REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DE MOHAMED BOUDIAF-M'SILA
FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE
Département d'Informatique

MEMOIRE de fin d'étude

Présenté pour l'obtention du diplôme de MASTER

Domaine : Mathématiques et Informatique
Filière : Informatique
Spécialité : Réseaux

Par : AMRI Yasser

SUJET

Prédiction des incidents dans les réseaux

Soutenu publiquement le : 14 / 06 /2015 devant le jury composé de :

Mr. TAHERI	**Université de M'sila Président**
Dr. MEHANNI	**Université de M'sila Rapporteur**
Ms. HELASSA	**Université de M'sila Examinateur**

Promotion : 2014/2015

Tables de matières :

Chapitre2 : Les modèles de prédiction

Chapitre3 : Prédiction d incident dans les réseaux

Chapitre 4 : implémentation et réalisation

Introduction :

Un réseau informatique est une connexion des ordinateurs et des ressources comme :

les imprimantes, les scanners…etc., dans le but de gagner quelques avantages tels que faire des partages des fichiers et des accès aux fichiers distant, le partage des ressources, capacité de stockage accrue, mais la taille des réseaux ne cessant de grandir et nous avons toujours des risques dans les réseaux informatiques : les risques d'un serveur qui tombent en panne , les risques de saturation des systèmes de stockage, les risques de sécurité…etc.

Le besoin de contrôler en temps réel leur qualité et leur état est rapidement devenu une priorité. C'est dans ce but qu'est apparu, il y a maintenant une vingtaine d'années, le concept de supervision de réseaux ou la gestion des incidents. Pour ces besoins et parce que logiquement «***il vaut Mieux prévenir que guérir*** » nous avons choisi de faire une prédiction des incidents dans les réseaux.

Notre projet est l'implémentation d'un modèle de prédiction des incidents (un prédicteur d'incident) dans les réseaux informatiques, et pour ce but on a divisé le travail en quatre chapitres :

- Chapitre1 : Généralités sur les incidents dans les réseaux : nous allons parler sur les incidents dans les réseaux d'une façon générale ainsi que la classification de ces incidents, et nous allons faire un résumé général sur les principaux indicateurs de ses derniers.
- Chapitre2 : Les modèles de prédiction : dans cette partie nous allons parler sur les modèles de prédiction en générale tels que : Réseaux de neurones, Machine a vecteur de support, Classement de bayésienne naïve.
- Chapitre3 : prédiction des incidents dans les réseaux : cette étapes est plus importante car nous allons faire notre conception de model de prédiction(choix de l'algorithme, choix des indicateurs, choix de variables a prédire, …etc.)
- Chapitre4 : implémentation et réalisation : c'est la dernière étape nous allons implémenter notre prédicteur, et les outils d'implémentation du model.

En fin nous allons faire une conclusion générale et les résultats obtenus ainsi que les prescriptives et les difficultés dans ce travail.

Conclusion :

Parmi les succès scientifiques, le plus impressionnant et le plus recherché est sûrement la réussite prédictive. Thalès a prédit une éclipse, Newton le retour de la comète de Halley et Einstein la courbure des rayons lumineux par le Soleil : l'histoire des progrès scientifiques est souvent l'histoire des prédictions réussies et s'y prédire n'est probablement pas le seul objectif de l'activité scientifique, mais aussi un objectif qui fait consensus. Personne ne nierait qu'une théorie dotée d'une forte capacité prédictive – qui prédit de nombreux phénomènes différents avec précision – est toujours préférable, toutes choses égales par ailleurs, à une théorie ayant une faible capacité prédictive.

Nous avons implémenté notre modèle de prédiction des incidents et nous avons fini les étapes de notre travail

- Première étape nous avons parlé sur les incidents dans les réseaux d'une façon générale ainsi que la classification de ces incidents, et nous avons fait un résumé général sur les principaux indicateurs de ses derniers.
- Deuxième étapes nous avons parlé sur les modèles de prédiction en générale
- Troisième étapes est la plus importante car nous avons fait notre conception de model de prédiction (choix de l'algorithme, choix des indicateurs, choix de variables à prédire, …etc.)
- La Quatrième et la dernière phase nous avons maintenant implémenté et fait un ensemble de tests sur notre prédicteur.

Merci ALLAH maintenant nous avons réussi de finir ce travail mais notre chemin n'était pas facile et nous avons vu un ensemble de difficultés spécialement la documentation pour le premier chapitre et une autre difficulté pour définir notre ensemble d'apprentissage (bases de données) a prédire.

Nous souhaitons que le travail dans ce domaine n'arrête pas car c'est juste le début, nous souhaitons implémenter d'autres algorithmes pour la prédiction les incidents et de faire des comparaisons avec notre résultat obtenu.

Bibliographie :

Thèses et mémoire de fin d'étude :

[1]H .Bouchentouf et R .Hboudghene Stambouli R, étude des performances des réseaux 4g (lte), thème en master télécommunication, Tlemcen, 2013.

[2]Olivier Dugeon , Architectures des réseaux pour le contrôle de la QoS, thème en master réseaux, orange labs, 2008 .

[3]Ahmed Ait ali, Amélioration de la Mesure de la Bande Passante dans un Réseau Bas´e sur IP, thèse doctorat , l'université Henri Poincaré – Nancy 1, 2007.

[4]Ricco Rakotomalala, Arbres de Décision, article de recherche, Laboratoire ERIC, Université Lumière Lyon 2, France ,2005.

[5]Olivier Schwander, Etude de critères de séparation pour les arbres de décision, Master 2 Recherche en Informatique École Normale Supérieure de Cachan, 2009.

[7]lousse jonathan, d'infrastructures distante sen réseaux avec gestion des alarmes et notification des alertes ,grade ingénieur industriel ,2005.

Ouvrage :

[8]Robert Longeon et Jean-Luc Archimbaud, Guide de la sécurité des systèmes d'information, 2012.

[9]Smail NIAR, introduction au mémoire cache, Organisation et architecture de l'ordinateur, William Stallings, 2010.

[10]Johan Balti, DataMining : ID3 et C4.5, école pour l'informatique et les techniques avancés EPITP, 2002.

[11]*Nadia Abchiche,* Systèmes intelligents Les arbres de décision, *Laboratoire IBISC, 2006.*

[12]N. Belgacem, "détection et classification des arythmies cardiaques par application des réseaux des neurones". juin 2002.

[12]O. Behadada, « Application des arbres de décision flous dans la reconnaissance des arythmies cardiaques » 06 décembre 2007.

[14]M. Stricker, Apprentissage des réseaux de neurones et régularisation, Laboratoire d'Électronique de l'ESPCI, 2000.

[15]Hai Anh, H. Usage des arbres de décision, Institut de la francophonie pour L'informatique, 2004.

[16]H. Mohamadally et B. Fomani. SVM : Machines à vecteurs de support ou

séparateurs à vastes marges. Versailles St Quentin, 2006.

[17]R. Clusif , Gestion des incidents de sécurité du système d'information, mai 2011

[18]Alexandre Fernandez-Toro, présentation de la norme ISO27035, Club 27001, janvier 2012

Les sites web :

[19] algorithme CART

« http://www.grappa.univlille3.fr/~gilleron/PolyApp/node12.html »

[20]les arbres de décision

« http://www.grappa.univlille3.fr/polys/apprentissage/sortie004.html » consulter le: avril 2015

[21]les problèmes de mémoire

« http://windows.microsoft.com/fr-fr/windows/preventing-low-memory-problems » consulter le: janvier 2015

[22] Wikipidia

« http://fr.wikipedia.org/wiki/Fuite_de_m%C3%A9moire » consulter le: janvier 2015

[24] l'outils Nagios

« http://www.int-evry.fr/mci/user/procacci/Doc/nagios/nagios.html#htoc21 » consulter le: janvier 2015

[24] Le protocole SNMP,

« http://www.commentcamarche.net/internet/snmp.php3 consulter le: janvier 2015 »

[25]le site officie de Nagios

« http://www.nagios.org » consulter le: janvier 2015

[26] wikipedia

« http://fr.wikipedia.org/wiki/Incident » consulter le: décembre 2014

Résume :

Notre projet vise a mettre au point un outil informatique pour la **prédiction** d'**incidents** dans une **infrastructure** supervisée (ex. prédire la **saturation** des systèmes de stockages). Le jeu de données est constitua d'un ensemble d'indicateurs qui sera défini en premier temps et un ensemble d'apprentissage(bases de données) qui est un résultat d'une supervision de réseaux, L'objective visé est l'implémentation d'un algorithme de prédiction (**arbre de décision**) capable de rendre compte des interactions possibles entre l'ensemble des variables disponibles et des événements que l 'on souhaite prédire (incidents)(ex. surcharge d'un serveur, **augmentation** de la latence, **saturation** mémoire. Etc.)

Mot clés: prédiction, incidents, infrastructure, surcharge, augmentation, saturation.

Abstract :

Our project aims to develop a software tool for the **prediction** of **incidents** in a supervised **infrastructure** (e.g. to predict the **saturation** of storage systems). The data set is constituted of a set of indicators that will be defined first and learning set (database) that is a result of a supervisory network, the objective is the implementation of a prediction algorithm (**decision tree**) can account possible interactions between all available variables and events that we want to predict (incidents) (ex. a server **overload**, **increased latency**, **saturation** memory. Etc.)

Keywords: prediction, incidents, infrastructure overload, increased latency, saturation.

ملخص:

يهدف مشروعنا لتطوير أداة الذي هو عبارة عن برنامج **للتنبؤ** عن الحوادث و المشاكل في **البنية التحتية** للشبكات الخاضعة للمراقبة (علي سبيل المثال :التنبؤ عن تشبع أنظمة التخزين). يتضمن هذا العمل تحديد مجموعة من المؤشرات لهذه **الحوادث** بالإضافة إلي قاعدة بيانات او المعطيات الناتجة عن المراقبة الدائمة لحالة الشبكات. الهدف من وراء هذا هو تنفيذ خوارزمية للتنبؤ(**شجرة القرار**) و التي من شانها تسهيل استغلال المعطيات المتوفرة لدينا من اجل معرفة الحوادث المراد التنبؤ بها (علي سبيل المثال: زيادة أوقات الانتظار في الشبكات, **تشبع أنظمة التخزين** و **تشبع الذاكرة**...الخ.

الكلمات المفتاحية : التنبؤ, البنية التحتية, الحوادث, شجرة القرار, تشبع أنظمة التخزين.