

An efficient IDS using hybrid Magnetic swarm optimization in WANETs

Ali Safaa Sadiq^a; Basem Alkazemi^b; Seyedali Mirjalili^c; Noraziah Ahmed^{d,e}; Suleman Khan^a; Ihsan Ali^f; Al-Sakib Khan Pathan^g; and Kayhan Zrar Ghafoor^h

^a School of Information Technology, Monash University, Bandar Sunway 47500, Malaysia

^b Department of Computer Science, College of Computer & Information Systems, Umm Al-Qura University, Mecca 715, Saudi Arabia

^c Institute for Integrated and Intelligent Systems, Griffith University, Brisbane, QLD 4111

Australia ^dFaculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang, Kuantan 26300, Malaysia

^e IBM Centre of Excellence, Universiti Malaysia Pahang, Kuantan 26300, Malaysia

^f Faculty of Computer Science & Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia

^g Department of Computer Science and Engineering, Southeast University, Dhaka 1213, Bangladesh

^h Department of Computer Science, Faculty of Science, Cihan University-Erbil, Erbil 066, Iraq

ABSTRACT

Sophisticated Intrusion attacks against various types of networks are ever increasing today with the exploitation of modern technologies which often severely affect wireless networks. In order to improve the effectiveness of intrusion detection systems (IDSs), data analysis methods such as data mining and classification methods are often integrated with IDSs. Though, numerous studies have contributed in various ways to improve the utilization of data mining for IDS, effective solution often depends on the network setting where the IDS is deployed. In this paper, we propose an efficient IDS based on hybrid heuristic optimization algorithm which is inspired by magnetic field theory in physics that deals with attraction between particles scattered in the search space. Our developed algorithm works in extracting the most relevant features that can assist in accurately detecting the network attacks. These features are extracted by tagged index values that represent the information gain out of the training course of the classifier to be used as a base for our developed IDS. In order to improve the accuracy of artificial neural network (ANN) classifier, we have integrated our proposed hybrid magnetic optimization algorithm-particle swarm optimization (MOA-PSO) technique. Experimental results show that using our proposed IDS based on hybrid MOA-PSO technique provides more accuracy level compared to the use of ANN based on MOA, PSO and genetic algorithm. Updated KDD CUP data set is formed and used during the training and testing phases, where this data set consists of mixed data traffics between attacks and normal activities. Our results show significant gain in terms of efficiency compared to other alternative mechanisms.

KEYWORDS:

Intrusion detection; feature extraction; optimization; security; network flow analysis; computational intelligence.