Redundancy and Its Applications in Wireless Sensor Networks: A Survey

DANIEL-IOAN CURIAC, CONSTANTIN VOLOSENCU
Automation and Industrial Informatics Department
"Politehnica" University of Timisoara
Bd.V. Parvan Nr.2, 300223 Timisoara
ROMANIA
daniel.curiac@aut.upt.ro http://www.aut.upt.ro/~curiac

DAN PESCARU
Computer Engineering Department
"Politehnica" University of Timisoara
Bd.V. Parvan Nr.2, 300223 Timisoara
ROMANIA
dan@cs.upt.ro http://www.cs.utt.ro/~dan/

LUCIAN JURCA
Department of Applied Electronics
"Politehnica" University of Timisoara
Bd.V. Parvan Nr.2, 300223 Timisoara
ROMANIA
lucian.jurca@etc.upt.ro

ALEXA DOBOLI
Electrical and Computer Engineering Department
State University of New York
Stony Brook, NY 11794-2350
UNITED STATES OF AMERICA
adoboli@ece.sunysb.edu http://www.ee.sunysb.edu/~adoboli/

Abstract: - In this paper we presented and classified various approaches for redundancy in the area of wireless sensor networks, related to sensing, communication and information processing. Sometimes an ally, sometimes a foe, redundancy is an inherent feature of sensor networks that has to be very carefully examined in order to improve important aspects of their functioning. Moreover, this paper presents two methodologies: one that implies both components of spatial redundancy and one that implies the use of temporal redundancy for achieving the objective of fault-tolerant and safe operation. In the end, the fields in which the redundancy could be applied with significant results are highlighted.

Key-Words: - wireless sensor networks, redundancy, sensing coverage, communication

1 Introduction

The word *redundancy* stems from the Latin verb "redundare" that means overflow and it can describe either something positive like the overflow in the sense of wealth, either something negative like ballast. This ambiguity makes this concept interesting in domains where a high degree of uncertainty is intrinsic. Such a domain is represented by wireless sensor networks (WSN) applications.

The amount of redundancy needed or required is one of the major factors influencing almost all strategies designed for WSN. Generally speaking, a low rate of redundancy is nearly always unfavorable for the reason that it's extremely error prone. With increasing redundancy the WSN becomes more and more fault-tolerant.

In this paper we examine the redundancy problem for wireless sensor networks taking into consideration different facets. In order to achieve the objective of real-

time and safe operation, exploiting redundancy can be a significant approach.

Redundancy in sensor networks is both ally and enemy, challenging us to reinforce the positive aspects and diminish the negative ones. In the last decade, an important idea arise: the redundancy must be exploited to increase data accuracy, sensing reliability, system lifetime and security even if the network price, the routing complexity and the time in which the provided measurements are ready to be used had to grow.

For example, for sensors with independent communication unit and sensing unit, although removing any type of redundancies enables a lot of energy saving, combining them is expected to save more energy. For instance, one of possible combination approaches is that some redundant nodes in sensing layers are picked out first and then the redundancy in communication layers is removed from the remainders.

The concept of redundancy has never been formally defined in all its aspects especially in the field of wireless sensor networks. There are many ways to define this attribute, but the one that we considered to be a good starting point is the following:

DEFINITION1: *Redundancy* is the provision of additional or duplicate resources, which can produce similar results.

Several explanations of redundancy are presented in the literature, frequently from widely different views. Therefore, a discussion of these diverse perspectives and the salient spots would be suitable. A comprehensive definition of redundancy in the case of wireless sensor networks is almost impossible to find, because it needs to cover a large spectrum of issues like: sensing coverage, communication, measurements data storage, etc; this implies that a general definition is not appropriate.

A classic technique to improve the consistency of measurements provided by WSN is to increase the redundancy, by either waiting for reports from multiple neighboring sensor motes (spatial redundancy), by waiting for several reports from the same sensor mote (temporal redundancy), or by including alternative checking data like parity bits in in-network messages (information redundancy). These perspectives will be followed in the next paragraphs, together with the implied main advantages and disadvantages.

Spatial redundancy is basically related to sensing and only sometimes with communication; temporal redundancy is much related with both sensing and communication; and information redundancy is related, in our view, with duplications in the structure of messages exchanged in the network and with duplications in the measurement storage at the level of base stations.

2 Spatial Redundancy

Spatial redundancy is based on the in-field geographic placement of the sensor nodes and involves the replication of resources in the network's coverage area. It is an established fact that in WSN there is tremendous spatial redundancy, i.e. information for a specific location may be available from multiple sensors. This type of redundancy is commonly used to provide fault tolerance, to improve the reliability of the measurement data and to increase the level of information security.

DEFINITION 2: *Spatial redundancy* means the possibility to obtain information for a specific location from different sources.

Spatial redundancy is almost inherent [1] and very practical in wireless sensor networks because they are typically deployed densely, thus providing a large amount of redundancy in network coverage and connectivity. It presumes that redundant resources, e.g. sensor motes, communication connections or even mathematical models, are available and allow the cross-monitoring based on comparison of duplicated information.

Spatial redundancy is described using a large variety of metrics [2][3]. Using graph theory and cutsets, Bagajewicz and Sanchez [4] defined the degree of redundancy for a sensor network, i.e. for measured variables, the degree of redundancy is the maximum number of sensors that can be eliminated and the measurement remains accurate.

There are two possibilities to imply spatial redundancy in the validation process of an in-field measurement provided by a specific sensor: physical redundancy and analytical (functional) redundancy. Both of them are related somehow with the coverage problem described by various authors [2][3][5].

2.1 Physical Redundancy

Physical redundancy, also known as direct redundancy or hardware redundancy [6] is the most common technique used to ensure the reliability of a system. It is based on the densely deployment of multiple independent nodes to cover a specific area [7].

Its definition may be simple:

DEFINITION 3: *Physical redundancy* is an attribute of a WSN that can measure a variable in a specific location using more than one sensor.

Physical redundancy implies the use of supplementary sensors and selection of data that appears similarly on the majority of sensors in an aggregation process.

This type of redundancy is somehow expected either because of the deployment method (e.g. aerial scattering), either because of the requirement to cover the area in case of malfunctioning of some sensor nodes.

Because of this simple relationship that directly connects two values provided by two sensors measuring the same variable in the same place, physical redundancy assures the protection of the WSN from hardware/software node failures, even in case of sensor nodes under security attacks [8].

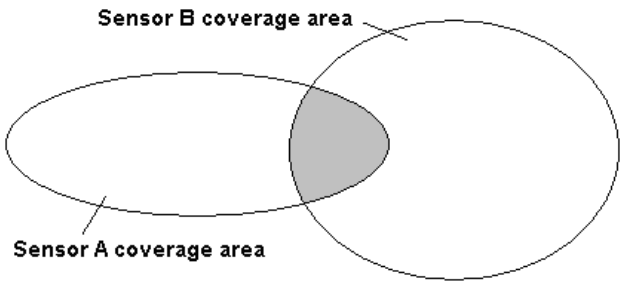

Fig.1: Area with physical sensing redundancy

There are also some disadvantages of the physical redundancy. Most important is that in an environment where source nodes are close to each other, and considerable redundancy exists in the sensed data, the source nodes generate a large amount of traffic on the wireless channel, which not only wastes the limited wireless bandwidth, but also consumes a lot of battery energy.

Methodologies to decrease or even eliminate the spatial redundancy are often needed to make a balance between benefits and disadvantages in a specific WSN application. This process is done by data aggregation.

2.2 Analytical Redundancy

Analytical redundancy can be seen as a generalization of physical redundancy, in which the sensing measurements are obtained not from other sensors already deployed in the field, but from virtual sensor nodes (also called software sensors or observers) that indirectly, based on mathematical models describing expected behavior, estimate the measurements.

Its definition can be summarized as follows:

DEFINITION 4: *Analytical redundancy* is an attribute of a WSN that can estimate a variable in a specific location using mathematical models based on real sensing data provided by neighboring sensors.

Analytical redundancy allows a process of comparison between the actual sensor value and the expected/estimated sensor value conducing to improvements in function and the detection of malfunctioning/malicious sensors [8][9]. This approach is based on a mathematical model that can estimate/predict the value of one sensor by taking into consideration the past and present values of neighboring sensors.

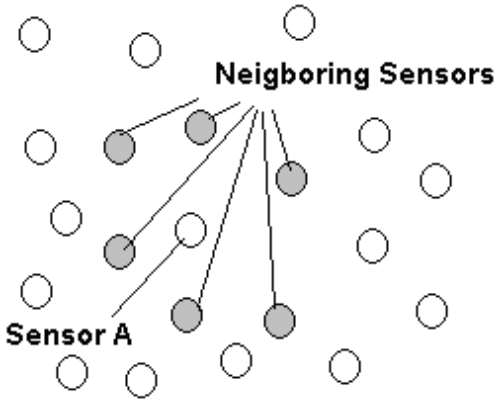

Fig.2: Neighboring sensors for sensor A

Solving this category of problems relies without doubt on interpolation/extrapolation between localized measurement values. In this way the data acquired from a limited number of sensor nodes could be extended using analytical methods upon the entire investigated area. This category of procedures of spreading localized information in neighboring area is known as space-filling phenomena and creates surfaces or statistical surfaces.

In 1997, DeMers [10] asserts that any measurable values occurring throughout an area can be considered as a surface and measurements act as Z-values i.e. attaching the vertical dimension. To estimate the level of that particular physical quantity (the one measured by sensor nodes deployed in that area) in any user defined point location, we have to know first whether the point of interest is exactly the location point of a sensor node, or in between. In the first situation, the value can be obtained directly from the WSN measurement database; in the second case we must use an interpolation/extrapolation technique to estimate it.

Interpolation is characterized as the analytical technique of estimating output values inside the range of discrete set of known/measured data points. On the other hand, extrapolation is defined as the analytical method of estimating output values outside the range of discrete set of known/measured data points.

Using proper interpolation techniques [11] at each instant in time we can obtain a surface representing

estimated physical quantities in each point of the bidimensional area under investigation.

The computational cost of analytical redundancy can become prohibitive as the number of sensors and model complexity is increased.

In addition, because the mathematical models used in estimation process are only an approximation of the reality, the data provided using analytical redundancy is affected by errors (model errors or calculus errors). Even more, the mathematical models, sometimes, due to the increased complexity of the process that is observed had to be modified frequently in terms of structure or/and parameters. This task is proved to be a very difficult one.

2.3 Spatial Redundancy Mathematical Description

In this paragraph we generalized the coverage (physical redundancy) description presented in [12] to include analytical redundancy.

Let's consider a set of n sensors $S = \{s_1, s_2, ..., s_n\}$ deployed in a bidimensional area A. Every sensor node s_i, $i = 1,...,n$, has a specified location within the area A, described by the pair of coordinates (x_i, y_i) and has a sensing range denoted by r_i, i.e., it can monitor a specified physical unit within a distance of r_i from s_i.

DEFINITION 7: A location in A is said to have a *k-degree of redundancy (k-DR)* if there are k possibilities to directly measure (physical redundancy) or estimate (analytical redundancy) the value of the specified physical unit.

In most of the cases, analytical redundancy contributes with only one unit to k_DR, due to the necessity to provide reliable estimation.

Let m be a finite integer number of the points of interest within the field A, and k_j the degree of redundancy in each of this m points.

DEFINITION 8: We define *q-degree of redundancy (q_DR)* to be a global parameter related to the area under investigation A, described by the following relation:

$$q\_DR = \min_{i=1,m}(k\_DR_i).$$

In other words, *q_DR* represents the minimum value of the *k_DR* for a set of already defined points of interest within the area A.

From another perspective we can define an average *k_DR* value in the area A, for the defined set of m points of interest:

DEFINITION 9: We define *w-degree of redundancy (w_DR)* to be a global parameter related to the area under investigation A described by the following average:

$$w\_DR = \frac{\sum_{i=1}^{m}(k\_DR_i)}{m}.$$

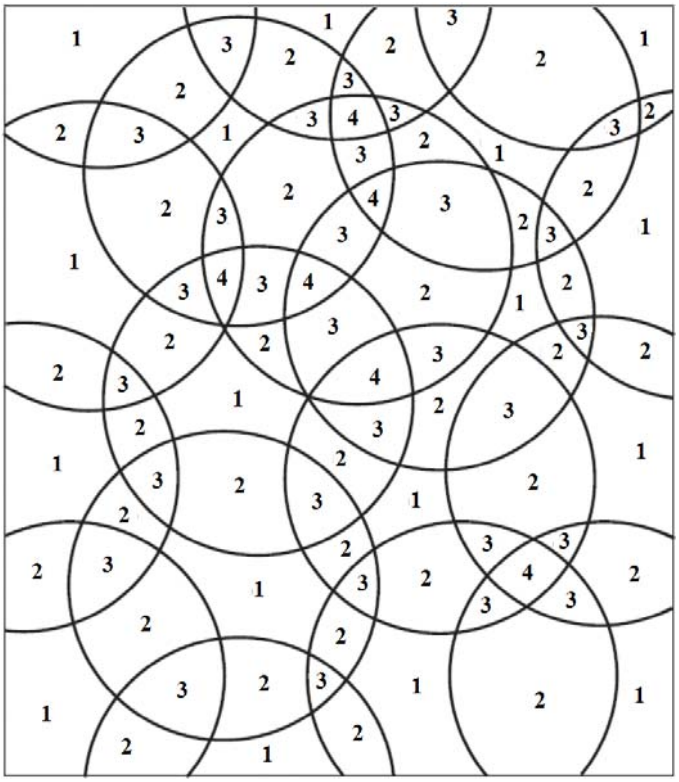

Fig. 3: Physical redundancy in a bidimensional area. The number in each sub-region is its coverage.

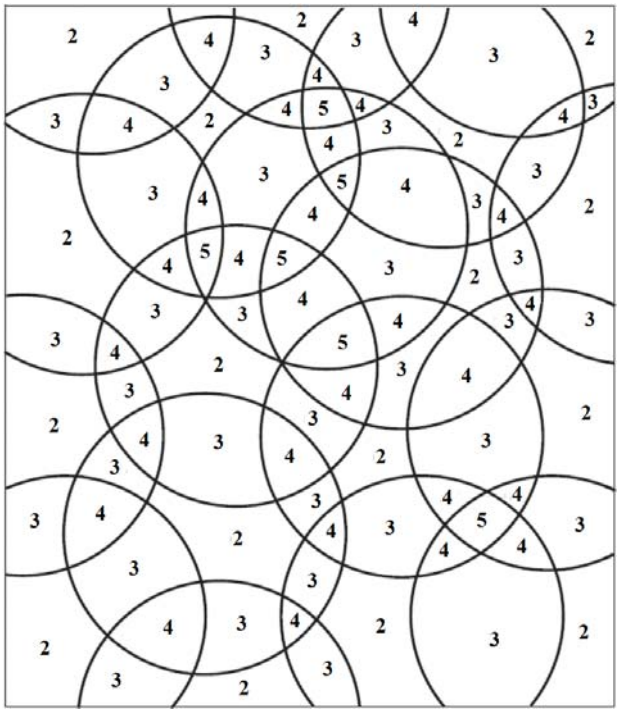

Fig. 4: The *k_DR* map. The number in each sub-region is *k_DR*.

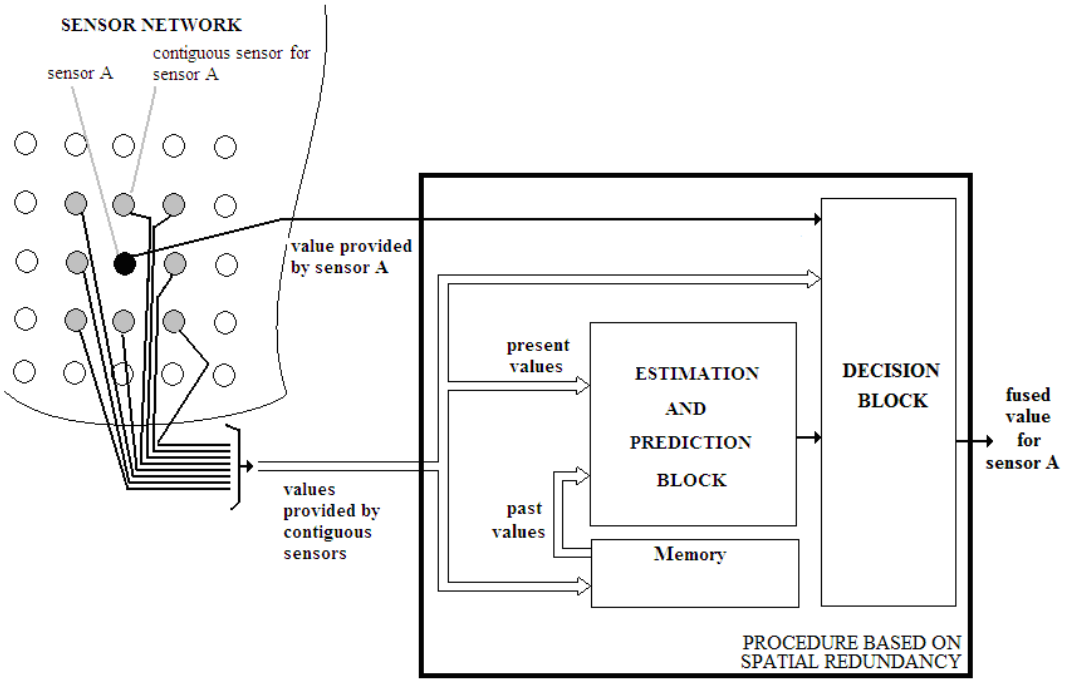

Fig. 5: Sensor fusion based on spatial redundancy

The local parameter *k_DR* and the global parameters *q_DR* and *w_DR* are time-varying due to sensor malfunctions or due to different strategies applied for increasing the wireless sensor network energy efficiency.

In Fig. 3 we presented an example of the sensing coverage of the field under investigation, representing only the component provided through physical redundancy.

In Fig. 4 we added the analytical redundancy component, obtaining a map with *k_DR* values.

2.4 Sensor Fusion Technique Based on Spatial Redundancy

The accuracy of a sensor system is enhanced through the use of redundancy. In a redundant sensor system we must rely on fusing/combining the data reported by each of the sensors monitoring a specified point or region to improve the sensing quality. A reliable sensor fusion methodology that implies both components of spatial redundancy (physical and analytical redundancy) can be divided into the following steps:

a) specify the location (x_i,y_i) in which the methodology will be applied;

b) compute the *k_DR* parameter for this in-field location;

c) decide the fused measurement for that specific location using voting algorithms;

First step requires the specification of the point(s) of interest in which the methodology will be applied. This set of points can include the location of one or more sensor nodes or any other location within the investigated area.

Second step requires the calculation of the localized redundancy parameter *k_DR* for each location, at that instant in time. This calculus is done using the known location of each sensor node, the sensing range of each WSN node, and the analytical redundancy contribution to *k_DR*. An efficient procedure to calculate *k_DR* in a specified set of locations is to compute a map of this parameter similar to the one presented in Fig.4 immediately after the WSN self-organization at the base station level. This map will be updated only when a sensor node is included in or excluded from the network.

Third step is always done by a component of WSN with higher computational power (e.g. base station), and usually implies a voting strategy.

The main voting algorithms used for solving this type of problems are: Majority Voting (MV), Distance Weighted Voting (DWV) and Confidence Weighted Voting (CWV) algorithms [13].

To complete a distributed Majority Voting (MV) scheme for a point of interest having the coordinates *(x,y)* and a specified *k_DR*, sensor measurements are first collected from neighboring sensor nodes, and the aggregated measurement value is achieved based on the majority opinion of the collected data. Supposing that the value obtained using analytical redundancy is in fact provided by a virtual sensor node, and that the possible report value of each sensor (including the virtual sensor node) is an integer from *1* to *n*, the Majority Voting scheme is described by the following equation:

$$MV(x,y) = \max_{k} \sum_{j=1}^{k\_DR} \delta_{kj} \; ; k = 1,2,...n \quad (5)$$

where

$$\delta_{kj} = \begin{cases} 0; \textit{if the report value from sensor } j \textit{ is not } k \\ 1; \textit{if the report value from sensor } j \textit{ is } k \end{cases}$$

The Distance Weighted Voting Algorithm is a weighted variant of MV and is inspired by the assumption that the sensor nearest to the point of interest provides the most accurate data. Supposing that $d_{j,(x,y)}$ is the distance from point *(x,y)* to sensor *j*, and that the virtual sensor mentioned before is placed at an average distance from the point *(x,y)*, DWV is described by the following equation:

$$DWV(x,y) = \max_k \sum_{j=1}^{k\_DR} \frac{1}{d_{j,(x,y)}} \delta_{kj}\ ; k = 1,2,...n \quad (6)$$

Somehow similar to DWV, the Confidence Weighted Voting (CWV) gives higher weights to those sensors that are more likely to be correct (i.e. with higher confidence of correctness). The confidence value of each sensor can be computed in a distributed manner by comparing its sensing results with its sensing neighbors that share overlapping coverage area. In this procedure we have to include the virtual sensor that provides the measurement through techniques based on analytical redundancy. The confidence value of sensor *i* is then defined as:

$$conf(i) = \frac{\sum_{j=1}^{k\_DR} \Delta_{ij}}{k\_DR} \quad (7)$$

where

$$\Delta_{ij} = \begin{cases} 0; \textit{ if sensor } i \textit{ and } j \textit{ report different results} \\ 1; \textit{if sensor } i \textit{ and } j \textit{ report the same result} \end{cases} \quad (8)$$

and CWV is formulized as:

$$CWV(x,y) = \max_k \sum_{j=1}^{k\_DR} conf(j)\delta_{kj}; k = 1,2,...n \quad (9)$$

2.5 Sensor Validation and Malicious Sensor discovery using Spatial Redundancy

In order to validate the behavior of the sensor nodes within WSN or to discover the malicious sensors we can develop a procedure based on spatial redundancy. Our proposed methodology relies on the fact that a corrupted/malfunctioning sensor node, even if it may still send authentic messages (e.g. it can use the cryptographic keys already stored in its memory), it may not work according to its original specifications sending erroneous readings to the base station.

In order to develop our strategy for anomaly detection, we started from three principles: (1) anomaly detection is based on observations and probing by neighbor nodes; (2) there is no full trust between observer nodes, since they could also be affected by malfunctions or malicious activity; (3) the specific application of the sensor network determines the modeling of "good" and "bad" behavior.

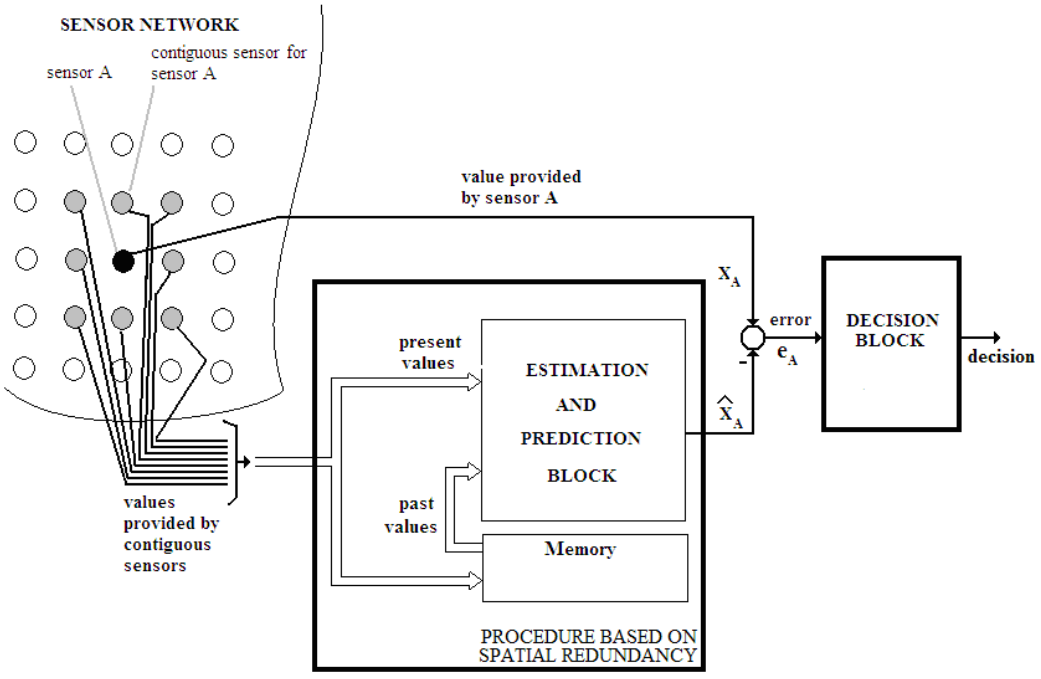

Fig.6. Fault operation discovery using spatial redundancy

The principle is the following: a malfunctioning/malicious sensor node that will send faulty information will be identified by comparing its output value x with the value $\hat{x}$ predicted using past/present values provided by contiguous sensors. Taken into consideration a specific node denoted by A (Fig.6), this process is done in the following steps:

a) Estimate the value $\hat{x}_A(t)$ provided by sensor node A, using the past/present values of adjacent sensors using a procedure that involves both physical and analytical redundancy;
b) Compare the present value $x_A(t)$ of the sensor node with its estimated value $\hat{x}_A(t)$ by computing the error $e_A(t) = x_A(t) - \hat{x}_A(t)$ (4);
c) Choose, based on a priori information (e.g. statistics), the type of decision that will be taken by the knowledge-based system against sensor A. One of the most common decisions in case of malfunctioning or malicious sensor activity is the expelling of the node from the WSN.

3 Temporal Redundancy

Temporal redundancy is used to improve the precision of sensor nodes readings and to endure transient faults in sensing and communication.

DEFINITION 10: *Temporal redundancy*, also known as time redundancy can be defined as performing a specific action more than once, skewed in time, followed by checking the results in order to increase reliability.

There are some cases when the use of time redundancy is complicated to be applied. One of these situations is the use of WSN in dynamic sensing environments where parameters are changing rapidly in time. In this case, there is no logic in repeating a measurement.

Temporal redundancy can be either related to sensing, either to communication, or with both of them.

3.1 Temporal Sensing Redundancy

Only in an ideal scenario where the sensing is perfect, a high level of confidence for measurement data can be obtained using a single sensor. In real world, the sensor devices are sometimes imprecise, reporting events or measurements that are not actually present. By this, a single sensor reading may not be very reliable. One way to improve the reliability of the entire system is to increase the redundancy, by using multiple reports from the same sensor motes [14].

DEFINITION 11: *Temporal sensing redundancy* is defined as obtaining multiple measurements from the same sensor mote, skewed in time.

This type of redundancy is often used in video surveillance and represents the support for multiple codec based on special data compression techniques.

3.2 Temporal Communication Redundancy

DEFINITION 12: *Temporal communication redundancy* is defined as sending the same package of data more then once, skewed in time.

In the case of network communication, temporal redundancy is applied mainly by retry and failover methods. Time-out and retry mechanisms used by several communication protocols like Transmission Control Protocol [15], or by Application Support Sub-layer (APS) in Zigbee/802.15.4 [16] can also be classified as temporal redundancies. Also, Automatic Repeat Request (ARQ) is an example of temporal redundancy [17].

Link retransmission can overcome the impact of increased number of hops on network link breakdown rates, but it will reduce the channel bandwidth and memory usage;

3.3 Sensor Validation and Malicious Sensor Discovery Using Temporal Redundancy

The strategy to detect malfunctioning or malicious sensor nodes using temporal redundancy is based on past/present values provided by the same sensor [8]. Basically, we will compare at each moment the sensor's output with its estimated value computed by an autoregressive predictor (Fig. 7). In case the difference between the two values is higher then a chosen threshold, the sensor node becomes suspicious and a decision block is activated.

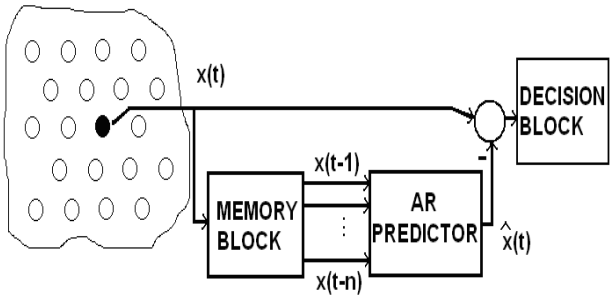

Fig. 7: Malfunctioning/malicious sensor node discovery using temporal redundancy

4 Information Redundancy

There are two perspectives upon information redundancy: one in which information redundancy is related only to the data representation; and another, more complex that includes all types of redundancies (e.g. spatial and temporal redundancy) based on the assumption that all of them are a source of information.

In our perspective, the information redundancy is linked only with the data representation.

DEFINITION 13: *Information redundancy* is defined as the use of redundant data, e.g. extra bits, to reconstruct lost information.

Thus, information redundancy implies that extra information is used to detect and recover from a fault. Parity bits appended to data blocks to enable error detection could be considered as an instance of information redundancy.

Another example of information redundancy is erasure codes, which can be thought as a generalization of parity code [18][19]. They use information redundancy to recreate original messages without link retransmission, though the number of messages cannot surpass the number of bits utilized to represent the message.

5. Significant Applications of Redundancy in WSN

5.1 Energy Saving

Energy saving is one of the most important issues in wireless sensor networks, where nodes are often relying on limited battery power. According to [8], individual sensor nodes can operate around one hundred hours on a pair of AAA batteries in active mode. Because sometimes the sensors are deployed in harsh environments, it is almost impossible to recharge or replace their batteries, so the conservation of energy is a must in order to augment the network lifetime.

A significant part of the energy saving strategies exploit the inherent spatial sensing redundancy by defining sub-sets of nodes active in distinct time periods, to allow sensors to save energy when inactive [20]. In densely deployed WSN it is established that the most efficient method to save energy is to put as many redundant nodes as possible in the sleep mode, therefore they use only an insignificant part of the energy spent in the active mode [21].

Topology control is an energy conserving method based on spatial communication redundancy that decreases the number of nodes involved in forwarding and routing packets created by the other nodes without reducing network connectivity and coverage. This method is practical in wireless sensor networks since the nodes are usually deployed densely, sometimes by aerial scattering, thus presenting a high degree of redundancy in network coverage and connectivity.

An energy saving solution should attain decisions through a distributed methodology, thus avoiding the unnecessary amount of message overhead (largest fraction of the energy consumption for a mote is linked to radio transmission [22]) related with the centralized approach.

5.2. Reliability Improvement

Redundancy is desired not only for the purpose of availability improvement but also for providing robust and fault-tolerant information, mainly when individual sensor nodes are faulty, malfunctioning or even malicious.

Since sensor motes are frequently deployed in harsh environments, incorrect readings from damaged sensors can unfavorably influence the accuracy of sensor network findings. Hence, to improve the dependability of network results, it is imperative for applications to have access to reliable information. It is established that: a) multiple nodes observing the same location at the same time can guarantee higher monitoring quality [23][24]; and b) readings from contiguous sensor nodes can be exploited to discern the correctness of local data [8].

It is obvious that redundant information can be used to improve the reliability of the results obtained from a specific sensor. These highly localized results can be aggregated using techniques as the ones presented in [25][26] to supply increased data reliability to requesting military applications such as event identification or target detection.

5.3. Security Upgrading

Information security improvements based on redundancy are particularly suitable to sensor networks.

Because of their deployment, sometimes in inhospitable environments, WSN can be seriously disturbed by any kind of sensor failure or, more dramatic, by malicious attacks from an opponent. Moreover, many standard mechanisms (e.g., public key infrastructures or agreement protocols) cannot be applied because they need too many resources or do not scale to thousands of nodes.

Sensor networks due to their restrictive constraints are exposed to some significant types of attacks that can not be prevented only using cryptographic methods: eavesdropping, traffic analysis, selective forwarding, spoofing, sinkhole attack, wormhole attack, Sybil attack

and Hello flood attack are the most relevant [27]. But the most annoying problem in sensor network security is node-capturing attack [28] where an opponent gets full control above sensor nodes through direct physical access. This kind of attack is essentially different from the attacks previously mentioned because it doesn't rely on security gaps in protocols, broadcasting, operating systems, etc. It is based on the geographic in-field deployment of the sensor nodes. Practically, we cannot presume a strong access control to thousands of nodes distributed over several miles and, by this, we increase the possibility of a node capturing attack.

To summarize, security goals in sensor networks need the development of specific approaches, most of them exploiting one inherent feature of sensor networks: redundancy. These approaches rely on the fact that a corrupted/attacked sensor node, even if it may still send authentic messages (e.g., it can use the cryptographic keys already stored in its memory), it may not work according to its original specifications sending some erroneous readings to the sink. Using spatial redundancy and comparing the readings with the ones obtained from redundant sensors/observers, a knowledge-based decision system can be developed [8][9] to expel malicious nodes from the network.

6 Conclusions

In this paper we investigated the redundancy problem for wireless sensor networks taking into consideration different facets. Moreover, we presented two basic methodologies that imply the use of spatial and temporal redundancy in order to achieve the objective of fault-tolerant and safe operation. From in-field distributed identification to event detection, the redundancy can be exploited for improving the fault-tolerance, for increasing the energy efficiency and even for enhancing security of wireless sensor networks. Property of redundancy may be used in all kind of application of sensor networks [29].

7 Acknowledgement

This work was developed in the frame of PNII-IDEI-PCE-ID923-2009 CNCSIS - UEFISCSU grant.

References:

[1] Park S.J., Vedantham R., Sivakumar R., Akyildiz I.F., "A scalable approach for reliable downstream data delivery in wireless sensor networks", *Proceedings of the 5th ACM Interational Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc2004)*,Tokyo, Japan, May 24-26, 2004 pp.78-89.

[2] Iyengar R., Kar K. and Banerjee S., "Low-coordination Topologies for Redundancy in Sensor Networks", *the Sixth ACM Annual International Symposium on Mobile Ad-Hoc Networking and Computing (MobiHoc)*, Urbana-Champaign, IL, 2005, pp.332-342.

[3] Gao Y., Wu K., and Li F., "Analysis on the Redundancy of Wireless Sensor Networks", *Proc.2nd ACM Intl. Workshop on Wireless Sensor Networks and Applications (WSNA)*, San Diego, CA, September 2003. pp.108-114.

[4] Bagajewicz, M., and Sanchez, M., "Design and Upgrade of Nonredundant and Redundant Linear Sensor Networks", *American Institute of Chemical Engineering Journal*, vol. 45, no. 9, 1999, pp. 1927–1938.

[5] Singh, M.P.; Gore, M.M., "A solution to sensor network coverage problem", *7th IEEE International Conference on Personal Wireless Communication (ICPWC 2005)*, Jan. 2005, pp.77 – 80.

[6] Duk-Sun Shim, Cheol-kwan Yang, "Method of detecting and isolating fault in redundant sensors, and method of accommodating fault in redundant sensors using the same", *USPTO Application #: 20080276155*, Nov. 2008.

[7] Bojkovic Z., Bakmaz B., "A survey on wireless sensor networks deployment", *WSEAS Transactions on Communications*, Vol 7, No 12, pp. 1172-1181, Dec. 2008.

[8] Curiac, D.-I. Banias, O. Dragan, F. Volosencu, C. Dranga, O., "Malicious Node Detection in Wireless Sensor Networks Using an Autoregression Technique", *Third International Conference on Networking and Services (ICNS2007)*, Athens, June 2007.

[9] Curiac D.I., Volosencu C., Doboli A., Dranga O., Bednarz T., Discovery of Malicious Nodes in Wireless Sensor Networks Using Neural Predictors, *WSEAS Transactions on Computer Research*, Issue 1, Vol. 2, Jan. 2007, pp. 38-44.

[10] DeMers, M.N., *Fundamentals of geographic information systems*. New York: Wiley (1997).

[11] Mastroianni, G.; Milovanovic, G.V., *Interpolation Processes: Basic Theory and Applications*, Series: Springer Monographs in Mathematics, Springer, 2008.

[12] Huang C.F, Tseng Y.C., The coverage problem in a wireless sensor network, *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*, September 19-19, 2003, San Diego, CA, USA .

[13] Sun T., Chen L.J., Han C.C., Gerla M., "Reliable Sensor Networks for Planet Exploration", *ICNSC 2005*, pp. 816-821.

[14] He T., Krishnamurthy S., Stankovic J.A., Abdelzaher T., Luo L., Stoleru R., Yan T., Gu L., "Energy-Efficient Surveillance System Using Wireless Sensor Networks", *Mobisys 2004*, June 2004, pp. 270-283.

[15] Tanenbaum A.S., *Computer Networks* (Fourth Edition ed.). Prentice Hall, 2003.

[16] Gislason D., "Zigbee Wireless Networking", *Newnes*, August 2008.

[17] Wu A., Abouzeid A.A., "Error robust image transport in wireless sensor networks," in *5th Workshop on Applications and Services in Wireless Networks (ASWN 2005)*, Paris, June-July 2005.

[18] Kim S., Fonseca R., Culler D., "Reliable Transfer on Wireless Sensor Networks", *IEEE*, 2004, 449-459.

[19] Wacker H.D., Boercsoek J., Hillmer H., "Redundant data transmission and nonlinear codes", *WSEAS Transactions on Communications*, Vol 7, No 6, pp. 594-604, June 2008.

[20] Wang, L., Xiao, Y., "Energy saving mechanisms in sensor networks". *Proceedings of the IEEE Broadnets 2005*, October, 2005, pp.777-785.

[21] Crossbow. Power management and batteries. http://www.xbow.com/Support/appnotes.htm, 2004.

[22] Perrig A., Szewczyk R., Wen V., Culler D., and Tygar J.D., "SPINS: Security protocols for sensor networks", *MobiCom 2001*, pp. 189-199, July 2001.

[23] Gao Y., Wu K., and Fulu Li, "Analysis on the Redundancy of Wireless Sensor Networks," *ACM WSNA*, 2003.

[24] Yan T., He T., Stankovic J., "Differentiate Surveillance for Sensor Networks," *ACM 1st Conference on Embedded Network Sensor Systems*, 2003.

[25] Xu Y., Heidemann J. and Estrin D., "Georgraph-informed Energy Conservation for Ad Hoc Routing," *ACM Mobicom 2001*, Rome, Italy, July 2001.

[26] Clouqueur T., Ramanathan P., Saluja K.K., and Wang K.-C., "Value fusion versus decision-fusion for fault tolerance in collaborative target detection in sensor networks," *Proceedings of Conf. on Information Fusion*, 2001.

[27] Karlof C., Wagner D., "Secure routing in wireless sensor networks: attacks and countermeasures", *Proceedings of the 1st IEEE International Workshop SNPA2003*, Anchorage, USA, May 2003, pp. 113-127.

[28] Becher A., Benenson Z., Dornseif M., "Tampering with motes: Real-world physical attacks on wireless sensor networks", *Proceedings of the 3rd International Conference on Security in Pervasive Computing (SPC)*, York, UK, April 2006, pp.104-118.

[29] Volosencu, C., Identification of Distributed Parameter Systems, Based on Sensor Networks and Artificial Intelligence, *WSEAS Transactions on Systems*, Issue 6, Vol. 7, June 2008. ISSN 1109-2777, pp. 785-801.