International Journal of Innovative Computing, Information and Control
Volume **x**, Number **0x**, x **2005**

 ISSN 1349-4198
pp. **0–0**

SECURITY IN HETEROGENEOUS LARGE SCALE ENVIRONMENTS USING GRID TECHNOLOGY

Michael Pilgermann, Evangelos Morakis

School of Computing
University of Glamorgan
Pontypridd, CF37 1DL, UK
Tel No: +44 1443 654086
Fax No: +44 1443 482715
(mpilgerm/emorakis)@glam.ac.uk

Stilianos Vidalis

School of Computing
University of Glamorgan
Pontypridd, CF37 1DL, UK
Tel No: +44 1443 482731
Fax No: +44 1443 482715
svidalis@glam.ac.uk

Andrew Blyth

School of Computing
University of Glamorgan
Pontypridd, CF37 1DL, UK
Tel No: +44 1443 482245
Fax No: +44 1443 482715
ajcblyth@glam.ac.uk

Abstract. *The Information Security Team of the University of Glamorgan has started developing a GRID for digital security in heterogeneous large-scale environments. This paper will present an overview of the next generation Intrusion Detection Systems that will unite organisations in forming Virtual Communities for collectively defending their informational infrastructures against cyber-threats. The solution will use Peer-to-Peer distributed data analysis/mining approaches in order to overcome the current architectural and design limitations that are hampering the use and wider development of IDSs.*
Keywords: Digital Security, GRID, Peer to Peer, Data Mining, Data Unification, IDS, Virtual Communities

1. **Problem Statement.** In our modern electronic world, securing a large-scale environment can be seen as a complex problem that requires a lot of resources and intensive computing power. Organisations are forced to allocate considerable resources in protecting their information assets but statistics [9] indicate that there is no stopping to hacking activities. The authors believe that security can only be achieved through effective policing.

One tool for "policing" the cyber-world is the Intrusion Detection Systems (IDS). Over the last decade IDSs have become increasingly important for the protection of computer

networks. Apart from other evolutions in the IDS area, such as everlasting new detection mechanisms [10], generalisation [14] and aggregation [18] of alerts, a tendency for implementing Enterprise Intrusion Detection Systems has become conspicuous. What we need is an automated tool that will be able to detect, deter and react to any type of illegal cyber activity. The Information Security Research Team (ISRG) of the University of Glamorgan has chosen the GRID approach for solving the complex problem of ensuring digital security in heterogeneous large-scale environments.

Current technologies do not easily facilitate the flow of information across organisational and political boundaries. Consequently many organisations are forced to face network-based intrusions into their systems with little to no help from other organisations in the same supply chain. There is a need for the defenders of the Computing Information Infrastructures to come together and form a number of communities in order to take actions collectively against the perpetrator of an attack, and promote a culture of security amongst and across the members of these communities. These communities should allow secure information sharing and facilitate organisations to be proactive in defending their networks against ongoing cyber attacks.

Grid for Digital Security (G4DS) is a "Knowledge Grid" [4] that represents a solution to the aforementioned issues. The implementation of a secure, reliable, encrypted and non-centralized communication architecture enables users to implement trust relationships between each other in order to exchange all kinds of sensitive information. In conjunction with an adequate permission model, data can be published whilst ensuring information is received only at authorised nodes.

2. **State of the Art.** Peer-2-Peer computing [2, 12], allows users to make use of the collective power in their network. The technology emerged as a promising new paradigm for large-scale distributed computing [8]. It helps organisations tackle the kind of large computational jobs they could not handle before. The biggest asset of peer-to-peer systems is not the ability to put everything everywhere but the ability to put anything anywhere. G4DS will have to address the fact that a P-2-P network is a continuously evolving system. This will have to be considered in the design of the P-2-P overlay structure, and in the design of the P-2-P maintenance protocol that will be responsible for the integrity of the GRID network.

Fault tolerance will also have to be addressed as the system will have to have no single point of failure, and be able to function even after the failure of some fraction (big or small) of nodes. To address that a maintenance protocol will be designed and implemented in order to continuously repair the overlay, ensuring that it remains globally connected and supports efficient knowledge sharing. Of course the maintenance protocol will have to be very lightweight, and be able to work correctly even when the system is not in its idealised stable state. The Chord overlay infrastructure [7] is considered for the maintenance protocol. Other architectures that are taken under consideration are: Tapestry [24], Pastry [21] and CAN [19]. All of these approaches assume that most nodes in the system are uniform in resources. This results in messages being routed with minimum consideration to actual network topology and differences between network nodes. This approach is a luxury and cannot be applied in G4DS as the aim of the project is to interconnect diverse network topologies with different and variable network resources.

As discussed by Stepanek, the amount of data that can be in transit in the network is a point of consideration. G4DS make use of "elephants" [22] so we cannot possibly predict bottlenecks, throughput and round trip times unless we actually deploy a complete system. Even then, because the system would be constantly evolving, there would be a need for the network performance assessment exercise to be dynamic and continuous. TCP buffers would have to be allocated dynamically and nodes configured in a continuous basis. It was decided that this approach, although ideal, was academic and that it would introduce hindrances in the enterprises that would be willing to participate and use G4DS. Hence, another approach was followed. We observed the default behaviour of TCP in order to decide on the optimum G4DS packet size that should be allowed on the GRID network.

Because of the TCP overheads, we achieve bigger throughput when we have big packet sizes. G4DS data though are not size demanding. Quite the contrary, the knowledge data that are being exchanged in the GRID network can be counted in bytes, so at any given time we will have a large number of small packets "in transit". Due to the nature of G4DS it is believed that the "many-to-one" routing problem (see [13]) will not be an issue.

Another goal of the project is to be able to provide near 100% functionality even when fractions of the P-2-P network are being congested due to active or inactive attacks. An approach that is considered to address this problem was presented by Zhao [25] in the 1st International Workshop on P-2-P Systems.

As it was shown in latest scientific conferences, P-2-P implementations are cost effective for both individuals and large organisations. The best example of a large P-2-P implementation is NAPSTER. The application was a great success until it encountered legal problems. Over 36 million people joined the NAPSTER community because they could see and understand the benefits. It is accepted that IDS have not achieved their desired use and potential. Almost every large enterprise is using one (IDS), many though fail to use the data collected by it in order to manage a security incident. Furthermore, IDSs do not communicate and do not exchange information in order to efficiently manage these incidents, resulting in them (the IDSs) being too slow and too resource-demanding. It is accepted that a modern IDS should be proactive and not reactive [3].The use of P-2-P technology will successfully tackle the drawbacks of modern IDSs. As we can see, the learning process of a threat (can be seen in Figure 1) is a longwinded procedure that requires a lot of intensive manual work.

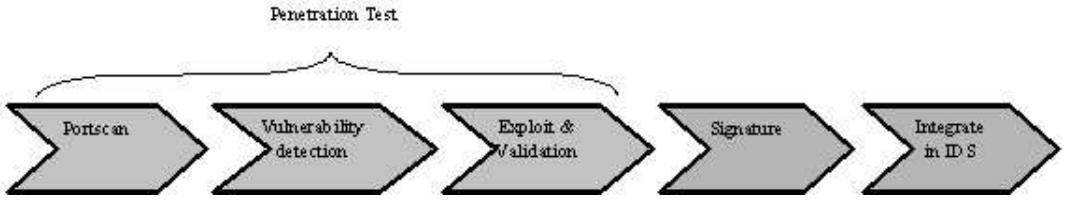

FIGURE 1. Threat Learning Process

The goal of the G4DS application is to reduce that learning process to 'near 0'. This will be achieved by replacing manual with automated procedures using artificial intelligence and data mining techniques. The first four stages of the learning process will be automated

by using history attack data and comparing them with data gathered in "real-time". In G4DS, knowledge and management instructions are being distributed; hence there is a need for criteria to identify valid and non-valid knowledge for each community and/or each member of the community. An example is that of the security permissions in Microsoft Windows. The administrator tailors the permissions and determines the type of access that each user has to the shared resources. Under the same context, the core technology of G4DS is responsible for the permissions, and the G4DS application is responsible for distributing the knowledge.

Nowadays IDSs are designed to determine if there is a real intrusion, or not, in a network [1]. The main problem is the high cost in human resources because of the amount of intelligence necessary to efficiently manage an IDS. An administrator when consulting an IDS has four alternatives with the same probability: Positives, Negatives, False positive, False negative. IDS should improve the rate of positive alerts and avoid false negatives. For instance, the algorithms used in this kind of devices are pattern matching that need to be complemented with some intelligence (human or automatic) in order to be useful in administration and security managing. Another problem an administrator has during the installation of an IDS, is to make it report only the interesting alerts, and after that, to manage the alerts and the reactions to the attacks. G4DS will address all of the above problems.

Taking into account the arguments presented above, and in particular the need of possibly the most up-to-date databases enabling not only detection of an intrusion but also identification of the intruder or attacker, and the necessity of the development of more effective methods of the analysis of data collected through monitoring of the network operation, five dynamically developing branches of computer science: GRIDs, P-2-P applications, sand boxing, data mining and distributed database systems, are taken as a basis for our research.

3. **Core Technology.** It was proven in latest scientific conferences that GRIDS is the way forward in the computing world. Agreeing to [5], until today there is no universal standard for creating GRIDS (Globus [11] is just a toolkit), the technology is immature and not widely used, the entry cost for creating a GRID is exceptionally high, and the outcome of any attempts made was specific to the needs of the organisation that developed it. Due to that, the maintenance cost is extremely high and many GRID projects have failed when it was discovered that they were not financially viable. G4DS is believed to be the next step.

Two major expressions are essential and very distinguished for this paper, namely the Grid for Digital Security (G4DS) and the Inter-Organisational Intrusion Detection System (IOIDS). The former one, Grid for Digital Security, describes all the issues, methodologies and technologies for the subjacent architecture. It is a knowledge based Grid architecture which deals with all issues related to provide and secure the communication channel and provides interfaces to distributed knowledge using this infrastructure.

The Inter-Organisational Intrusion Detection System instead is an application running on top of the Grid for Digital Security. It makes use of the provided architecture and provides an infrastructure for exchanging security related information such as incidents, attack descriptions, information about new attacks in general or related information about countermeasure and the like.

The system will consist of the following components (check also Figure 2):

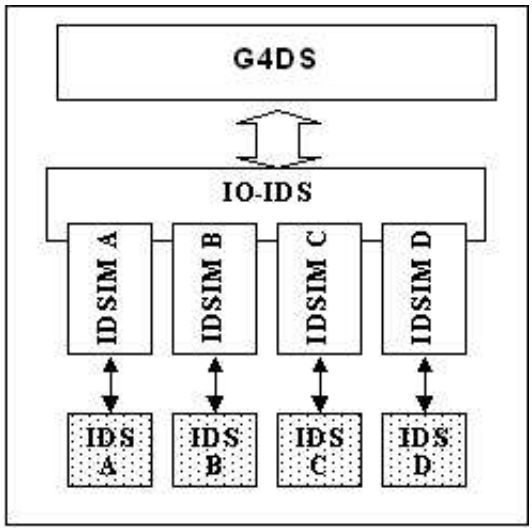

FIGURE 2. General Architecture

1. *Grid for Digital Security (G4DS)* - The G4DS represents the fundamental architecture the whole system is built upon. Several issues such as encryption and authorization are addressed in this module. Due to a decentralized approach users of this module will benefit from a robust and reliable architecture. Trust relationships are built up in this module which will enable applications to make publishing decisions based on the role of the members.
2. *Inter Organisational Intrusion Detection System (IO-IDS)* - The IO-IDS is an implementation that utilizes the G4DS. It deals with all issues directly related to Distributed Intrusion Detection Systems such as Intrusion Detection message formats and exchange standards.
3. *IDS-Integration Module (IDS-IM)* - The system will be applicable for a variety of different Intrusion Detection Systems. The integration of the actual IDS is performed by modules which allow an easy plug-in of the different products. At the end of the day, communication can be established between totally different (Enterprise) IDS utilizing this Inter Organisations Intrusion Detection System.
4. *Connected (Enterprise) Intrusion Detection System (EIDS)* - Currently, there are a plenty of Intrusion Detection Systems available implementing different detection and integration technologies. For this research, no separate IDS will be developed but integration of IDS will be performed. Nevertheless the (Enterprise) Intrusion Detection Systems represents one component of the overall solution.

4. **IOIDS Application.**

4.1. **Topology.** The members are grouped in communities and they agree on the exchange of certain information and on their initial roles of how to maintain and develop that community over time. Communities consist of members without any special privileges and the Community Authorities (CA). Each community has at least 2 CAs; (their

responsibilities are the subject of another paper). There is no upper limitation on the number of Community Authorities; in fact, for small and medium scale topologies each node is supposed to be a Community Authority, which mirrors the peer based attitude of the approach and makes it very attack resistant. The changes to be applied for establishing large scale communities (approaches such as the widely employed hierarchical one could be considered) are examined in another paper.

Members, no matter which role they have, may belong to several Trusting Communities (TCs),. They are only allowed to forward messages across community boundaries if they have got the additional role of a Gateway. The forwarding of the message must align to the forwarding policy provided by the CAs of the TCs in conjunction with the settings made in the message. Mappings of privileges from one TC to another one are defined in the TCs; however they are cached on the Trusting Community Gateways (TCGWs). Each message travelling inside the G4DS topology has to be signed by the sender of the message as well as by each gateway it is passing for crossing communities.

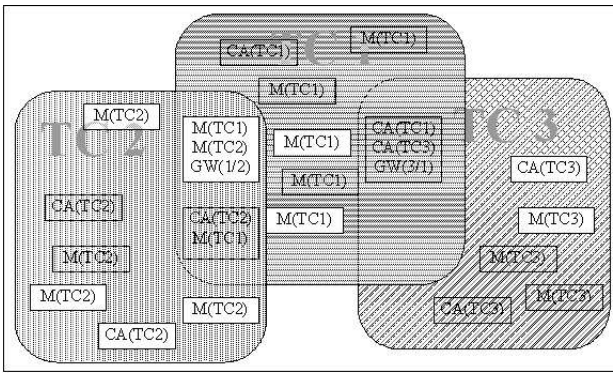

FIGURE 3. Overlapping of Trusting Communities

Figure 3 describes the basic idea of Trusting Communities, the possibilities of memberships of different nodes and finally the overlapping of different communities with its message population across community boundaries.

4.2. **IOIDS architecture.**

4.2.1. *Overview of parties and components involved.* Figure 4 - Communication between two Nodes provides an overview for the communication between to nodes whenever application data between two IOIDS nodes is to be exchanged. Issues such as Trusting Communities are not addressed with this drawing; however, they will be addressed further down in detailed descriptions.

Basically, the exchange of information is comparable with the ISO 7-layer OSI model [16, 23]. Although, a logical connection is established between the IOIDS components of the two nodes, they are not able to communicate with each other directly. Instead, they are making use of communication facilities provided by the G4DS layer. Furthermore, the IOIDS components gather and process information from connected Intrusion Detection Systems.

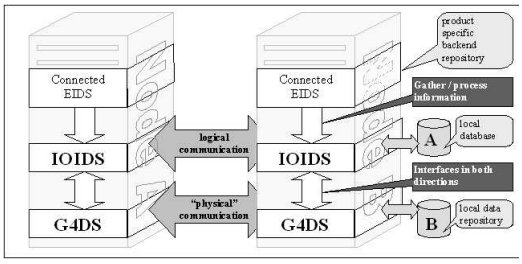

FIGURE 4. Communication between nodes

4.2.2. *Communication on the IOIDS layer.* Basically, each node in the overall topology may act as both a source and a consumer of knowledge. However, regarding to roles, certain nodes may only be allowed to either send information or receive information. Each IOIDS node maintains its database for storing all information about incidents, attack descriptions, countermeasures, etc. (marked as 'A' in Figure 4 - Communication between two Nodes). This database maintains information about both local events as well as events occurring remotely on any node throughout the Knowledge Grid topology.

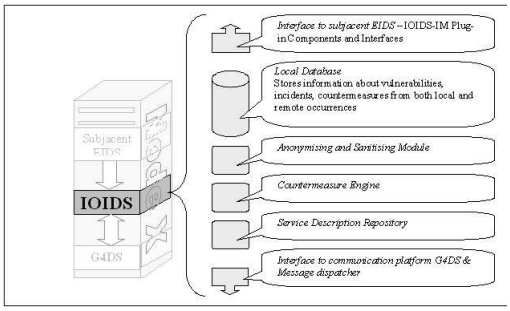

FIGURE 5. Architecture of IOIDS Module

Figure 5 - Architecture of IOIDS Module visualizes the major components of the Inter-Organisational Intrusion Detection System Module. The following sections describe the components in brief:

- *Interface to subjacent (Enterprise) Intrusion Detection System:* The IOIDS architecture is supposed to be connected to a locally deployed Intrusion Detection System. In order to allow the integration of a variety of products from different vendors, a plug-in mechanism was put into place. Interfaces are defined which have to be implemented for integrating a new product. In order to connect a new product, a so-called IOIDS-Integration Module has to be developed. It is supposed to implement the aforementioned interface and, mainly, care about the transformation between the local IDS specific data format and the common IOIDS data format and of course vice versa. After implementing the IOIDS-IM this product can be registered with IOIDS core and will be handled as part of the overall topology. (for details see also Error! Reference source not found. further down in this section.)
- *Local Database:* The Local Database of the IOIDS core is the central point of storage for this node. In more detail it holds information concerning the following matters:
  – Detected attacks

  - Vulnerabilities in general
  - Information about ways to identify attacks (as for example signatures for rule based Intrusion Detection Systems)
  - Suggestion for countermeasure procedures

  Basically, the architecture of the database will be aligned to the Intrusion Detection Message Exchange Format (IDMEF) [6] since we are dealing with information about intrusions (and related) and IDMEF is on the one hand able to transport most of the information to be exchanged for our needs, however, on the other hand it allows extensions for the bits which are not addressed directly.
- *Anonymising and Sanitising Module:* Very sensitive information is to be exchanged using the IOIDS infrastructure. Organisations are forced to take care of their assets, their reputation and trustworthy. This way there will be situations when organisations totally need to unlink information about threats or attacks from their identity; however, in order to protect other node's infrastructure the corresponding information shall be shared. To address this need, the Anonymising and Sanitising Module is introduced. Anyway, most of the anonymising is performed in G4DS layer; however, parts of the sanitizing are application specific and need to be addressed on IOIDS layer directly. After all, this topic is beyond the scope of this paper; the module has been listed for purposes of a complete overview only - finally, the basic idea of anonymising and sanitising was discussed in an earlier publication [15].
- *Countermeasure Engine:* The IOIDS system itself will be able to carry out countermeasure actions. For these purpose this separate module has been introduced. The additional value in comparison to other modern countermeasure engines with their support for e.g. TCP session termination or firewall reconfiguration is the opportunity to exchange information across the IOIDS application infrastructure. Having the ability to describe countermeasure actions in a common way and to execute them on many sides in conjunction with the opportunity to interlink them with certain attacks, vulnerabilities or detection descriptions pushes the benefits of counter measuring to a new level. Countermeasure will be briefly addressed when we talk about message formats for exchanging security related information; however, the architecture and implementation of the countermeasure engine itself is beyond the scope of this paper.
- *Service Description Repository (SDR):* The Service Description Repository maintains all these bits of information related to the distribution process though out the grid architecture, which may not be abstracted down to the G4DS layer; hence, they are application specific. For example, roles for the messages have to be defined and applied to each message to be sent. The following list is a collection of bits of information to be stored in the SDR for the Inter Organisational Intrusion Detection System architecture:
  - Roles of messages and mapping rules
  - Rules about sanitising
- *Interface to communication platform G4DS:* Finally, the IOIDS subsystem must be connected to the subjacent communication platform G4DS. In order to allow integration with other platforms this issue will be solved using its own module, too. The employment of a dispatcher will perform the processing of incoming message sent over through the Grid for Digital Security.

4.2.3. *Communication in the G4DS layer.* The G4DS layer represents an abstraction layer for a secure and reliable communication mechanism independent from any application. The following issues are addressed here:

- Authentication between the communication participants.
- Encryption of all messages.
- Signatures for providing non-repudiation and message integrity.

These issues suggest already the employment of a Private Key Infrastructure (PKI). [20] Although the basic approach for PKI has been employed for the G4DS sub-layer, one significant modification was applied; namely the abortion of Trusting Authorities. Trusting Authorities are central instances in a network topology and using them would undermine the peer-approach taken.

For the integration of our Trusting Communities together with the Public Key Architecture, the following information is stored on each node:

- Trusting Community Pool holding information about all TCs the specific node is a member of
- For each Trusting Community:
  - ID of the TC
  - Name, version and description of the TC
  - Some information about Creation date, time, initiator and life time and expiring
  - Administrative information such us authorities
  - Information about subscription policy and process
  - A list of the services available in this TC
  - Some status information about updates and current members
  - List of members
- Each item on the member list within the TC description holds the following information:
  - ID of the member
  - Name of the member
  - Public key of the member

5. **Problems & Solutions.** Enterprises and individuals must trust the organisation deploying the P-2-P application and the other members of the community. Any computer that forms part of the P-2-P application will be effectively sharing resources with the other computers of the community. In the case of G4DS the concept of the "Virtual Community" negates this problem (the problem of trust). The nodes of a "Virtual Community" are likely to be enterprises from the same supply chain that already trust each other, or organisations that will sign SLAs to exchange services towards a common goal (minimising the cyber threats against their infrastructures).

Enterprises and individuals will not participate in a GRID project if they do not receive any tangible benefits. In our case the benefits are more than tangible. The adoption of the G4DS technology will ensure the protection of tangible and intangible assets like user trust and reputation. Both assets are considered to be very sensitive and critical for all enterprises involved in one of the different levels of E-Commerce.

A P-2-P application usually runs along with other critical applications and it is heavyweight. This has an impact in the performance of the intranet of the enterprise resulting

in the cancellation of the participation. In our case, due to the modularity of the G4DS technology, the performance drop will be minimal to non-existent. Each G4DS module is light weight and do not encumber the infrastructure of the enterprise unnecessarily.

Each enterprise has a number of different systems and platforms. Furthermore, a GRID will go over a number of infrastructure changes over the years of its existence. It is unlikely that an enterprise will spend resources for an application that is technology specific and will only run on a certain platform. G4DS technology though, is platform independent. One of the aims of this project is to achieve a great level of modularity and generality, so that G4DS components will be able to run in any environment and exchange information with any application able to understand XML. Furthermore, G4DS will be open source, hence free for the enterprises to use without paying extreme running costs.

6. **Conclusion.** The characteristics of G4DS technology are:

- It is open source, hence it is free,
- It presents the world with an open standard for GRIDs,
- It minimises the development costs of P-2-P and GRID applications,
- It unites enterprises in a single international supply chain across Europe, and
- It truly presents SMEs with a European customer base.

With Grid for Digital Security an approach was developed that provides a very secure and reliable architecture. Encryption and authorization build up the base for the introduced trust relationships allowing members to distinguish between several roles for nodes inside the community. The implemented Peer-To-Peer architecture is a precondition for the reliable system and the total avoidance of central instances is a further enhancement for a stable architecture. With implementation of an access matrix each member may define the permissions of the member roles and therefore the members belonging to each role.

G4DS technology will promote economic growth across Europe. The E-IDS application will eliminate the cyber threats by effectively policing the cyber space. This will have an effect in the user perspective of the Internet and on-line purchases, which will be greatly enlarged. Users will feel comfortable in buying goods electronically, and slowly it will become part of their culture. A European survey [17] in 2000 showed that more than 50% of Europeans are on-line and more than 50% of those have made at least one electronic purchase. The effect of G4DS will be to "limit up" of those figures. E-IDS will also have an effect in the enterprises, as the existing expensive security technology will become obsolete. It is believed that running security costs for the enterprises could be nearly nullified.

REFERENCES

[1] Allen, J., A. Christie, W. Fitchen, J. McHugh and J. Pickel, *State of the Practice of Intrusion Detection Technologies*, Technical Report, Carnegie Mellon University, Pittsburg, January 2000.

[2] Barkai, B., *P2P Computing*, Intel Computing, Santa Clara, 2002

[3] Biermann, E., E. Cloete and L. M. Venter, A Comparison of Intrusion Detection Systems, *Computer & Security*, vol.20, no8, pp.676-683, 2001

[4] Cannataro, Mario and D. Talia, The knowledge grid, *Communications of the ACM*, vol.46, no.1, pp.89-93, 2003

[5] Coddington, P.D., L. Lu, D. Webb, and A.L. Wendelborn, Extensible job managers for GRID computing, *26th Australasian Computer Science Conference*, Australian Computer Society, Adelaide, Australia, pp.151-159, 2003
[6] Curry, D, H. Debar and M. Lynch, *Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition*, IETF, 2002
[7] Liben-Nowell, D., H. Balakrishnan and D. Karger, Observations on the dynamic evolution of Peer-to-Peer networks, *1st international Workshop on Peer-to-Peer Systems*, Springer, Cambridge, MA, USA, pp.22-33, 2002
[8] Druschel, P., F. Kaashoek and A. Rowstron, *Peer-to-Peer Systems*, Springer, Berlin, Germany, 2002
[9] Goodwin, B., *Record Wave of Hacking Targets UK Business*, 6 pages, accessed on 31 October 2002, 2002
[10] Lee, Wenke, R.A. Nimbalkar, K.K. Yee, S.B. Patil, P.H. Desai, T.T. Tran and S.J. Stolfo, A Data Mining and CIDF Based Approach for Detecting Novel and Distributed Intrusions, *Recent Advantages in Intrusion Detection*, Herve Debar, Ludovic Me, S. Felix Wu, Toulouse, France, Department of Computer Science (North Caroline State University), Department of Computer Science (Columbia University), pp.49-65, 2000
[11] Li, M. and M. Baker, *The GRID: core technologies*, Wiley, Chichester, England, 2005
[12] Loo, A. W., The future of P2P computing, *ACM Communications*, vo.46, no.9, pp.57-67, 2003
[13] Mansour, Y. and B. Patt-Shamir, Many-to-one packet routing on GRIDS, *27th annual ACM symposium on theory of computing*, ACM Press, Las Vegas, Nevada, USA, pp.258-267, 1995
[14] Morakis, E., S. Vidalis and A. Blyth, A Framework for Representing and Analysing Cyber Attacks Using Object Oriented Hierarchy Trees, *The 2nd European Conference On Information Warfare And Security (ECIW)*, Reading, UK, 2003
[15] Pilgermann, M. and A. Blyth, Anonymizing Data in a Peer-To-Peer based Distributed Intrusion Detection System - A possible Approach, *European Conference on Information Warfare (ECIW) 2004*, London, 2004
[16] Piscitello, D.M. and A.L. Chapin, *Open Systems Networking: TCP/IP and OSI*, Addison-Wesley Longman Publishing Co. Inc., 1993
[17] Pounder, C., The European Union Proposal for a Policy Towards Network and Information Security, *Computers & Security*, vo.20, no.7, pp.573-576, 2001
[18] Quin, Xinzhou and W. Lee, Statistical Causality Analysis of INFOSEC Alert Data, *Recent Advances in Intrusion Detection (RAID) 2003*, Pittsburgh, PA, USA, pp.73-93, 2003
[19] Ratnasamy, S., P. Francis, M. Handley, R. Karp and S. Schenker, A scalable content-addressable network, *SIGCOMM*, 2003
[20] Rhee, M.Y., *Internet Security - Cryptographic principles, algorithms and protocols*, John Wiley & Sons Ltd, The Atrium, Chichester, West Sussex, England, 2003
[21] Rowstron, A. and P. Druschel, Pastry: scalable, distributed object location and routing for large-scale peer-to-peer systems, *IFIP/ACM Middleware 2001*, 2001
[22] Stevens, W.R., *TCP/IP Illustrated, Volume 1: the protocols*, Addison Wesley, USA, 1994
[23] Stevens, W.R. and G.R. Wright, *TCP/IP Illustrated, Volume 2 - The Implementation*, Addison-Wesley Publishing Company, USA, 1995
[24] Zhao, B. Y., J.D. Kubiatowicz and A.D. Joseph, *Tapestry: an infrastructure for fault-tolerant wide-area location and routing*, Technical Report, UC Berkeley, no.UCB/CSD-01-1141, 2001
[25] Zhao, B. Y., Y. Duan, L. Huang, A.D. Joseph and J.D. Kubiatowicz, Brocade: Landmark Routing on Overlay Networks, *1st International Workshop on Peer-to-Peer Systems*, Springer, Cambridge, MA, USA, pp.34-44, 2002