Contribution to Securing Connections in a Communications Network: Modeling and Conception of a Fraud Detector

Souad EZZBADY
Dept. of Mathematics and Computer Science
Faculty of Sciences Ben M'sik
Hassan II University Mohammedia, Casablanca, Morocco

Abdelwahed NAMIR
Dept. of Mathematics and Computer Science, Faculty of Sciences Ben M'sik
Hassan2 University - Mohammedia, Casablanca, Morocco

***Abstract*—With the explosion in the volume of data, it became primordial for businesses and responsible to implement new tools to detect in real time the unusual changes in its communications network to address all security holes. In this sense, one of the most recently used solutions is the migration of relational databases to the directed graph databases, thanks to his capacity to manage huge and complex bases, and his easiness of management of security. It is in this sense that this work is located, whose objective is firstly to model the data as a graph with nodes representing users and arcs represent the connection between users. And secondly to monitor connections of links between the different nodes to facilitate the task to one who will handle this data with the ultimate goal of detecting cases of fraud. Indeed, it is to propose a modeling and conception of a technique to improve the communication network management to monitor and report real-time alerts in the event of fraud.**

Keywords—Directed graph database; strongly connected components; Security Management; Theorem graph; communication network

I. Introduction

The databases are increasing day by day in all areas. So to present such a large volume of data, we must find a useful method that will facilitate access to information securely, at any time and will represent the users and the links between them [1], [8].

Moreover, it is increasingly difficult today to secure the information correlated data collected. Therefore, we must find a way to solve this problem.

At this fact, numerous studies and developments have proposed solutions such as graph database with its strengths, its issues and challenges. These bases are provided for storing and processing of highly connected data, easily manage a complex and highly interdependent network of users and transactions [1].

To benefit from effective security of data, companies need a protective layer bonded to the data, to identify, prioritize and optimize risk. From where the need to develop new tools to help detect real-time changes to make the best decisions [6], [7].

We suggest in this paper a method to improve management and communication network security, proposing a conception of a technique used to demonstrate this approach. That said, network monitoring, and is another entity security and essential to achieve complete protection. To do this, first we model the communication network (eg a company) by a directed and connected graph. Second, it turns this graph in its reduced graph to identify connections to monitor and instantly control. Thirdly we focus on the field of access (read and write within the company) and detect, in real time, all that adds or removes or accesses a maliciously.

The result of this work consists of three sections: in the first paragraph, it addresses the problem being treated. In the second paragraph, it gives a solution to the problem and in the latter; it is proposed a conception computerized fraud detection. The conclusion shows the outline of the study and of our contribution and also provides various extensions and possible future works.

II. Issues and Problematic Addressed

A security database has become increasingly a paramount need, before the large volume and complex data. Especially security threats are becoming more frequent and dramatic. So the information system seeks to protect the actions of hackers looking to surpass the protections put in place.

Take the example of a communications network made up of several departments:

- IT department
- HR Department
- Administrative department
- The exterior ...

Each department has access to separate directories, for example the HR department to files concerning the salaries of employees who are confidential and access a collaborator in this matter is considered FRAUD. But when users have access privileges to a database that exceeds the requirements of their job function, they can abuse these privileges for malicious purposes. Therefore, the objective of our research is to perform modeling and technical design to detect in real time any changes in the database whatsoever modified from the application or directly from the comics.

We model the data as a graph consisting of nodes and relationships, for displaying the access rights of each user with its corresponding files. If a third party has added a direct access to the database without using the application, it is considered fraud and illegal and the app will generate a signal indicating the properties of the added relationship in an illegal manner.

This issue of fraud or attack resulting changes in two levels of programs is:

The fraudulent character changes

- To assign the benefits of the program, according to the purpose of fraud.

Example: transfer money to another account.

Sabotage character changes

- To destroy with varying motivations systems or data.

So the goal of our research is to fill this gap by facilitating the security of important data.

III. The Proposed Mathematical Solution

To address the problem addressed, we modeled the data or information related to a user by a directed graph that maps all nodes with their corresponding relationships.

The basic function of the proposed solution is to keep an eye on the graph, and report a warning if there is a fraud.

Later we will see two parts:

- The modeling part: aims to model the data as a graph and recall the points which will be needed to construct the reduced graph.
- The application part: it is explained in this part of the various components of the application.

A. Mathematical modeling

We modeled these data as a graph, where the user will be represented by a node, and the relationship between the nodes will be materialized by a directed arc from node A to node B, that is to say, users A and B and the connection from A to B. Then we translated this graph in its reduced graph to optimize the connections to monitor.

We will present a number of concepts that will be needed in the next chapters. For this one begins with a reminder on graph theory, strongly connected components, reduced graph...[2],[3],[4],[5].

B. Communication network

1) Directed Graph

- A directed graph G is a relation on a finite set X, denoted G = (X, U). X is the set of vertices or nodes (representing in this case the users) and U consists of all couples$(x, y) \in XxX$ which are related, it is called the set of arcs (representing in this case the connections); [2], [3], [4], [5].
- A path G width $p\epsilon N^*$ of a vertex x to a vertex y is a sequence of vertices;$(x_1, x_2, \dots x_p)$ such as $x = x_0, y = x_p$ and $(x_{i-1}, x_i) \in U$ for $i = 1,2, \dots, p$. x is the original and there is the end of the path (the orientation is followed); [2], [3], [4], [5].
- A chain of G the length $p\epsilon N^*$ a vertex x to a vertex y is a sequence of such summits $(x_1, x_2, \dots x_p)$ such as $x = x_0, y = x_p$ and $(x_{i-1}, x_i) \in U$ or $(x_i, x_{i-1}) \in Ui = 1,2, \dots, p$. x and y are the ends of the chain; [2], [3], [4], [5].
- G is said to be connected if for any pair $(x, y) \in X \times X$ with x≠y, there is a chain of x to y; [2],[3],[4],[5].
- G is called strongly connected if for all couples $(x, y) \in X \times X$ with x≠y, there is a path from x to y and another path from y to x. [2], [3], [4], [5].
- G A circuit is a path to a summit itself. [2], [3], [4], [5].

Note 1 : Numerically, G

- ✓ Connected, if there is a chain which passes through all the vertices;
- ✓ Strongly connected, if there is a circuit which passes through all the vertices.

- Called strongly connected component of G, any subset of X formed of top connected by the following relationship:

$x\,R'y \iff$ **there is a path x to y and another path from y to x**.

Note 2: Family $\{C_i\}_{i=1}^{k}$ all strongly connected components of G form a partition of X, that is to say:

- ✓ $C_i \cap C_j = \emptyset$ par $i \neq j$
- ✓ $\cup_{i=1}^{i=k} C_i = X$.

- A reduced graph of the graph G is the graph G' to which each node is associated with a strongly connected component of G. In addition, an arc connects a node x' to a node y' in the graph G' if there is an arc connecting x to y in G where x is in the strongly connected component of G associated with x 'and y belongs to the strongly connected component of G associated with y'.

Note 3: the vertices of the reduced graph are strongly connected components of G.

Example 1: Let the communications network modeled by the given graph G:

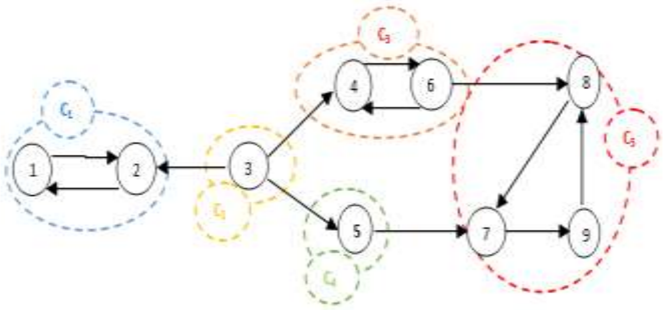


Fig. 1. Graph G

- G is connected because (1, 2, 3, 4, 6, 8, 9, 7, 5) is a chain that passes through all the vertices. But it is not strongly connected because there is no path from the node 2 to node 3.
- The strongly connected components are:

$C_1 = \{1,2\}$, $C_2 = \{3\}$, $C_3 = \{4, 6\}$, $C_4 = \{5\}$ and $C_5 = \{7, 8, 9\}$.

- It gets its reduced following graph:

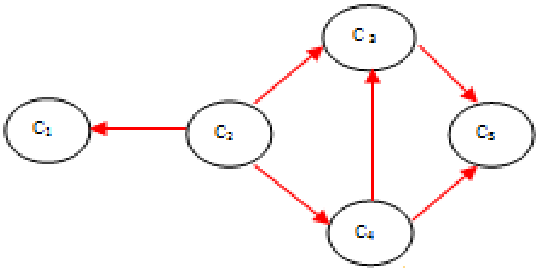


Fig. 2. Graph reduced G'

It adds another strongly connected component E which is external clients (all that is external to the company's communication network) and connected by an arc facing the strongly connected components of the graph reduces E. obtained the following graph:

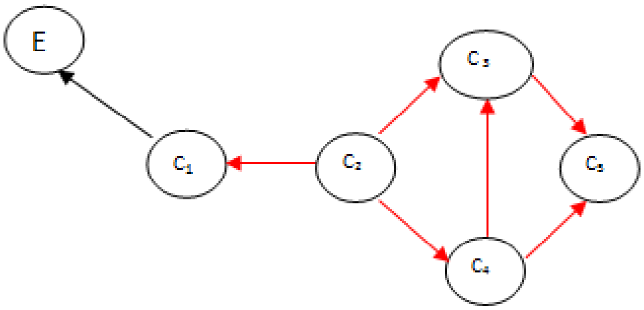


Fig. 3. Graph reduced G' with external clients

C. The important connections to control or monitor instantly

Is a communication network, it can be modeled by a connected graph G whose nodes are the users and the arcs are connections.

- Arc called critical any arc between the strongly connected components of the reduced graph.
- Called non-critical arc any arc between the vertices of a strongly connected component.

Example 3: Example 1 arc (3.2) is critical, and the arc (8.7) is not critical.

Result:

There is Fraud, If there is an addition of an arc oriented in the opposite direction of a critical arc.

Can be mathematically modeled fraud in a communications network by a directed arc. This arc cannot beings within a strongly connected component because otherwise it would have no influence due this fraud cannot uncritical beings arc. So fraud is an arc oriented in the opposite direction of a critical arc.

In fact there are two types of addition of directed edges:

- In the addition of a modeled oriented arc in the strongly connected component in this case it has no influence.
- An addition of an arc oriented in the opposite direction of a critical arc, in this case there is a fraud, as in the graph G if there is an addition of an arc oriented summit a node 2 to the node 3 so it is considered fraud because the node 2 has no relay to reach the node 3.

IV. Conception and Realization a Detector

After the modeling of the communication network by a graph, one shows the different objectives of this conception:

- Facilitate access to databases of users who are connected when linked together in the graph via a simple user interface without the need for SQL scripts.
- Visualize, analyze and quickly correlate database activities from any angle via a simple user interface without the need for SQL scripts.
- Monitor and record all activities authorized and unauthorized access to sensitive data in real time.
- Detect vulnerabilities and fraud and leakage in real time databases.
- Report and block attacks to databases and unauthorized activities in real time. Whether original application or a privileged user on the network or locally on the server database,

So to answer all security aspects of a database server by providing real-time protection, we must control the various access.

These aspects include:

- Defining a security policy, preserve confidentiality,
- integrity
- Data availability.

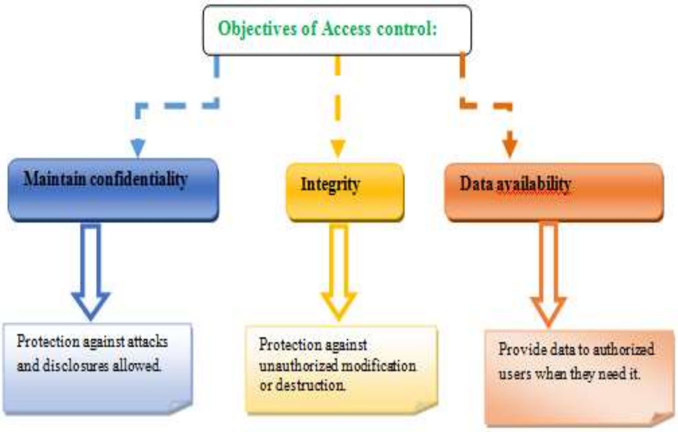

Objectives of Access control:
Maintain confidentiality
Integrity
Data availability
Protection against attacks and disclosures allowed.
Protection against unauthorized modification or destruction.
Provide data to authorized users when they need it.

Fig. 4. Access Control Objectives

D. *Computerization of problem*

In this paragraph, we will submit the application with the different components, explaining the role of each. Our application showing "Who, What, Where and How" each share between users.

This application has 3 parts:

- *User management*: This part aims to add, modify and delete users (that is to say that user will make use of this application).
- *Accordion users*: This part aims to add, modify and delete users. (Create the graph that is to say nodes and arcs)
- *Dashboard:* with all interconnected nodes (all given access rights).
- *List of actions*: Containing a list of actions or facts access via the application, if access is allowed nothing is reported, otherwise a warning will be triggered indicating the fraudulent act with the name of the affected user.

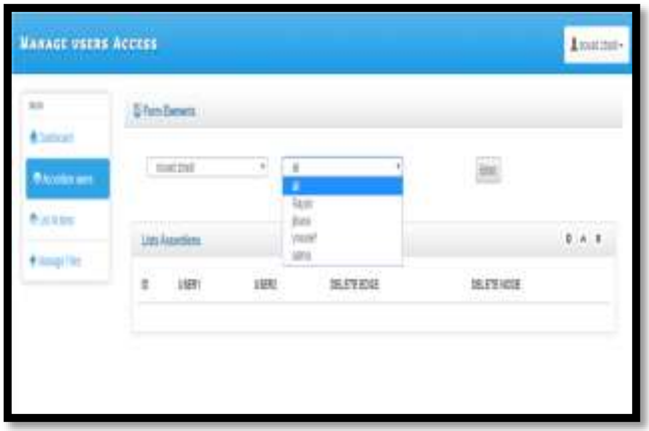


Fig. 5. First window in the application

For more explanation we will give an example of the application:

- The following windows is reserved for users, it contains all the components of the application as the note:
- The interface reserved for single users only contains two parts. the first for file management and second for the dashboard:

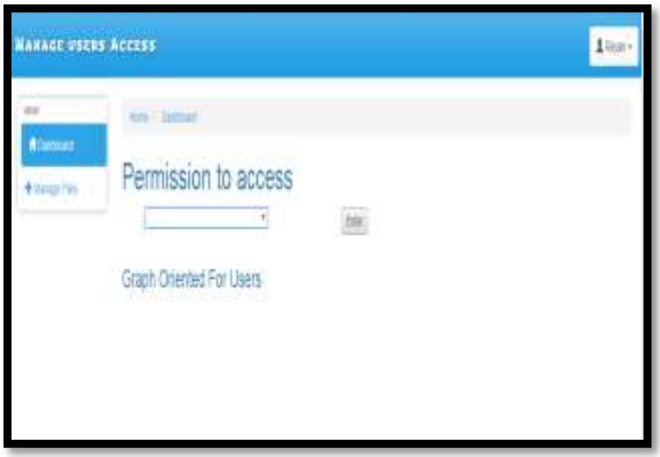


Fig. 6. Permission to access for users

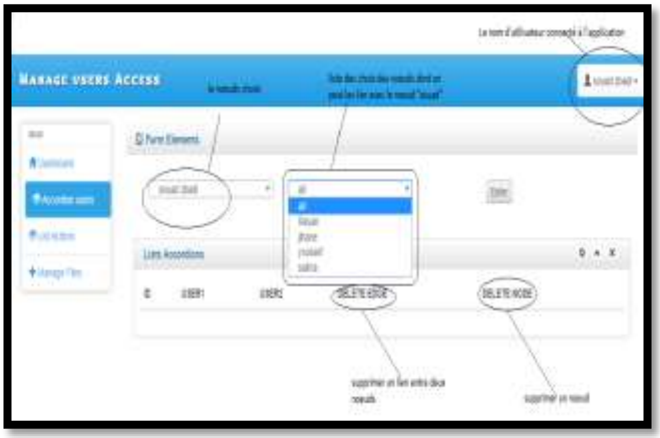


Fig. 7. First window with the components of the application

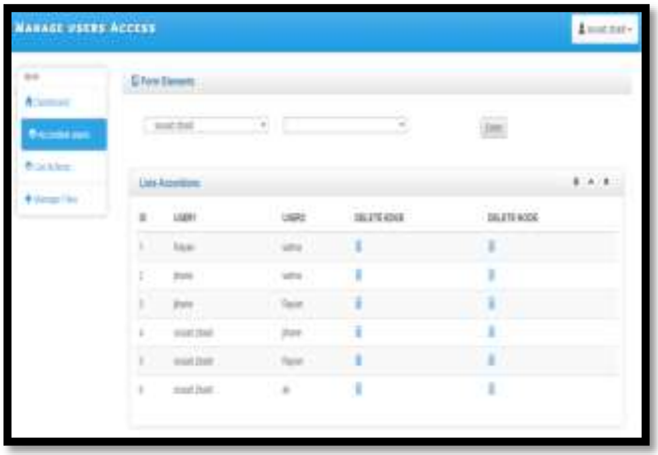


Fig. 8. The Building of links between nodes

- We start with present the first part of the application, this windows and defines the different interconnections between the nodes:
- After defining the paths or links between different users or nodes (that is to say, user "Souad" in "Ali" user so on) is obtained:
- At the application level, we tried to achieve the following points:
  - ➢ All nodes in the system visualize exactly the same data at the same time (data consistency).
  - ➢ Loss or deletion of nodes does not prevent other nodes to continue to function properly, the data remains accessible (data availability).
  - ➢ No less a total failure of the network failure may cause the system to respond properly.

If partitioning into sub-networks, each must operate autonomously.

- We get the following graph on which will monitor the links between the nodes and their reactions and a graph data structure, it is possible to find data in a very powerful way, browsing a graph, ie by navigating relationships. It is at this level that the graph takes all its power: find the shortest path between two nodes, find - from a given node - all nodes having a relationship "Rayan" for example.

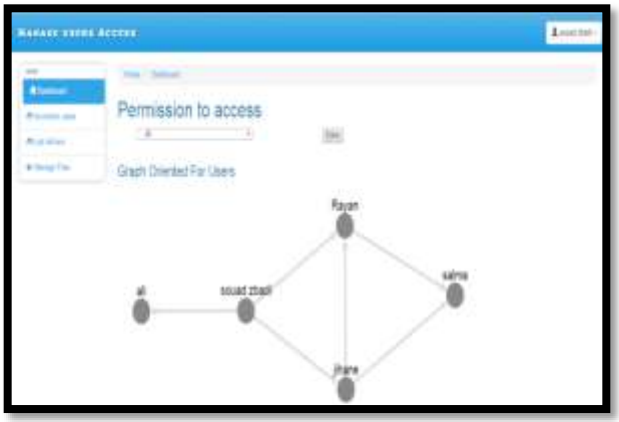


Fig. 9. The result of built graph

- In this interface is treated two cases:
  - ✓ the first case: The "A" user is allowed to access the user "B".

Eg "Souad" user permission to access the user database "Rayan" as shown in the graph above.

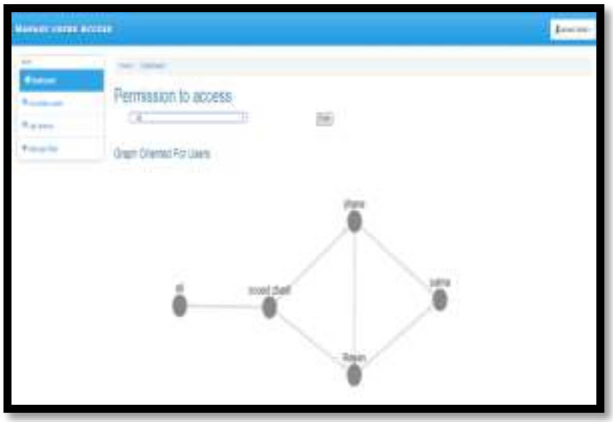


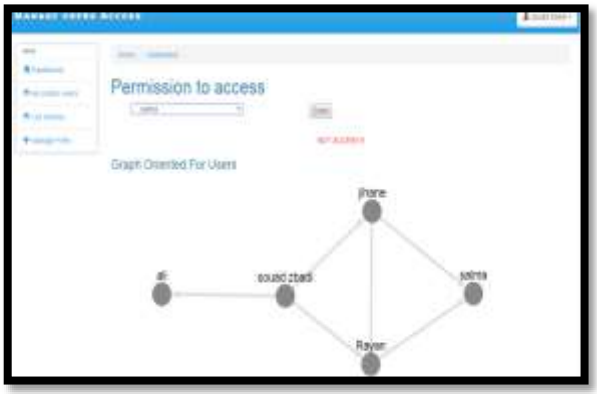
Fig. 10. Example for permission of user to access

So when is connected to the user database "Rayan" you can download the files you need:

Fig. 11. Access to the data

- The second case: If, for example "Souad" user has no right to access the user database "Salma" is at this level that our proposal acquires its importance. That is to say any connection to a database whose context does not match the defined information for which the user profile triggers an alert.

Previously, the user of a database can end up with excessive privileges for the simple reason that database administrators do not have the time to define or update the control mechanisms of the conditions of access for each user. Consequently, all users or large groups of users have the default set of access rights which far exceed the requirements of their specific function.



MANAGE USERS ACCESS

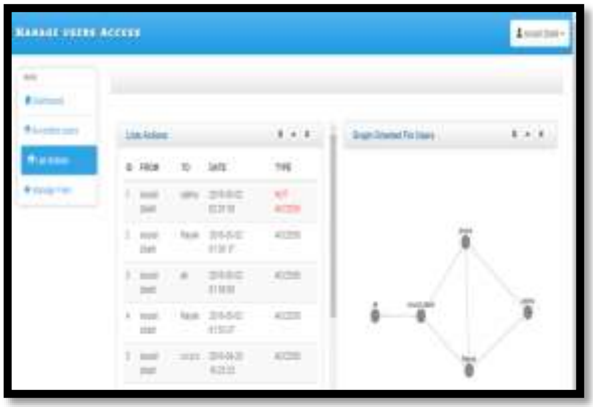
Permission to access

Graph Oriented For Users

Fig. 12. Case of fraud

When unauthorized access is made via the application, an alert will be triggered indicating the name of the user who made the fraudulent act, and when exactly. This access control mechanism would allow the official (High placed malicious) University; described above; update students coordinates, but would trigger an alert if it tried to edit notes.

As shown in the following interface accordions users pane, which indicates that the user "Souad" attempted to access the database of "Salma" and what time, another highlight of this section is that the history of the list of actions is always archived, and no one can erase. So despite that "Souad" be responsible for the management of the application, if it commits fraud it will automatically added to the list in real time.



MANAGE USERS ACCESS

Graph Oriented For Users

Fig. 13. History of all cases of fraud and cases of permission access

Throughout this document we presented the proposed solution to the problem on two levels: the theory and practice.

To demonstrate that in most cases, simply a relational database associated with a relational schema properly made to meet your needs.

But now whether to store enormous amounts of data (Peta bytes), with many users that generate high traffic, a distributed architecture is necessary. These data are extremely valuable and confidential require agencies to audit access to sensitive data and protect against attacks and malicious behavior.

V. Conclusion

As the threats and risks to databases and vital resources are becoming increasingly important, the implementation of controls is now essential. Given the increased risks, particularly the risk of fraud, it is essential to find effective solutions to block those who want to commit or conceal fraud and minimize the risk of loss that may arise from various types of threats.

In this sense is this work. Whose objective is to propose a design technique based on graphs, and whose ultimate goal is to secure the data and detect fraud. It opens the way to various research perspectives:

- Extend this work and write to the graph-oriented databases.
- Connect this application to large databases that is to say the Big Data
- Use Orient DB to develop this application.

References

[1] Odile PAPINI Part II Course 3 (continued): Security basesde data: ESILUniversité the Mediterranean Odile.Papini@esil.univ-mrs.fr

[2] J.A. Bondy, U.S.R. Murty, Graph Theory with Applications, North-Holland, New-York, (1976).

[3] C. Godsil, G. Royle, Algebraic Graph Theory, Graduate Text in Math. 207, Springer,(2001).

[4] Ministère de l'éducation nationale, Introduction d'éléments de la théorie des graphes, accompagnent de la mise en oeuvre des programmes, (2001).

[5] V. Chandola, A. Banerjee, et V. Kumar, Anomaly detection - a survey (Technical Report TR 07-017). Computer Science Department, University of Minnesota.

[6] V. Chandola, A. Banerjee, et V. Kumar, Anomaly detection - a survey. ACM Computing Surveys, 41, 2009.

[7] Y. Bejerano and R. Rastogi. Robust Monitoring of Link Delays and Faults in IP Networks. In Proceedings of IEEE Infocom, 2003.

[8] N. Biggs, Algebraic Graph Theory, 2nd Edition, Cambridge Math. Library, (1993).

[9] L. Page, S. Brin, R. Motwani, T.Winograd, The PageRank Citation Ranking: BringingOrder to the Web, Technical Report, Stanford University, 1998.

[10] J. Miles Prystowsky, L. Gill, Calculating Web Page Authority Using the PageRankAlgorithm,http://online.redwoods.cc.ca.us/instruct/darnold/LAPROJ/.

[11] S. P. Radziszowski, Small Ramsey Number, Dynamic surveys, The Electronic Journal of Combinatorics, http://www.combinatorics.org/Surveys/ds1.pdf

[12] O. Ore, Graphs and their uses, version r´evis´ee par R. J. Wilson, New Mathematical Library 34, Math. Association of America.

[13] R. Cabane, Th_eorie des graphes, Techniques de l'Ing_enieur, Trait_e Sciences fondamentales, document AF205.