Available online at www.sciencedirect.com

ScienceDirect

Journal of Network and
Computer Applications 30 (2007) 1–3

Journal of NETWORK and COMPUTER APPLICATIONS

www.elsevier.com/locate/jnca

Editorial

Network and information security: A computational intelligence approach Special Issue of Journal of Network and Computer Applications

The global economic infrastructure is becoming increasingly dependent upon information technology, with computer and communication technology being essential and vital components of Government facilities, power plant systems, medical infrastructures, financial centres and military installations to name a few. Finding effective ways to protect information systems, networks and sensitive data within the critical information infrastructure is challenging even with the most advanced technology and trained professionals. The increasing number of Information Security (IS) related incidents, organized crimes and phishing scams mean that IS deserves much closer attention. Efforts must be stepped up to ensure a safe and secure IT environment throughout the globe. It is important to bear in mind that effective security cannot be achieved by relying on technology alone. A tight coordination is required between the people and technology and weakness in one of these could directly affect the security. Some of the leading challenges which administrators often face when a decision is made to design, develop and implement IS technologies into a security system are cost benefit analysis, trade-off analysis between increased security and privacy and convenience and how the new technology will be used.

Computational intelligence is a well-established paradigm, where new theories with a sound biological understanding have been evolving. The current experimental systems have many of the characteristics of biological computers and are beginning to be built to perform a variety of tasks that are difficult or impossible to do with conventional computers. In a nutshell, which becomes quite apparent in light of the current research pursuits, the area is heterogeneous as being dwelled on such technologies as neurocomputing, fuzzy systems, probabilistic reasoning, artificial life, evolutionary algorithms, multi-agent systems, etc.

The Third International Conference on Hybrid Intelligent Systems (HIS'03) attracted Information Assurance and Security experts representing various problem

1084-8045/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2005.06.004

domains. This special issue comprising of 7 papers present some of the cutting edge research results on using modern computational intelligent techniques for solving information and network security related problems such as visual cryptography, watermarking, secured information sharing, Internet security and intrusion detection. Papers were selected on the basis of fundamental ideas/concepts rather than the thoroughness of techniques deployed. The papers are organized as follows.

In the first paper, Wang et al. present a novel watermarking scheme by enhancing the conventional vector quantization system. The proposed scheme partitions the main codebook into two sub-codebooks by referring to the user key. Genetic algorithm is used for splitting the codebook (genetic codebook partition) in an optimal way. Empirical results reveal that the new method is robust and easy to implement and also provides faster coding time, better imperceptibility than some related vector quantization schemes proposed in the literature.

Yue and Chiang in the second paper propose a semi-public encryption scheme for visual cryptography using Q'tron neural networks. This encryption scheme describes the public information of a document which appears in the *public share* while leaving its confidential part undisclosed. A piece of confidential information is retrievable if and only if a right *user share* is available. Authors have presented detailed procedure to construct Q'tron neural networks and an application that uses the scheme for key distribution in a public area is also illustrated.

Pervasive computing is the next generation computing environments with information and communication technology everywhere, for everyone, at all times. Such highly dynamic network-based environments pose a difficult challenge in formally accessing the resources. In the third paper, Ahn and Mohan address the issue of how to advocate selective information sharing while minimizing the risks of unauthorized access. Authors integrated a role based delegation framework to propose system architecture and the framework is illustrated through a proof-of-concept implementation.

Intrusion Detection is the art of detecting inappropriate, incorrect, or anomalous activity. Intrusion Detection System (IDS) that operate on a host to detect malicious activity on that host are called host-based IDS, and IDS that operate on network data flows are called network-based IDS. The last four papers are dedicated to designing various types of computationally intelligent IDS. Anomaly detection holds great potential for detecting previously unknown attacks. Liao et al. in the fourth paper propose a novel anomaly detection scheme using evolving connectionist systems. Experiment results reveal that their adaptive anomaly detection schemes based on fuzzy adaptive resonance theory and evolving fuzzy neural networks could significantly reduce the false alarm rate while the attack detection rate remains high.

In the fifth paper, Abraham et al. propose a Distributed IDS (DIDS) comprising of several IDS over a large network, all of which communicate with each other, or with a central server that facilitates advanced network monitoring. In a distributed environment, DIDS are implemented using co-operative intelligent agents distributed across the networks. Authors evaluated three fuzzy rule based classifiers to detect intrusions in a network. Results are then compared with other machine learning techniques like decision trees, support vector machines and linear genetic programming. Further, the Distributed Soft Computing based IDS (D-SCIDS) are designed as a combination of different classifiers to model light weight and more accurate (heavy weight) IDS. Empirical results clearly show that soft computing approach could play a major role for intrusion detection.

Özyer et al. in the sixth paper propose an iterative rule learning using a fuzzy rule-based genetic classifier to design an IDS. First, a large number of candidate rules are generated for each class using fuzzy association rules mining, and they are pre-screened using two rule evaluation criteria in order to reduce the fuzzy rule search space. Candidate rules obtained after pre-screening are used in the genetic fuzzy classifier to generate rules to detect the various types of attacks. During the next stage, boosting genetic algorithm is employed for each class to find its fuzzy rules required to detect the attacks each time a fuzzy rule is extracted and included in the system. Empirical results reveal that the proposed method is efficient and could significantly reduce the number of rules.

In the last paper, Peddabachigari et al. present a two hybrid approaches for modelling IDS. Decision Trees (DT) and Support Vector Machines (SVM) are combined as a hierarchical hybrid intelligent system model (DT-SVM) and an ensemble approach combining the base classifiers. The hybrid intrusion detection model combines the individual base classifiers and other hybrid machine learning paradigms to maximize detection accuracy and minimize computational complexity. Empirical results illustrate that the proposed hybrid systems are useful to model more accurate intrusion detection systems.

The guest editors wish to thank Jeremy Thompson, Troubador Publishing Ltd., UK for all the help and providing the opportunity to edit this special issue on '*Network and Information Security: A Computational Intelligence Approach*'. We would also like to thank all our referees who have critically evaluated the papers within the short stipulated time. Finally we hope the reader will share our joy and find this special issue very useful.

Ajith Abraham
Chung-Ang University, Seoul, Republic of Korea
E-mail address: ajith.abraham@ieee.org

Kate Smith
Monash University, Australia
E-mail address: Kate.Smith@infotech.monash.edu.au

Ravi Jain
University of South Australia, Australia
E-mail address: Ravi.Jain@unisa.edu.au

Lakhmi Jain
University of South Australia, Australia
E-mail address: lakhmi.jain@unisa.edu.au