**RESUME**

Les métaheuristiques constituent une famille d'algorithmes stochastiques destinés à résoudre des problèmes d'optimisation difficile. Utilisées dans de nombreux domaines de secteurs d’activité différents, ces méthodes présentent l'avantage d'être généralement efficaces. C’est le cas dans le domaine de la sécurité informatique que nous abordons dans le premier volet de la thèse qui traite de la détection d’intrusion dans les systèmes d’information et les réseaux informatiques. Il s’agit plus particulièrement du problème d’optimisation combinatoire NP-difficile de la détection d’intrusion par l’analyse des traces d’audit de sécurité. Ce problème a été introduit par Ludovic Me en1994, étendu par Gomez et Hougen en 2006, puis par Ahmim en 2011. Les différents auteurs utilisent dans leurs travaux les Algorithmes Génétiques comme moteur de détection d’intrusion. Nous proposons deux méthodes de détection d’intrusion utilisant les métaheuristiques Biogeography Based Optimization (BBO) and Harmony Search (HS), qui sont deux algorithms évolutionnaires bien adaptés pour les problèmes d’optimisation sous contraintes. Les tests réalisés sur chacune des deux méthodes de détection proposées ont pour but de régler dans un premier temps les paramètres des métaheuristiques utilisées, puis d’évaluer leurs performances respectives. Les tests sont réalisés d’abord sur un benchmark, puis sur des données générées aléatoirement. Des résultats expérimentaux de détection d’attaques simulées sont donnés. Les deux modèles sont évalués par leur capacité à faire des prévisions correctes, et se sont avérés efficaces et capables de produire des méthodes fiables pour la détection d'intrusion. Une comparaison des deux approches a été réalisée, montrant un temps d’exécution plus court avec la métaheuristique Harmony Search.

L’utilisation de toute métaheuristique nécessite le réglage de ses paramètres. C’est une opération souvent coûteuse en temps et nécessitant un savoir-faire et une expérience de la part de l’utilisateur, d’autant que ces paramètres peuvent avoir une grande influence sur l'efficience et l'efficacité de la recherche de la solution. Utiliser une métaheuristique sans paramètre pourrait palier à ce type de problèmes. C’est dans ce contexte, que nous proposons dans le deuxième volet de notre thèse, une approche de résolution d’un problème d’optimisation combinatoire NP-difficile, à savoir le Problème du Voyageur de Commerce, par une métaheuristique sans paramètre. Cette dernière est adaptée de la métaheuristique sans paramètre « TRIBES » qui a été développée par Maurice Clerc [Clerc, 2003] pour résoudre des problèmes continus. Ainsi, une extension de TRIBES à la résolution de problèmes discrets est développée et adaptée à la résolution du Problème du Voyageur de Commerce. Cela est rendu possible par l’introduction d’une distance dans l’espace des solutions défini par l’ensemble des cycles Hamiltoniens dans le graphe représentatif du PVC. Les différents mécanismes développés dans TRIBES, comme le processus de génération des particules ou les stratégies de déplacement développées dans les phases d’adaptation structurelle et comportementale de TRIBES sont modifiés. Nous avons observé le bon comportement de TRIBES discrétisée sur plusieurs tests. Une comparaison avec un algorithme génétique a montré des résultats compétitifs.

**Mots-clés:** Optimisation combinatoire, métaheuristiques, sécurité informatique, audit de sécurité, Biogeography Based Optimization, Harmony Search, Tribes.

**ABSTRACT**

Metaheuristics are a family of stochastic algorithms to solve hard optimization problems. Used in many fields of different aria, these methods have the advantage of being generally effective. This is the case in the field of computer security that we address in the first part of the thesis and concerns intrusion detection in information systems and computer networks. More specifically, we treat of a particular NP-Hard combinatorial optimization problem that is the security audit trail analysis, initiated by Ludovic Me in 1994, and extended by Gomez and Hougen in 2006, and Ahmim in 2011. They all use genetic algorithms as intrusion detection engine in their works. We suggest two intrusion detection methods using the metaheuristics Biogeography Based Optimization (BBO) and Harmony Search (HS). They are evolutionary algorithms, well suited for constrained optimization problems. Tests are performed to fix the metaheuristics parameters values and to evaluate the proposed approaches. Results on simulated intrusions’ detection are given. The effectiveness of the models is evaluated by their ability to make correct predictions. They are effective and capable of producing reliable methods for intrusion detection. An important result was the consistency of detection results, irrespective to the number of attacks actually present in the analysed audit file. A comparison of both approaches is made. The execution time in the HS-based method is far better.

However the calculation of execution time does not take into consideration the time required to determine the values ​​of the parameters used. Indeed, as with any metaheuristic, the parameter setting is time consuming and requires expertise and experience from the user, especially since these parameters can have a great influence on the efficiency and effectiveness of the search for the solution. Use a metaheuristic with no parameters could compensate for such problems. It is in this context, we propose in the second part of our thesis, an approach to solving the well-known NP-hard combinatorial optimization problem, namely the Travelling Salesman Problem, using a parameter-free metaheuristic. This latter is adapted from “TRIBES”, a parameter-free metaheuristic, developed by Maurice Clerc in 2003 to solve continuous problems. Our work is concerned with an extension of TRIBES algorithm to solve discrete problems. An adaptation to solve TSP problem is made possible when defining a distance in the search space of the Hamiltonian cycles in the TSP representative graph. The different mechanisms developed in TRIBES are modified, such as the particles generating process or the displacement strategies developed during the structural and behavioral adaptation phases in TRIBES. Experimentation results are given and a comparison with a Genetic Algorithm showed competitive results.

**Key-words:** Combinatory optimization, metaheuristics, computer security, security audit , Biogeography Based Optimization, Harmony Search, Tribes.