An Interdisciplinary Approach to Machine Learning for Critical Infrastructure Protection

Mario LA MANNA
Evoelectronics
Rome, Italy

ABSTRACT

Critical infrastructure protection faces increasing challenges, both in quality and in quantity. Most of the present security systems fully rely on automated mechanisms, which replace human operators, in order to perform computation intensive tasks and/or to work in extreme conditions. However, this solution presents some drawbacks with respect to the system performance. In order to provide effective measures against the pressure of new and sophisticated threats, an interdisciplinary approach, based on suitably coupling machine learning with human judgment, results as the right choice. In fact, this solution is particularly helpful for implementing efficient solutions capable of controlling critical scenarios and reacting effectively towards sophisticated threats. This paper discusses the proposed approach and demonstrates that this approach is the best choice for the effective protection of critical infrastructures.

Keywords: Critical infrastructures, machine learning, situational awareness, environment monitoring, network security.

1. INTRODUCTION

An advanced security system for critical infrastructures (Fig. 1) is composed of the following subsystems: a) Sensor subsystem, whose function is to collect raw data coming from the environment; b) Data and Information Fusion subsystem, which has the function to merge data coming by the sensors and data and information coming from external intelligence sources; c) Human Agent in the Loop subsystem, which performs operations by means of a human operator in the decision loop; d) Intelligence subsystem, which gathers data coming from intelligence (mainly produced by human experts) and e) Core Processor, which combines all the information produced by the previous subsystems, performs machine learning and extracts real time outputs.

The system is based on an interdisciplinary (human/machine) approach, having to cope with the heterogeneity of the data produced by the system itself, those collected by the monitoring tools and secure information coming from different sources. Monitoring data are derived from different types of sensing units, while secure information comes from intelligent external sources, human in the loop agents and system intelligence. This paper focuses on a novel methodology, embedded in the system, which is based on the synergy between automated machine learning and human judgment and demonstrates that the application of this methodology is beneficial for the effective protection of critical infrastructures.

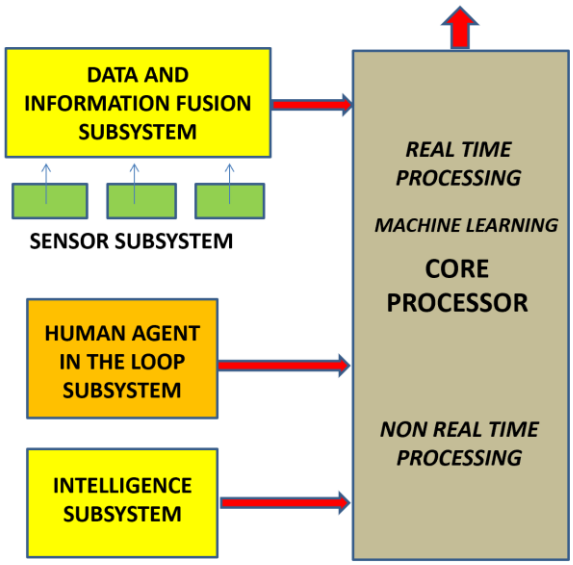

Fig. 1: Advanced Security System Architecture for the protection of Critical Infrastructures.

2. MACHINE LEARNING FOR CRITICAL INFRASTRUCTURE PROTECTION

The machine learning approach to the protection of critical infrastructures is based on artificial intelligence techniques (e.g. statistical modelling) and on computational intelligence techniques (e.g. nature inspired methodologies).

The techniques based on artificial intelligence are traditionally classified into supervised and unsupervised learning techniques. In the first category (supervised learning), the main solutions are: decision trees [7], rule learners [8], Bayesian networks [9], Naive Bayes approach [10], instance-based learners [11] and perceptron-based technique [12]. In the second category (unsupervised learning), the main techniques are: association rule learning [13], clustering techniques [14] and Markov chains [15].

The techniques based on computational intelligence are: genetic algorithms [16], artificial neural networks [17], fuzzy logic [18] and artificial immune systems [19].

3. THE ROLE OF HUMAN JUDGMENT

The previously listed machine learning techniques are derived from a high number of scientific fields, namely logics, statistics, optimization theory, etc.

Independently from the technique chosen for a specific case, the application of machine learning is structured in a number of steps, which constitute a process, typical of the protection chain. This process is composed of the following sub-processes (Fig.2).

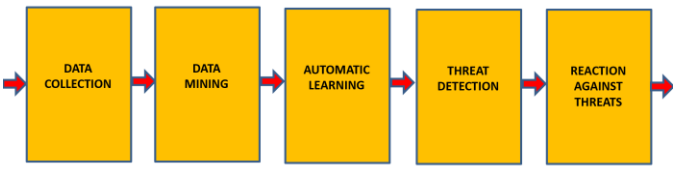

Fig. 2: Machine learning process for critical infrastructure protection.

1) Data collection: this sub-process consists of capturing and recording a huge amount of data coming from external sensors and/or communicated by intelligence actors (typically represented by human experts) for subsequent processing and training.
2) Data mining: this sub-process incudes pre-processing, standardizing and preparing the collected data, in order to correctly feed the system inputs inside the system.
3) Automatic learning: this sub-process implements three different steps, namely training, tuning and validating the previously prepared data. It allows to build internal intelligence and automatic capabilities, in order to respond to the incoming threats. Learning can be unsupervised (the system has not any knowledge about the learned variables) and supervised (there is knowledge about these variables).
4) Threat detection: this sub-process provides the crucial function of discovering threats and evaluating the relative risks for the system integrity and survival.
5) Reaction against threats: this sub-process has the function of defining appropriate actions to counteract the discovered threats and to minimize damages and risks for the whole system.

Independently from the technique adopted for machine learning during the whole process, from the experience gathered in real case studies, the synergy between man and machine is particularly important during Sub-process 3 (Automatic Learning) and Sub-process 5 (Reaction against threats). In particular, the most relevant aspects of the man-machine cooperation are; a) supervision in the machine learning prior to the training and b) human support to the reaction process.

We include the aforementioned aspects into a Man-Machine Sinergy Algorithm, which allows to provide the necessary intelligence and automatic capabilities, in order to neutralize rapidly and efficiently the incoming threats.

4. MAN-MACHINE SYNERGY ALGORITHM

The Man-machine Synergy Algorithm starts from the concept, derived from practical experience in real cases, that situation assessment (i.e. real time detailed information on what is happening on a determined scenario) is strongly dependent on the total amount of known significant characteristics of the environment. In particular, we observe that the main knowledge about these characteristics derives from human experience, more than from data coming from external sensors. This means that, in order to build a true model of the environment, the knowledge of a human expert is generally prevalent above the contribution given by an automated function. Moreover, a further contribution comes from the Human Agent in the Loop subsystem, which instructs the automated system to gather information contained in a certain amount of raw data. According to the above observation, the first section of the Man-Machine Synergy Algorithm has a direct impact on the automatic machine learning, In particular, independently from the adopted methodology for learning (supervised/unsupervised), a predefined knowledge scheme is introduced before the traditional automatic learning. This scheme is used to create a knowledge base, also with variables different from the ones involved in the automated sub-process. These variables come from the Intelligence and Human Agent in the Loop sub-systems.

The role of intelligence and human in the loop is to create a solid knowledge background, which can steadily improve the efficiency of the subsequent learning activity, mainly with respect to the known attacks and known attack strategies, but in most cases also regarding unknown attacks. From direct experience in real cases, the percentage of human information (coming from intelligence and human in the loop) vs. the total information gathered by a system can be described as a function of the system complexity, as reported in Fig. 3.

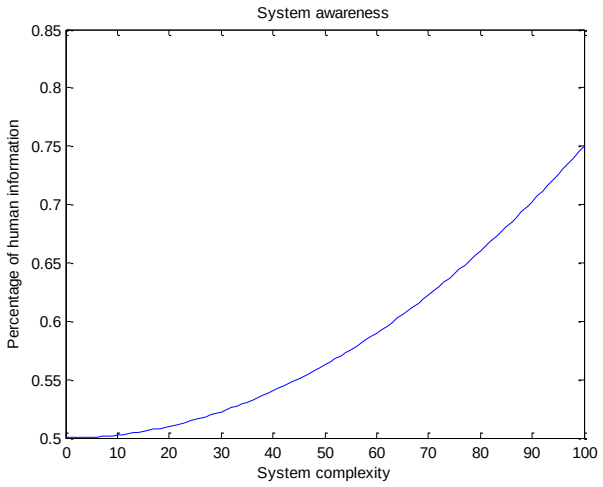

Fig. 3: Percentage of human information in system awareness as a function of system complexity.

The same Man-machine Synergy Algorithm has another impact on the reaction sub-process. According to its characteristics, the system reaction can be either passive or active. Passive reaction consists of raising an alarm or switching off the system. An active reaction means to counteract the threat, in order to avoid a system failure. This second type of reaction requires more judgment and deep knowledge coming from experience. For this reason, the a-priori knowledge base, created by intelligence and human in the loop, has the function to funnel the machine function to the most efficient actions. This part of the man-machine synergy algorithm can be described as an integrated recovery action. From direct experience, the percentage of human information (coming from intelligence and human in the loop) vs. the total information necessary for an efficient recovery as a function of the system complexity, can be approximated in the diagram reported in Fig. 4.

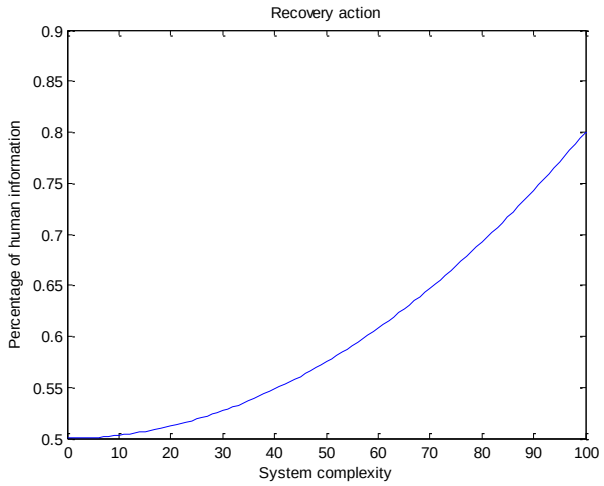

Fig. 4: Percentage of human information in a recovery action as a function of system complexity.

5. THE INTEGRATED SYNERGY PROCESS

This section has the goal to estimate quantitatively the benefit of the man-machine synergy algorithm with respect to system awareness. As discussed in the previous section, the knowledge base created by the operator, by means of the intelligence and human in the loop sub-systems has the function of improving the quality of the subsequent learning activity. In fact, the automation introduced by machine learning is quite useful when the tasks involved are intensive in computation or they occur when working conditions are extreme. On the other hand, human judgment results decisive to setup the system to a correct functioning in a determined context. Taking only into account the quantity of data that can be gathered by human operators, in order to be used by the learning process, as discussed in the previous section, the system awareness is considerably enhanced by introducing the man-machine synergy algorithm. In particular, if we consider the system awareness of a typical system [6] and take into account the results reported previously (see Fig.3), we can derive the diagram of a typical system awareness as a function of system complexity, with and without man-machine synergy (Fig.5). From this diagram, we can observe that the synergy between man and machine can sensibly improve system awareness, starting from low complexity systems (starting from value 0) to very complex systems (up to value 100) .

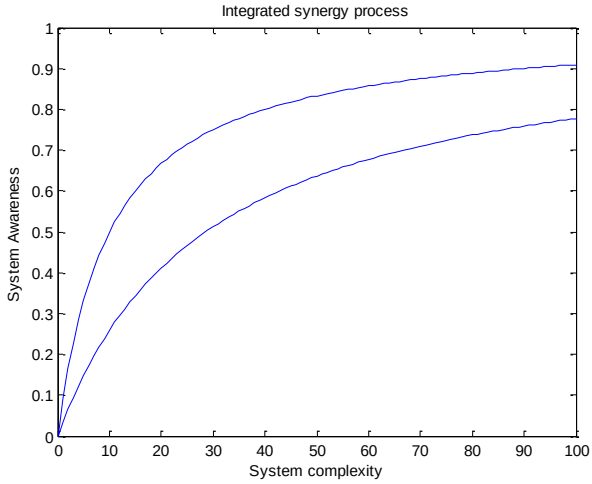

Fig. 5: System awareness as a function of system complexity, with (upper diagram) and without (lower diagram) man-machine synergy.

6. THE INTEGRATED RECOVERY ACTION

This section has the goal to estimate quantitatively the benefit of the man-machine synergy algorithm with respect to a recovery action. As discussed in Section 4, the knowledge base created by the operator, by means of the intelligence and human in the loop sub-systems, can also improve the effectiveness of the recovery action. If we take only into account the quantity of data that can be gathered by human operators, in order to be used by the recovery action, as discussed in the Section 4, the probability of recovery is considerably enhanced by introducing the man-machine synergy algorithm. In particular, if we consider the probability of recovery of a typical system [6] and take into account the results reported previously (see Fig.4), we can derive the typical probability of recovery as a function of system complexity, with and without man-machine synergy (Fig.6). From this last diagram, we can observe that the synergy between man and machine can sensibly improve the recovery action, in particular when the system complexity grows up and the number of environment characteristics tends to be high. In fact, the defensive action of the network has to be based on a suitable knowledge of the common vulnerabilities and exposures of the network, together with a deep understanding of the strategies of the possible attacker.

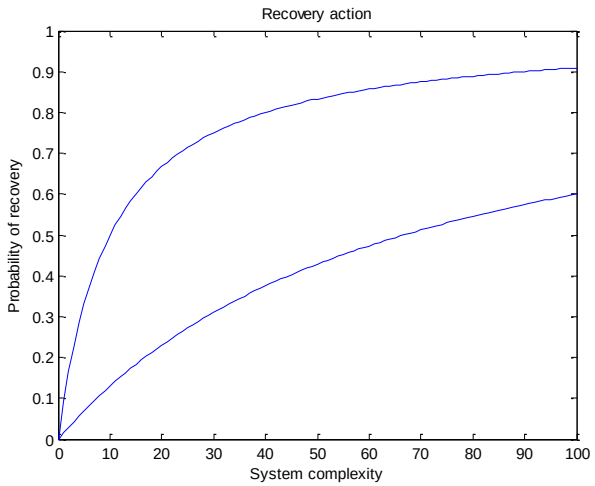

Fig. 6: Probability of recovery as a function of as a function of system complexity, with (upper diagram) and without (lower diagram) integrated recovery action.

7. CONCLUSIONS

This paper describes how to increase the effectiveness of the systems dedicated to the protection of critical infrastructures by building a synergy between human judgment and automated machine learning. In particular, we present a novel methodology, based on a mixture of automated machine learning and human judgment and demonstrate that this joint approach is beneficial for the effective protection of critical infrastructures. The advantages of our approach are measured quantitatively, taking into account two main critical aspects of the machine learning process, namely situation assessment and recovery action. Starting from data collected on the field in real applications, we show that both situation assessment and recovery action are considerably improved by merging machine learning and human judgment in a cooperative way.

8. REFERENCES

[1] M. LaManna ”Urban Environment Monitoring: System and Technology Issues”, IMCIC 2012, 25-28 March 2012, Orlando, FL.

[2] M. LaManna “Data Fusion of Heterogeneous Sensors in Urban Environment Monitoring” IMCIC 2013, 9-12 July 2013, Orlando, FL.

[3] M. LaManna “Cost-Benefit Analysis of Automated Systems for the Control of Urban Critical Infrastructures” WMSCI 2015, 12-15 July 2015, Orlando, FL.

[4] M. LaManna “Future Trends for Cyber Security for Critical Infrastructures” WMSCI 2016, 5-8 July 2016, Orlando, FL.

[5] M. LaManna “Technology Intercepts for Cyber Security applied to Critical Infrastructures” WMSCI 2017, 8-11 July 2017, Orlando, FL.

[6] M. LaManna “Multisensor Data Fusion for Cyber Security in Critical Infrastructures” WMSCI 2018, 8-11 July 2017, Orlando, FL.

[7] B. Kamiński, M. Jakubczyk, P. Szufel "A framework for sensitivity analysis of decision trees". Central European Journal of Operations Research, 2017.

[8] R.J. Urbanowicz, J.H.Moore "Learning Classifier Systems: A Complete Introduction, Review, and Roadmap". Journal of Artificial Evolution and Applications. 2009.

[9] N.Friedman, D. Geiger, M. Goldszmidt "Bayesian Network Classifiers". Machine Learning, Nov. 1997.

[10] H.Zhang “The Optimality of Naive Bayes”, Florida Artificial Intelligence Research Society Conference, 2004.

[11] W. Daelemans, A. Van den Bosch, “Memory-Based Language Processing”. Cambridge University Press, 2005.

[12] M. L. Minsky, S. A. Papert “Perceptrons, Expanded Edition”. MIT Press, 1988.

[13] M.Hahsler "Introduction to arules, a computational environment for mining association rules and frequent item sets”, Journal of Statistical Software, 2005.

[14] E. Achtert, C. Böhm, P. Kröger, A. Zimek "Mining Hierarchies of Correlation Clusters", International Conference on Scientific and Statistical Database Management, 2006.

[15]P.A.Gagniuc “Markov Chains: From Theory to Implementation and Experimentation”, John Wiley & Sons, 2017.

[16] S.Skiena, “The Algorithm Design Manual”, Springer Science and Business Media, 2010.

[17] S.Haykin “Neural networks : a comprehensive foundation”, Prentice Hall, 1999.

[18] V. Novak, I. Perfilieva, J. Močkoř “Mathematical principles of fuzzy logic”, Dordrecht: Kluwer Academic, 1999.

[19] L.N.de Castro, J. Timmis “Artificial Immune Systems: A New Computational Intelligence Approach”. Springer, 2002.