Tenth International Conference on

Hybrid Intelligent Systems (HIS 2010)

&

Sixth International Conference on

Information Assurance and Security (IAS)

Georgia Tech Global Learning Center, Atlanta, USA
August 23-24, 2010

Organized by

MIR Labs
Innovation First

Machine Intelligence Research Labs

Technically Sponsored by

IEEE

IEEE Systems Man and Cybernetics Society
IEEE Intelligent Transportation Society

Welcome from HIS 2010 General Chairs

Welcome to Atlanta and to the 10th International Conference on *Hybrid Intelligent Systems* (HIS 20010), held at the Georgia Tech Global Learning Center, Atlanta (USA), August 23-25th, 2010.

Hybridization of intelligent systems is a promising research field of modern artificial/computational intelligence concerned with the development of the next generation of intelligent systems. A fundamental stimulus to the investigations of Hybrid Intelligent Systems (HIS) is the awareness in the academic communities that combined approaches will be necessary if the remaining tough problems in

Artificial and computational intelligence are to be solved. Recently, Hybrid Intelligent Systems are getting popular due to their capabilities in handling several real world complexities involving imprecision, uncertainty and vagueness.

HIS 2010 builds on the success of nine previous editions, starting in 2001. HIS 2009, took place in Shenyang, China, during August 12-14, 2009. The HIS 2010 International conference provides a unique opportunity to bring together researchers, developers, practitioners, and users of soft computing, computational intelligence, agents, logic programming, and several other intelligent computing techniques.

Like previous editions, HIS 2010 is technically co-sponsored by IEEE Systems, Man & Cybernetics Society. Many people have collaborated and worked hard to produce a successful HIS 2010 conference. First and foremost, we would like to thank all the authors for submitting their papers to the conference, for their presentations and discussions during the conference. Our thanks go to the Program Committee members and reviewers, who carried out the most difficult work by carefully evaluating the submitted papers. We would like to give special thanks to the PC Chairs Andre Carvalho (University of Sao Paulo, Brazil) and Mario Köppen (Kyushu Institute of Technology, Japan) for their work and great efforts in preparing an interesting technical programme.

In this edition of HIS 2010 we will have 2 plenary talks. We would like to thank Ronald Yager (Iona College, USA) and Tadahiko Murata (Kansai University, Japan, and University of Chicago, USA) for providing very interesting plenary talks and support to HIS 2010.

We would like to thank all the Local Organizing Committee members for their support and help in local arrangements of the conference. HIS 2010 conference used EDAS Conference system; the support of the creators of this system is much appreciated.

We look forward to seeing you in Atlanta, USA, during HIS 2010.

Ashraf Saad and Ajith Abraham

Welcome from the HIS 2010 Program Chairs

We initially would like to warmly welcome all the participants of the 10th International Conference on Hybrid Intelligent System (HIS 2010) and to say how glad we are to have such a rich collection of works. The papers you will see during the presentation represent a careful selection of the current researches in theories and applications of hybrid intelligent systems, soft computing and computational intelligence, an important step forward the development of the next generation of hybrid intelligent systems.

HIS 2010 received 117 submissions. Each paper was reviewed by at least 3 reviewers in a standard peer-review process. Accepted papers were assigned to two categories: regular papers of 6 pages and short papers of 4 pages. 30 papers were accepted as full papers, with an acceptance rate of the regular papers equal to 25.6%. Additionally, 13 papers were accepted as short papers. The contributions distributed in the scientific sessions include theoretical and applied works, these last covering a wide spectrum of relevant applications of hybrid intelligent systems and computational intelligence.

The success of this conference was possible only because due the enthusiasm and best efforts of many people, to who we are very much grateful. We would like to thanks all authors for their submissions, session and workshop organizers, and also the reviewers for their continued interest, energy, and support.

We heartily wish all HIS 2010 participants enjoy attending conference sessions and activities, meeting friends and colleagues, getting inspiring new ideas and having a pleasant stay in Atlanta.

Mario Köppen and André C P L F de Carvalho

Welcome from the IAS 10 Chairs

We are pleased to welcome our colleagues to The Sixth International Symposium on Information Assurance and Security (IAS 2010). The International Symposium on Information Assurance and Security aims to bring together researchers, practitioners, developers, and policy makers involved in multiple disciplines of information security and assurance to exchange ideas and to learn the latest development in this important field. The Sixth conference will bring together the world's most respected authorities on Information assurance and security in networked and distributed information sharing environments.

IAS 2010 is technically co-sponsored by the IEEE Intelligent Transportation Systems Society. Each paper was peer reviewed by at least three or more program committee members and based on the recommendations of the reviewers, about 50 full papers and 11 short papers were included in the final Program.

We would like to thank the IAS 2010 international program committee and the additional reviewers for providing the reviews in time. We look forward to seeing you during IAS 2010, August 23-25, 2010.

General Chairs
Ajith Abraham, Ashraf Saad and Dharma Agrawal

Program Chairs
Huirong Fu, Daniel Zeng and Emilio Corchado

HIS 2010 - Plenary Keynotes

Plenary Talk 1

On the Fusion of Soft Information

Ronald Yager
Iona College, USA

Abstract: We discuss the nature and representation of soft information using granular and other hybrid technologies. We discuss technologies for fusing and aggregating this type of knowledge. We consider the problem of fusing soft information with hard information. Methodologies for formalizing the instructions on how to fuse information are described. We look at learning as a type of fusion.

Plenary Talk 2

Designing Social Simulation Using Actual Data

Tadahiko Murata
Faculty of Informatics, Kansai University, Japan
Computation Institute, University of Chicago, USA

Abstract: Aims of social simulation include to predict a future, to find reasons of current situations, or to notice problems of a target society. Recently this research field attracts a lot of researchers from computer science, artificial intelligence, economics, political science, and son on. However, most simulations are not based on actual data. That is, models of target societies are not tuned or identified by the actual data collected from their target societies. This is because the cost of collecting actual data from their target societies is expensive. Therefore, most researches tend to show their simulation results by varying values of parameters in their model and explain several scenarios according to the corresponding parameter values. From these simulation results, we are able to learn several lessons about the nature of target societies, though, it is difficult to see a quantitative results or consequences for them. In this talk, we show several trials to design and develop models of social simulations based on actually collected data from target societies. We employ multi-agent simulation models for our social simulations, and show simulation results for polling place assignment, or assessment for hospital scrap-and-build. We also show an approach for collecting actual data within the budget by using a web-based.

IAS 2010 - Plenary Keynotes

Plenary Talk 1

Amy Neustein
Linguistic Technology Systems
USA

Abstract: Sequence Package Analysis (SPA) identifies another kind of speaker trait: the unique conversational sequence patterns that are associated with each speaker. In stressed environments where extraction features, acoustic vectors, and classifications, and other classical speaker biometric features are compromised by noisy texts, which include speakers who deliberately alter their voices when colluding on crimes and terrorist acts, SPA finds the speaker traits which are not obscured by such conditions. What this means is that when there is a mismatch, a non match or a low confidence match between a suspect's normal speech sample and the speech sample obtained by law enforcement during a high stressed situation (for example, the unidentified speaker is making a threat and is naturally agitated) SPA identifies the conversational sequence patterns that remain constant and identifiable notwithstanding the stressed environment. As such, SPA may be seen as a complementary biometric measure to improve accuracy of speaker verification in stressed environments. For future study is a determination of whether conversation sequence patterns (because they are not subject to the acoustic compromises of stressed environments) outperform standard biometrics or, at least, serve as a complementary biometric to improve accuracy of speaker verification in stressed environments. Associated Press and the New York Times.

Plenary Talk 2

Kwok-L. Tsui
H. Milton Stewart School of Industrial & Systems Engineering
Georgia Institute of Technology
Manufacturing Engineering & Engineering Management
City University of Hong Kong

Abstract: Due to (i) concerns in public health safety, product reliability, system safety and failure prevention, and (ii) latest advancement in data collection technologies and modelling tools, there are tremendous opportunities in quantitative modelling research in system informatics (SI) as well as system

prognostics and health management (PHM). First, we will present our view on research in system informatics, including data mining, surveillance, simulation, and system integration in healthcare and public health applications. In health surveillance, we will review and classify the various types of health surveillance research problems. In simulation, we review the latest research in disease spread simulation models and hospital operation simulation models. In system integration, we explore the opportunities for integrating surveillance, simulation, diagnostics, prognostics, data mining, and bioinformatics for personalized health management. Second, we will then discuss the recent research in system prognostics and health management and how they are connected to research in system informatics and human health management. In particular, we will explain the characteristics of PHM and how they are different from traditional reliability modelling research.

Plenary Talk 3

Václav Snášel
VSB-Technical University of Ostrava,
Czech Republic

HIS – IAS 2010 - Technical Progam

August 23, 2010

08:00 – 15:00
Registration

Room: 433

08: 30 – 09:00
Opening Ceremony

09:00 - 09:50
Plenary 1: Plenary Session 1: Kwok-L Tsui

09:50 - 10:40
Plenary Session 2: Tadahiko Murata

10:40 - 11:00
Coffee break

11:00 - 11:50
Plenary Session 3: Ronald Yager

11:50 - 12:30
Plenary Session 4: Amy Neustien

12:30 - 13:00
Plenary Session 5: Vaclav Snasel

13:00 - 14:00
Lunch

HIS 2010 Conference Technical Progam

August 23, 2010

14:00 - 15:30

Session: Hybrid Fuzzy Systems

Room: 323

A Comparison of Positive, Boundary, and Possible Rules Using the MLEM2 Rule Induction Algorithm

We explore an extension of rough set theory based on probability theory. Lower and upper approximations, the basic ideas of rough set theory, are generalized by adding two parameters, denoted by alpha and beta. In our experiments, for different pairs of alpha and beta, we induced three types of rules: positive, boundary, and possible. The quality of these rules was evaluated using ten-fold cross validation on five data sets. The main results of our experiments are that there is no significant difference in quality between positive and possible rules and that boundary rules are the worst.

Improving Black Box Testing By Using Neuro-Fuzzy Classifiers and Multi-Agent Systems

Automated software testing has become a fundamental requirement for several software engineering methodologies. Software development companies very often outsource the test of their products. In such cases, the hired companies sometimes have to test softwares without any access to the source code. This type of service is called black box testing, which includes presentation of some ad-hoc input to the software followed by an assessment of the outcome. The common place for black box testing is sequential approach and slow pace of work. This ineffectiveness is due to the combinatorial explosion of software parameters and payloads. This work presents a neuro-fuzzy and multi-agent system architecture for improving black box testing tools for client-side vulnerability discovery, specifically, memory corruption flaws. Experiments show the efficiency of the proposed hybrid intelligent approach over traditional black box testing techniques.

A New Hybrid Nature-Inspired Metaheuristic for Problem Solving Based on the Social Interaction Genetic Algorithm Employing Fuzzy Systems

This paper has the purpose to present a new hybrid nature inspired metaheuristic developed based on three fundamentals pillars extremely well known: Genetic Algorithms, Game Theory and Fuzzy Systems. This new approach tries to mimic a little bit more closer how a population of individuals evolves along time, like human social evolution emphasizing the social interaction between individuals and the non-binary behavior of human decision making against the classical cooperate-defect behavior present in the Prisoner's Dilemma (PD), for example. In this way it is presented the Social Interaction Genetic Algorithm (SIGA), to establish the necessary basis for the application of fuzzy concepts to get the F-SIGA Algorithm. Besides that, it is also presented the structure of an individual more complex with a genotype composed of two chromosomes, one for the solution of the problem and the other representing its behavior's strategy, which could be binary or fuzzy. At least the F-SIGA approach is presented in details, including all its steps. And finally some results are presented to an instance of the Traveling Salesman Problem.

Fuzzy Based Hybrid Multispectral Image Fusion Method Using DWT

Standard Pan-sharpening methods do not allow control of the spatial and spectral quality of the fused image. The color distortion is also most significant problem in standard pan-sharpening methods. In this paper a novel hybrid multispectral image fusion method using wavelet transform is proposed which provides novel tradeoff solution between the spectral and spatial fidelity and preserves more detail spectral and spatial information. New hybrid image fusion rules are also proposed. Proposed method is applied on number of registered Panchromatic and Multispectral images and simulation results are compared with standard image fusion parameters. The simulation results of proposed method also compared with five different standard and recently proposed Pan sharpening methods. It has been observed from simulation results that proposed algorithm preserves better spatial and spectral information and better visual quality compared to earlier reported methods.

HIS 2010 Conference

August 23, 2010

15:45 - 17:45

Session: Hybrid Systems in Applications

Room: 323

Internet Traffic Classification using a Hidden Markov model

This paper examines the performance of a new Hidden Markov Model (HMM) structure used as the core of an Internet traffic classsifier and compares the results with those produced by other models in the literature. Traffic modeling and classification finds importance in many areas such as bandwidth management, traffic analysis, prediction and engineering, network planning, Quality of Service provisioning and anomalous traffic detection. The new HMM structure, which takes into account the packet payload size (PS) and the inter-packet times (IPT) sequences, is obtained by concatenation of a first part which is framed with a HMM profile with another part whose structure is that of a fully-connected HMM. The first part captures the specific properties of the first protocol packets while the second part captures the statistical properties of the whole sequence present in the flow. Models generated are found to increase the accurate in classifying different traffic classes in the analysed dataset. The average accuracy obtained by the classifier is 62.5\% having seen only five packets, 80.0\% after examining 13 packets and 95.5\% after seeing the unidirectional entire flow.

An intelligent web interface to generate and update adaptive virtual environments

In recent years, three-dimensional Virtual Environments developed with virtual reality and graphical computation technologies have evolved in the Web. Thus, users with different profiles, cultures and knowledge levels can access such environments remotely. In such a way, it is necessary to use an efficient interface to manage Web accesses and to actualize virtual environments in order to adapt them to each user characteristics. This article presents an intelligent Web interface managed by a society of software agents that follows and identifies users' actions in order to propose modifications in the current virtual environment, through 3D objects updating. The latter can be done in real time with no performance losses. Objects used in the construction and adaptation of a Virtual Environment are stored into a database and are retrieved by agents, according to the specific negotiation rules defined in an ontology for the domain.

A Short-Term Bus Load Forecasting System

This paper proposes a methodology for a short-term bus load forecasting. This approach calculates the short-term bus load demand forecast using few aggregated models. The idea is to cluster the buses in groups with similar daily load profile and for each cluster one bus load forecasting model is adjusted. For each cluster, aggregated forecasting model is built based on the analysis of individual bus load data. The solution obtained through aggregated approach is similar to the solution obtained by individual bus load forecasting model, but requiring much less computational time. This proposed methodology was implemented in a friendly computational forecasting support system described in this paper.

Evaluating Classification Methods Applied to Multi-Label Tasks in Different Domains

In traditional classification problems (single-label), patterns are associated with a single label from the set of disjoint labels (classes). When an example can simultaneously belong to more than one label, this classification problem is known as multi-label classification problem. Multi-label classification methods have been increasingly used in modern application, such as music categorization, functional genomics and semantic annotation of images. This paper presents a comparative analysis of some existing multi-label classification methods applied to different domains. The main aim of this analysis is to evaluate the performance of such methods in different tasks and using different evaluation metrics.

On The Improvement Of Knowledge Management Status Through Case-Based Reasoning In A Hybrid Approach

From an enterprise point of view, Knowledge Management (KM) enables organizations to capture, share, and apply the collective experience and know-how (knowledge) of their staff. Up to now, little effort has been devoted to apply Artificial Intelligent techniques to KM systems. This paper proposes the application of case-based reasoning, in combination with a neural model, to develop a KM system. This combined approach profiles the KM status of the whole organization and automatically generates proposals, aimed at improving the KM situation of organization units. The system is fed with KM data collected at the organization and unit contexts. The outcome consists of customized solutions for different areas of expertise related to the organization units, once a lack of knowledge in any of those has been identified.

Aiida-Sql: an Adaptive Intelligent Intrusion Detector Agent For Detecting Sql Injection Attacks

SQL Injection attacks on web applications have become one of the most important information security concerns over the past few years. This paper presents a hybrid approach based on the Adaptive Intelligent Intrusion Detector Agent (AIIDA-SQL) for the detection of those attacks. The AIIDA-SQL agent incorporates a Case-Based Reasoning (CBR) engine which is equipped with learning and adaptation capabilities for the classification of SQL queries and detection of malicious user requests. To carry out the tasks of classification and detection, the agent incorporates advanced algorithms in the reasoning cycle stages. Concretely, an innovative classification model based on a mixture of an Artificial Neuronal Network together with a Support Vector Machine is applied in the reuse stage of the CBR cycle. This strategy enables to classify the received SQL queries in a reliable way. Finally, a visualisation neural technique is incorporated, which notably eases the revision stage carried out by human experts in the case of suspicious queries. The experimental results obtained in a real-traffic case study show that AIIDA-SQL performs remarkably well in practice.

HIS 2010 Conference

August 24, 2010

08:30 - 13:00

Session: Hybrid Metaheuristics

Room: 323

Impact of the Random Number Generator Quality on Particle Swarm Optimization Algorithm Running on Graphic Processor Units

Particle swarm optimization (PSO) is a bio-inspired technique widely used to solve real optimization problems. In the recent years, the use of Graphics Processing Units (GPU) has been proposed for some general purpose computing applications. Some PSO implementations on GPU were already proposed. The major benefit to implement the PSO for GPU is the possibility to reduce the execution time. It occurs due to the higher computing power presented nowadays on GPUs plataform. A study on the impact of the quality of Random Number generator has been made but it only covered some variations of the algorithm on a sequential plataform. In this paper, we present an analysis of the performance of the random number generator on GPU based PSOs in terms of the RNG statistical quality. We showed that the Xorshift random number generator for GPU presents enough quality to be used by the PSO algorithm.

A Particle Swarm Optimization Based Approach for the Maximum Coverage Problem in Cellular Base Stations Positioning

The demand for cellular systems has grown in recent years and sometimes it is not an easy task to design such systems. We propose in this paper a new approach to tackle the maximum coverage problem in cellular systems using Particle Swarm Optimization (PSO). We adapted the PSO since we have associated the position of the base stations to the particles. We also developed two mechanisms to avoid overlaping among the cells and to maximize the coverage of the entire system. We tested our approach in two scenarios in different configurations. We believe that the results are interesting and with future works we can create a commercial tool to solve the real problem.

Analyzing the Control of Dominance Area of Solutions in Particle Swarm Optimization for Many-Objective

The interest in the application of particle swarm optimization to solve different problems, especially multi-objective problems, grew in recent years. This metaheuristic is particularly suitable to solve real life problems, but like other multi-objective metaheuristics, has some limitations when dealing with problems with many objectives, typically more than three. Recently, some many-objective techniques were proposed to avoid the deterioration of the search ability of Pareto dominance based multi-objective evolutionary algorithms for many-objective problems. This work presents a study of the influence of the many-objective technique called the control of dominance area of solutions (CDAS) in multi-objective particle swarm optimization. It is presented an empirical analysis to identify the influence of the CDAS technique on the convergence and the diversity of a multi-objective PSO algorithm in many-objective scenarios through the analysis of some quality indicators and statistical tests.

Efficient Protein-Ligand Docking Using Sustainable Evolutionary Algorithms

AutoDock is a widely used automated protein docking program in structure-based drug-design. Different search algorithms such as simulated annealing, traditional genetic algorithm (GA) and Lamarckian genetic algorithm (LGA) are implemented in AutoDock. However, the docking performance of these algorithms is still limited by the local optima issue of simulated annealing or the premature convergence issue typical in traditional evolutionary algorithms (EA). Due to the stochastic nature of these search algorithms, users usually need to run multiple times to get reasonable docking results, which is time-consuming. We have developed a new docking program AutoDockX by applying a sustainable GA named ALPS to the protein docking problem. We tested the docking performance over three different proteins (pr, cox and hsp90) with more than 20 candidate ligands for each protein. Our experiments showed that the sustainable GA based AutodockX achieved significantly better docking performance in terms of running time and robustness than all the existing search algorithms implemented in the latest version of AutoDock. AutodockX thus has unique advantages in large-scale virtual screening.

The Swarm Computer, an Analog Cellular-Swarm Hybrid Architecture

The "killer apps" of cellular and swarm computing are image processing and optimization, respectively; however, applying these platforms to general-purpose computing remains impractical. Designing systems within the restrictive framework of cellular automata is extremely difficult, though often very efficient and scalable. On the other hand, swarm networks are very powerful but difficult to implement in hardware. Here we introduce a hybrid model, the Swarm Computer, which is both practical to program and efficient to implement. Applications in astrophysics and image processing are considered.

An Optimization Heuristic for Siting Observers in Huge Terrains Stored in External Memory

We present an algorithm (and implementation) which sites multiple (perhaps hundreds) of observers on a DEM terrain that is too large to store in internal memory. Tests show it to use a median of fifteen percent fewer observers to obtain the same joint visibility index (coverage) on huge terrains, compared to a naive partitioning of the terrain into subregions. This will permit more efficient positioning of facilities such as mobile phone towers, fire observation towers, and vigilance systems.

A GRASP heuristic with path-relinking for a bi-objective p-median problem

This paper deals with the a bi-objective p-median problem that consists in finding p-locals from a set of m location points to install facilities in which two objective functions are simultaneously minimized: the sum of distances of servers and the total fixed costs for opening facilities. To determine a set of non-dominated solutions, that is, to find an approximation of the Pareto-optimal solutions is proposed a novel method based on GRASP (Greedy Randomized Adaptive Search Procedure) heuristic that constructs iteratively non-dominated solutions (constructive phase) and some of these solutions are improved by a local search procedure. An intensification strategy based on the Path-Relinking is also applied. To test the performance of the proposed heuristic was developed a Mathematical Programming Algorithm, called e-Restrict, that find Pareto-optimal solutions solving the Integer Programming model of the problem with additional restrictions.

Search Personalization in Hyperlinked Environments by Relevance Propagation and Ant Colony Optimization

Personalization is a promising way of improvement of search services in large document collections and on the Web. User modeling is in the core of many personalization efforts because accurate user model can provide essential information for user specific search adjustments and result set processing. In this paper, we propose and study user modeling technique based on click-through data, relevance propagation and ant colony optimization.

Evolutionary Improvement of Search Queries and Its Parameters

The formulation of user queries is an important part of the information retrieval process. In the complex environment of the World Wide Web and other large data collections, it is often not easy for the users to express their information needs in an optimal way. In this paper, we investigate evolutionary algorithms (in particular genetic programming) as a tool for the optimization of user queries and seek for its good settings

A Gaussian Artificial Immune System for Multi-Objective Optimization in Continuous Domains

This paper proposes a Multi-Objective Gaussian Artificial Immune System (MOGAIS) to deal effectively with building blocks (high-quality partial solutions coded in the solution vector) in multi-objective continuous optimization problems. By replacing the mutation and cloning operators with a probabilistic model, more specifically a Gaussian network representing the joint distribution of promising solutions, MOGAIS takes into account the relationships among the variables of the problem, avoiding the disruption of already obtained high-quality partial solutions. The algorithm was applied to three benchmarks and the results were compared with those produced by state-of-the-art algorithms.

An Integral Approach for Geno-Simulated Annealing

Global optimization is the problem of finding the global optimum of any given function in a certain search space. Simulated Annealing (SA) and Genetic Algorithms (GA) are among the well-known techniques used for global optimization. Adjusting the parameters of SA such as the temperature schedule and the neighborhood range plays an important role in the performance of the algorithm. Furthermore, many studies in literature showed that the best values for SA parameters depend on the optimization problem. We introduce a novel hybrid approach that uses SA to solve an optimization problem and uses GA simultaneously to adapt the parameters of SA. This new approach is referred to as Geno-Simulated Annealing (GSA). It does not require any predefined values for the parameters of SA. To evaluate the performance of the proposed approach, we used seven well-known benchmark optimization functions. The obtained results indicate the superiority of the proposed approach as compared to a similar approach and to conventional SA.

A New Third Order Particle Swarm Optimization and Applications to Optimum Solutions of Various Test Functions

In this paper, we present a new third order particle swarm optimization. The original PSO has position and velocity vectors. However, the proposed algorithm has three vectors: i.e. a position vector, a velocity vector and an acceleration vector. From the proposed PSO, we obtain the third order difference equation and from the equation we obtain the convergence region for four parameters. By setting four appropriate parameters near the convergence region with the proposed PSO algorithm, we try to find optimal points for function minimization. We show that the proposed algorithm has better performance than the original PSO for the optimal solution of function minimization.

Examination of the Performance of Objective Reduction Using Correlation-Based Weighted-Sum for Many Objective Knapsack

Problems

In this paper, we show the effectiveness of an EMO (Evolutionary Multi-criterion Optimization) algorithm with objective reduction using a correlation-based weighted-sum in many objective knapsack problems. Recently many EMO algorithms are proposed for various multi-objective problems. However, it is known that the convergence performance to the Pareto-frontier becomes weak in approaches using archives of non-dominated solutions since the size of archives becomes large as the number of objectives becomes large. In this paper, we show the effectiveness of using information of correlation between objectives to construct groups of objectives. Our simulation results show that while an archive-based approach, such as NSGA-II, produces a set of non-dominated solutions with better objective values in each objective, the correlation-based weighted sum approach can produce better compromise solutions that have better minimum objective values in every objective in many objective knapsack problems.

Mixing Theory of Retroviruses and Genetic Algorithm to Build a New Nature-Inspired Meta-Heuristic for Real-Parameter Function Optimization Problems

This paper describes the development of a new hybrid meta-heuristic of optimization based on a viral lifecycle, specifically the retroviruses (the nature's swiftest evolvers'), called Retroviral Iterative Genetic Algorithm (RIGA). This algorithm uses Genetics Algorithms (GA) structures with features of retroviral replication, providing a great genetic diversity, confirmed by better results achieved by RIGA comparing with GA applied to some Real-Valued Benchmarking Functions.

HIS 2010 Conference

14:00 - 17:00

Session: Hybrid neural networks

Room: 323

Hybrid System for a Never-Ending Unsupervised Learning

We propose a Hybrid System for dynamic environments, where a "Multiple Neural Networks" system works with Bayes Rule. One or more neural nets may no longer be able to properly operate, due to partial changes in some of the characteristics of the individuals. We assume that each expert network has a reliability factor that can be dynamically reevaluated on the ground of the global recognition operated by the overall group. Since the net's "degree of reliability" is defined as "the probability that the net is giving the desired output", in case of conflicts between the outputs of the various nets the reevaluation of their "degrees of reliability" can be simply performed on the basis of the Bayes Rule. The new vector of reliability will be used for making the final choice, by applying two algorithms, the "Inclusion based" and the "Weighted" one over all the maximally consistent subsets of the global outcome.

Modular Robot with Adaptive Connection Topology

In this study, we physically built hardware modules which enable us to freely construct robots with various morphologies. As opposed to the existing studies of modular robotics where the connection topology among the modules has to be hand-designed, our modules are able to adaptively modify their connection topology which enables them to generate an overall behavior as one robot. We run several physical experiments where robots with various morphologies are assembled from the proposed modules to acquire several target behaviors.

Metaheuristic Techniques for Support Vector Machine Model Selection

The classification accuracy of a Support Vector Machine is dependent upon the specification of model parameters. The problem of finding these parameters, called the model selection problem, can be very computationally intensive, and is exacerbated by the fact that once selected, these model parameters do not carry across from one dataset to another. This paper describes implementations of both Ant Colony Optimization and Particle Swarm Optimization techniques to the SVM model selection problem. The results of these implementations on some common datasets are compared to each other and to the results of other SVM model selection techniques.

A Hybrid Approach for IEEE 802.11 Intrusion Detection Based on AIS, MAS and Naïve Bayes

Many problems with wireless networks are directly related to the very means used to transport data, in this case, radio waves. In addition to mis-configured equipment lack of adaptable algorithms and wireless networks are major targets for attacks. New tools to refrain that are greatly in need. Due to the fact that it is easy to attack and not so to defend wireless networks, good candidate tools would be the ones that could profit from intelligent techniques. In this paper, we use the Danger Theory (DT) and a Bayesian classifier (using naïve Bayes) embedded in a military style multi-agent system (MAS) to create a lightweight, adaptable and dynamic detection system for wireless networks (WIDS). Experimental results show that the artificial immune aspect of the proposed system is capable of detecting unknown intrusion and to identify them automatically with considerable few false alarms and low cost for the network traffic.

The Application of a CICA Neural Network on Farsi License Plates Recognition

In this paper a new license plates recognition method using a Neural Network, trained by Chaotic Imperialistic Algorithms (CICA), is introduced. In this paper the background of the plate image is omitted, the characters are separated, then the features of the characters are extracted. The features vector is feed into a multi layered perception neural network trained by CICA. Our dataset include 250 Farsi license plate images for train and 50 images for test in which the test images were noisy. The empirical results of the CICA-NN for license plate recognition are compared with the PSO-NN, GA-NN and MLP neural network. The results show that our method is faster and more accurate than the other methods.

DPF-Based Japanese Phoneme Recognition Using Tandem MLNs

This paper presents a method for automatic phoneme recognition for Japanese language using tandem MLNs. The method comprises three stages (i) multilayer neural network (MLN) that converts acoustic features into distinctive phonetic features DPFs (ii) MLN that combines DPFs and acoustic features as input and generates a 45 dimensional DPF vector with less context effect and (iii) the 45 dimensional feature vector generated by the second MLN are inserted into a hidden Markov model HMM based classifier to obtain more accurate phoneme strings from the input speech. From the experiments on Japanese Newspaper Article Sentences JNAS, it is observed that the proposed method provides a higher phoneme correct rate and improves phoneme accuracy tremendously over the method based on a single MLN. Moreover, it requires fewer mixture components in HMMs.

Using a Reinforcement-Based Feature Selection Method in Classifiers Ensemble

In the design of Classifiers Ensembles, diversity is considered as one of the main aspects to be taken into account, since there is no gain in combining identical classification methods. One way of increasing diversity is to use feature selection methods in order to select subsets of attributes for the individual classifiers. In this paper, it is investigated the use of a simple reinforcement-based method, called ReinSel, in ensemble systems. More specifically, it is aimed to evaluate the capability of this method to select the correct attributes of a dataset, avoiding unimportant and noisy attributes.

Embedding a Neural Network Into WSN Furniture

Wireless Sensor Networks (WSN) is an emerging technology that is developed with a large number of useful applications. On the other hand, Artificial Neural Networks (ANN) have found many successful applications in nonlinear system identification and control, digital communication, pattern recognition, pattern classification, etc. However, there are many similarities between WSN and ANN. For example, the sensor node itself can be seen as an artificial neuron since the WSN application show characteristics such as distributed representation and processing, massive parallelism, learning generalization ability, adaptively, inherent contextual information processing, fault tolerance and low computation. All these similarities can be explored to improve the WSN application development process by reducing the development costs without efficacy lost. This paper examines the possibility of embedding ANN and WSN into an appliance called Smart Table. Preliminary prototypal results have shown that ANN models such as Perceptrons and MLP are good candidates particularly for using it deployed into low cost System-on-a-Chip (SoC) such as PIC microcontrollers.

Local and Global Gaussian Mixture Models for Hematoxylin and Eosin Stained Histology Image Segmentation

This paper presents a new algorithm for hematoxylin and eosin (H&E) stained histology image segmentation. With both local and global clustering, Gaussian mixture models (GMMs) are applied sequentially to extract tissue constituents such as nuclei, stroma, and blood cells from background. Specifically, local GMM is firstly applied to detect nuclei by scanning the input image, which is followed by global GMM to separate other tissue constituents from background. Regular RGB (red, green and blue) color space is employed individually for the local and global GMMs to make use of the H&E staining features. Experiments on a set of cervix histology images show the improved performance of the proposed algorithm when compared with traditional K-means clustering and state-of-art multiphase level set methods.

GPUMLib: a New Library to Combine Machine Learning Algorithms with Graphics Processing Units

The Graphics Processing Unit (GPU) is a highly parallel, multi-threaded, many-core device with enormous computational power, especially well-suited to address Machine Learning (ML) problems that can be expressed as data-parallel computations. As problems become increasingly demanding, parallel implementations of ML algorithms become critical for developing hybrid intelligent real-world applications. The relative low cost of GPUs combined with the unprecedent computational power they offer, makes them particularly well positioned to fulfill the need to automatically analyze and capture relevant information from large amounts of data. Although in ML field there are countless powerful learning algorithms suitable for a wide range of applications, the true potential of these methods is underused, because many implementations are not openly shared. In the GPU arena the panorama is even worse, because few algorithms have yet been implemented. In order to mitigate this problem we propose the creation of an open source GPU Machine Learning Library (GPUMLib) that aims to provide the basis and the building blocks for the scientific community to develop GPU ML algorithms.

IAS 2010 Conference Technical Progam

August 23, 2010

13:00 – 17:30
P1: Poster Presentation
Room: Foyer area

Secure Universal Plug and Play Network

Universal Plug and Play (UPnP) is a set of specifications to enable and simplify the networking of electronic devices. UPnP does not generally provide any security and assumes that only trusted devices have access to the network. For networks where untrusted devices have to be taken into account, this paper proposes a secure UPnP network architecture, including key management. The architecture uses Transport Layer Security (TLS) to secure all TCP traffic, which carries most of UPnP messages. To establish a TLS session, each node must have an X.509 certificate for authentication. Certificates are granted by a local Certificate Authority (CA) but only if the Administrator has accepted the new node. UPnP discovery phase uses User Datagram Protocol (UDP) where it is not possible to use TLS, but we encrypt UDP data. UDP encryption key is shared by the whole network and distributed using TLS. We verified the architecture by implementation.

Safeguarding Malaysia's Critical National Information Infrastructure (CNII) Against Cyber Terrorism: Towards Development of a Policy Framework

Critical National Information Infrastructure (CNII) is crucial to the survivability of a nation. The destruction or disruption of these systems and communication networks would significantly affect the economic strength, image, defense and security, government capabilities to function, and public health and safety. CNII would probably become an attractive target for terrorists as the result of cyber attacks could leave the nation with difficult conditions due to the disruption of critical services. This paper provides an overview on the concept and fundamental elements of cyber terrorism. This paper also highlights the cyber security policy initiatives as a guideline for the development of the policy framework. This paper further recommends the need of policy development addressing the protection of CNII from cyber terrorism activities specifically for Malaysia.

Specification of Attribute Relations for Access Control Policies and Constraints Using Policy Machine

Attribute relations in access control mechanisms or languages allow accurate and efficient specification of some popular access control models. However, most of the access control systems including today's de-facto access control protocol and specification language, XACML, does not provide sufficient syntactic and semantic support for the specification of attribute relations in their scheme. In this paper, we show the deficiencies of XACML in specifying such capabilities in the implementations of the Multilevel Security, Hierarchical Role Based policies and Separation of Duty requirements of access control systems. In comparison, we then demonstrate the attribute relation mechanism provided by a relation-based access control mechanism – the Policy Machine.

A Hybrid Authentication and Authorization Process for Control System Networks

This paper presents a new authentication protocol for control systems that draws from Extensible Authentication Protocol and Kerberos. Traditional authentication schemes do not meet control system requirements of very high availability, failsafe operation, noninterruption of devices and networks, and resilience to loss of connectivity. Our hybrid protocol meets all these requirements and provides device-to-device authentication both within a remote station and between remote stations and control centers. Additionally, our protocol takes into account the unprecedented complexity arising from the intertwining of control systems with information technology (IT) components and networks.

Security preferences specification and implementation in a service-based workflow

The development of web 2.0 increases the call for agile and simple Business process support. SOA (Service oriented Architecture) provides companies with a new model to build their IT applications around their business processes and combine them dynamically and flexibly with the services of partner companies. In this open and distributed context, it is required to implement an appropriate security at each service. So, during the composition of service, it will be good for user to specify the security preference to associate to each service. In this article we describe in a first step, the difficulty of using analytical risk methods such as EBIOS, Mehari and OCTAVE to specify the constraints of security to associate with services. Then we present the SOA and its security component, therefore start the service bus ESB will act as an intermediary between the client and service provider. In a second step, we develop our method that can lead to the specification of security and describe how it would be possible to specify these security constraints during the service composition.

IAS 2010 Conference

August 23, 2010

14:00 – 15:30

Session: Secure System Architectures

Room: 334

Detecting Memory Spoofing in Secure Embedded Systems using Cache-Aware FPGA Guards

Embedded systems of an inherently distributed and highly replicated nature are vulnerable to a class of attacks that require local access and physical tampering. Processors using Encrypted Execution and Data (EED) technology, where instructions and data are stored in encrypted form in memory and locally decrypted, form an attractive solution for securing embedded systems, as these platforms have been shown to protect software and limit information leakage. However, numerous realistic attacks are still possible on EED platforms given the assumption of an adversary with physical access. In this paper, we present an integrated compiler and architectural approach to address a class of memory spoofing attacks, in which a sophisticated attacker is able to control off-chip buses and modify data blocks as they are loaded into the processor. Our approach, which utilizes cache boundaries to greatly simplify the integrity checking process, prevents an attacker from tampering, injecting, or replaying code and data. We make use of an on-chip reconfigurable logic component to implement our security mechanisms. This use of reconfigurable logic greatly simplifies the required hardware modifications - no changes are necessary to the CPU, cache, or off-chip memory. Our simulations on a number of benchmarks show that a high level of security can be achieved with a low performance overhead. The average overhead incurred is dependent on the cache size and type of integrity checking scheme used, but is less than 16% even for the most computationally intensive scheme. We present a hardware/software prototype mapped to a Field Programmable Gate Array (FPGA) platform in order to evaluate the space required and demonstrate the feasibility of our approach.

Secure Architecture for Healthcare Wireless Sensor Networks

In this paper, we propose a secure architecture for healthcare wireless sensor networks. After a careful examination of the security requirements and the security threats to healthcare sensor networks, we argue that security measures for Wireless Sensor Networks (WSN) must take application context in consideration rather than seek security solutions in a one-size-fits-all fashion. We integrate security mechanisms into our architecture for WSN in healthcare applications rather than add-on values after a general WSN architecture. Our secure architecture is unique in that it decouples patient level and system level, each of which possesses drastic differences in security requirements and computation resources. Under such architecture, security schemes/protocols are readily deployed.

End-to-end Security Policy Description and Management for Collaborative System

End-to-end security in collaborative system has two inferences: the secure delivery of service and the 'due usage' of it. The fulfillment of this requirement involves re-thinking the security policy model of collaborative systems. This paper analyses the factors that impact security in such systems. Based on this a general architecture is proposed, with a group-based policy model specified for managing end-to-end security. An ontology base is introduced to enable different concept levels in policy expression and facilitate interoperability.

Two Tier Detection Model for Misbehavior of Low-Power Nodes in Virtual MIMO based Wireless Networks

MIMO (Multiple-Input-Multiple-Output) is a promising structure for wireless communication. While virtual MIMO structure has been proposed for distributed and cooperative wireless networks, this proposed structure has also put additional energy consumption where energy stands in the important position. At the same time, we have observed that this-problem-caused low energy nodes' mibehavior will degrade the whole system efficiency. In this paper, we propose a two-tier correlation matrix based low power nodes detection system which can capture and mitigate relays' malicious behavior before signal combining. This mechanism can effectively find out the low power node in virtual MIMO structure and thus improve the system efficiency. The simulation results show that a better bit error rate performance of this structure in the presence of low power node and our detection mechanism as well is achieved.

Detect Multi-Hop Stepping-Stone Pairs with Clock Skew

Stepping-stone attacks in network intrusion detection are attackers who use a sequence of stepping-stone hosts to initiate attacks in order to hide their origins. The goal of this paper is to find algorithms to correctly detect the attacks and have the ability to tolerate the clock skew or/and chaff while exhibiting low time complexity. We propose three novel algorithms for detecting correlation and similarity of two connections not only into and out of a single stepping stone host (consecutive streams), but also across multiple stepping-stone hosts. To evaluate the accuracy and efficiency, we conduct extensive experiments. We also evaluate how chaff packets and clock skew may affect these methods. We present a comparison of the algorithms in terms of false rates of detection, and identify one of the approaches that can efficiently achieve good performance under a variety of circumstances.

IAS 2010 Conference

August 23, 2010

14:00 – 17:00

Session: Intrusion Detection

Room: 433

Benchmarking IP Blacklists For Financial Botnet Detection

Every day, hundreds or even thousands of computers are infected with financial malware (i.e. Zeus) that forces them to become zombies or drones, capable of joining massive financial botnets that can be hired by well-organized cybercriminals in order to steal online banking customers' credentials. Despite the fact that detection and mitigation mechanisms for spam and DDoS-related botnets have been widely researched and developed, it is true that the passive nature (i.e. low network traffic, fewer connections) of financial botnets greatly hinder their countermeasures. Therefore, cyber-criminals are still obtaining high economical profits at relatively low risk with financial botnets. In this paper we propose the use of publicly available IP blacklists to detect both drones and Command & Control nodes that are part of financial botnets. To prove this hypothesis we have developed a formal framework capable of evaluating the quality of a blacklist by comparing it versus a baseline and taking into account different metrics. The contributed framework has been tested with approximately 500 million IP addresses, retrieved during a one-month period from seven different well-known blacklist providers. Our experimental results showed that these IP blacklists are able to detect both drones and C&C related with the Zeus botnet and most important, that it is possible to assign different quality scores to each blacklist based on our metrics. Finally, we introduce the basics of a high-performance IP reputation system that uses the previously obtained blacklists' quality scores, in order to reply almost in real-time whether a certain IP is a member of a financial botnet or not. Our belief is that such a system can be easily integrated into e-banking anti-fraud systems.

Scaling IDS Construction Based on Non-negative Matrix Factorization Using GPU computing

Jan Platos

Attacks on the computer infrastructures are becoming an increasingly serious problem. Whether it is banking, e-commerce businesses, health care, law enforcement, air transportation, or education, we are all becoming increasingly reliant upon the networked computers. The possibilities and opportunities are limitless; unfortunately, so too are the risks and chances of malicious intrusions. Intrusion detection is required as an additional wall for protecting systems despite of prevention techniques and is useful not only in detecting successful intrusions, but also in monitoring attempts to security, which provides important information for timely countermeasures. This paper presents some improvements to some of our previous approaches using a Non-negative Matrix factorization approach. To improve the performance (detection accuracy) and computational speed (scaling) a GPU implementation is detailed. Empirical results indicate that the speedup was up to 500x for the training phase and up to 190x for the testing phase.

A Structured Approach to Anomaly Detection for In-Vehicle Networks

The complexity and connectivity of modern vehicles has constantly increased over the past years. Within the scope of this development the security risk for the in-vehicle network and its components has risen massively. Apart from threats for comfort and confidentiality, these attacks can also affect safety critical systems of the vehicle and therefore endanger the driver and other road users. In this paper the introduction of anomaly detection systems to the automotive in-vehicle network is discussed. Based on properties of typical vehicular networks, like the Controller Area Network (CAN), a set of anomaly detection sensors is introduced which allow the recognition of attacks during the operation of the vehicle without causing false positives. Moreover, important design and application criteria for a vehicular attack detection system are explained and discussed.

Intelligent Response System to Mitigate the Success Likelihood of Ongoing Attacks

Intrusion response models and systems have been recently an active field in the security research. These systems relies on fine diagnosis to perform and optimize their response. In particular, previous papers focus on the balancing the cost between of the response with the impact of the attack. In this paper, we present a novel attack response system, based on the assessment of the likelihood of success of attack objectives. First, the ongoing potential attacks are identified, and their success likelihood are calculated dynamically. The success likelihood depends mainly on the progress of the attack and the state of the monitored system. Second, candidate countermeasures are identified, and their effectiveness in reducing the pre-calculated success likelihood are assessed. Finally, the candidate countermeasures are prioritized.

RAPID: Reputation based Approach for Improving Intrusion Detection Effectiveness

Reducing false positives have been one of the toughest challenges and a very practical problem in real life deployments of intrusion detection systems. It leads to decreased confidence in the IDS alerts. The security analyst is faced with the choice between disabling valuable signatures that also generate false positives on one hand, and missing true alerts among the flood of false positives on the other hand. In this paper we present an architecture designed to reduce false positives and thereby increase the effectiveness of the IDS. In the proposed approach the IDS signatures are classified and grouped into various levels based on their false positive rating, and the incoming traffic is analyzed by one or more of the signature levels based on the reputation of the IP addresses. We also discuss a prototype implementation of the proposed approach that is based on open source IDS - Snort. Evaluation showed promising results in reducing false positives and corresponding improvement in Bayesian detection rate for the prototype system as compared to Snort.

Integrated Security Risk Management for IT-Intensive Organizations

Security risk management is becoming increasingly important in a variety of areas related to information technology (IT), such as telecommunications, cloud computing, banking information systems, etc. In this paper, we develop a systematic quantitative framework for security risk management in IT-intensive organizations. This framework provides a unified viewpoint for considering a wide array of security risk factors which can disrupt business continuity. Our approach integrates the three phases of security risk management, namely risk modeling, assessment, and control/mitigation, through a formulation based on directed graphs, cascades of failures, and mathematical optimization. We consider how security events can propagate through an organization and how resource allocation decisions can be made in order to mitigate the amount of damage they cause. The applicability and effectiveness of our framework is demonstrated through a numerical study which shows significant cost reductions when compared to heuristic methods.

Fast Intrusion Detection System based on Flexible Neural Tree

Computer security is very important in these days. Computers are used probably in any industry and their protection against attacks is very important task. The protection usually consists of several levels. The first level is preventions. Intrusion detection system (IDS) may be used as a next level. IDS is useful in detection of intrusions, but also in monitoring of security issues and traffic. This paper presents IDS based on Flexible Neural Trees. Flexible neural tree is a hierarchical neural network like structure, which is automatically created using evolutionary algorithms to solve the given problem. This is very important, because it is not necessary to set the structure and the weights of neural networks prior the problem is solved. The accuracy of proposed technique is always above the 98\% of correctly classified records and the speed of decision making process enables its using in real-time applications.

Towards Intrusion Detection by Information Retrieval and Genetic Programming

Fuzzy classifiers and fuzzy rules are powerful tools in data mining and knowledge discovery. In this work, intrusion detection is approached as a data mining task and genetic programming is deployed to evolve fuzzy classifiers for detection of intrusion and security problems. We train the fuzzy classifier on a data set modeled as a fuzzy information retrieval collection and investigate its ability to detect records that describe illegitimate actions. Proposed approach is experimentally evaluated on the popular KDD Cup intrusion detection data set.

IAS 2010 Conference

15:45 – 17:00

Session: Cryptography

Room: 324

The Number of the Isomorphism Classes of Hyperelliptic Curves of Genus Four over Finite Fields

Hyperelliptic curves of genus no larger than 4 over finite fields have been researched and recommended for cryptography. Hyperelliptic curve classification based on isomorphism is helpful for suitable hyperelliptic curve choices for secure and practical cryptosystems. The isomorphism classes of hypereilliptic curves of genus 2 or 3 over finite fields have been studied in other works. Here, the number of isomorphism classes of hyperelliptic curves of genus 4 over a finite field with the characteristic different from 2, 3 is given.

Fault Attack on AES with Single-Bit Induced Faults

This work presents a novel differential fault attack against AES of any key size, without relying on any special relation in the key schedule. Only a few works in the open literature deal with the possibility of attacking all the key sizes of the AES, while most of them focus on the 128-bit version. Although the recovery of the last round subkey weaken the security of the scheme, the description of a fault attack on an AES implementation with longer key sizes possibly using a key-schedule strategy different from the ones described by the standard, is lacking. The proposed attack relies on the possibility of injecting single bit flips, while detecting whether the faults have been injected in the correct position a posteriori. This stronger fault model nicely fits the possibility to inject precise faults through underfeeding the device in a reliable and easily reproducible way even with a simple low cost workbench. This fault injection technique, which had been successfully applied to hardware implementations of AES, receives a further validation in this paper, where the target computing device is a system-on-chip based on the widely adopted ARM926EJ-S CPU core. The attack is successfully lead against two different devices, etched with two different technologies (a generic 130nm and a low-power oriented 90nm library), running a software implementation of AES-192 and AES-256.

Extending the Definition of Guesswork

To be able to perform an analytical and more exact description of security, quantitative security measures are desirable. In this paper, we continue our investigation of the quantitative security measure guesswork, which gives the average number of guesses in an optimal brute force attack. The definition of guesswork is extended to joint and conditional guesswork. We show that joint guesswork is always at least equal to the marginal guessworks, and that conditioning reduces guesswork. Hence, guesswork possesses the same two properties as entropy, i.e., joint entropy is always at least equal to the marginal entropies, and conditioning reduces entropy. However, unlike entropy, guesswork does not possess the chain rule property. For entropy, this rule states that joint entropy is equal to marginal entropy plus the corresponding conditional entropy.

Efficient Defense Strategies to Minimize Attackers' Success Probabilities in Honeynet

In this paper, we consider the problem of minimizing attackers' success probability in a protected network subject to attacker profile/behavior constraints and defender resource/strategy constraints. Compared with previous research, the following 2 enhancements are made. First, we no longer assume that perfect knowledge regarding the network topology and defense resource allocation is fully available for attackers (a worst case scenario for the defender). Second, all combinations of attacker classes can be considered, where each attacker class may be associated with any number of attributes, including ratio, intelligence/experience level, available attack resource and sophisticated attack strategies. The problem is modeled as a generic mathematical programming problem, and a novel two-phase solution approach, which well combines mathematical programming and simulation techniques, is proposed. More specifically, in the "Objective Function Evaluation Phase", efficient and effective simulations are conducted to evaluate the effectiveness of the current defense policy; whereas, in the "Defense Policy Enhancement Phase", specially-proposed and easy-to-collect information from the "Objective Function Evaluation Phase" is adopted to calculate gradients of the decision variables. From computational experiments on honeynet, applicability and effectiveness of the proposed framework and algorithm are clearly demonstrated.

IAS 2010 Conference

August 24, 2010

15:45 - 17:00

S2: Anonymity and User Privacy

Room: 433

Anonymous Service Access for Vehicular Ad Hoc Networks

Communications through road side units in Vehicular Ad hoc Networks (VANETs) can be used to track the location of vehicles, which makes serious threat on users' privacy. In this paper, we propose and evaluate a novel location privacy enhancement protocol for VANETs. Firstly, we propose an Anonymous Online Service Access (AOSA) protocol. Secondly, we analytically evaluate the anonymity and the unlinkability of the proposed protocol. Finally, a series of simulation studies are conducted to evaluate the performance of our protocol in the real VANET environments such as Manhattan and Urban scenarios. According to analytical evaluation and simulations, our protocol provides higher level of anonymity and location privacy for on-line service access applications. Simulation results further show that our protocol is feasible and produces better performance in real VANET environments by producing higher success ratio and smaller delay.

Reconciling IHE-ATNA Profile with a Posteriori Contextual Access and Usage Control Policy in Healthcare Environment

Traditional access control mechanisms prevent illegal access by controlling access right before an action takes place; they belong to a class of a priori security solutions and, from this point of view, they have some disadvantages, like inflexibility in unanticipated circumstances. By contrast, a posteriori mechanisms enforce policies not by preventing unauthorized access, but rather by deterring it. Such access control needs evidence to prove violations. Evidence is derived from one or several log records, which trace each user's actions. Efficiency of violation detection mostly depends on the compatibility of log records with the access control policy used. In order to develop an efficient method for finding these violations, we propose restructuring log records according to a security policy model. We illustrate our methodology by applying it to the healthcare domain, taking care of the IHE (Integrating the healthcare enterprise) framework, particularly its basic security profile, ATNA (Audit Trail and Node Authentication). This profile defines log records established on the analysis of common health practice scenarios. We analyze and establish how ATNA log records can be refined in order to be integrated in to an a posteriori access and usage control process, based on an expressive and contextual security policy like the OrBAC policy.

Anonymous Communication System Using Probabilistic Choice of Actions and Multiple Loopbacks

This paper proposes a new anonymous communication system using probabilistic choice of actions and multiple loopbacks. Our system can provide both sender anonymity and receiver anonymity. Our system also decreases the computation load of each relay node, because there exist no encryption and decryption processes in our system. Applying an analysis method in an anonymous communication system called 3-Mode Net, we evaluate the number of relay nodes and sender anonymity.

IAS 2010 Conference

August 24, 2010

8:00 AM - 11:00 AM

SPEDA 2010: Security and Performance in Emerging Distributed Architectures (SPEDA2010)

Room: 324

Cooperative Access Control for the Grid

The access to Grid resources depends on rules defined by the administrators of the physical organizations and of the Grid middleware. This approach does not require support for access control in the middleware, but since changes in the access control policy of the Virtual Organization imply the involvement of one or more administrators, it lacks the flexibility needed in a several application scenarios. In this paper we propose a group-based access control model for Grid environments that increases the flexibility of the access control model offered by state-of-the-art Grid platforms without requiring changes in the middleware. The approach is based on collaboration among Grid users and allows them to exchange access permissions to Virtual Resources without the intervention administrators. We show that our solution can be defined on top of the access control mechanisms offered by state-of-the-art Grid middleware and illustrate how the proposed model can be implemented as a service in a service oriented Grid environment.

CARMA: Composable-Adaptive Resource Management Authorization for Ubiquitous Environments

The ever increasing diversity and mobility of devices have originated a marked rise in ubiquitous resources; a great number of collaborative applications could be exploited just by employing an efficient ubiquitous resource management mechanism. The CARM (Composable-Adaptive Resource Management) middleware-based architecture provides a flexible infrastructure where personal devices create seamlessly on demand interconnections links to share ubiquitous resources. In this article we address CARM's security challenges and to overcome these we propose the CARM Authorization (CARMA) module; in CARMA each user acts as an Attribute Authority (AA) responsible of issuing Attribute Certificates (ACs) and defining for each resource a set of policy-based authorization decisions; CARMA's Alerting System (AS) allows users to work in a collaborative mode by warning others of malicious nodes even when no infrastructure is available. This research mainly describes ongoing work towards a proof-of-concept implementation in the given scenarios. Our proposal enforces security considering the bandwidth efficiency and therefore enhancing the dynamic resource management experience in ubiquitous environments.

A semantic based methodology to classify and protect sensitive data in medical records

The e-Health is going to change the way how patients and health care providers interact. The exchange of confidential and integer information is one of the major open issues for the health care sector. While it is quite easy to enforce fine grain access control policies to new well structured medical records managed by newly designed information systems, many eHealth systems are based on "document management systems". In the practice the system provides a digital version of the whole medical record and it is impossible to enforce fine grain access rules. In this paper we propose the adoption of a semantic based methodology that is able to automatically retrieve the security level associated to a portion of a medical record and use this information to classify resources and locate the proper security rules to apply.

A Naming System Applied to a RESERVOIR Cloud

In Cloud Computing environments naming and resource location become critical issues. Nowadays, the Internet is using the Domain Name System (DNS), that is not suitable to new emerging cloud scenarios. A cloud environment offers a variety of concrete and abstracted entities which need to be identified. An example of cloud environment is the European project RESERVOIR, which as well as other platforms characterized by a high level of dynamism, needs to identify and resolve resources. RESERVOIR has to manage allocation, deallocation and migration of virtual machines from an execution context to another one. Such tasks could trigger identity and name alterations, in addition a virtual machine may hold one or more names, identifiers, and representations in various execution environments. This paper aims to explore several RESERVOIR use cases, demonstrating how a flexible cloud naming system enables organizations to simplify the management of their assets deployed into the cloud.

Identity Federation in Cloud Computing

Both cloud and GRID are computing paradigms for the large-scale management of distributed resources. Even if the first is usually oriented to transaction-based applications, and the latter to High Performance Computation, there is a lot of interest in their integration. This is typically obtained through the Infrastructure-as-a-Service cloud model, which is exploited in the GRID context to offer machine with full administration rights to users. In this paper the focus is on the security problems linked to the integration of cloud and GRID computing. It is proposed the adoption of identify federation between different security domains to manage the relationship between the user machines and the standard GRID infrastructure. This solution is experimented within PerfCloud, a cloud implementation that exploits an underlying GRID platform.

Securing a Tiered Re-Taskable Sensing System

Sensor Networks are widely used in several application domains thanks to their data acquisition and data processing capabilities. They are well suited to a multitude of monitoring and surveillance applications and are often involved in mission-critical tasks, thus making security a primary concern. Many architectures and protocols have been proposed to address this issue, mainly based on cryptographic operations, but it still represents an open research area: such techniques in fact, to be effective, often require complex computations and a large amount of dedicated resources, which are not available on sensor platforms according to the existing technology. Nevertheless, if considering tiered sensor networks, where tiny motes coexist with more powerful nodes, it is possible to perform some complex and efficient security schemes by exploiting the different capabilities of such nodes. In this paper we present an secure architectural proposal of the Tenet system, a tiered re-taskable sensor network architecture. Specifically, we have integrated some security library into the Tenet architecture in order to implement a hybrid cryptosystem. The latter combines symmetric and asymmetric cryptographic schemes to benefit of the security provided by asymmetric protocols and the better performance of symmetric ones.

Integrating a Network IDS into an Open Source Cloud Computing Environment

The success of the Cloud Computing paradigm may be jeopardized by concerns about the risk of misuse of this model for conducting illegal activities. In this paper we address the issue of detecting Denial of Service attacks performed by means of resources acquired on-demand on a Cloud Computing platform. To this purpose, we propose the use of a distributed strategy to detect and block attacks, or other malicious activities, originated by misbehaving customers of a Cloud Computing provider. In order to check the viability of our approach, we also evaluate the impact on performance of our proposed solution. This paper presents our distributed defence strategy and illustrates the preliminary results of the performance evaluation.

IAS 2010 Conference

11:15 - 13:00

Session: Authentication and Identity

Room: 324

A Two-Tiered Authentication and Encryption Scheme in Secure

Healthcare Sensor Networks

This paper presents a novel two-tier authentication and encryption scheme that explores the unique characteristics of Wireless Sensor Networks (WSN) in Healthcare Applications. The first phase authenticates among the sensor nodes of a Body Area Network (BAN) fused in a patient, where a U key is generated in a decentralized fashion. Based on the rule of separating user and platform credentials, U key approaches maximize security in a non-trusted environment. The second phase authenticates the data aggregation node elected among the sensor nodes of a patient with the base station in the vicinity to securely relay the U key as a session key. Encryption, secure hash, random number padding, and time stamp follow to meet the security requirements for WSN in Healthcare Applications: confidentiality, integrity, authorization, availability, and freshness. The scheme takes in consideration of WSN's resource constraints and mobility that hinder the applicability of conventional security schemes in WSN. Apart from general WSN-targeted security approaches that over-emphasize on energy consumption, this scheme provides robust, prompt, and scalable security services to healthcare systems.

Data Aggregation for Information Authentication in VANETs

Wireless communication between vehicles, known as Vehicular Ad hoc NETworking (VANET), will allow providing drivers with information to increase safety, efficiency and comfort in road travel. In this type of networks, warning messages affect decisions taken by drivers so that any wrong message could lead to loss of drivers' time, high money expenditure on fuel, and in the worst-case scenario, traffic accidents. For this reason, a prerequisite for the use of VANETs is the existence of a scheme that allows determining whether the road traffic information available to the driver is trustful. It is almost impossible to check received messages without accepting additional communication overhead and network delay. In this paper, we propose a new solution scheme based on data aggregation by using probabilistic checking to detect attacks attempts in an efficient way.

Quantifying Authentication Levels of Assurance in Grid Environments

We envisage a fine-grained access control solution that allows a user's access privilege to be linked to the assurance level in identifying the user. Such a solution would be particularly attractive to a large-scale distributed resource-sharing environment, where resources are likely to be more diversified and may have varying levels of sensitivity and resource providers may wish to adjust security protection levels in adaptation to resource sensitivity levels or the risk levels in the underlying environment. However, existing electronic authentication systems largely identify users through the verification of their electronic identity (ID) credentials. They take into account neither assurance levels of the credentials, nor any other factors that may affect the assurance level of an authentication process. This binary approach to access control may not provide cost-effective protection to resources with varying sensitivity levels. To realise the vision of assurance level linked access control, there is a need for an authentication framework that is able to capture the confidence level in identifying a user, expressed as an authentication Level of Assurance (LoA), and link this LoA value to authorisation decision-making. This paper investigates the feasibility of estimating a user's LoA at run-time by designing and evaluating an authentication algorithm that derives a LoA value, based upon not only users' ID credentials, but also other factors such as access location, system environment and depth of credential delegations.

A distributed and cooperative user authentication framework

As the requirement for companies and individuals to protect information and personal details comes more into focus, the implementation of security that goes beyond the ubiquitous password or Personal Identification Number (PIN) is paramount. With the ever growing number of us utilizing more than one device simultaneously, the problem and need is compounded. This paper proposes a novel approach to security that leverages the collective confidence of user identity held by the multiplicity of devices present at any given time. User identity confidence is reinforced by sharing established credentials between devices, enabling them to make informed judgments on their own security position. An Adaptive Security Control Engine (ASCE) is outlined, illustrating how an environment sensitive and adaptive security envelope can be established and maintained around an individual.

IAS 2010 Conference

14:00 - 15:30

Session: Multimedia Security

Room: 324

Patient's Perception of Health Information Security

Information security in health sector is getting growing attention. In connection to this, patient's perception about different aspects of health sector is worth considering. In this study attempt has been made to assess and analyze patient's perception of health information security at some selected public and private hospitals in Addis Ababa, Ethiopia. Quantitative research approach using questionnaire as an instrument was employed in an attempt to empirically address the topic. The research result reveals that patient's perception of health information security is generally low. And major determinant factors for their perception include their educational background, age and general awareness. It is also worth mentioning that patient's perception has strong implication on the service delivery and satisfaction of both service providers and patients themselves

Optimum Fusion of Visual and Thermal Face Images for Recognition

In this paper one investigation has been done to find the optimum level of fusion to find a fused image from visual as well as thermal images. Because of the use of face recognition system in critical areas like, authenticating an authorized person in highly secured areas, investigation of criminals, online monitoring etc, face recognition system should be very robust and accurate one. This work is an attempt to fuse visual and thermal face images at optimum level to extract the advantages of visual as well as thermal images. In our work, Object Tracking and Classification Beyond Visible Spectrum (OTCBVS) database has been used for the visual and thermal images. Among all the experiments a maximum recognition result obtained is 93%.

Automatic semantic annotation of images based on Web data

Image annotation is a promising approach to bridging the semantic gap between low-level features and high-level concepts, and it can avoid the heavy manual labor. Most existing automatic image annotation approaches are based on supervised learning. They often encounter several problems, such as insufficiency of training data, lack of ability in dealing with new concept, and a limited number of semantic concepts. Web images are massive, rich information, customized etc. Therefore, Web data is a potential repository to provide a sufficient source for semantic annotation. In this paper, we proposed a novel image annotation method based on Web data, which aims to utilize Web data to perform automatic image annotation. Web data, collected from several image search engine, are first preprocessed, clustered and mined to construct a concept clustering model. And then candidate annotation terms are extracted through the model for query image. Afterwards, a rank algorithm is designed to filter out noise terms. Finally, an update phase is implemented to improve the whole method. Evaluations on benchmark image datasets have indicated the effectiveness of our proposal.

Comparison of Real-time DSP-Based Edge Detection Techniques for License Plate Detection

In this paper, edge detection techniques and their performance are compared when applied in license plate detection using an embedded digital signal processor. License plate detection remains to be the crucial part of a vehicle's license plate recognition process. The edge detection algorithms compared in this work are those reported capable of delivering real-time performance. These are Canny-Deriche-FGL, Haar and Daubechies-4 wavelet transform and the classic Sobel. These particular algorithms are chosen and compared due to their good performance on digital signal processors. The comparison is drawn in terms of speed and detection success of a license plate. The results show Haar wavelet-based edge detector performs better on a DSP with LP detection speed of 7.32 ms and 98.6% success using 45,032 UK images containing license plates at 768X288 resolutions.