Recent Advances in Computational Intelligence in Defense and Security

Rami Abielmona, Rafael Falcon, Nur Zincir-Heywood and Hussein Abbass

1 Introduction

Given the rapidly changing and increasingly complex nature of *global security*, we continue to witness a remarkable interest within the defense and security communities in novel, adaptive and resilient techniques that can cope with the challenging problems arising in this domain. These challenges are brought forth not only by the overwhelming amount of data reported by a plethora of sensing and tracking modalities, but also by the emergence of innovative classes of decentralized, mass-scale communication protocols and connectivity frameworks such as *cloud computing* [5], *sensor and actuator networks* [7], *intelligent transportation systems* [1], *wearable computing* [2] and *the Internet of Things* [6]. Realizing that traditional techniques have left many important problems unsolved, and in some cases, not adequately addressed, further efforts have to be undertaken in the quest for algorithms and methodologies that can accurately detect and easily adapt to emerging threats.

Computational Intelligence (CI) [4] lies at the forefront of many algorithmic breakthroughs that we are witnessing nowadays. This vibrant research discipline offers a broad set of tools that can deal with the imprecision and uncertainty prevalent in the real world and can effectively tackle ill-posed problems for which traditional (i.e., hard computing) schemes do not provide either a feasible or an efficient solution. The term CI is not exclusive to a single methodology; rather, it acts as a large umbrella under which several biologically and linguistically motivated techniques have been developed [3]—some of them enjoying unprecedented popularity these days [4]. CI has expanded its traditional foundation (pillared on *artificial neural networks*, *fuzzy systems* and *evolutionary computation*) to accommodate other related

R. Abielmona · R. Falcon (✉)
Larus Technologies Corporation, 170 Laurier Ave West - Suite 310, Ottawa, ON K1P 5V5, Canada
e-mail: rafael.falcon@larus.com

N. Zincir-Heywood
Dalhousie University, Halifax, Canada

H. Abbass
University of New South Wales, Canberra, Australia

R. Abielmona et al. (eds.), *Recent Advances in Computational Intelligence in Defense and Security*, Studies in Computational Intelligence 621,
DOI 10.1007/978-3-319-26450-9_1

problem-solving approaches that have recently emerged and also functionally pursue the same goals of tractability, robustness and low solution cost [3, 4], including but not withstanding: *rough sets*, *multi-valued logic*, *connectionist systems*, *swarm intelligence*, *artificial immune systems*, *granular computing*, *game theory*, *deep learning* and the *hybridization* of the aforementioned systems.

As a recognition of the influence CI algorithms are increasingly having upon the security and defense realm, the IEEE Computational Intelligence Society (CIS) created a *Task Force on Security, Surveillance and Defense*[1] (SSD) in February 2010 to showcase recent and ongoing efforts in the application of CI methods to the SSD domain. The flagship event organized by the Task Force, as a forum to exchange ideas and contributions in these topics, is the *IEEE Symposium on Computational Intelligence for Security and Defense Applications* (CISDA), which originated in 2007 and has been annually held since 2009. Other related initiatives are the *Computational Intelligence for Security, Surveillance and Defense* (CISSD) Special Session held at WCCI 2010/2014 and at SSCI 2011/2013; the *Soft Computing applied to Security and Defense* (SoCoSaD) Special Session organized under ECTA 2014; the *Workshop on Genetic and Evolutionary Computation in Defense, Security and Risk Management* held during GECCO 2014 and 2015; and the Canadian Tracking and Fusion Group (CTFG) annual workshops since 2011.

This volume is another endeavour undertaken by the IEEE CIS SSD Task Force and a step in the right direction of consolidating and disseminating the role of CI techniques in the design, development and deployment of security and defense solutions. The book serves as an excellent guide for surveying the state of the art in CI employed within SSD projects or programs. The reader will find in its pages how CI has contributed to solve a wide range of challenging problems, ranging from the detection of buried explosive hazards in a battlefield to the control of unmanned underwater vehicles, the delivery of superior video analytics for protecting critical infrastructures or the development of stronger intrusion detection systems and the design of military surveillance networks, just to name a few. Defense scientists, industry experts, academicians and practitioners alike (mostly in computer science, computer engineering, applied mathematics or management information systems) will all benefit from the wide spectrum of successful application domains compiled in this volume. Senior undergraduate or graduate students may also discover in this volume uncharted territory for their own research endeavors.

We received 53 initial submissions in November 2014 as a response to the Call for Book Chapters, out of which 25 were accepted following the recommendations emanating from the peer-review process conducted by the Technical Program Committee composed of 74 experts and researchers in the field from 22 countries. The 25 accepted chapters were co-authored by 75 contributors from the following countries: Australia (2), Belgium (1), Canada (24), China (1), Cuba (3), India (5), Italy (9), Saudi Arabia (1), Singapore (3), Spain (7), Thailand (3), Tunisia (1), UK (2) and USA (13). It is important to note that 73 % of the contributors are affiliated with academic institutions, 17 % with industry and the remaining 10 % with government.

[1] http://www.ieeeottawa.ca/ci/ssdtf/.

1.1 Volume Organization

The book is structured into five major parts corresponding to the themes that naturally emerged out of the accepted contributions, i.e., physical, cyber and biometric security, situational/threat assessment and mission planning/resource optimization. They are representative of five strategic areas within defense and security that evidence the burgeoning interest of the CI community in developing cutting-edge solutions to entangled problems therein.

Part I: Physical Security and Surveillance [4 chapters]
The problem of detecting buried explosive hazards using forward-looking infrared and ground-penetrating radar sensors is described in Chap. 2 "*Computational intelligence methods in forward-looking explosive hazard detection*". The authors elaborate on the prescreening phase (detection of candidate points in the image) and then on the classification phase. They report the performance of different approaches in the latter phase, ranging from kernel methods to more advanced algorithms like deep belief and convolutional networks to learn new image space features and descriptors.

In the Chap. 3 entitled "*Classification-driven video analytics for critical infrastructure protection*", the authors are concerned with alleviating the burden of an operator that constantly monitors several video feeds to detect suspicious activities around a secured critical infrastructure. The automated solution proposed in this chapter extracts the objects of interest (i.e., car, person, bird, ship) from the image using an iteratively updated background subtraction method, then the object is classified by an artificial neural network (ANN) coupled to a temporal Bayesian filter. The next step is determining the behavior of the object, e.g., entering a restricted zone or stopping and dropping an object. Relevant alerts are issued to the operator should a suspicious event be identified. The authors tried their approach in the automated monitoring of a dumpster, a doorway and a port.

A model-based event correlation framework for critical infrastructure surveillance is put forward in Chap. 4 "*Fuzzy decision fusion and multiformalism modeling in physical security monitoring*". The framework named DETECT (DEcision Triggering Event Composer & Tracker) stores detected threat scenarios using event trees and then recognizes those scenarios in real time. A multiformalism approach for the evaluation of fuzzy detection probabilities using fuzzy operators upon Bayesian Networks and Generalized Stochastic Petri Nets is presented. The authors considered a threat scenario of a terrorist attack in a metro railway station to illustrate the applicability of their methodology.

Chapter 5 "*Intelligent radar signal recognition and classification*" investigates a classification problem for timely and reliable identification of radar signal emitters by implementing and following an ANN-based approach. The idea is to determine the type of radar given certain characteristics of its signal described by a group of attributes (some of them having missing values). Two separate approaches were considered. In the first one, missing values are removed using listwise deletion and then a feedforward neural network is used for classification. The other approach leans on a multiple-imputation method to produce unbiased estimates of the missing data

before it is passed to the ANN. In both cases, competitive classification accuracies were obtained.

Part II: Cyber Security and Intrusion Detection Systems [5 chapters]
Chapter 6 "*An improved decision system for URL accesses based on a rough feature selection technique*" addresses corporate security; in particular, internal security breaches caused by employees accessing dangerous Internet locations. The authors propose a classification system that detects anomalous and potentially insecure situations by learning from existing white (allowed) and black (forbidden) URL lists. It then decides whether an unseen new URL should be allowed or denied. The system's performance is boosted by the removal of irrelevant features (guided by rough set theory) and handling class imbalances, with a reported classification accuracy reaching about 97 %.

Chapter 7 "*A granular intrusion detection system using rough cognitive networks*", the authors designed an intrusion detection system from a Granular Computing angle to classify network traffic as either normal or abnormal. The proposed methodology relies on rough cognitive networks (RCNs), a recently introduced granular system that combines the causal representation inherent to fuzzy cognitive maps with the imprecision-handling abilities provided by rough set theory. The RCN parameters are learned from data using Harmony Search as the underlying optimization engine. RCNs were evaluated against seven other traditional classifiers and were found to be a competitive model that produces high detection rates and low false alarm rates.

Chapter 8 "*NNCS: randomization and informed search for novel naval cyber strategies*" argues that software security can be improved by providing adequate degrees of redundancy and diversity to counter both hardware and software faults. The proposed scheme relies on component rule bases written in a schema-based Very High Level Language. Deviations from the constructed model are likely indicators of a cyber attack. The authors illustrate the benefits of their proposal with a battle management example.

Developing classifiers that can identify sophisticated types of cyber attacks is the main goal of Chap. 9 "*Semi-supervised classification system for the detection of Advanced Persistent Threats*". The authors define an anomaly score metric to detect the most anomalous subsets of traffic data. The human expert is then required to label the instances within this set, after which a classifier is built based on both labeled and unlabeled data. Genetic programming, decision trees and support vector machines were independently used to construct the classifier.

Chapter 10 "*A benchmarking study on stream network traffic analysis using active learning*" aims at comparing the performance of previously existing active learning and query budgeting strategies as well as an adaptive ANN approach on streaming network traffic to detect malicious network activity such as botnets. The analysis revolves around two new metrics that account for class imbalance as well as the traditional accuracy and detection rate measures. Results are quite encouraging and confirm that the Hoeffding Tree classifier behaves particularly well on the data sets under consideration.

Part III: Biometric Security and Authentication Systems [5 chapters]
Handwritten signatures have long been used as an authentication system given that they are intrinsically endowed with specificity related to an individual. In Chap. 11 "*Visualization of handwritten signatures based on haptic information*", the authors discuss how to integrate haptic technologies to capture other aspects like kinesthetic and tactile feedback from the user. The study is centered around visualizing and understanding the internal structure of the haptic data (position, force, torque and orientation) in an unsupervised fashion. Special emphasis is made on several dimensionality reduction methods, including CI-based ISOMAP and Genetic Programming.

Reducing the number of false positives in a biometric identification system is at the heart of Chap. 12 "*Extended metacognitive neuro-fuzzy inference system for biometric identification*". The authors introduce a neurofuzzy inference system along with a sequential evolving learning algorithm as a cognitive component of an architecture that also features a metacognitive component. The latter is responsible for actively regulating the learning of the cognitive component by deciding what, when and how to learn from the available data. The proposed architecture is first benchmarked on a set of medical datasets and then on two real-world biometric security applications, namely signature verification and fingerprint recognition. The comparison with four other authentication systems confirms that the proposed architecture yields a superior performance.

Travel documentation at this time relies either on paper documents or on electronic systems requiring connectivity to core servers and databases for verification purposes. Chapter 13 "*Privacy, security and convenience: biometric encryption for smartphone-based electronic travel documents*" proposes a new paradigm for issuing, storing and verifying travel documents. This smartphone-based approach enables a new kind of biometric checkpoint to be placed at key points throughout the international voyage that does not require storage of biometric information, which simplifies things from a policy and privacy perspective. The authors expect their architecture to enhance system security as well as the privacy and convenience of international travelers.

Digital watermarking allows enforcing authenticity and integrity of an image, which is a major security concern for many industries. The optimization of the embedding parameters for a bi-tonal watermarking system is pursued in Chap. 14 "*A dual-purpose memory approach for dynamic particle swarm optimization of recurrent problems*". The authors propose a memory-based Dynamic Particle Swarm Optimization method. This memory can operate in either generative or regression mode and is implemented via a Gaussian Mixture Model of candidate solutions estimated in the optimization space, which provides a compact representation of previously found PSO solutions. Results indicate that the computational burden of this watermarking problem is reduced by up to 90.4 % with negligible impact on accuracy.

Chapter 15 "*Risk assessment in authentication machines*" presents an approach for building a risk profiler for use in authentication machines. The proposed risk profiler provides a risk assessment at all phases of the authentication machine

life-cycle. The key idea is to utilize the advantages of belief networks to solve large-scale multi-source fusion problems. The authors have extended the abilities of belief networks by incorporating Dempster-Shafer Theory measures. The main goal is to increase the reliability of security risk assessment for authentication machines using the computational-intelligence-based fusion of results from different models, metrics, and philosophies of decision-making under uncertainty.

Part IV: Situational Awareness and Threat Assessment [5 chapters]
To counter piracy attempts, maritime operators need to quickly and effectively allocate some mobile resources (defender units) to assist a target given the available information about the attackers. In Chap. 16 "*Game theoretical approach for dynamic active patrolling in a counter-piracy framework*", the authors introduce a decision support system (DSS) to that end. The DSS has been designed using Game Theory in order to handle the attractiveness of targets and model strategies for attackers and defenders. Game Theory has proved to be a robust tool to identify the best strategy for the defenders given the information and capabilities of opponents. In the proposed framework, the optimal strategy is modeled as the equilibrium of a time-varying Bayesian-Stackelberg game.

A naval mine is an underwater explosive device meant to damage or destroy surface ships or submarines. An influence mine is a type of naval mine that is triggered by the influence of a vessel or submarine rather than requiring direct contact with it. The ship classification unit (SCU) of an influence mine determines whether the sensed vessel is a target or not, which will cause it to detonate accordingly. In Chap. 17 "*mspMEA: the microcones separation parallel multiobjective evolutionary algorithm and its application to fuzzy rule-based ship classification*", the author uses a parallel multiobjective evolutionary algorithm (MOEA) based on the concept of microcones to speed up the optimization of the fuzzy rule-based classifiers used to emulate the SCU contained in modern influence mines. A speedup factor of 16.58 % was achieved over a cone-based MOEA algorithm.

Detecting a target in a Synthetic Aperture Radar (SAR) image is a challenging issue since SAR images do not look similar to optical images at all. In Chap. 18 "*Synthetic aperture radar (SAR) automatic target recognition (ATR) using fuzzy co-occurrence matrix texture features*", the authors put forward a methodology for detecting three types of military vehicles from SAR images without using any preprocessing methods. The texture features generated from the fuzzy co-occurrence matrix are passed on to a multi-class SVM and to a radial basis function (RBF) neural network. The ensemble average is utilized as an information fusion tool. The classification results are superior to those obtained via gray level co-occurrence matrices.

Text mining techniques are important for security and defense applications since they allow detecting possible threats to security and public safety (such as mentions of terrorist activities or extremist/radical texts). Chapter 19 "*Text mining in social media for security threats*" discusses information extraction techniques from social media texts (Twitter in particular) and showcases two applications that make use of these techniques: (1) extracting the locations mentioned in tweets and (2) inferring the users' location based on all the tweets generated by each user. The former task

is accomplished via a sequence-based classifier followed by disambiguation rules whereas the latter is tackled through deep neural networks.

The increasing worldwide use of mobile devices has also sparked a growing number of malware apps that should be automatically flagged and vetted by security researchers. Chapter 20 "*DroidAnalyst: synergic Android framework for static and dynamic app analysis*" features an automated web-based app vetting and malware analysis framework for Android devices that integrates the synergy of static and dynamic analysis to improve the accuracy and efficiency of the identification process. DroidAnalyst generates a unified analysis model that combines the strengths of the complementary approaches with multiple detection methods to boost the app code analysis. Machine learning methods such as random forests are employed to generate a set of features with multiple detection methods based on the static and dynamic module analysis.

Part V: Strategic/Mission Planning and Resource Management [6 chapters]

Chapter 21 "*Design and development of intelligent military training systems and wargames*" elaborates on an architectural approach for designing composable, multi-service and joint wargames that can meet the requirements of several military establishments. This architecture is realized by the design and development of common components that are reused across applications and variable components that are customizable to different training establishments' training simulators. Some of the important CI techniques (such as fuzzy cognitive maps, game trees, case-based reasoning, genetic algorithms and fuzzy rule-based systems) that are used to design these wargame components are explained with suitable examples, followed by their applications to two specific cases of Joint Warfare Simulation System and an Integrated Air Defence Simulation System for air-land battles.

Due to operational requirements, helicopters are now being frequently used for missions beyond what their original design permits. There is thus the need to monitor their usage and more accurately determine the life of its critical components. The methodology outlined in Chap. 22 "*Improving load signal and fatigue life estimation for helicopter components using computational intelligence techniques*" enables the prediction of the load signals (i.e., the time-varying measurement of the load) on the helicopter components using existing flight data and avoiding the installation of additional sensors. The prediction is performed by means of CI techniques (e.g., fuzzy sets, neural networks, evolutionary algorithms) and statistical techniques (e.g., residual variance analysis). The predicted load signals then form the basis for estimating the fatigue life of the component, i.e., the length of time that the component can be safely operated with minimal or acceptable risk of failure. The presented techniques certainly attained a more accurate prediction of the peak values in the load signal.

Defense and security organizations rely on the use of scenarios for a wide range of activities. Scenarios normally take the form of linguistic stories, whereby a picture of a context is painted using storytelling principles. In Chap. 23 "*Evolving narrations of strategic defense and security scenarios for computational scenario planning*", the authors illustrate how evolutionary computation techniques can be used to evolve

different narrations of a strategic story. A representation of a story is put forth that allows evolution to operate on it in a simple manner. Through a set of linguistic constraints and transformations, it is guaranteed that any random chromosome gets transformed into a unique coherent and causally consistent story. The same representation could be used to design simulation models that evaluate these stories. The proposed approach paves the way for automating the evaluation process of defense and security scenarios on multiple levels of resolution, starting from a grand strategic level down to a tactical level.

Chapter 24 "*A review of the use of computational intelligence in the design of military surveillance networks*" surveys the state of the art in the application of CI methods to design various types of sensor networks, including wireless/fixed sensor, mobile ad hoc and cellular networks, as these constitute the backbone for realizing Intelligence, Surveillance and Reconnaissance (ISR) military operations. The authors also list important defense and security applications of these networked systems, review the CI methods and their usage and outline a number of research challenges and future directions.

Given the prolific number of sensing modalities available nowadays, determining on which platform a sensor should be mounted to collect measurements during the next observation period is far from being a trivial task. Chapter 25 "*Sensor resource management: intelligent multi-objective modularized optimization methodology and models*" proposes a new sensor tasking framework named OPTIMA that aims at solving this problem. OPTIMA features a Sensor Resource Analyzer module and a Sensor Tasking Algorithm (Tasker) module. The latter leans on multiobjective evolutionary optimization methods to consider timing constraints, resolution and geometric differences among the sensors with the goal of fulfilling some tasking requirements related to maximizing the available sensor resources for search, optimizing sensor resources for tracking and better defending the high-priority assets.

Chapter 26 entitled "*Bio-inspired topology control mechanism for unmanned underwater vehicles*" addresses the problem of having a group of unmanned underwater vehicles (UUVs) cooperatively self-organize in order to protect valued assets in unknown 3D underwater spaces. The topology control mechanism is rooted in particle swarm optimization and employs Yao-graph-inspired metrics to craft its fitness function. The self-organization protocol only requires neigborhood-limited UUV information to collectively guide the UUVs to make movement decisions in these unknown 3D spaces. The algorithm is able to provide a user-defined level of protection for different maritime vessel applications. The proposed methodology is illustrated with three examples: (1) uniform coverage of the underside of a maritime vessel; (2) plane formation to cover a given dimension in the 3D space and (3) forming a sphere around a given asset such as a fully submerged submarine while maintaining connectivity.

Our hope is that the wealth of technical contributions gathered in this book helps create further momentum and drive forward many other theoretical and practical aspects of the fascinating synergy between CI methods and the defense and security problem spaces. Enjoy the reading!

References

1. Barfield, W., Dingus, T.A.: Human Factors in Intelligent Transportation Systems. Psychology Press, New York (2014)
2. Hong, J., Baker, M.: Wearable computing. IEEE Pervasive Comput. **2**, 7–9 (2014)
3. Kacprzyk, J., Pedrycz, W.: Springer Handbook of Computational Intelligence. Springer, New York (2015)
4. Kruse, R., Borgelt, C., Klawonn, F., Moewes, C., Steinbrecher, M., Held, P.: Computational Intelligence: a Methodological Introduction. Springer Science & Business Media, Berlin (2013)
5. Lu, G., Zeng, W.H.: Cloud computing survey. In: Applied Mechanics and Materials, vol. 530, pp. 650–661. Trans Tech Publ (2014)
6. Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D.: Context aware computing for the internet of things: a survey. Commun. Surv. Tutor. IEEE **16**(1), 414–454 (2014)
7. Verdone, R., Dardari, D., Mazzini, G., Conti, A.: Wireless Sensor and Actuator Networks: Technologies, Analysis and Design. Academic Press, London (2010)