheme for supporting low latency, low packet loss mobility management scheme called Transport Layer Seamless Handover (SIGMA). We also show the applicability of SIGMA to mange handoffs in space networks. Similar in principle to a number of recent transport layer handover schemes (Koh et al., 2004; Xing et al., 2002; Li, 2002), the basic idea of SIGMA is to decouple location management from data transfer, and achieve seamless handover by exploiting IP diversity to keep the old path alive during the process of setting up the new path during handover. Although we illustrate SIGMA using SCTP, it is important to note that SIGMA can be used with other transport layer protocols that support multihoming. It can also cooperate with IPv4 or IPv6 infrastructure without any support from Mobile IP.

1.3 Contributions of Current Research

The contributions of this paper are:

- Propose and develop transport layer based seamless handover (SIGMA). Here, "seamless" means low latency and low packet loss.
- Adapt SIGMA for satellite handovers in space networks.
- Evaluate the survivability and security of SIGMA, and compare with those of MIP.

1.4 Structure of this Paper

The rest of this paper is structured as follows: First, Sec. 2 describes the basic concept of SIGMA, including handover signalling procedures, timing diagram, and location management of SIGMA. We then apply the concept of SIGMA for satellite handovers in Sec. 3. The survivability and security issues of SIGMA are evaluated in Secs. 4 and 5, respectively. Finally, concluding remarks are presented in Sec. 6.

2 ARCHITECTURE OF SIGMA

In this section, we outline SIGMA's signalling procedure for mobility management in IP networks. The procedure can be divided into five parts which will be described below. The main idea of SIGMA is to decouple location management from data transfer, and achieve seamless handover by exploiting IP diversity to keep the old path alive during the process of setting up the new path during handover.

In this paper, we illustrate SIGMA using SCTP. SCTP's multi-homing allows an association between two end points to span multiple IP addresses or network interface cards. An example of SCTP multihoming is shown in Fig. 1, where both endpoints A and B have two interfaces bound to an SCTP association. The two end points are connected through two types of links: satellite at the top and ATM at the bottom. One of the links is designated as the primary while the other can be used as a backup link in the case of failure of the primary, or when the upper layer application explicitly requests the use of the backup.

A typical mobile handover in SIGMA, using SCTP as an illustration, is shown in Fig. 2, where MH is a multi-homed node connected to two wireless access networks. Correspondent node (CN) is a node sending traffic to MH, representing services like file download or web browsing by mobile users.

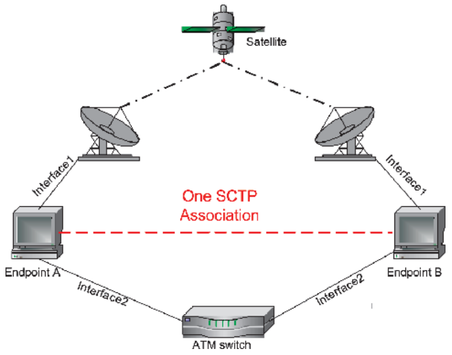


Figure 1: An SCTP association with multi-homed endpoints.

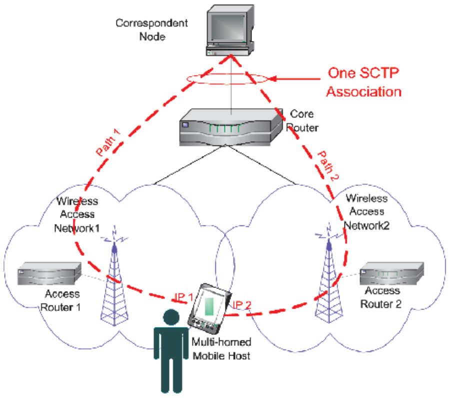


Figure 2: An SCTP association with multi-homed mobile host.

2.1 Handover Process

The handover process of SIGMA can be described by the following five steps.

STEP 1: Layer 2 handover and obtain new IP address

Refer to Fig. 2 as an example, the handover preparation procedure begins when MH moves into the overlapping radio coverage area of two adjacent subnets. In the state of the art mobile system technologies, when a mobile host changes its point of attachment to the network, it needs to perform a Layer

2 (data link layer) handover to cutoff the association with the old access point and re-associate with a new one. As an example, in IEEE802.11 WLAN infrastructure mode, this Layer 2 handover will require several steps: detection, probe, and authentication and reassociation with new AP. Only after these procedures have been finished, higher layer protocols can proceed with their signaling procedure, such as Layer 3 router advertisements. Once the MH finishes Layer 2 handover and receives the router advertisement from the new access router (AR2), it should begin to obtain a new IP address (IP2 in Fig. 2). This can be accomplished through several methods: DHCP, DHCPv6, or IPv6 stateless address auto-configuration (SAA) (Thomson and Narten, 1998).

STEP 2: Add IP addresses into the association

Initially, when the SCTP association is setup, only CN's IP address and MH's first IP address (IP1) are exchanged between CN and MH. After the MH obtained the IP address IP2 in STEP 1, MH should bind IP2 also into the association (in addition to IP1) and notify CN about the availability of the new IP address through SCTP Address Dynamic Reconfiguration option (Stewart et al., 2004). This option defines two new chunk types (ASCONF and ASCONF-ACK) and several parameter types (Add IP Address, Delete IP address, and Set Primary Address etc.).

STEP 3: Redirect data packets to new IP address

When MH moves further into the coverage area of wireless access network2, CN can redirect data traffic to new IP address IP2 to increase the possibility that data can be delivered successfully to the MH. This task can be accomplished by sending an ASCONF from MH to CN, through which CN set its primary destination address to MH's IP2. At the same time, MH need to modify its local routing table to make sure the future outgoing packets to CN using new path through AR2.

STEP 4: Update location manager (LM)

SIGMA supports location management by employing a location manager which maintains a database recording the correspondence between MH's identity and MH's current primary IP address. MH can use any unique information as its identity, such as home address (like MIP), or domain name, or a public key defined in Public Key Infrastructure (PKI).

Following our example, once MH decides to handover, it should update the LM's relevant entry with the new IP address, IP2. The purpose of this procedure is to ensure that after MH moves from wireless access network1 into network2, subsequent new association setup requests can be routed to MH's new IP address (IP2). Note that his update has no impact on the existing active associations.

We can observe an important *difference* between SIGMA and MIP: the location management and data traffic forwarding functions are coupled together in MIP, while in SIGMA they are decoupled to speedup handover and make the deployment more flexible.

STEP 5: Delete or deactivate obsolete IP address

When MH moves out of the coverage of wireless access network1, no *new* or *retransmitted* data should be directed to address IP1. In SIGMA, MH notifies CN that IP1 is out of service for data transmission by sending an ASCONF chunk to CN to delete IP1 from CN's available destination IP list.

A less aggressive way to prevent CN from sending data to IP1 is to let MH advertise a zero receiver window (corresponding to IP1) to CN. This will give CN an impression that the interface (on which IP1 is bound) buffer is full and can not receive data any more. By deactivating, instead of deleting, the IP address, SIGMA can adapt more gracefully to MH's zigzag movement patterns and reuse the previous obtained IP address (IP1) as long as the IP1's lifetime is not expired. This will reduce the latency and signalling traffic caused by obtaining a new IP address.

2.2 Timing Diagram of SIGMA

Figure. 3 summarizes the signalling sequences involved in SIGMA, the numbers before the events correspond to the step numbers in Sec. 2.1. Here we assume IPv6 SAA is used for MH to get new IP address. It should be noted that before the old IP is deleted at CN, it can receive data packets (not shown in the figure) in parallel with the exchange of signalling packets.

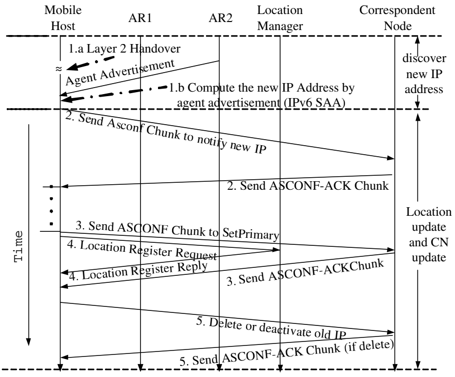

Mobile Host
AR1
AR2
Location Manager
Correspondent Node
1.a Layer 2 Handover
Agent Advertisement
1.b Compute the new IP Address by agent advertisement (IPv6 SAA)
discover new IP address
2. Send Asconf Chunk to notify new IP
2. Send ASCONF-ACK Chunk
3. Send ASCONF Chunk to SetPrimary
4. Location Register Request
4. Location Register Reply
3. Send ASCONF-ACKChunk
Location update and CN update
5. Delete or deactivate old IP
5. Send ASCONF-ACK Chunk (if delete)
Time

Figure 3: Timing diagram of SIGMA.

2.3 Location Management

As mentioned in STEP 4 of Sec. 2.1, SIGMA needs to setup a location manager for maintaining a database of the correspondence between MH's identity and its current primary IP address. Unlike MIP, the location

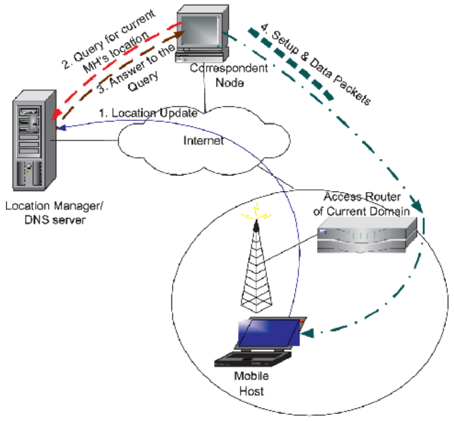


Figure 4: Location management in SIGMA.

manager in SIGMA is not restricted to the same subnet as MH's home network (in fact, SIGMA has no concept of home or foreign network). The location of the LM does not have impact on the handover performance of SIGMA. This will make the deployment of SIGMA much more flexible than MIP.

The location management can be done in the following sequence as shown in Fig. 4: (1) MH updates the location manager with the current primary IP address. (2) When CN wants to setup a new association with MH, CN sends a query to the location manager with MH's identity (home address, domain name, or public key, etc.) (3) Location manager replies to CN with the current primary IP address of MH. (4) CN sends an SCTP INIT chunk to MH's new primary IP address to setup the association.

If we use the domain name as MH's identity, we can merge the location manager into a DNS server. The idea of using a DNS server to locate mobile users can be traced back to (Awerbuch and Peleg, 1991). The advantage of this approach is its transparency to existing network applications that use domain name to IP address mapping. An Internet administrative domain can allocate one or more location servers for its registered mobile users. Compared to MIP's requirement that each subnet must have a location management entity (HA), SIGMA can reduce system complexity and operating cost significantly by not having such a requirement. Moreover, the survivability of the whole system will also be enhanced as discussed in Sec. 4.

3 SIGMA-SN: SIGMA IN SPACE NETWORKS

Spacecrafts, such as satellites, communicate among themselves and with ground stations on the earth to enable space communications. Depending on the altitude, satellites can be classified into three types: Low Earth Orbit (LEO), Medium Earth Orbit (MEO) and Geosynchronous Earth Orbit (GEO). GEO satellites are stationary with respect to earth, but LEO and MEO satellites move around the earth, and are handed over between ground stations as they pass over different areas of the earth. This is analogous to mobile computers being handed over between access points as the users move in a terrestrial network.

The National Aeronautics and Space Administration (NASA) has been studying the use of Internet protocols in spacecrafts for space communications (Bhasin and Hayden, 2002). For example, the Global Precipitation Measurement (GPM) project is studying the possible use of Internet technologies and protocols to support all aspects of data communication with spacecraft (Rash et al., 2002b). The Operating Missions as Nodes on the Internet (OMNI) (NASA, Hogie et al., 2001) project at GSFC is not only involved in prototyping, but is also testing and evaluating various IP-based approaches and solutions for space communications. Other efforts in using Internet protocols for space communications have also been reported in the literature (Minden et al., 2002).

Some of the NASA-led projects on IP in space involve handoffs in space networks. Such projects include OMNI (Hallahan, 2002; NASA,), Communication and Navigation Demonstration on Shuttle (CANDOS) mission (Hogie, 2002), and the GPM project (Rash et al., 2002a). NASA has also been working with Cisco on developing a Mobile router (Leung et al., 2001). It is also anticipated that MIP will play a major role in various space related NASA projects such as Advanced Aeronautics Transportation Technology (AATT), Weather Information Communication (WINCOMM) and Small Aircraft Transportation Systems (SATS) (Leung et al., 2001). In this section, we will investigate the use of SIGMA in space networks to support IP mobility. First, the scenarios of network layer handoffs in satellite environment is identified. Then we introduce SIGMA-SN — the mapping of SIGMA in space network.

3.1 Handoffs in a Satellite Environment

LEO satellites have some important advantages over GEO satellites for implementing IP in space. These include lower propagation delay, lower power requirements both on satellite and user terminal, more efficient spectrum allocation due to frequency reuse between satellites and spotbeams. However, due to the non-geostationary nature and fast movement of LEO satellites, the mobility management in LEO is much more challenging than in GEO or MEO.

If one of the communicating endpoint (either satellite or user terminal) changes its IP address due to the movement of satellite or mobile user, a network layer handoff is required to migrate the connection of higher level protocol (e.g. TCP, UDP, or SCTP) to the new IP address. We describe below two scenarios requiring network layer handoff in a satellite environment.

1. *Satellite as a router* (Fig. 5): When a satellite does not have any on-board equipment which generates or consumes data, but is only equipped with on-board IP routing devices, the satellite acts as a router in the Internet. Hosts are handed over from one satellite to another as the hosts come under the footprint of different satellites due to the rotation of the LEO satellites around the Earth. Referring to Fig. 5, the Fixed Host/Mobile Host (FH/MH) needs to maintain a continuous transport layer connection with the correspondent node (CN) while their attachment points change from Satellite A to satellite B. Different satellites, or even different spot-beams within a satellite, can be assigned with different IP subnet addresses. In such a case, IP address change occurs during an inter-satellite handoff, thus requiring a network layer handoff. For highly dense service areas, a spot-beam handoff may also require a network layer handoff. Previous research (Nguyen et al., 2001; Sarikaya and Tasaki, 2001) have used Mobile IPv6 to support mobility management in LEO systems, where the FH/MH and Location Manager are mapped to Mobile IP's Mobile Node and Home Agent, respectively.
2. *Satellite as a mobile host* (Fig. 6): When a satellite has on-board equipment (such as earth and space observing equipment) which generates data for transmission to workstations on Earth, or the satellite receives control signals from the control center, the satellite acts as the endpoint of the communication, as shown in Fig. 6. Although the satellite's footprint moves from ground station A to B, the satellite should maintain continuous transport layer connection with its corespondent node (CN). A network layer handoff has to be performed if the IP address of the satellite needs to be changed due to the handover between ground stations.

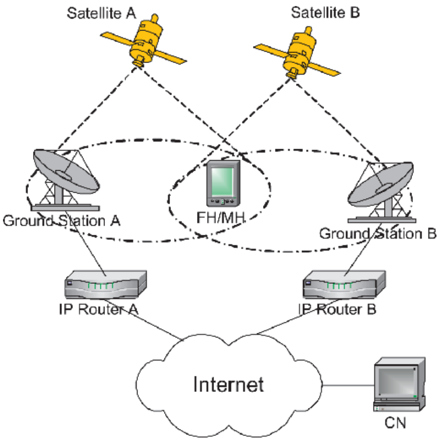


Figure 5: User handoff between satellites.

3.2 SIGMA-SN: Application of SIGMA in Space Networks

Having described our proposed SIGMA scheme and handoffs in space networks in Secs. 2 and 3.1, respectively, we describe below the mapping of SIGMA into a space handoff scenario, using satellites as examples of spacecrafts. We call this application and mapping of SIGMA to a space environment as SIGMA-SN.

1. *Satellite as a router:* Research results desribed in (Kwon and Sung, 2001) showed that the mean number of available satellites for a given FH/MH is at least two for latitudes less than 60 degrees. This means the FH/MH is within the footprint of two satellites most of the time, which makes SIGMA-SN very attractive for handoff management with a view to reducing packet loss and handoff latency. The procedure of applying SIGMA in this handoff scenario is straightforward; we just need to map the FH/MH and satellites in Fig. 5 to the MH and access routers, respectively, in the SIGMA scheme (see Fig. 2) as given below:
   - *Obtain new IP*: When FH/MH receives advertisement from Satellite B, it obtains a new IP address using either DHCP, DHCPv6, or IPv6 Stateless Address Autoconfiguration.
   - *Add new IP address to the association*: FH/MH binds the new IP address into the association (in addition to the IP address from Satellite A domain). FH/MH also notifies CN about the availability of the new IP address by sending an ASCONF chunk (Stewart et al., 2004) to the CN with the parameter type set as "Add IP Address".

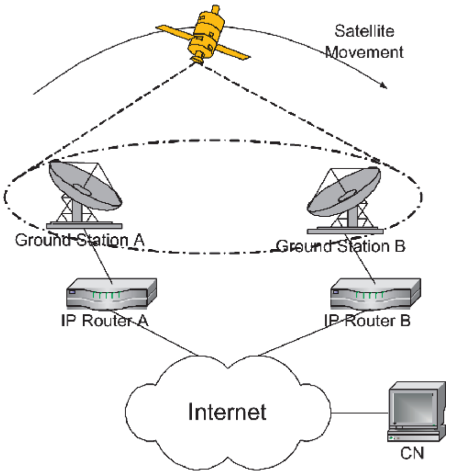


Figure 6: Satellite handoff between ground stations.

- *Redirect data packets to new IP address*: CN can redirect data traffic to the new IP address from Satellite B to increase the possibility of data being delivered successfully to the FH/MH. This task can be accomplished by sending an ASCONF chunk with the Set-Primary-Address parameter to CN, which results in CN setting its primary destination address to FH/MH as the new IP address.
- *Updating the Location manager*: `SIGMA-SN` supports location management by employing a location manager that maintains a database which records the correspondence between FH/MH's identity (such as domain name) and its current primary IP address. Once the Set-Primary-Address action is completed successfully, FH/MH updates the location manager's relevant entry with the new IP address. The purpose of this procedure is to ensure that after FH/MH moves from the footprint of Satellite A to that of Satellite B, further association setup requests can be routed to FH/MH's new IP address.
- *Delete or deactivate obsolete IP address*: When FH/MH moves out of the coverage of satellite A, FH/MH notifies CN that its IP address in Satellite A domain is no longer available for data transmission by sending an ASCONF chunk to CN with parameter type ”Delete IP Address”.

Due to the fixed movement track of the satellites in a space environment, FH/MH can predict the movement of Satellites A and B quite accurately. This a-priori information will be used to decide on the times to perform the set primary to the new IP address and delete the old IP address. This is much easier than in cellular networks, where the user mobility is hard to predict precisely.

2. *Satellite as a mobile host:* In this case, the satellite and IP Router A/B (see Fig. 6) will be mapped to the MH and access routers, respectively, of `SIGMA`. In order to apply `SIGMA-SN`, there is no special requirement on the Ground Stations A/B and IP routers A/B in Fig 6, which will ease the deployment of `SIGMA-SN` by not requiring any change to the current Internet infrastructure. Here, the procedure of applying `SIGMA-SN` is similar to the previous case (where the satellite acts as a router) if we replace the FH/MH by the satellite, in addition to replacing Satellites A/B by IP routers A/B.

   Since a satellite can predict its own movement track, it can contact Ground Station B while it is still connected to Ground Station A. There may be multiple new Ground Stations available to choose from due to the large footprint of satellites. The strategy for choosing a Ground Station can be influenced by several factors, such as highest signal strength, lowest traffic load, and longest remaining visibility period.

3.3 Vertical Handoff between Heterogeneous Technologies

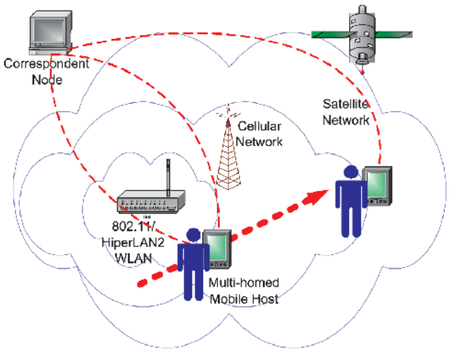


Figure 7: Vertical handoff using `SIGMA-SN`.

Different types of wireless access network technologies can be integrated to give mobile users a transparent view of the Internet. Handoff will no longer be limited to between two subnets in Wirless LAN (WLAN), or between two cells in a cellular network (horizontal handoff). In the future, mobile users will expect seamless handoff between heterogeneous access networks (vertical handoff), such as WLANs and cellular networks.

MIP operates in Layer 3 and is independent of the underlying access network technology. Although it can be used for handoffs in a heterogeneous environment, there are a number of disadvantages in using MIP for vertical handoffs (Dixit, 2002). The disadvantages include complexity in routing, high signaling overhead, significant delay especially when CN is located in foreign network, difficulty in integrating QoS protocols such as RSVP with triangular routing and tunnelling.

SIGMA-SN is well suited to meeting the requirements of vertical handoff. Figure 7 illustrates the use of SIGMA-SN to perform vertical handoffs from WLAN to a cellular network, and then to a satellite network. A multi-homed mobile host in SIGMA-SN is equipped with multiple interface cards that can bind IP addresses obtained from different kinds of wireless network access technologies.

4 SURVIVABILITY COMPARISON OF SIGMA AND MIP

In this section we discuss the survivability of MIP and SIGMA. We highlight the disadvantages of MIP in terms of survivability, and then discuss how those issues are taken care of in SIGMA.

4.1 Survivability of MIP

In MIP, the location database of all the mobile nodes are distributed across all the HAs scattered at different locations (home networks). According to principles of distributed computing, this approach appears to have good survivability. However, there are two major drawbacks to this distributed nature of location management as given below:

- If we examine the actual distribution of the mobile users' location information in the system, we can see that each user's location and account information can only be accessible through its HA; these information are not truly distributed to increase the survivability of the system. The transparent replication of the HA, if not impossible, is not an easy task as it involves extra signaling support as proposed in (Lin and Arul, 2003).
- Even if we replicate HA to another agent, these HAs have to be located in the home network of an MH in order to intercept the packets sent to the MH. The complete home network could be located in a hostile environment, such as a battlefield, where the possibility of all HAs being destroyed is still relatively high. In the case of failure of the home networks, all the MHs belonging to the home network would no longer be accessible.

4.2 Centralized Location Management of SIGMA offers Higher Survivability

Referring to Fig. 4, SIGMA uses a centralized location management approach. As discussed in Sec. 2.1, the location management and data traffic forwarding functions in SIGMA are decoupled, allowing it to overcome many of the drawbacks of MIP in terms of survivability (see Sec. 4.1) as given below:

- The LM uses a structure which is similar to a DNS server, or can be directly combined with a DNS server. It is, therefore, easy to replicate the Location Manager of SIGMA at distributed secure locations to improve survivability.
- Only location updates/queries need to be directed to the LM. Data traffic do not need to be intercepted and forwarded by the LM to the MH. Thus, the LM does not have to be located in a specific network to intercept data packets destined to a particular MH. It is possible to avoid physically locating the LM in a hostile environment; it can be located in a secure environment, making it highly available in the network.

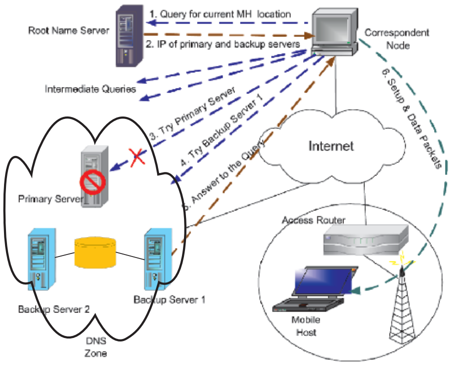


Figure 8: Survivability of SIGMA's location management.

Figure 8 illustrates the survivability of SIGMA's location management, implemented using DNS servers as location servers. Currently, there are 13 servers in the Internet (R. Bush et al., 2000) which constitute the root of the DNS name space hierarchy. There are also several delegated name servers in the DNS zone (Stevens, 1994), one of which is primary and the others are for backup and they share a common location database. If an MH's domain name belongs to this DNS zone, the MH is managed by the name servers in that zone. When the CN wishes to establish a connection with the MH, it first sends a request to one of the root name servers, which will direct the CN to query the intermediate name servers in the hierarchy. At last, CN obtains the IP addresses of the name servers in the DNS zone to which the MH belongs. The CN then tries to contact the primary name server to obtain MH's current location. If the primary server is down, CN drops the previous request and retries backup name server 1, and so on. When a backup server replies with the MH's current location, the CN sends a connection setup message to MH. There is an important difference between the concept of MH's DNS zone in SIGMA and MH's home network in MIP. The former is a logical or soft boundary defined by domain names while the latter is a hard boundary determined by IP routing infrastructure.

If special software is installed in the primary/backup name servers to constitute a high-availability cluster, the location lookup latency can be further reduced. During normal operation, heart beat signals are exchanged within the cluster. When the primary name server goes down, a backup name server automatically takes over the IP address of the primary server. A query requests from a CN is thus transparently routed to the backup server without any need for retransmission of the request from the CN.

Other benefits SIGMA's centralized location management over MIP's location management can be summarized as follows:

- *Security*: Storing user location information in a central secure database is much more secure than being scattered over various Home Agents located at different sub-networks (in the case of Mobile IP).

- *Scalability*: Location servers do not intervene with data forwarding task, which helps in adapting to the growth in the number of mobile users gracefully.

- *Manageability*: Centralized location management provides a mechanism for an organization/service provider to control user accesses from a single server.

5 SECURITY OF SIGMA

In this section, we discuss the security issues of SIGMA and its interoperability with the current security mechanisms of the Internet.

5.1 Interoperability between MIP and Ingress Filtering

Ingress filtering is widely used in the Internet to prevent IP spoofing and Denial of Service (DoS) attacks. Ingress filtering is performed by border routers to enforce topologically correct source IP address. Topological correctness requires MH to use COA as the source IP address, since the COA is topologically consistent with the current network of the MH. On the other hand, TCP keeps track of its internal session states between communicating endpoints by using the IP address of the two endpoints and port numbers (Stevens, 1994). Therefore, applications built over TCP require the MH to always use its home address as its source address. The solution to this contradiction caused by combined requirements of user mobility, network security and transport protocols is *reverse tunnelling*, which works but lacks in terms of performance as illustrated below.

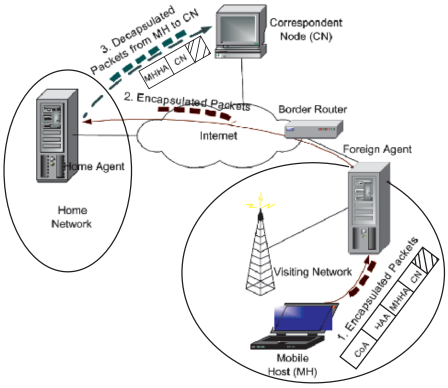


Figure 9: Interoperability between Mobile IP and Ingress Filtering.

Reverse tunnelling in MIP is shown in Fig. 9 which consists of the following components (Perkins, 2002):

1. *Encapsulation*: A data packet sent from the MH to the CN has two IP headers: the inner header has source IP address set to MH's home address (MHHA) and destination IP address set to CN's IP address; the outer header has its source IP address set to MH's CoA and destination IP address set to HA's IP address (HAA). Since the MH's CoA is topologically correct with the foreign network address, ingress filtering at foreign network's border routers allows these packets to pass through.
2. *Decapsulation*: The packets from the MH are routed towards the MH's HA because of the outer

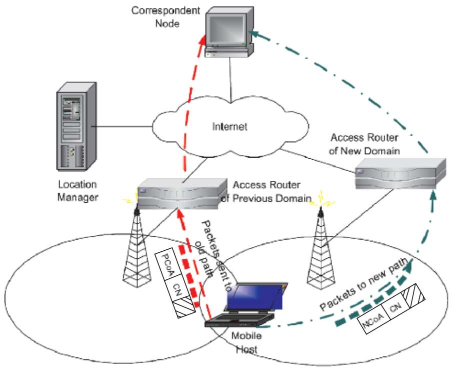


Figure 10: Interoperability between SIGMA and Ingress Filtering.

IP destination address. The HA decapsulates the packets, resulting in data packets with only one IP header (same as the previous inner header), which are then forwarded to their actual destination, i.e. the CN.

3. *Data Delivery*: When data packets arrive at the CN with the source and destination addresses being that of MH's home address and CN's address, respectively, they are identified by its TCP connection and delivered to the upper layer application.

Reverse tunnelling makes it possible for MIP to interoperate with Ingress filtering. However, the encapsulation and decapsulation of packets increase the end-to-end delay experienced by data packets, and also increase the load on the HA, which may become a performance bottleneck as the number of MHs increases.

5.2 Interoperability between SIGMA and Ingress Filtering

In SIGMA, the transport protocol uses IP diversity to handle multiple IP addresses bound to one association. The CN can thus receive IP packets from multiple source IP addresses belonging to an association, identify the association, and deliver the packets to the corresponding upper layer application. This improved capability of endpoint transport protocol permits smooth interoperability between SIGMA and Ingress Filtering.

As shown in Fig. 10, MH can use the CoA that belongs to the subnet which is responsible for sending data for the MH. In the new network, after the new CoA (NCoA) has been bound into the current association through ADDIP chunks (discussed in Sec. 2.1), the MH uses the NCoA to communicate directly with the CN. Since the NCoA is topologically correct with the subnet address, the border router of the foreign network allows packets with source IP set to the new CoA to pass. Thus, SIGMA does not require encapsulation and decapsulation as done in MIP. The transport protocol stack at the CN takes care of delivering packets coming from both previous CoA (PCoA) and NCoA to the upper layer application. SIGMA, therefore, interoperates well with ingress filtering without the need for reverse tunnelling.

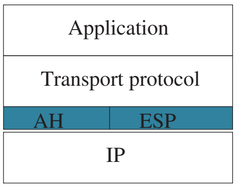


Figure 11: Use of IPSec with SCTP.

5.3 Enhancing the Security of SIGMA by IPSec

IPSec has been designed to provide an interoperable security architecture for IPv4 and IPv6. It is based on cryptography at the network layer, and provides security services at the IP layer by allowing endpoints to select the required security protocols, determine the algorithms to use, and exchange cryptographic keys required to provide the requested services. The IPSec protocol suite consists of two security protocols, namely Authentication Header (AH) and Encapsulating Security Payload (ESP). ESP provides data integrity, authentication, and secrecy services, while the AH is less complicated and thus only provides the first two services. The protocol stack, when IPSec is used with a transport protocol (SCTP in our case), is shown in Fig. 11.

SIGMA is based on dynamic address reconfiguration, which makes the association vulnerable to be hijacked, also called *traffic redirection attack*. An attacker claims that its IP address should be added into an established association between MH and CN, and further packets sent from CN should be directed to this IP address. Another kind of security risk is introduced by dynamic DNS update. An attacker can send a bogus location update to the location manager, resulting in all future association setup messages being sent to illegal IP addresses. The extra security risk introduced by SIGMA gives rise to the authentication problem: CN and LM need to determine whether the MH initiated the handover process. Since both AH and ESP support authentication, in general, we can

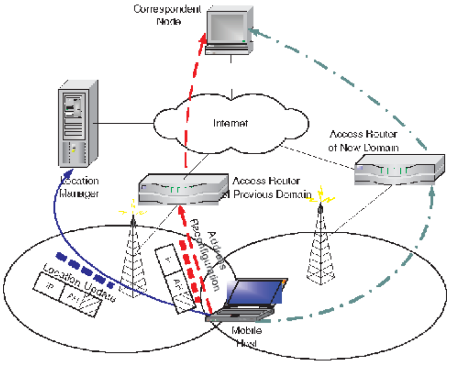


Figure 12: Interoperability between SIGMA and IPSec.

choose either of them for securing SIGMA. ESP has to be used if data confidentiality is required. Assume that we are only concerned with authentication of MH by CN and LM to prevent redirection attack and association hi-jacking. In this case, AH can be used as shown in Fig. 12. All address reconfiguration messages and location updates sent to CN and LM should be protected by IPSec AH header.

6 CONCLUSIONS

We have presented the architecture of Seamless IP diversity-based Generalized Mobility Architecture (SIGMA) to manage handovers of mobile nodes in the Internet architecture. We have shown the applicability of SIGMA to space networks for performing inter-satellite handovers, and presented the survivability and security of SIGMA. It has been shown that SIGMA has a higher survivability than MIP – thanks to its centralized location management scheme. SIGMA can also easily interoperate with existing network security infrastructures such as Ingress filtering and IPSec.

ACKNOWLEDGMENTS

We thank William Ivancic for the numerous discussion that greatly improved the quality of this paper.

REFERENCES

Atiquzzaman, M. and Ivancic, W. (2003). Evaluation of SCTP multistreaming over wireless/satellite links. In *12th International Conference on Computer Communications and Networks*, pages 591–594, Dallas, Texas.

Awerbuch, B. and Peleg, D. (1991). Concurrent online tracking of mobile users. In *ACM SIGCOMM Symposium on Communications, Architectures and Protocols*, pages 221–233.

Bhasin, K. and Hayden, J. L. (2002). Space Internet architectures and technologies for NASA enterprises. *International Journal of Satellite Communications*, 20(5):311–332.

Caire, G., Taricco, G., and Biglieri, E. (1998). Bit-interleaved coded modulation. *IEEE Transactions on Information Theory*, 44(3):927–946.

Cambell, A. T., Kim, S., and et al., J. G. (1999). Cellular IP. IETF DRAFT, draft-ietf-mobileip-cellularip-00.txt.

Dixit, S. (2002). Wireless IP and its challenges for the heterogeneous environment. *Wireless Personal Communications*, 22(2):261–273.

Fu, S. and Atiquzzaman, M. (2003). Improving end-to-end throughput of Mobile IP using SCTP. In *Workshop on High Performance Switching and Routing*, pages 171–176, Torino, Italy.

Fu, S. and Atiquzzaman, M. (2004). SCTP: State of the art in research, products, and technical challenges. *IEEE Communications Magazine*, 42(4):64–76.

Fu, S., Atiquzzaman, M., and Ivancic, W. (2002). Effect of delay spike on SCTP, TCP Reno, and Eifel in a wireless mobile environment. In *11th International Conference on Computer Communications and Networks*, pages 575–578, Miami, FL.

Fu, S., Atiquzzaman, M., and Ivancic, W. (2003). SCTP over satellite networks. In *IEEE 18th Annual Workshop on Computer Communications*, pages 112–116, Dana Point, California.

Fu, S., Atiquzzaman, M., and Ivancic, W. (2005). Evaluation of SCTP for space networks. *IEEE Wireless Communications*, 12(5):54–62.

Glossner, J., Iancu, D., Lu, J., Hokenek, E., and Moudgill, M. (2003). A software-defined communications baseband design. *IEEE Communications Magazine*, 41(1):120–128.

Gustafsson, E., Jonsson, A., and Perkins, C. (2001). Mobile IP regional registration. IETF DRAFT, draft-ietf-mobileip-reg-tunnel-04.txt.

Hallahan, F. (2002). Lessons learned from implementing Mobile IP. In *The Second Space Interent Workshop*, Greenbelt, MD.

Hogie, K. (2002). Demonstration of Internet technologies for space communication. In *The Second Space Internet Workshop*, Greenbelt, Maryland.

Hogie, K., Criscuolo, E., and Parise, R. (2001). Link and routing issues for Internet protocols in space. In *IEEE Aerospace Conference*, pages 2/963–2/976.

Holzbock, M. (2003). IP based user mobility in heterogeneous wireless satellite-terrestrial networks. *Wireless Personal Communications*, 24(2):219–232.

Hsieh, R. and Seneviratne, A. (2003). A comparison of mechanisms for improving Mobile IP handoff latency for end-to-end TCP. In *ACM MobiCom*, pages 29–41, San Diego, USA.

Johnson, D., Perkins, C., and Arkko, J. (2004). Mobility support in IPv6. IETF RFC 3775.

Jung, M., Park, J., Kim, D., Park, H., and Lee, J. (2002). Optimized handoff management method considering micro mobility in wireless access network. In *5th IEEE International Conference on High Speed Networks and Multimedia Communications*, pages 182–186.

Koh, S. J., Lee, M. J., Ma, M. L., and Tuexen, M. (2004). *Mobile SCTP for Transport Layer Mobility*. draft-sjkoh-sctp-mobility-03.txt.

Koodli, R. (2004). Fast handovers for Mobile IPv6. IETF DRAFT, draft-ietf-mipshop-fast-mipv6-03.txt.

Kwon, Y. and Sung, D. (2001). Analysis of handover characteristics in shadowed LEO satellite communication networks. *International Journal of Satellite Communications*, 19(6):581–600.

Leung, K., Shell, D., Ivancic, W., Stewart, D., Bell, T., and Kachmar, B. (2001). Application of Mobile-IP to space and aeronautical networks. *IEEE Aerospace and Electronic Systems Magazine*, 16(12):13–18.

Li, L. (2002). PKI based end-to-end mobility using SCTP. In *MobiCom 2002*, Atlanta, Georgia, USA.

Liao, W., Ke, C., and Lai, J. (2000). Reliable multicast with host mobility. In *IEEE Global Telecommunications Conference (GLOBECOM)*, pages 1692–1696.

Lin, J. and Arul, J. (2003). An efficient fault-tolerant approach for Mobile IP in wireless systems. *IEEE Transactions on Mobile Computing*, 2(3):207–220.

Malki, K. E. (2003). Low latency handoffs in Mobile IPv4. IETF DRAFT, draft-ietf-mobileip-lowlatency-handoffs-v4-07.txt.

Maltz, D. A. and Bhagwat, P. (1998). MSOCKS: An architecture for transport layer mobility. In *INFOCOM*, pages 1037–1045, San Francisco, USA.

Minden, G., Evans, J., Baliga, S., Rallapalli, S., and Searl, L. (2002). Routing in space based Internets. In *Earth Science Technology Conference*, Pasadena, CA.

Montenegro, G. and Gupta, V. (1998). Sun's SKIP firewall traversal for Mobile IP. IETF RFC 2356.

NASA. Omni: Operating missions as nodes on the internet. ipinspace.gsfc.nasa.gov.

Nguyen, H., Lepaja, S., Schuringa, J., and Vanas, H. (2001). Handover management in low earth orbit satellite IP networks. In *GlobeCom*, pages 2730–2734.

Perkins, C. (1998). Mobile Networking Through Mobile IP. *IEEE Internet Computing*, 2(1):58–69.

Perkins, C. and Wang, K. (1999). Optimized smooth handoffs in Mobile IP. In *IEEE International Symposium on Computers and Communications*, pages 340–346.

Perkins, C. E. (2002). IP Mobility Support. IETF RFC 3344.

Ramjee, R., Porta, T., and et al., S. T. (1999). IP micromobility support using HAWAII. IETF DRAFT, draft-ietf-mobileip-hawaii-00.txt.

Rappaport, T. S. (1996). *Wireless Communications Principles and Practice*. Prentice Hall, Upper Saddle River, NJ.

Rash, J., Casasanta, R., and Hogie, K. (2002a). Internet data delivery for future space missions. In *NASA Earth Science Technology Conference*, Pasadena, CA.

Rash, J., Criscuolo, E., Hogie, K., and Praise, R. (2002b). MDP: Reliable file transfer for space missions. In *NASA Earth Science Technology Conference*, Pasadena, CA.

Bush, R., Karrenberg, D., Kosters, M., and Plzak, R. (2000). Root name server operational requirements. IETF RFC 2870.

Sarikaya, B. and Tasaki, M. (2001). Supporting node mobility using mobile IPv6 in a LEO-satellite network. *International Journal of Satellite Communications*, 19(5):481–498.

Snoeren, A. C. and Balakrishnan, H. (2000). An end-to-end approach to host mobility. In *ACM MobiCom*, pages 155–166, Boston, MA.

Soliman, H., Catelluccia, C., and et al., K. M. (2004). Hierarchical Mobile IPv6 mobility management (HMIPv6). IETF DRAFT, draft-ietf-mipshop-hmipv6-04.txt.

Stevens, W. R. (1994). *TCP/IP Illustrated, Volume 1 (The Protocols)*. Addison Wesley.

Stewart, R., Ramalho, M., and et al., Q. X. (2004). Stream control transmission protocol (SCTP) dynamic address reconfiguration. IETF DRAFT, draft-ietf-tsvwg-addip-sctp-09.txt.

Thomson, S. and Narten, T. (1998). IPv6 stateless address autoconfiguration. IETF RFC 2462.

Wu, I., Chen, W., Liao, H., and Young, F. (2002). A seamless handoff approach of Mobile IP protocol for mobile wireless data networks. *IEEE Transactions on Consumer Electronics*, 48(2):335–344.

Xing, W., Karl, H., and Wolisz, A. (2002). M-SCTP: Design and prototypical implementation of an end-to-end mobility concept. In *5th Intl. Workshop on the Internet Challenge: Technology and Applications*, Berlin, Germany.

Ye, G., Saadawi, T., and Lee, M. (2002). SCTP congestion control performance in wireless multi-hop networks. In *MILCOM2002*, pages 934–939, Anaheim, California.