Experiences in Ensemble-based Decision Systems for Wireless Sensor Networks

Madalin Plastoi, Ovidiu Banias, Constantin Volosencu and Daniel-Ioan Curiac
Automation and Applied Informatics Department
"Politehnica" University of Timisoara
Timisoara, Romania
{madalin.plastoi, ovidiu.banias, constantin.volosencu, daniel.curiac}@aut.upt.ro

Abstract— **Wireless sensor networks are often used to monitor and measure physical characteristics from remote or hostile environments. In these conditions, data accuracy is a very important aspect for the way these applications complete their objectives. In this paper, we introduce a new approach for detecting wireless sensors anomalies. Our methodology relies on an ensemble-based system, composed of multiple binary classifiers adequately selected to implement a complex decisional system on network base station.**

Keywords- wireless sensor networks, ensemble-based systems, sensors anomalies, data accuracy.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are collections of small hardware devices responsible for monitoring and detecting different kinds of events, in almost any types of environments. Very often, the correctness of the measured values provided by each sensor node is a critical factor for the evolution of the investigated environments. Therefore, for a WSN application it is very important to have robust and fail safe sensors that expose correct measurements and, respectively, to receive and work with correct sets of data. There are situations when one or several network sensors measurements are affected by a deliberate or an accidental anomaly, anomaly that can cause erroneous data, compromising the objectives of the entire network. These behaviors are usually caused by sensor hardware related problems or by security attacks, especially, intrusion attacks for compromising node and network data.

Previous relevant researches in the field of anomaly detection are developed around single binary classifiers that decide if the wireless sensor network activity is normal or abnormal by comparing the actual state of the WSN nodes with an intricate model of "correct behavior". This stratagem was implemented in different forms using intelligent algorithms.

In [1], Bhuse and Gupta enforce the idea of reusing the already available system information that is generated by different protocols, at various layers of the network. Their method incurs very little additional cost and thus is ideally suited for resource constrained WSNs.

The research described in [2] proposes a novel scheme to detect anomalies based on the localization of sensor nodes, called LAD – Localization Anomaly Detection. The scheme takes advantage of the deployment knowledge that is available in many sensor network applications and is implemented in a distributed way at the sensor node level.

Another interesting anomaly detection scheme is depicted in [3]. The proposed approach is able to detect anomalies accurately by employing only significant features of in-network data signals. For this, the authors used a mixture between the Discrete Wavelet Transform (DWT) and a competitive learning neural network called Self-Organizing Map (SOM).

In [4], a cooperative monitoring scheme to detect the displacements of sensor nodes by the cooperation of implicated nodes is described. The methodology is mainly based on the feasible Received Signal Strength Indicator (RSSI) values to collect the data of anomalous actions in WSNs.

In our paper, we propose a new approach for tackling these kinds of issues by implementing a powerful anomaly detection mechanism using an Ensemble-Based System (EBS). This ensemble-based system consists of multiple binary classifiers, each classifying every network node functioning as being accurate or erroneous. In our view, when dealing with dynamic and complex WSN's environments, we can model this proper functioning state based on past measurements recorded by the investigated node and respectively, on measurements recorded by all adjacent nodes.

Numerous research studies have exposed that EBS can outperform the single classifier approach [5]-[7]. The motivation behind this result is that by combining diverse and accurate models, we may improve the ensemble decision over each single classifier decision. The keystone of every EBS is represented by the notion of diversity between base classifiers which plays a crucial role in the success of ensemble learning techniques [8]. Intuitively classifiers are diverse if they make different errors.

The rest of the paper is organized as follows: Section 2 describes the proposed methodology. Section 3 presents the implementation and a case study. Finally, conclusions and future works are offered in Section 4.

II. METHODOLOGY FOR ENSEMBLE-BASED ANOMALY DETECTION

Generally, sensor anomalies are handled by dedicated rule-based decisional systems. For taking node behavior related decisions, it makes more sense to "ask" more than one decision making entities, because this practice assures undoubtedly a better, more informed, and trustable final decision.

 ISBN: 978-1-61208-166-3

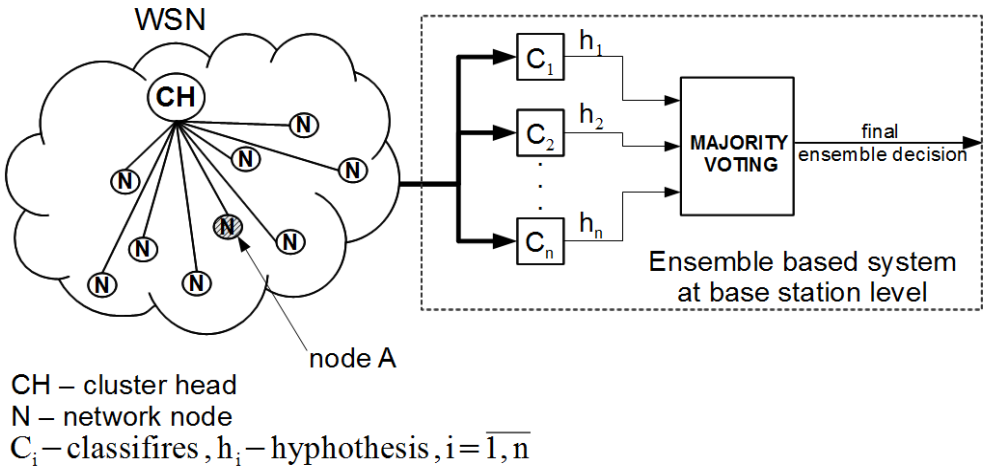


Figure 1. WSN with ensemble-based system at base station level

We name these decisional instances as classifiers or experts, and their collection an ensemble-based system [8][9].

Assuming that all the transmitted data within the network is confidential, the network may be a target for security attacks. In this paper, we address only those security attacks that try to prevent the network from the correct functioning by injecting erroneous sensor measurements. Worst, the network could experience hardware failures for one or more attached sensors that also mean erroneous sensor measurements. We developed and used an ensemble-based system to periodically investigate and detect each and every sensor node's anomaly. As presented in Fig. 1, this ensemble contains several binary classifiers that separately classify the state of each sensor as "reliable" or "unreliable". All the classifier outputs will be aggregated and the final ensemble decision will be generated, using a specific combination pattern [10]. The final ensemble decision will be further used by the base station to take all the required actions for the unreliable nodes.

The proposed methodology describes how the ensemble-based system is designed and used, and consists in the following set of steps:

- **Step 1.** First step in building the EBS is to choose both, the network data that needs to be classified, and the classification results set. Data for classification represents the measurements gathered by a specific node A, at a specific moment in time . Regarding the classification results, all possible results of a classification are called classes and form a set like:

$$\{\omega_1, ..., \omega_C\}, \quad (1)$$

where each ω_i represents a label or property associated with the classified data, and C represents the cardinal or the results set. In the case of anomaly detection, binary classification is used, meaning that we deal with only two possible classes: ω_1 - accurate data, labeled as "0" and ω_2 - erroneous data, labeled as "1".

- ***Step 2.*** In the second phase, the number of classifiers and their input data boundary are decided. In the case of a WSN cluster the EBS input data are represented by past measurements gathered by the node A and respectively, past and present measurements gathered by each of the node A neighbors $x_k(t)$, where k represents one of the neighbor nodes.

- ***Step 3.*** In the third phase, we design and train all classifiers. For EBS, when it comes to designing classifiers, there are several approaches that can be used, depending on the type of data and the real application [11]. All the designed classifiers need to be trained with real or sampled data accordingly to each classification class ω_i . Structurally, each classifier may contain prediction based algorithms, decisional trees and other artificial intelligence algorithms. As presented in (2), each classifier makes a hypothesis $h_j(t)$, indicating the class which better suits the classified data.

$$h_j(t) \in \{\omega_1, ..., \omega_C\} \quad (2)$$

- ***Step 4.*** The obtained classifiers form the EBS residing at base station level. Through a data acquisition interface, every measurement provided by a node A is classified by the ensemble-based system within the base station. This happens for a

 ISBN: 978-1-61208-166-3

fixed period of time and always ends by issuing $h_j(t)$ hypothesis.

- ***Step 5.*** All the classifiers results, $h_j(t)$, are then combined using a voting schema for taking the final ensemble decision. In this context, there are several approaches for combining classifiers results, some of them requiring additional trained classifiers, while others requiring only the $h_j(t)$ hypothesis [12]. The class ω_i that obtains the greatest number of votes $V_i(t)$ is established as the final ensemble decision. A simple vote $v_{ij}(t)$ indicates that hypothesis $h_j(t)$ selected the class ω_i, in other words, the classifier with *j* index, selected the class with *i* index. As presented in (3) and (4) the total number of votes V_i for the class ω_i counts all simple votes for that class.

$$V_i(t) = \sum_{j=1}^{C} v_{ij}(t) \tag{3}$$

$$v_{ij}(t) = \begin{cases} 1, & \text{if } h_j = \omega_i \\ 0, & \text{if } h_j \neq \omega_i \end{cases} \tag{4}$$

The ω_i class is chosen as final ensemble decision if it was chosen by at least one more than half the number of the classifiers; e.g: when having an ensemble of three classifiers, a decision is taken when at least two of three classifiers pass the same vote.

- ***Step 6.*** After the ensemble final decision has been taken, if the investigated node is found as having sensor anomalies, the network base station acts in consequence and excludes node's sensor from network functioning sensors sets for a limited period of time. As an example, this can be achieved based on the following rule: if the EBS indicated at least three times that the node A suffers from a sensor anomaly, the base station decides to inactivate the sensor. The base station could later reuse the sensor after repeating the EBS investigation for testing if new readings became appropriate.

III. IMPLEMENTATION AND CASE STUDY

For demonstrating the above concept and methodology we performed a case study that assumes the existence of a clustered WSN responsible for the temperature measurements into an unsupervised environment. Using an experimental network composed of nine Crossbow-Imote2 nodes equipped with ITS400 sensors boards, we developed an ensemble-based system that detects sensor measurements anomalies.

The experimental network measures the temperature in nine locations $\theta(t)$ and reports all measurements to a base station machine, through a gateway. This process is repeated for a fixed period of time. The measured temperature has values from 21°C to 21.6 °C. We simulate erroneous measurements gathered by a certain node of the network (node A), by artificially increasing the node A measured temperature using a heat lamp placed in the vicinity of node A at three distinct moments in the supervised period *T*. We designed and used three binary classifiers:

1. C_1 - an average based classifier that receives all present measurements of each of the node's A neighbors and computes an average measurement value as presented in (5).

$$x_{A(AV)}(t) = \sum_{i=1}^{k} x_i(t) / k \tag{5}$$

where *k* represents the number of neighbors. The classifier C_1 consists of an average computing block that provides a value that will be subtracted from the current measurement value of the sensor A. If the absolute value of the result exceeds a given threshold ε_{C_1} then the measurement provided by the node A is classified as abnormal.

2. C_2 - an autoregressive predictor based classifier that receives all past measurements of the node A and predicts its current measurement as shown in (6):

$$x_{A(AR)}(t) = a_1(t) \cdot x_A(t-1) + \ldots + a_n(t) \cdot x_A(t-n) + \xi(t) \tag{6}$$

where a_i are the autoregression coefficients, *n* is the order of the autoregression and ξ is assumed to be the Gaussian white noise. This classifier consists of a 3rd order autoregressive predictor that provides an estimated measurement for the sensor A that will be subtracted from the current measurement value of sensor A. If the absolute value of the result exceeds a given threshold ε_{C_2} then the measurement provided by the node A is classified as abnormal. The autoregressive predictor is designed and used similar as in [13].

3. C_3 - a neural prediction based classifier that receives all past and present measurements values

 ISBN: 978-1-61208-166-3

of each of the node's A neighbor nodes and predicts the present measurement of the node A using a transformation function similar with equation (7):

$$f(x) = K(\sum_i v_i g_i(x)) \quad (7)$$

where K is a composition function, v_i are the network weights, and g_i is a vector containing neurons inputs $g = (g_1, g_2, ..., g_n)$. This classifier consists of a 3rd order feed forward neural network with two hidden layers of neurons, trained to provide a value that will be subtracted from the current measured value of sensor A. If the absolute value of the result exceeds a given threshold ε_{C_3} then the measurement provided by the node A is classified as abnormal.

In order to illustrate how our methodology works, we gathered temperature values from a group of nine sensor nodes placed in an indoor environment. The measurements provided by the sensor under investigation (sensor A) were intentionally perturbed using a heat lamp at three instants in time (t=15, t=20 and t=27 seconds). The temperature time series for sensor A and two of its neighbors are presented in Fig.2.

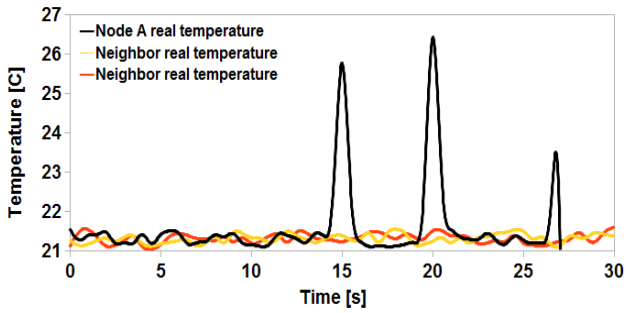
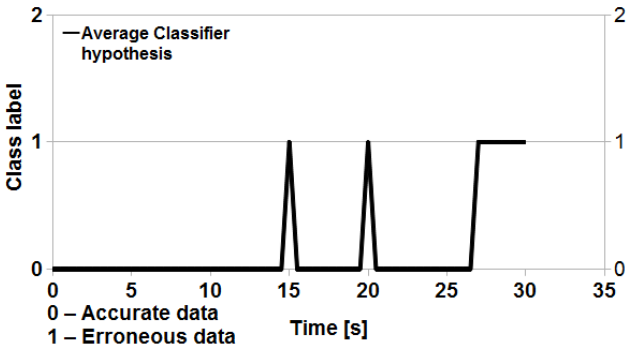


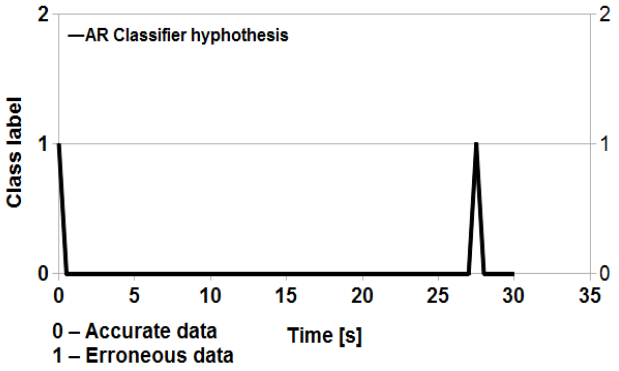
Figure 2. Measured temperatures for the node A and two of its neighbors

Each individual classifier uses an internal threshold value $\varepsilon_{C_i} = 2°C$, the order of autoregression for AR classifier was chosen to be n=3 and the neural network included in the NN classifier was trained using Levenberg-Marquardt algorithm.

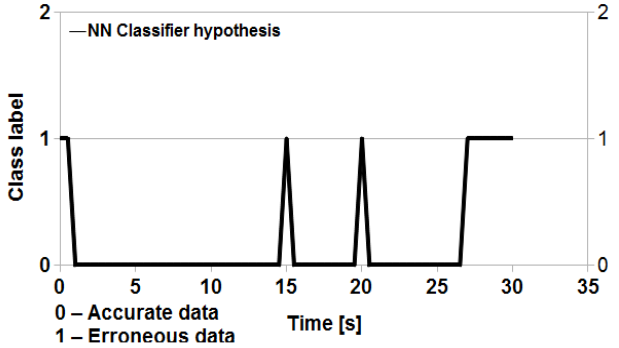
The required heterogeneity of the three binary classifiers included in ensemble plays its role, resulting different classifier hypothesis (Figs. 3a, 3b and 3c). Even if none of the classifiers works accurately in every situation, the ensemble decision obtained through the voting procedure is correct proving the power of ensemble (Fig. 3d).



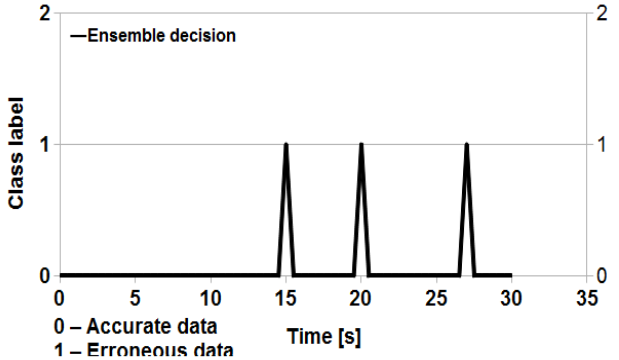
a) Average classifier hypothesis



b) AR classifier hypothesis



c) NN classifier hypothesis



d) Ensemble decision

Figure 3. The outputs of the three classifiers and of the EBS

IV. CONCLUSIONS AND FUTURE WORKS

Whenever we take a decision we want to have confidence in what we have decided. This is also applicable for all technical systems in general and wireless sensor network applications in particular. Being exposed to numerous risks, WSN often implement and use complex decisional systems for controlling their lifecycle, processed data and external threats [14]. In this paper we proposed an anomaly detection solution for WSN sensors using an ensemble-based system. The main advantage brought by this solution is that the final decision is taken based on the interrogation of multiple and different systems.

To fully assess the expected benefits, we continue to go further by improving the ensemble with new binary classifiers based on Adaptive Neuro-Fuzzy Inference Systems (ANFIS) or Support Vector Machine (SVM) and by automating the training and tuning processes of individual classifiers base on pair-wise diversity metrics.

ACKNOWLEDGMENT

This work was developed in the frame of PNII-IDEI-PCE-ID923-2009 CNCSIS - UEFISCSU grant and was partially supported by the strategic grant POSDRU 6/1.5/S/13-2008 of the Ministry of Labor, Family and Social Protection, Romania, co-financed by the European Social Fund – Investing in People.

REFERENCES

[1] Bhuse, V., and Gupta, A.: Anomaly intrusion detection in wireless sensor networks. In Journal of High Speed Networks, vol. 15, no. 1, pp. 33–51, 2006.

[2] Du, W., Fang, L., and Ning, P.: LAD: localization anomaly detection for wireless sensor networks. In Journal of Parallel and Distributed Computing, Volume 66, Issue 7, pp. 874-886, July 2006.

[3] Siripanadorn, S., Hattagam, W., and Teaumroong, N.: Anomaly Detection in Wireless Sensor Networks using Self-Organizing Map and Wavelets. In International Journal of Communications, Issue 3, Volume 4, pp. 74-83, 2010.

[4] Tang, J. and Fan, P.: A RSSI-based cooperative anomaly detection scheme for wireless sensor networks. International Conference on Wireless Communications, Networking and Mobile Computing, IEEE WiCom 2007, pp. 2783 – 2786 Shanghai, China, September 21-25, 2007.

[5] Giacinto G., Roli F., and Didaci L.: Fusion of multiple classifiers for intrusion detection in computer networks, Pattern Recognition Letters Journal, Volume 24, Issue 12, pp. 346-355, 2003.

[6] Giacinto, G., Roli, F.: Dynamic classifier selection. In MCS '00, Proceedings of the 1st International Workshop on Multiple Classifier Systems, pp. 177–189, 2000.

[7] Duin, R., Tax. D.: Experiments with classifier combining rules. In MCS'00, Proceedings of the 1st International Workshop on Multiple Classifier Systems, pp. 16–29, 2000.

[8] Polikar, R.: Ensemble Based Systems in Decision Making. IEEE Circuits and Systems Magazine, vol. 6, no. 3, pp. 21-45, 2006.

[9] Zhang C., Jiang J., and Kamel M.: Intrusion detection using hierarchical neural networks, Pattern Recognition Letters Journal, Volume 26, Issue 6, pp. 779-791, 2005.

[10] Ho, T.K., Hull, J.J., and Srihari, S.N.: Decision combination in multiple classifier systems. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 16, no. 1, pp. 66–75., 1994.

[11] Dietterich, T.G.: Experimental comparison of three methods for constructing ensembles of decision trees: bagging, boosting, and randomization. Machine Learning, vol. 40, no. 2, pp. 139–157, 2000

[12] Kittler, J., Hatef, M., Duin, R.P.W, and Matas, J.: On combining classifiers. In: IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 3, pp. 226-239, 1998.

[13] Curiac, D. I., Plastoi, M., Banias, O., Volosencu, C., Tudoroiu, R., and Doboli, A.: Combined Malicious Node Discovery and Self-Destruction Technique for Wireless Sensor Networks. In: Third International Conference on Sensor Technologies and Applications, SENSORCOMM '09, pp. 436 – 441, Athens, 2009.

[14] Plastoi, M., Curiac, D. I., and Banias, O.: Experiences in complex software development for wireless sensor networks. In: IEEE International Conference on Automation, Quality and Testing, Robotics, AQTR, vol. 3, pp. 1-6. Cluj Napoca, Romania, 2010.

 ISBN: 978-1-61208-166-3