An Adaptive Immune Based Anomaly Detection Algorithm For Smart WSN Deployments

M. Salvato, S. De Vito, S. Guerra, A. Buonanno, G. Fattoruso, G. Di Francia
ENEA – Italian National Agency for New Technologies, Energy and Sustainable Economic Development
P. le E. Fermi, 1, 80055 Portici (NA), Italy,
saverio.devito@enea.it

***Abstract*— The growing attention in smart WSN deployments for monitoring, security and optimization applications urges the design of new tools in order to recognize, as soon as a possible, anomalous states of systems whenever they occur. In order to develop an anomaly detection system enabling to discover unusual events in a non-stationary process, a scalable immune based strategy has been adopted. The algorithm works as an instance based 1-class classifier capable to un-supervisedly model the "normal" spatial-temporal variable behavior of the system identifying first order anomalies. Typical immune-like processes guarantee a slow adaptation of the set of local patterns to long term variation in the monitored system. The algorithm has been applied to a several real scenarios showing to be able to work on both on resource constrained WSN nodes and on dealing with large data streams in centralized data processing facilities.**

***Keywords*—Artificial immune system; anomaly detection; dynamic learning; cyclostationary process**

I. INTRODUCTION

Pervasive deployments of WSNs nodes are continuously growing meeting the requirements of complex cities infrastructures monitoring. Several applications require the deployments of self or battery powered low cost nodes that operated on severe resource constraints conditions, that may affect computational power, memory resources, transmission capabilities, available energy, etc. On board data intelligence may help the node to save on transmission energy identifying significant data to be transmitted [1]. Moreover, often the system to be monitored is characterized by processes showing non stationary behavior as in the case of water cycle monitoring systems [2], air quality monitoring [3], HVAC System monitoring [4]. In order to efficiently monitor non stationary processes, the typical wireless sensors network node could be equipped with an anomalies detection system enabling to identify unusual, significant and/or dangerous events. The anomaly definition task, already hard to be defined in static conditions, assumes hence a more difficult spatial-temporal configuration. Indeed, in static condition, a sample in a dataset is defined to be anomalous if it does not fall in the statistical distribution of the dataset, representing its "normal" model. However, a priori knowledge about the underlying distribution of the monitored variables may not be available. Even when it could, it may be related to a limited timeframe being unrepresentative of the whole system evolution during time. Indeed, in the employed WSN distributed architectures, each node, depending on its different spatial position, deal with recording and analysis of a specific time series data. Local behavior of each node can be modeled as a non-stationary process in a multi-varied space, i.e. parameters describing its statistical distribution significantly change over time. Many relevant processes related to human activities actually show behaviors that can be defined as cyclostationary. So, sensors data distribution can not be described in absolute global sense rather it should be represented locally in both space and time sense. This condition practically prevents to obtain complete a-priori knowledge about local ordinary trends of process variables. This, in turn, does not allow the use of supervised anomalies detection approaches. For these reasons, an adaptive and unsupervised anomaly detection strategy, capable to continuously learn normality patterns adapting them to slow changes over time, is requested.

In this paper, in order to locally and un-supervisedly identify sensorial patterns that locally (first order anomalies) deviates from a «normal» cyclostationary measure context, we propose a novel algorithm based on adaptive immune artificial system. Statistical tests allow us to define a «normal» configuration of the process starting from a total agnosticism about the underlying distribution of monitoring parameters and taking advantage just on field recorded data deriving from sensor readings. Typical immune processes as selection, mutation and cloning guarantee instead to build and sustain a time-variable «normality» model. In this way, the algorithm works as statistical one-class instance based classifier labelling a local space-temporal event as anomalous whenever it falls out the "normal" samples distribution in a current spatial-temporal configuration. Such an anomaly detection methodology can have many potential applications. Indeed, the algorithm is designed to work both on resource constrained WSN nodes and in centralized data processing facilities where it could deal with large data streams.

We plan to employ this algorithm in three different real world scenarios. In the SiMonA (Integrated waste water monitoring system) project, a whole sewer system is monitored by means of a distributed WSN deployment enabling the fast identification of local anomalies due to illegal drains or faults on the system while automatically sending alerts, in order to minimize the environmental and infrastructure damages. A subset of sensors is forced to work with very harsh battery constraints hence the need of on board identification of anomalies. In the SEM (Smart Energy Master) project, the above methodology is employed for energy efficiency monitoring reasons. In this framework, the algorithm is able to recognize local anomalous patterns in energy usage data on different aggregation scale (single appliance or office, group of buildings, HVAC systems or micro-PV production sites)

978-1-4799-8591-3/15/$31.00 ©2015 IEEE

and over multiple timescales. In this way, it is possible not only the identification but also the forecasting of faults on the power network. In the Baitah project, local anomalies are recognized for indoor and outdoor air monitoring purposes in order to ensure alerting for anomalous air pollution events.

In this work we present results related with an air quality monitoring deployment using data recorded by conventional air quality station operated by regional environmental protection agency and located in a large city spot characterized by harsh cars traffic.

II. AN IMMUNE BASED ALGHORITHM

In this section, the overall architecture as well as the primary steps of our immune based algorithm are described. The targeted application framework concerns the monitoring of parameters that are strongly influenced by human activities and weather conditions, typically characterized by daily and weekly cyclostationarity, with slow seasonally changes. Relying on this assumption, an initial weekly knowledge about data distribution is built up by ingesting sensor observations. Building on an instance-based architecture and adopting Euclidean distance, all dataset features but time dimension, are expressly normalized. This furthers a time based data clusterization that allow for obtaining a concise and efficient representation of the "normal" behavior. Afterwards, the gathered knowledge is slowly adapted by means of immune based actions including cloning, mutation and selection in order to follow long term variations. In this way, by building on the work of O.Nasraoui et al. [4], we aim to describe an immune based approach capable to learn and adapt to the characteristics of the field recorded data simultaneously retaining knowledge of the past and being robust to burst of outliers.

A. Alghoritm Prototypes representation

Immune based algorithms typically operate with two principal entities, i.e. antibodies and antigens. Specifically, in the initial boot phase, and for a fixed one week long time window, each sensor measurement is stored in an antibodies set, a *dynamic B-cells* (DBs) reservoir. Each subsequent incoming samples is indicates instead as *antigen*. The DBs reservoir acts as the "normal" prototypes set, actually representing the algorithm internal knowledge. Each DBs can be described, by means its features vector, as a point in the multivariate space, having an own influence sphere, a stimulation level *s* and a specific age *a*. Specifically, the radius $c*\sigma^2$ of its influence sphere represents the variance of the Gaussian distribution prototyped by each DB . The algorithm, dynamically adapts each DB radius size on the strength of the novel incoming field recorded sensor readings. This allows for the efficient computing of the actual feature space coverage of an antibody simultaneously adapting it to short term evolutions. The dynamic antibodies characterization is completed with a stimulation and age parameters. Specifically, the stimulation level allows to model, over time, the DB cell local representativeness with regards to the set of incoming sensor readings. Large stimulation levels actively slow down the ageing process of a DB cell rejuvenating its age parameter. The DBs characterization by these parameters guarantees at all times an accurate ad faithful representation of the system evolution. In order to obtain a scalable model, DBs, competing each other for the memory resources, are partitioned in clusters (Fig.1) by means of a density based clustering algorithm (DBSCAN). In this way, the problem of the anomalies recognition involves only a set of cluster representative instances (cluster centroids) and not all DBs with considerable computational advantages obtained with an immune network approach.

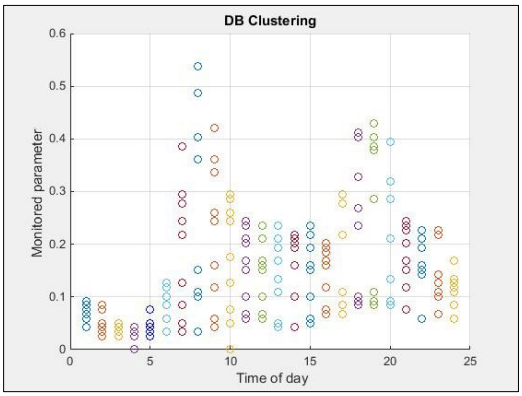

Fig. 1. Hourly DBs clustering sphere representation. Different colours for each cluster.

On the basis of the DB based representation, antigens are hence classified as "normal" or otherwise "anomalous" if their feature vector significantly differs from the current normality pattern described by closest hourly DBs.

B. Alghoritm stages

The algorithm encompasses several steps. After a clustering phase in which DBs are organized in a clusterized immune network, the presentation phase starts. Specifically, in this phase, each new incoming antigen is actually exhibited to the immune network to recognize its closer cluster C_n according to its distance with respect to the centroid of clusters. From this point onwards, the issue of classification of the current antigen is so simplified no more involving the whole network but just the antigen and its closer cluster. Without loss of the generality, the current antigen classification is performed evaluating just its distance to the closest DB in the selected cluster C_n. Indeed, the antigen that does not fall in the influence sphere of this DB is then labelled as an "anomalous" pattern. Otherwise it is flagged as an "activator" if the following *activation condition* is satisfied:

$$\frac{d_{ij}}{\sigma_{DB}} < c \qquad (1)$$

where d_{ij} is the distance of the i-th DBs with respect to j-th current antigen. The *c* parameter, instead, efficiently tune the algorithm sensitivity to abnormal patterns acing as a statistical coverage factor. We will refer to it also as *sensitivity factor*. Higher *c* values correspond to a limited sensitivity of the algorithm, conversely lower values will probably lead to an increased number of detected anomalies triggering an enhanced sensitivity to diversity. On the basis of antigen classification, C_n's DBs parameters are updated accordingly. In case of an anomalous antigen detection, DBs stimulation level

978-1-4799-8591-3/15/$31.00 ©2015 IEEE

and influence sphere radius do not change, whereas DBs' age increases modeling antibodies ageing process. Otherwise, the presence of an "activator" indicates that the antigen falls in the influence sphere of the closest DB in C_n. This DB is flagged as "activated". For its inherent representativeness, the activated DB modifies its characterization in a way that differs from the others DBs belonging to C_n. While all C_n DBs rejuvenates, the activated antibody's age is zeroed. Specifically, the others ones decreases their age proportionally to their distance with respect to the activating antigen. DBs influence spheres radius instead are updated considering their distance to the antigen and their current value:

$$\sigma_{i,j}^2 = \frac{e^{-\frac{1}{\tau}} * \sigma_{i,j-1}^2 \; * \sum_{t=1}^{j-1} w_{i,t} + w_{ij} \; * d_{ij}^2}{(e^{\frac{1}{\tau}} * \sum_{t=1}^{j-1} w_{i,t} + w_{ij})} \qquad (2)$$

where w_{ij} is the weight associated to i-th antibody. It is re-defined, whenever a new j-th antigen incomes, as

$$w_{ij} = e^{-\frac{d_{ij}^2}{2 * \sigma_{i,j-1}^2}} \qquad (3)$$

allowing to estimating the DB-antigen distance regard to DB current sphere influence radius. Otherwise, parameter τ acts as a *resilience factor*. It, weighting antibodies past history, allows to tune the adaptation speed of the local patterns configurations to the long term variation of the stochastic process. Actually, τ value modulates the algorithm plasticity/stability trade off. Finally, DBs stimulation level changes with the inverse of the updated influence sphere's radius, in this way:

$$s_{ij} = \frac{e^{-\left(\frac{1}{\tau}\right) * \sum_{t=1}^{j-1} w_{i,t} + w_{ij}}}{\sigma_{i,j}^2} \qquad (4)$$

Cloning and mutation processes are then implemented for the activated DB. The number of DB clones is proportional to its contribute to the total amount of cluster stimulation. The rate of mutation, instead, is inversely proportional to its stimulation contribution to mean cluster stimulation. Specifically, the DBs copies are a translation in the multivariate space of the activated DB, so their features vectors change while their stimulation level, influence sphere and age are set at the same value of its parent. Finally, two selection strategies have been introduced in order to eliminate redundancies in the representative antibodies population improving scalability. A first type of selection concerns the redundancy removal from the DBs dataset. For each clusters, those DBs with an influence sphere totally lying within the influence zone of others DBs are deleted. Actually, their contribution does not enhance the knowledge about the local statistical distribution of the sensorial node. Furthermore, those antibodies, simultaneously showing a low stimulation level (wrt the average stimulation level of its cluster) and a significant age are removed. This account for the removal of antibodies being no more representative of the current time local "normality" pattern evolution. In this sense, they are not more competitive in the local set pattern description.

Pseudo code
1. Clustering phase: DBSCAN clustering of the certain fixed number of antibodies (about 200 samples) ; For each antigen:

Pseudo code
2. Presentation phase: 2.1 Compute the closest cluster C_n; 2.2 Increase the age of DBs belonging to furthest clusters; 3. Activation phase: 3.1 Compute in C_n the closest DB (DB_{cl}) wrt the antigen 3.2 Compute the *activation condition (1)* for DB_{cl} If it is satisfied, DB_{cl} is said *activated* – go to (3.3) ; otherwise: antigen is flagged as anomaly- go to (3.4) ; 3.3 Update σ and s for each DBs in C_n like in *(2)-(4);* Set DB_{cl} age to zero; Decrease the age of the other DBs in C_n; 3.4 Increase the age of all DBs in C_n; 4. Clonation-Mutation phase: 4.1 Clone and mutate only the activated DB_c; 5. Suppression phase 5.1 Suppression of the oldest and less stimulated DBs when the population size goes beyond a threshold; 5.1.1 Re-clustering of DBs; 5.2 Elimination of redundant DBs

III. RESULT

In order to test the developed algorithm, a real world recorded air pollution data set has been employed. City air pollution process is known to follow daily and weekly ciclostationary pattern with slow concept drifts mostly induced by seasonal changes in weather and atmospheric conditions. Data are sampled from a conventional air pollution analyzer, operated by the regional environmental protection agency (ARPA) in an Italian city [5]. The multidimensional features set is built up by the hourly averages (not normalized) and the monitored parameters (min-max normalized with respect the whole dataset). The hourly averages of the concentration values were sampled from 10/03/2004 to 4/4/2005. We make use of a features vector with three variables including weather and pollution data (time of day (h), carbon monoxide (CO (mg/m^3)), temperature (T/°C)). The first 200 samples data are used for the first representation of local distribution of the time series data, while the remaining are used as antigens, and thus presented one-by-one to the clusterized antibodies network.

In the below figures, the identification of a local anomalous measure at 11 p.m of an April day is shown. It is characterized by the following normalized feature vector F_v=(h=11, CO=0.344, T=0.91), that it has been identified to be anomalous in correspondence of sensitivity and resilience factors respectively equal to c=2.5 and τ=1.5. This sample (Fig. 3) is recognized to be abnormal in the current day at 11p.m. The same patter would be recognized as normal, for example, at 7 p.m., a time of day where instead generally an high air pollution level is registered. This shows the capabilities of the algorithm to model time local behavior. Fig. 4 shows trends exhibited by the main descriptive parameters of the algorithm. In particular, by analyzing the trends of average influence sphere radius and antibodies population size, it is possible to note an inverse trend. This is caused by the algorithm dynamic that further the development of an efficient coverage of the normality manifold by means of a small number of partially overlapped DBs. In figure 5, a 3D-view of the DBs distribution identifying the above mentioned anomaly pattern, is shown. Each DBs is plotted with its influence sphere differently colored depending on clusters to which it

978-1-4799-8591-3/15/$31.00 ©2015 IEEE

belongs. The sample, outlined with the red point, is falling outside of green spheres represents an usual CO measure for that time of day. It is hence flagged as a first order anomaly.

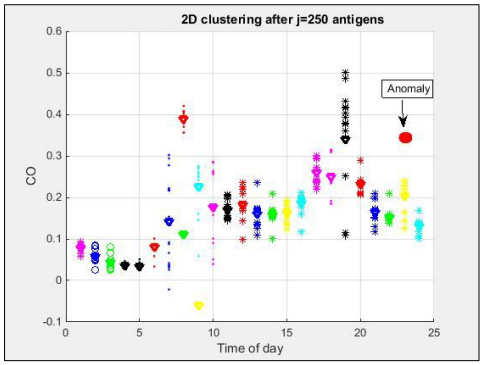

Fig. 3. The 2D (h-CO) view shows an anomalous pattern at 11 p.m (red point).

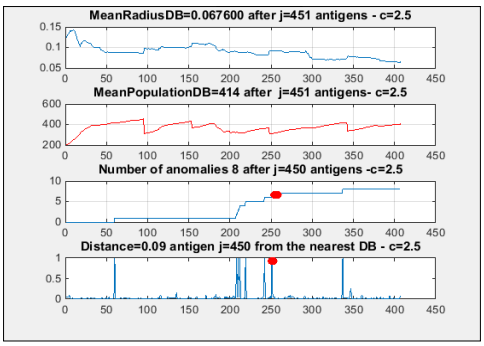

Fig. 4. The average trend of the main attributes of the alghoritm

Finally, in order to test the actual algorithm sensitivity to the abnormal samples, in figure 6 the number of local observed anomalies, as a function of sensitivity parameter *c* after 500 antigens presentations, are plotted. The number of local anomalies decreases significantly from c=0.5 to c=2 , while for greater values of c, it reachs stable values around to 20 anomalies.

IV. Conclusions

Here we presented an immune inspired algorithm devised to efficiently model the slowly changing cyclostationary pattern encountered in monitoring human activity related processes. This property emerges by a time local set of evolving representative instances acting as antibodies in an immune network while competing on memory and computation resources. Long term adaptation is allowed by means of cloning-mutation-selection process while short term adaptation is enforced by adapting antibodies coverage zone to antigens distribution. Algorithm parameters allow to tune sensitivity and adaptivity rates to inherent changes in the incoming data patterns. The preliminary results obtained on a real world deployment show the capability to model time local behavior and robustness to outliers encouraging us to continue the algorithm development. In particular we will focus on both on board implementation in the framework of a smart cyber physical system and on producing specific tests in order to verify and to improve adaptive capability over long terms.

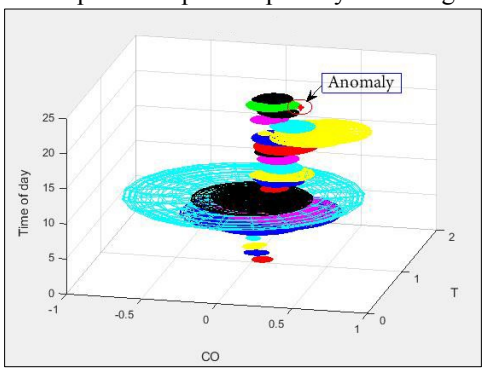

Fig. 5. A 3D view DBs distribution with their influence sphere. The red point typifies a first order anomaly

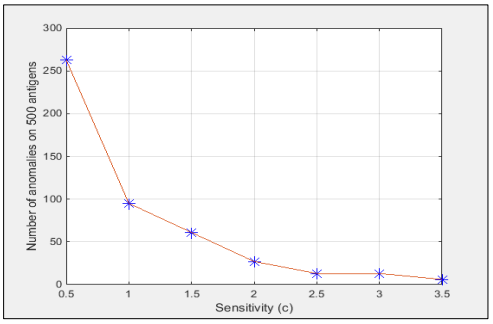

Fig. 6. The number of observed anomalies as a function of sensitivity parameter c.

Acknowledgment

This work has received funding from the POR SiMonA - Integrated waste water monitoring system-, PON SEM -Smart Energy Master and PON Baitah projects .

References

[1] S. De Vito, et al. “Wireless sensor networks for distributed chemical sensing: Addressing power consumption limits with on-board intelligence”,"Sensors Journal, IEEE",11,4,947-955,2011

[2] N. Oliker, A.Ostfeld. "Minimum volume ellipsoid classification model for contamination event detection in water distribution systems." Environmental Modelling & Software , 2014, 1-12.

[3] M. I., Mead, et al. "The use of electrochemical sensors for monitoring urban air quality in low-cost, high-density networks." Atmospheric Environment 70 (2013): 186-203.

[4] J. Liang, R. Du, “Model-based Fault Detection and Diagnosis of HVAC systems using SVM method”, International Journal of Refrigeration, 30, 6, 2007, 1104-1114, ISSN 0140-7007

[5] O. Nasraoui, et al., “A scalable artificial immune system model for dynamic unsupervised learning”, Genetic and Evolutionary Computation—GECCO, 2003, Springer Berlin Heidelberg ,219-230.

[6] S. De Vito,et al. “On field calibration of an electronic nose for benzene estimation in an urban pollution monitoring scenario”, Sensors and Actuators B: Chemical, 129, 2, 2008, 750-757, ISSN 0925-4005

[7] S. Rajasegarar,et al., “Ellipsoidal neighbourhood outlier factor for distributed anomaly detection in resource constrained networks”. Pattern Recognition, 47(9), 2867-2879, 2014.